Understanding Quantum Technologies

Fifth edition

Volume 2: software, telecoms, crypto, sensing, ecosystem, society

2022

Olivier Ezratty

le lab quantique

Understanding Quantum Technologies

Fifth edition

Volume 2

2022

Olivier Ezratty

About the author

Olivier Ezratty
consultant and author
0000-0003-3944-2896
olivier (at) oezratty.net, www.oezratty.net, @olivez
+33 6 67 37 92 41

Olivier Ezratty advises and trains businesses and public services in the development of their innovation strategies in the quantum technologies realm. He brings them a 360° understanding of these: scientific, technological, marketing as well as the knowledge of the quantum ecosystems.

He has covered many other topics since 2005, with among others digital television, Internet of things and artificial intelligence. As such, he carried out various strategic advisory missions of conferences or training in different verticals and domains such as the **media and telecoms** (Orange, Bouygues Telecom, TDF, Médiamétrie, BVA, Astra), **finance and insurance** (BPCE group, Caisse des Dépôts, Société Générale, Swiss Life, Crédit Agricole, Crédit Mutuel-CIC, Generali, MAIF), **industry and services** (Schneider, Camfil, Vinci, NTN-STR, Econocom, ADP, Air France, Airbus) and the **public sector** (CEA, Météo France, Bpifrance, Business France).

In the quantum realm:

- He is a keynote speaker in a large number of quantum technology events since 2018.
- He published the reference book **Understanding Quantum Technologies** (September 2021 and 2022) following three previous editions in French in 2018, 2019 and 2020. The 2021 and 2022 editions are also available in paper-back version on Amazon.
- He runs **two series of podcasts** on quantum technologies with Fanny Bouton (in French): a monthly « Quantum » on tech news (since September 2019) and Decode Quantum, with entrepreneurs and researchers since March 2020, with a total of over 80 episodes.
- He is a trainer on quantum technologies for **Capgemini Institut** and for **CEA INSTN**. In September 2021, he took in charge an elective curriculum on quantum technologies for **EPITA**, an IT engineering school in France.
- He is the cofounder of the **Quantum Energy Initiative** with Alexia Auffèves (CNRS MajuLab Singapore) and Robert Whitney (CNRS LPMMC).
- He is advising **Bpifrance** on quantum projects evaluations, a member of the strategic committee for **France 2030**, the French government innovation strategy plan and also a lecturer at IHEDN.

He also lectures in various universities such as CentraleSupelec, Ecole des Mines de Paris, Télécom Paristech, EPITA, Les Gobelins, HEC, Neoma Rouen and SciencePo, on artificial intelligence, quantum technologies as well as entrepreneurship and product management, in French and English as needed. He is also the author of many open source ebooks in French on entrepreneurship (2006-2019), the CES of Las Vegas yearly report (2006-2020) and on artificial intelligence (2016-2021).

Before all that, Olivier Ezratty started in 1985 at **Sogitec,** a subsidiary of the Dassault group, where he was successively Software Engineer, then Head of the Research Department in the Communication Division. He initialized developments under Windows 1.0 in the field of editorial computing as well as on SGML, the ancestor of HTML and XML. Joining **Microsoft France** in 1990, he gained experience in many areas of the marketing mix: products, channels, markets and communication. He launched the first version of Visual Basic in 1991 and Windows NT in 1993. In 1998, he became Marketing and Communication Director of Microsoft France and in 2001, of the Developer Division, which he created in France to launch the .NET platform and promote it to developers, higher education and research, as well as to startups.

Olivier Ezratty is a software engineer from **Centrale Paris** (1985), which became CentraleSupelec in 2015.

Credits

Cover illustration: personal creation associating a Bloch sphere describing a qubit and the symbol of peace (my creation, first published in 2018) above a long list of over 400 scientists and entrepreneurs who are mentioned in the ebook.

This document contains over 1600 illustrations. I have managed to give credits to their creators as much as possible. Most sources are credited in footnotes or in the text. Only scientists' portraits are not credited since it's quite hard to track it. I have added my own credit in most of the illustrations I have created. In some cases, I have redrawn some third-party illustrations to create clean vector versions or used existing third-party illustrations and added my own text comments. The originals are still credited in that case.

Table of contents

Content

This is the second volume of the book “Understanding Quantum Computing”, that is also downloadable from https://www.oezratty.net/wordpress/2022/understanding-quantum-technologies-2022/. The downloadable PDFs are available in a single volume A4 and Letter version, containing the two volumes in sequential order. You can also download compressed PDFs for both volumes in A4 and Letter formats. Their size fits into the constraints of ebook readers like the Kindle from Amazon.

This book printed version separates volume 1 and volume 2.

The **first volume** contains an history of quantum physics, some quantum physics 101 and everything about quantum computing basics and hardware, including enabling technologies.

This **second volume** contains the parts dedicated to quantum algorithms, software development tools and quantum computing business applications. It describes unconventional computing solutions which are potential alternate routes between classical and quantum computing. It then covers quantum telecommunications, quantum cryptography, post-quantum cryptography and quantum sensing. It ends with an inventory of quantum investments per country, various societal topics, corporate adoption methodologies and quantum fake sciences.

The two-volume index and glossary are at the end of this second volume.

The book is split into two volumes to make its printing easier, some online printing services including Amazon being limited to a maximum of 600 pages. Here, we have two more or less equally sized volumes of respectively 576 pages and 568, covers included.

You can order the printed version of this book in two volumes on all **Amazon** sites with searching for the book title, edition 2022.

Page intentionally left blank

Quantum algorithms

It is now time to put aside quantum hardware that was the main topic of the previous parts of this book and to turn to quantum algorithms and software!

Gate-based quantum computers use quantum algorithms, some of which being theoretically much more efficient than their equivalents designed for classical computers. There are not that many algorithms and their relative performance compared to classical algorithms is not always obvious to prove. It is even sometimes contested. The assertion "*quantum computers are faster than classical computers*" is therefore debatable and must be discussed and analyzed on a case-by-case basis.

Richard Feynman described the idea of creating quantum simulators in 1982[1527]. His idea was to create devices using the effects of quantum mechanics to simulate them, which would be almost impossible with traditional computers. This corresponds today to so-called quantum simulators, a specific breed of analog quantum computers. But we're dealing here mostly with gate-based quantum computing, based on **Yuri Manin**'s idea from 1980 and then refined by **David Deutsch** between 1985 and 1992.

Mathematicians have been working since the mid- and late 1980s on creating algorithms for quantum computers and simulators, long before any hardware was available.

The first quantum algorithms were published in the early 1990s, while the first two-qubit quantum systems appeared around 2000/2002. Researchers have been regularly creating new algorithms for the past 25 years, regardless of the relatively slow progress with hardware. The Quantum Algorithm Zoo launched in 2011 identifies 62 classes in the scientific literature and 430 algorithms (as of April 2021), organized in 4 algorithms groups (algebraic and number theory, oracle-based problems, approximation and simulations, optimization - numerics and machine learning). The list is maintained by Stephen Jordan, a researcher at Microsoft Quantum. This is still a modest number compared to the thousands of non-quantum algorithms[1528]. Even though most classical computing developers don't know and use many algorithms in practice!

Quantum algorithms creation is thus a parallel research path with hardware progress, even though they might be sometimes closely related. This is not the first time in history. The emblematic **Ada Lovelace** did formalize the first algorithms and lines of code to run on **Charles Babbage**'s machine, which only saw the light of day in 2002 in London, 153 years after its conception (video) (see the sample program *below*). In 1842/1843, she had annotated a translation of her own of a paper by the Italian **Luigi Federico Menabrea** describing Babbage's machine. It took 102 years for the first electronic computers to see the light of day at the end of World War II! A beautiful game... of patience!

It is also reminiscent of **Leonardo da Vinci**'s helicopter designs dating from 1487-1490. A first human-powered helicopter created by the University of Toronto flew in 2013, AeroVelo (video) followed by another fairly close specimen from the University of Maryland flying in 2018 (video)! So, more than five centuries apart! And even taking into account the flight of the first motorized helicopter in 1907, the time lag is still over four centuries. This same University of Maryland is one of the most advanced in the world in quantum computers based on trapped ions!

[1527] See Simulating Physics with Computers, Richard Feynman, 1982 (22 pages).

[1528] For an extensive coverage of the key gate-based quantum algorithms, see Lecture Notes on Quantum Algorithms by Andrew M. Childs, April 2021 (181 pages) and Quantum Computing Lecture Notes by Ronald de Wolf, 2021 (184 pages).

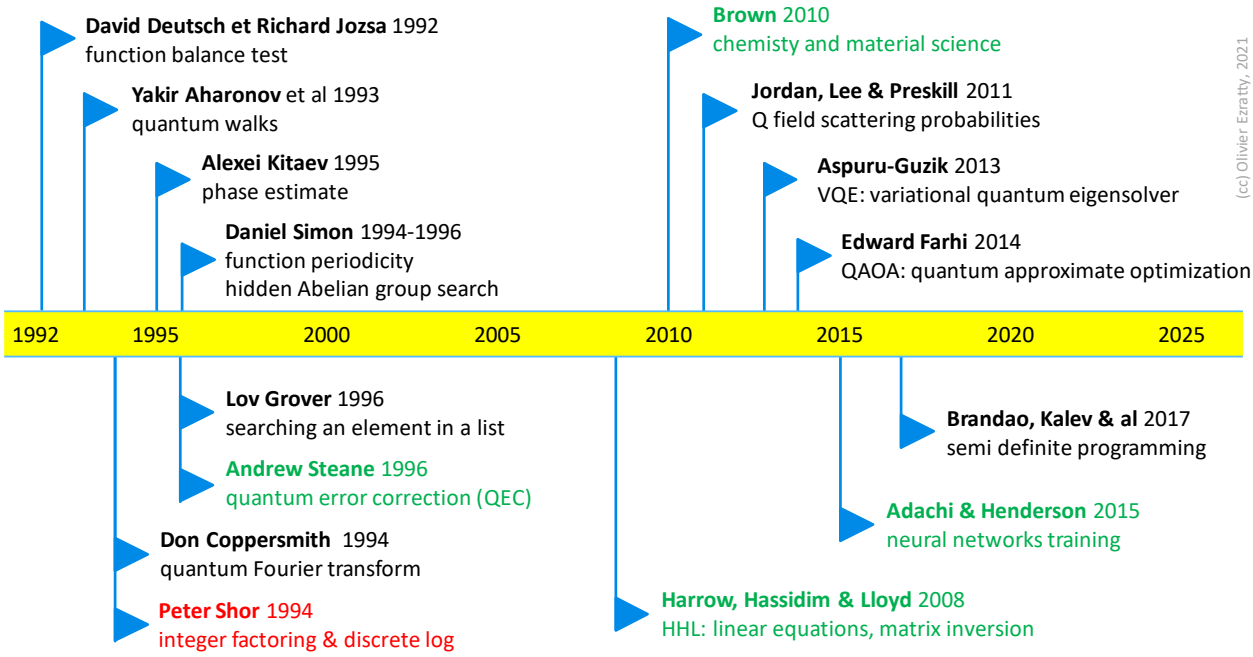


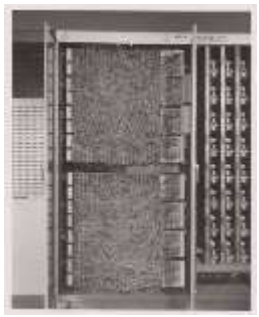
Figure 547: a quantum computing algorithms creation timeline. It is a three-decade story. (cc) Olivier Ezratty, 2021.

After the war, history repeated itself in part for much of the work in the vast field of artificial intelligence, where researchers were also working on algorithms, especially neural network-based algorithms, before any computers could execute them properly on a useful scale such as for objects recognition in images. The first computers running perceptrons, the ancestors of today's artificial neural networks, were rudimentary. The rise of deep learning since 2012 is partly linked to the power of machines and GPUs able to train such neural networks. Hardware has once again joined algorithms that were ahead of their time.

Ada Lovelace
1842, first program for Babbage's analytical machine which didn't exist

ENIAC
1945, first electronic computer

McCulloch & Pitts
1943, artifical neurons concept



Mark I Perceptron computer
1957, first synaptic processor

Alexnet on Nvidia GTX 580
2012, first neural network with a recognition rate having less than 30% error rate.

Léonard de Vinci
1487, aerial screw

Paul Cornu, 1907
first motorized hélicopter
1.5 m altitude

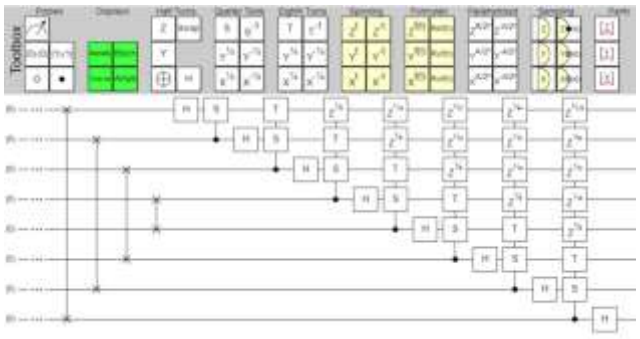
AeroVelo, 2013
first human power helicopter flight

Figure 548: a perspective on the time gap between algorithms creation and their underlying hardware. One century between Ada Lovelace's Bernoulli equations programming and the advent of the first electronic computer. And 6 decades to implement neural networks practically. Same for helicopters in another domain! (cc) Olivier Ezratty with various image sources. 2020.

Even today, many of the quantum algorithms that are invented are not yet executable on a large problem scale on current quantum computers or on classical computing quantum emulators. There are not enough quality qubits available to be of any use and, more importantly, to be more powerful in any dimension than classical computers. Supercomputers can emulate about 50 qubits but no operational quantum computer can reach this number with error corrected qubits.

In another analogy with the History of Computer Science, we are still programming quantum computers with rather low layers of machine language, a bit like machine language or macro-assembler used 30 to 50 years ago, or more recently, for those who program low-level embedded systems or peripheral drivers. Today's quantum algorithms are mid- to low-level logical chunks of quantum code. Their assembly is even not yet done in practice.

visual quantum circuits design



https://algassert.com/quirk

online open source tool to learn, program and emulate up to 16 qubits

scripted Python code

```
# Initialize counting qubits
# in state |+>
for q in range(n_count):
    qc.h(q)

# And auxiliary register in state |1>
qc.x(3+n_count)

# Do controlled-U operations
for q in range(n_count):
    qc.append(c_amod15(a, 2**q),
              [q] + [i+n_count for i in range(4)])

# Do inverse-QFT
qc.append(qft_dagger(n_count), range(n_count))

# Measure circuit
qc.measure(range(n_count), range(n_count))
qc.draw(fold=-1)  # -1 means 'do not fold'
```

IBM Qiskit, Google Cirq, Atos myQLM

Figure 549: gate-based programming can be done graphically with tools like Quirk, mostly for learning purpose and also, to visualize interactively qubits values (Bloch sphere, vector state, density matrix) in emulation mode. Scripted code with Python is used for professional programming. (cc) Olivier Ezratty, 2022.

The creation of quantum algorithms requires a capacity for abstraction that is beyond that of classical algorithms and programs, even taking into accounts object-based or events-based programming. We'll have to groom a new generation of mathematicians and developers capable of reasoning with the mathematical formalism of quantum programming as quantum computers mature. They will have to be able to conceptualize algorithms that are not easy to mentalize. Most of the times, though, quantum algorithms won't be simple language translation from classical programming language. They will solve problems that classical computers and classical programming languages can't solve efficiently.

One day, the abstraction level of quantum programming may rise to a point where it is no longer necessary to understand the low-level intricacies of quantum gates, Hilbert spaces, Hamiltonians and quantum interferences. But this is just a conjecture!

Today's classical quantum algorithms use quantum gates. But there are other variations:

- **Quantum annealing problem solving** such as those for D-Wave machines which are based on the initialization of relations between average quality qubits and on the search for a minimum energy based in particular on the tunnel effect. The basic algorithm there is about solving an Ising model. We will describe it when discussing about D-Wave.

- **Analog quantum simulators** are used to simulate quantum phenomena, for example to predict the organization of atoms in molecules. These include cold atom quantum simulators. An algorithm here is about preparing the state of the qubits in the system and their link weights. It's a process similar to D-Wave quantum annealing, with variations on the degrees of liberty handled in the system and qubits coherence.
- **Continuous variable quantum computers** that use quantum objects whose physical quantity can be measured as a continuous, not binary, quantity. This creates yet another programming model. They are mainly based on photons[1529].
- **Topological quantum computers**, which do not yet exist. This is the research path of Microsoft and some research laboratories, especially in China. We cover this on page 372. It should still be programmable with gate-based classical code.
- **Hybrid algorithms** combining traditional algorithms and quantum algorithms running on any of the above system[1530]. This is notably the case of the Variational Quantum Eigensolver (VQE) which allows the resolution of chemical simulation problems as well as neural network training.

We can also mention **Quantum inspired algorithms** which are algorithms running on classical computers that are inspired by quantum algorithms for solving complex problems. Their creation started long before the first experimental quantum computers were created.

In practice, the noisy intermediate scale quantum computers (NISQ) that are emerging now and will dominate the landscape for at least a good decade cannot run "deep" algorithms.

Namely, because of quantum gates and readout error rates is too high and limits the number of quantum gates that can be chained. We are thus limited to use algorithms that chain a rather small number of quantum gates.

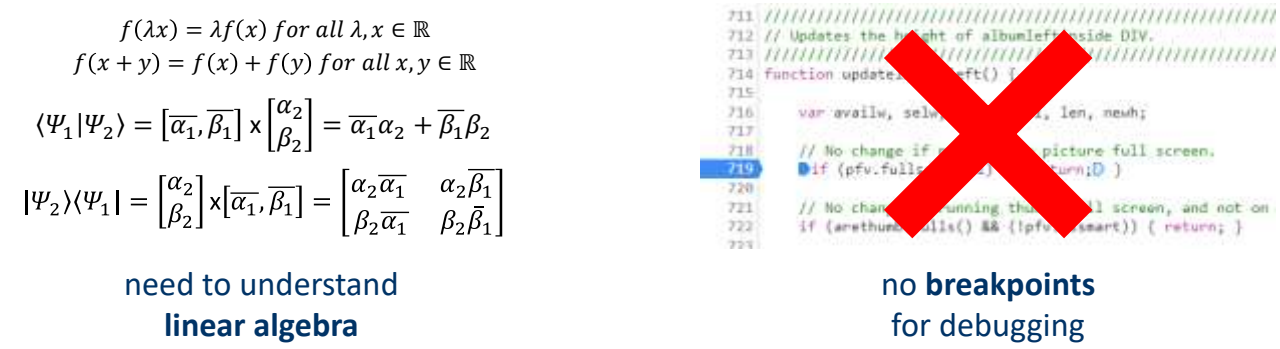


Figure 550: the key differences with quantum programming. A need to understand linear algebra and do some maths, different debugging techniques and coping with the impossibility to copy data and playing with the probabilistic nature of quantum measurement. (cc) Olivier Ezratty, 2022.

[1529] See for example Perspective: Toward large-scale fault-tolerant universal photonic quantum computing by S. Takeda et al, April 2019 (13 pages) and Continuous-variable quantum neural networks by Nathan Killoran et al, June 2018 (21 pages) which deals with the use of continuous variable qubits to create neural networks.

[1530] See Hybrid Quantum Computation by Arun, 2011 (155 pages).

This is the case for **VQE** (Variational Quantum Eigensolver), **QAOA** (Quantum Approximate Optimization Algorithm), **QAO-Ansatz** (Quantum Alternating Operator Ansatz, sometimes confusingly also named QAOA), Variational Quantum Factoring and some Quantum Machine Learning algorithms (Support Vector Machine, Principal Component Analysis and Quantum Variational Autoencoder). We will have the opportunity to study some of them later on.

Algorithms classes

Before getting deep into quantum algorithms, let's take a detour with covering their practical usefulness known to date and for which category of quantum hardware they are designed. Then, how they are organized and what is the basic algorithms toolbox available to developers.

Classes and use cases

Here's a simple classification of high-level algorithms by use cases[1531].

Oracle function-based algorithms can fasten the search of a needle in a haystack and find solution of some complex problems. Some are useful, some are not. The most famous oracle-based algorithms are Deutsch-Jozsa, Simon, Bernstein-Vazirani and Grover.

Complex optimization problems, particularly combinatorial problems like finding an optimal route for deliveries or automated drive, aka the traveling salesman problem. Such algorithms can also optimize the design of integrated circuits where one generally seeks to minimize the links between functional blocks, transistors and to minimize energy consumption, forms of sub-constrained optimization adapted to quantum processing. This category of algorithms can find solutions to combinatorial optimization problems (like discrete log, traveling salesperson problem and QUBO) and continuous optimization problems used in many other fields (linear programming, gradient descent, LPs, convex optimizations and semidefinite programming).

Quantum machine learning algorithms which under some circumstances could be more efficient than machine learning algorithms running on classical hardware, including GPGPUs and TPUs. This can impact both training machine and deep learning models and running inferences.

Quantum physics simulations is a broad field with applications in inorganic and organic chemical processes optimization and new material designs. This is based on simulating at the lowest level the interactions between atoms in molecules and crystal structures or magnetism, which themselves depend on the laws of quantum mechanics. This may help invent new solutions such as more efficient batteries that can be charged more quickly and with greater energy density, craft chemical processes for carbon capture or nitrogen fixation or create superconducting materials operating at room temperature.

Biological molecule simulation requires a much larger number of qubits, and therefore are positioned in the longer term. Quantum simulation may eventually help run simulations of biological molecules. This will start with the simulation of peptides, then polypeptides, and finally proteins folding and interactions. Biological molecules have the particularity of being overly complex, with structures that can reach tens of thousands of atoms. The top of the line would be the ability to simulate the assembly and then the operation of a ribosome, which is more than 100,000 atoms. It is the most magical molecular structure in living organisms, the one that assembles amino acids to build proteins from the messenger RNA code resulting from the transposition of gene DNA. This would be followed by the simulation of the functioning of a whole cell. But we are here bordering on with science fiction.

[1531] There are many such classifications around. I've used the most common one.

Key factoring problems relate to cryptography and breaking public encryption keys like RSA keys with Shor's integer factoring algorithm. These may be implemented over a very long-term, when highly scalable gate-based quantum computers are available.

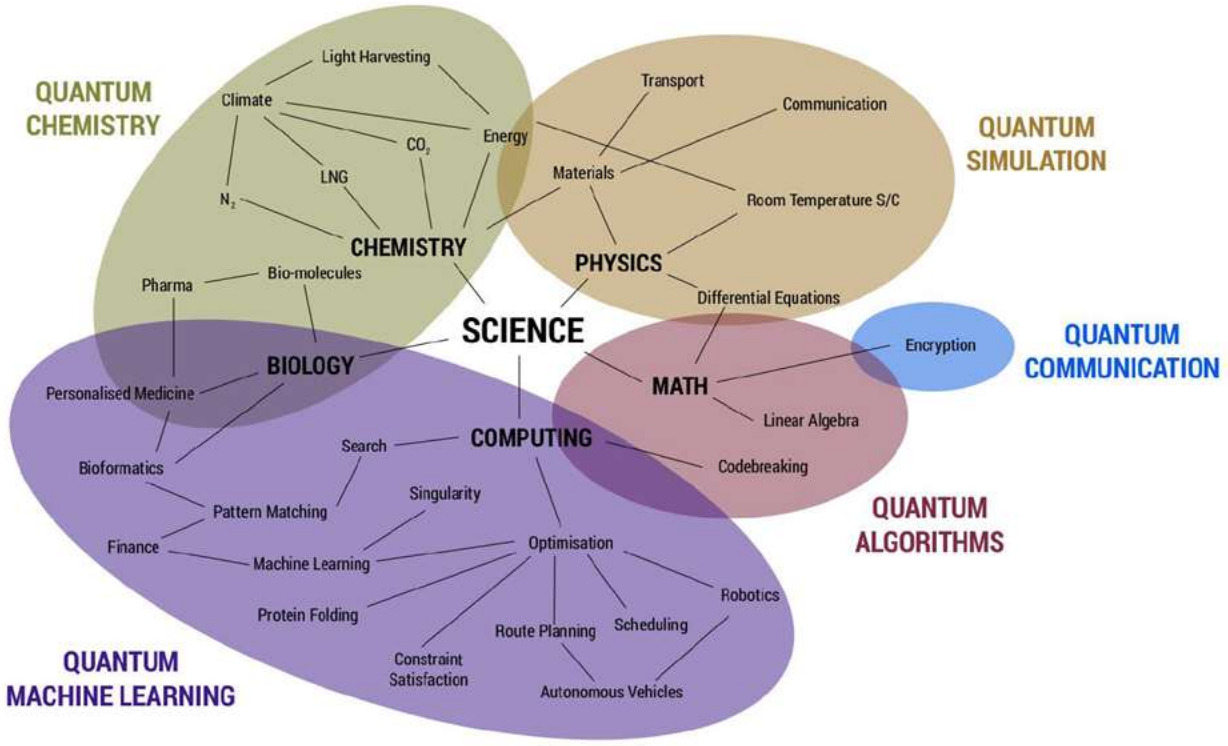


Figure 551: the breadth of science domains covered by quantum algorithms. Source: Silicon Photonic Quantum Computing by Syrus Ziai, PsiQuantum, 2018 (72 slides).

Hybrid algorithms, as already mentioned, use a mix of quantum and classical algorithms. These are mostly used for chemical simulations but also quantum machine learning. Most quantum algorithms are actually hybrid: QAOA, VQE, oracle-based algorithms when the oracle is retrieving classical data and even Shor's integer factoring algorithm.

Quantum inspired algorithms are classical algorithms inspired by quantum algorithms, particularly those that rely on interferences which are key characteristics of quantum algorithms.

See also this mapping of applications of quantum computing in Figure 551, which is however a bit fanciful, linking the learning machine to "singularity", which does not mean much.

Algorithms and quantum computing paradigms

There's a relation between these broad classes of algorithms and the class of quantum computers they can run on. Reusing the quantum algorithms paradigm classification used earlier in this book, this gives an idea of what works where and when, given these computer classes span from available systems (quantum annealing), to NISQ systems in the short to mid-term, to very long-term availability (large scale quantum computing). It's still an open question to find relevant and useful algorithms running on NISQ systems, if not reaching a quantum advantage with these[1532].

[1532] See the review paper Noisy intermediate-scale quantum (NISQ) algorithms by Kishor Bharti, Alán Aspuru-Guzik et al, Review of Modern Physics, October 2021 (91 pages) and Simultaneous quantum circuits execution on current and near-future NISQ systems by Yasuhiro Ohkura et al, Dec2021 (10 pages) which addresses some limitations of NISQ systems with running smaller QPUs in parallel.

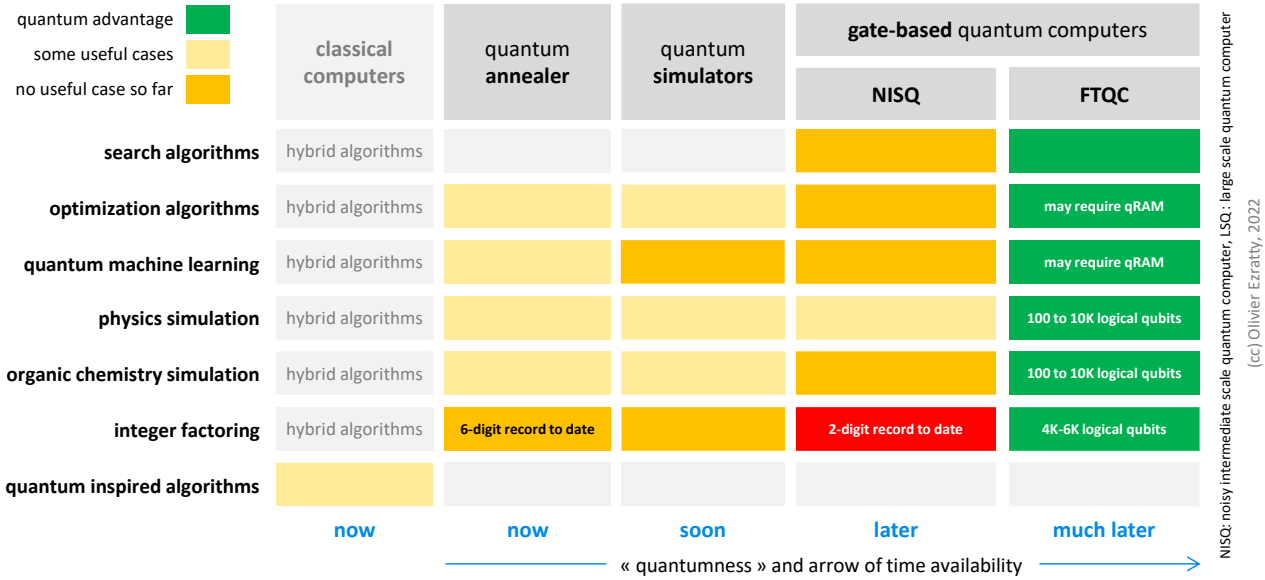


Figure 552: classes of quantum algorithms, the quantum computing paradigm (gate-based, simulation annealing) they can run on and a time scale for their practical availability. Surprisingly, integer factoring algorithms are also available on quantum annealers and simulators, but it may not scale as well as future FTQC systems. (cc) Olivier Ezratty, 2021-2022.

Algorithms process and compilation

As we have seen in a previous section describing the structure of gate-based quantum computing, page 161, a quantum algorithm is built with three key parts: data initialization or preparation, computing and qubits readouts. This is always done on a data structure called a quantum register, made of N qubits. Data initialization, preparation and computing are implemented with quantum gates.

Results. The algorithm result comes from the classical measurement of some qubits giving out a mix of 0s and 1s bits. In general, it is necessary to run several times the algorithm entirely and compute an average of the generated results. How many times must it be done? It depends on the nature of the algorithm and the speed at which we'll move from a probabilistic output (one run) to a deterministic result (average of several runs).

Time constraints. The algorithm run must be compatible with the quantum computer characteristics. The main ones are qubits numbers, gates and readout fidelities and coherence time. These parameters will condition the usable depth of computing, *aka*, the number of series of gates that can be executed. This verification is generally performed by quantum code compilers. It will also have to consider the error correction codes that will be implemented in the hardware, either autonomously or through the control of the code compiler that will drive all logical qubits programming.

Gates conversion. Compilers play another key role: they translate the qubit gates used by the programmer into the set of physical qubit gates implemented at the hardware layer. Many quantum gates used by developers will be converted by the compiler into a set of universal quantum gates supported by the quantum computer. This will multiply the number of executed physical quantum gates compared to what shows up in the initial algorithm.

Geometry. They also take into account the physical geometry of qubits, i.e. how are they connected together. A simple two-qubit gate might require chaining a lot of SWAP gates because the two related qubits are far from each other in the quantum register physical layout.

Efficiency. An important consideration in creating quantum algorithms is to ensure that they are more efficient than their optimized counterparts for traditional computers or supercomputers. There are theories to verify this to evaluate the exponential, polynomial, logarithmic or linear rise in computing time as a function of the size of the problem to be solved, or a combination of all four. But nothing can replace experience!

Everything is linear. Quantum algorithms are practical applications of linear algebra, the branch of mathematics that handles vector spaces and matrix-based linear transformations. They are applied in large dimensional spaces, the vectors that define the states of qubit registers. Mathematically speaking, a qubit is a 2-dimensional vector space using complex number and N-qubit register manipulates a vector in a 2^N dimensional space of complex numbers. Their manipulation is based on matrix-based calculations that allow the qubit state to be modified without reading the content of the qubits. One way to look at a gate-based quantum algorithm would be the following: it's about finding the shortest path on a hypersphere of dimension 2^N from an initialized register to the problem solution[1533].

Conditional programming. Since quantum algorithms usually prohibits reading intermediate results, conditional programming is not obvious. Like running a given calculation depending on the value of some intermediate. However, multi qubits quantum gates (CNOT & co) are tools allowing conditional programming, but in another fashion than with classical computing. Conditional branching can be implemented in some situation and is implemented with hybrid algorithms using ancilla qubits for intermediate values measurements.

Algorithms toolbox

All these algorithms are based on a small set of classical low-level algorithms that we'll describe in detail in the Basic algorithms toolbox section starting page 589:

- **Quantum Fourier Transforms** (QFT), which helps find periods in a signal. It's used in the famous Shor integer factoring, in many other algorithms (HHL, QML), discrete log search, solving the hidden subgroup problem (HSP) and even for simple reversible arithmetic[1534].
- **Quantum Phase Estimation** are relying on a QFT to find the eigenvalues or eigenvalues' phase of a unitary matrix or quantum subcircuit. It is used in HHL and many other quantum linear algebra algorithms.
- **Amplitude amplification** is used to amplify and select the desired state of a quantum superposition. It is used in the Grover algorithm and with combinatorial searches like the traveling salesperson problem search (TSP).
- **Quantum Amplitude Estimation** is a variation of Grover's amplitude amplification that is used to evaluate the average amplitude of an oracle function. It is used in many algorithms such as in the quantum variations of quantum Monte Carlo integrations.
- **Quantum phase kickback** is an interference trick used in most oracle-based search algorithms and quantum walks, and then in quantum machine learning.
- **Hamiltonian Simulation** are used to find a point of equilibrium of a complex system such as in quantum physics simulation, neural networks training, the search for optimal paths in networks or process optimization. It can be implemented in all quantum paradigms: annealing, simulation and gate-based computing.
- **Ising model** is the mechanism used to drive quantum annealing and quantum simulators. This is the underlying model used with D-Wave machines. Many physics simulation, combinatorial and optimization problems can be translated or converted into some Ising model problem.
- **Quantum teleportation** is also an algorithm basic, used mostly in cryptography and telecommunication. It will also play a key role in distributed quantum computing and also in some non-telecom related algorithms.

[1533] It even seems to have a name: minimizing Wasserstein complexity as seen in Wasserstein Complexity of Quantum Circuits by Lu Li, Seth Lloyd et al, August 2022 (14 pages).

[1534] See A New Approach to Multiplication Opens the Door to Better Quantum Computers by Kevin Harnett, 2019.

We'll add here several other key basic algorithms components:

- **Data preparation**: how is data loaded in an algorithm? This is particularly important for quantum machine learning and optimization algorithms.
- **Uncompute trick**: which consists in reversing some parts of an algorithm after it is run. It allows to get rid of garbage states and cleaning up ancilla qubits.
- **Oracle**: which are binary functions implemented as unitaries that can be used for parallelizing their operation on all computational state basis (all combinations of 0s and 1s in part of a qubits register).
- **Linear equations**: and the famous HHL algorithm.

Classifying quantum algorithms is a tedious task due to the many dependencies they have with each other. For example, a QFT is used in HSP and phase estimate algorithms which themselves are used in integer factoring and linear equations solving. I have found many different if not inconsistent algorithms classifications in the available literature (Wikipedia, John Preskill, Algorithm Zoo, etc). Some for example consider oracle-based algorithms as a separate algorithm class when other split these algorithms in various classes depending on the sub-algorithms they are using.

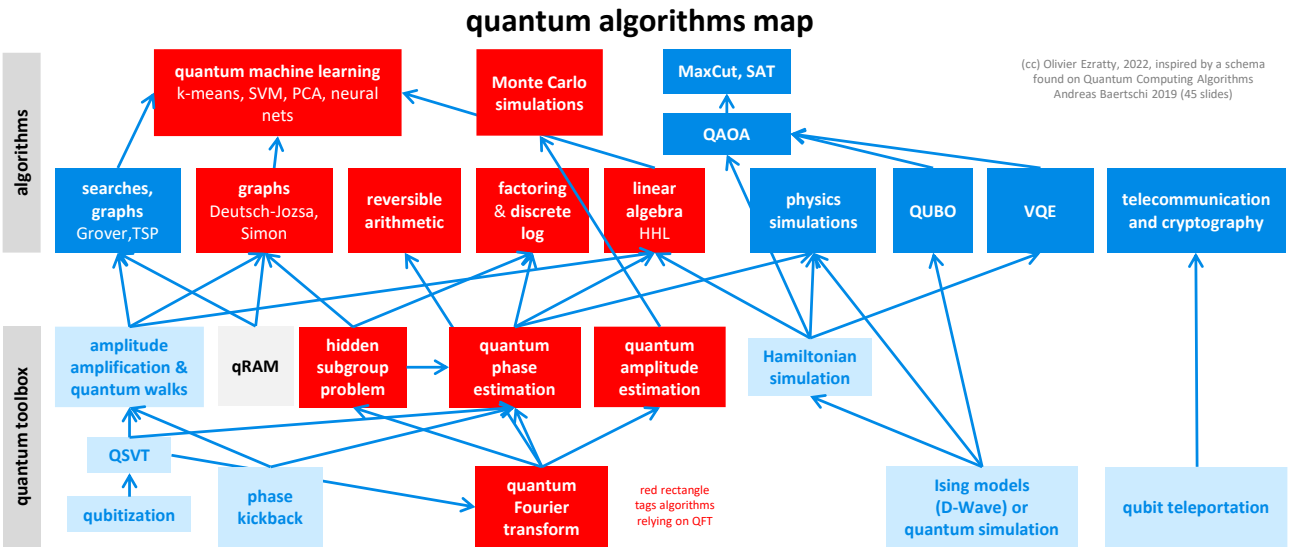


Figure 553: a quantum algorithms map and their interdependencies. One interesting example comes with QSVT which can be used to generate search, phase estimation and Fourier transforms. (cc) Olivier Ezratty, 2022, inspired by a schema found on Quantum Computing Algorithms by Andreas Baertschi, 2019 (45 slides).

The relationship between these low-level algorithms and higher-level ones is showcased in Figure 553. It shows qRAM for quantum RAM, which is not an algorithm per se, but a hardware tool that is indispensable to run the related algorithms, particularly Grover algorithm and a lot of quantum machine learning algorithms.

The chart in Figure 554 shows a more detailed connection between the QFT and the many algorithms that rely on it (those algorithms relying on a QFT are in red rectangles in Figure 553).

Algorithm	Description	Reference
Algorithms Based on QFT		
Shor's; $O\left(n^2 (\log N)^1\right)$	Integer factorization (given integer N find its prime numbers); discrete logarithms, hidden subgroup problem, and order finding	Peter W. Shor, "Algorithms for Quantum Computation Discrete Log and Factoring," AT&T Bell Labs, shor@research.att.com
Simon's; *exponential*	Exponential quantum-classical separation. Searches for patterns in functions	Simon, D.R. (1995), "On the power of quantum computation", Foundations of Computer Science, 1996 Proceedings., 35th Annual Symposium on: 116–123, retrieved 2011-06-06
Deutsch's, Deutsch's – Jozsa, an extension Deutsch's algorithm	Depicts quantum parallelism and superposition. "Black Box" inside. Can evaluate the input function, but cannot see if the function is balanced or constant	David Deutsch (1985). "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer", Proceedings of the Royal Society of London A. 400: 97 David Deutsch and Richard Jozsa (1992). "Rapid solutions of problems by quantum computation". Proceedings of the Royal Society of London A. 439: 553
Bernstein/Vazirani; *polynomial*	Superpolynomial quantum-classical separation	Ethan Bernstein and Umesh Vazirani. *Quantum complexity theory.* In Proc. 25th STOC, pages 11–20, 1993
Kitaev	Abelian hidden subgroup problem	A. Yu. Kitaev. *Quantum measurements and the Abelian stabilizer problem,* arXiv:quant-ph/9511026, 1995
van Dam/Hallgren	Quadratic character problems	Wim van Dam, Sean Hallgren, *Efficient Quantum Algorithms for Shifted Quadratic Character Problems.* CoRR quant-ph/0011067 (2000)
Watrous	Algorithms for solvable groups	John Watrous, Quantum algorithms for solvable groups, arXiv:quant-ph/0011023, (2001)
Hallgren	Pell's equation	Sean Hallgren. *Polynomial-time quantum algorithms for pell's equation and the principal ideal problem,* Proceedings of the thirty-fourth annual ACM symposium on the theory of computing, pages 653–658. ACM Press, 2002.
Algorithms Based on Amplitude Amplification		
Grover's; $O\left(\sqrt{N}\right)$	Search algorithm from an unordered list (database) for a marked element, and statistical analysis	Lov Grover, *A fast quantum mechanical algorithm for database search,* In Proceedings of 28th ACM Symposium on Theory of Computing, pages 212–219, 1996
Traveling Salesman Problem; $O\left(\sqrt{N}\right)$	Special case of Grover's algorithm	https://en.wikipedia.org/wiki/Traveling_salesman_problem

Figure 554: Source: Quantum computing (QC) Overview by Sunil Dixit from Northrop Grumman, September 2018 (94 slides).

Quantum algorithms are classifiable and explainable at a high level, but their detailed understanding is not easy. You must develop some conceptual capacity in a rather analog world[1535].

One key thing developers have to learn is how to translate customer needs into existing quantum algorithms. How to assemble various quantum algorithms, frequently combined with classical algorithms, is another key skill.

Algorithms figures of merit

It is rarely talked about, but what are the key figures or merits for quantum algorithms? In a generic way, they should showcase either a provable speedup compared with classical algorithms running on classical computers or some other quantitative advantage (precision, error rates for quantum machine learning, energy consumption advantage). They should generate a relative small-size data output since N qubits generate only N useful bits of information. At last, there should be some correctness guarantee on the results and of course, it should solve some useful problem. In the case of NISQ algorithms, they should add two requirements: a shallow depth circuit (not many quantum gate cycles) and a resilience to qubit noise[1536].

[1535] Here are a few sources of information to explore the topic: Quantum Computing Applications by Ashley Montanaro from the University of Bristol, 2013 (69 slides), an interesting course on the algorithmic part, An Introduction to Quantum Computing by Phillip Kaye, Raymond Laflamme and Michele Mosca, Oxford, 2017 (284 pages), Lecture Notes on Quantum Algorithms by Andrew M. Childs, University of Maryland, 2017 (174 pages), Quantum Computation and Quantum Information by Nielsen and Chuang, 2010 (10th edition, 704 pages) and A Course in Quantum Computing for the Community College by Michael Locef, 2016 (742 pages) which sets out in great detail the mathematical foundations of linear algebra with complex numbers, Euler formulas, vector and Hilbert spaces, matrix calculus, tensors, eigenvectors and eigenvalues, and quantum algorithms. It takes several weeks to be browsed and understood. It is a course for the second and third year of the Foothill Community College in Los Altos Hills, California (so Bac+1/+2 in French equivalent). In addition, here are some videos on this subject: Quantum Algorithms by Andrew Childs in 2011 (2h31), Language, Compiler, and Optimization Issues in Quantum Computing by Margaret Martonosi, 2015 (39 minutes and slides) and What Will We Do With Quantum Computing? by Aram Harrow, MIT, 2018 (32 minutes).

[1536] This inventory is inspired from the second page chart in Towards Quantum Advantage on Noisy Quantum Computers by Ismail Yunus Akhalwaya et al, September 2022 (32 pages) which presents a NISQ QML-based algorithm matching all these figures of merit. But … requiring 96 qubits with 99,99% 2-qubit gate and measurement fidelities which are yet to come, even with trapped ions.

Basic algorithms toolbox

We'll describe here the overall structure of basic low-level gates-based quantum algorithms. We separate three stages: **data preparation**, **unitary transformations** (caveat: data preparation also relies on unitaries) and **measurement**.

We have already covered **error correction** in a previous chapter of this book, starting page 216.

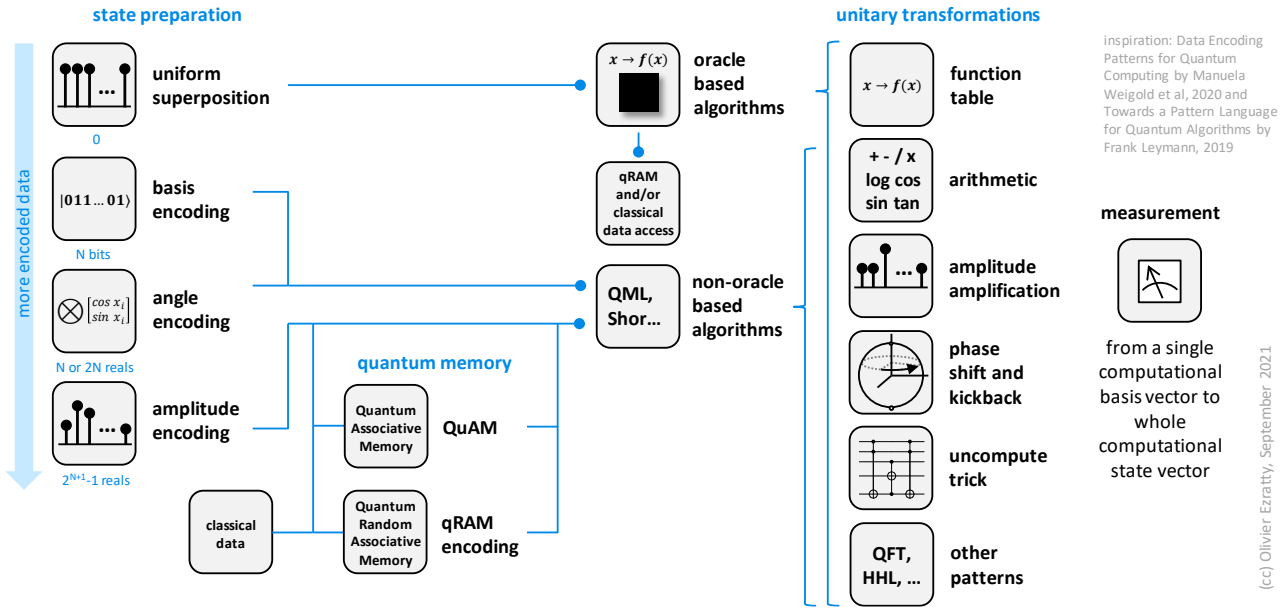


Figure 555: how is data fed into a quantum algorithm depending on whether it uses or not an oracle. (cc) Olivier Ezratty, 2021.

Data preparation

The data preparation stage is also named data loading. Its complexity covers a large range from the simple process of uniform superpositions associated to oracle-based algorithms like Deutsch-Jozsa, Simon or Grover to the most complicated, linked to quantum machine learning algorithms requiring full computational basis state vector amplitude encoding.

Data loading is only implemented with non-oracle-based algorithms. It may be a long process for large sets of inputs and significant number of qubits. It thus may require using some form of quantum memory, a sort of qubits buffer used only for data preparation.

It can use addressable qubits like with qRAM where a program can ask to "*put this information in qubits at index i*". This memory can be a qubit register with a longer coherent lifespan than computing qubits or a classical data structure used along a quantum circuit to load a specific addressable quantum state. The data is not necessarily stored in some qubits. When the data is loaded in quantum memory, this one must be transferred to the computing qubits. This is a data transfer and not a data copy process due to the no-cloning theorem. All in all, quantum memory is just some sort of intermediate memory used before computing.

Let's first look at the various techniques used for data encoding[1537].

Uniform superpositions correspond to the simplest qubits register initialization with a register state where all the computational basis states have the exact same amplitude.

[1537] Here are the various sources I used to reconstruct this map: Loading Classical Data into a Quantum Computer by John Cortese and Timothy Braje, 2018 (38 pages), Circuit-centric quantum classifiers by Maria Schuld, Krysta Svore et al, 2018 (17 pages), Robust data encodings for quantum classifiers by Ryan LaRose and Brian Coyle, 2018 (24 pages), Towards a Pattern Language for Quantum Algorithms by Frank Leymann, 2019 (12 pages), Quantum linear systems algorithms: a primer by Danial Dervovic et al, 2018 (55 pages) and The Bitter Truth About Quantum Algorithms in the NISQ Era by Frank Leymann and Johanna Barzen, 2020 (42 pages).

It is used by an oracle-based algorithm where the "real data" sits in the oracle function f(x) that outputs such and such values depending on the entry (usually, a 1 for a single entry and 0 for all the others). The oracle can evaluate this function simultaneously for all superposed computational basis values in the prepared superposed register. This superposition is done with applying Hadamard gates on all computing qubits where some data must be prepared.

Basis encoding consists in directly transferring N classical bits in N qubits, using a set of X gates (Y gates would also make it), to change individual qubits from $|0\rangle$ to $|1\rangle$. It creates a simple encoding of a computational basis single state, combining 0s and 1s matching classical bits. The 2^N dimensions computational basis state vector thus contains only zeros and a single one related to this combination. Before this encoding, we select the method to encode the problem data which can be for example a floating-point number or an integer in a given number of classical bits before converting them on a computational basis state. Such a basis encoding is used in Shor's algorithm to provide the integer that must be factorized.

Angle encoding is about encoding a vector of real values of dimension N into N qubits. It's also named product encoding. Each qubit is individually encoded with single qubit gates R_x (which themselves are usually decomposed in simple Pauli and T gates) to encode one of the (Bloch sphere) qubit angle. Since the register is the tensor product of each qubit, with no entanglement, we don't have any exponential gain in the encoding. The dense angle encoding variation uses two angles in the encoding for each qubit and can make use, additionally of R_y and R_z gates for the sake of adding some phase in each qubit state. We end up here with a maximum of 2N real numbers encoded in the N qubits register. And the qubit register is separable, its quantum state being separable into the quantum states of each of its qubits. It reminds us that without entanglement, you can't benefit from the exponential storage (or, better, data handling) capacity of quantum computing. In that case, data encoding requires a depth of $\log_2(N)$ gates.

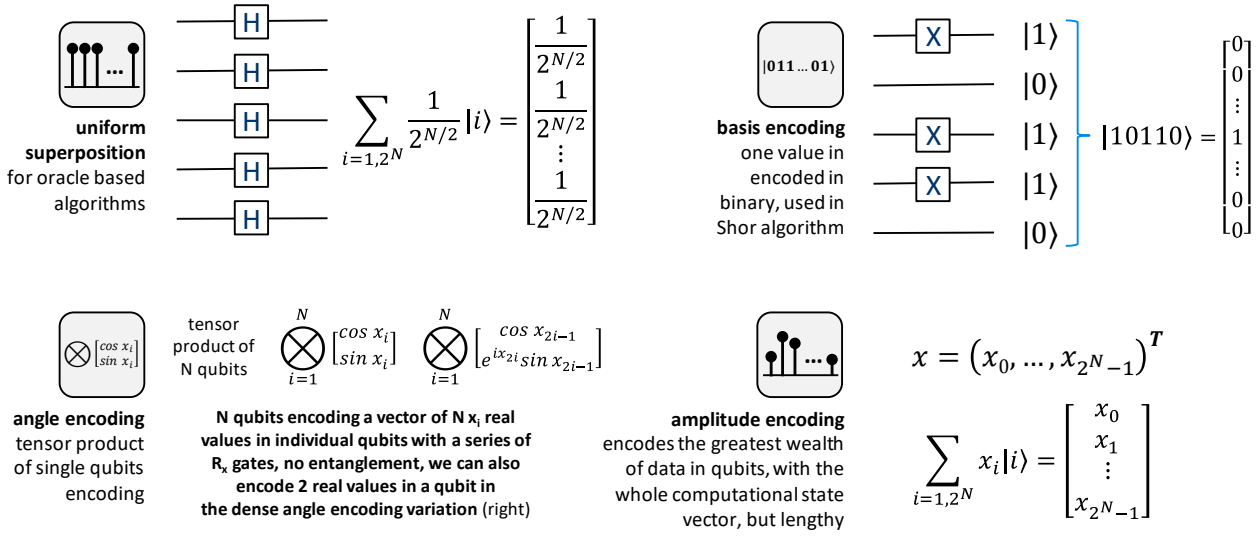


Figure 556: details on the four ways to encode data in a qubit register, the most resource and time consuming being amplitude encoding. (cc) Olivier Ezratty, 2021.

Amplitude encoding is about creating an arbitrary superposed state associating computational basis states with given real number amplitudes. It is also called an arbitrary state preparation, quantum embedding or wavefunction encoding. It creates a computational state vector with real numbers in several rows. To encode a vector of L real values, you need N=ceil($\log_2$(L+1)) qubits. Meaning you round up the $\log_2$ of the vector size and don't use the left-over values in the register vector. Why +1? Because of the normalization constraint, the sum of amplitude being equal to 1. So with 3 qubits, you have 7 available values, not $8=2^3$. Since the size of your encoded vector may be smaller than the 2^N states of your register, you'll pad the encoded vector with 0s.

To create an arbitrary amplitude set for N qubits, you need at least $\frac{1}{N}2^N$ gates operations combining single and two qubit gates since an arbitrary amplitude encoding will create an entangled state contrarily to a simple product encoding. The usual encoding algorithms use 2^N gates. So, unless the encoded data is sparse (with a lot of zeros), data preparation grows exponentially with the number of qubits, erasing any computing advantage we could get afterwards. It explains why quantum computing is not ideal for any big data computation task, and, at this point, for data intensive machine learning tasks[1538]!

Encoding precision. Angle and amplitude encoding theoretically deals with real numbers. But what is their precision, particularly on NISQ computers? It is at least bound by the cumulative error rates coming from the encoding qubit gates. It can easily reach a couple %, meaning the encoding precision is limited to a couple digits.

Non linearities. Quantum computing is based on using linear unitaries. This creates limitations on the kinds of computing that can be processed quantumly. But we can handle nonlinearities indirectly. One way lies with the way real numbers are turned into the raw data to be encoded with angle or amplitude encoding. Another way is to use angle encoding with repetition, creating powers of encoded values in the computational state vector of the input vector[1539]. Finally, we can apply non linearities on the classical data before it's quantumly encoded. It can also be implemented as a classical Boolean nonlinear circuit embedded in a quantum reversible circuit.

How many registers? In a classical microprocessor, the computing unit is handling data in multiple registers and the arithmetic logical unit can pull data from registers, make calculations and update registers with its results. In a quantum computer, there is usually only one register of N qubits. It can however be logically and dynamically partitioned by the algorithm. There are usually computing qubits and ancilla qubits. Computing qubits contain the input data related to the problem to be solved and that's on this data that most algorithm patterns will be executed, particularly with an oracle. The remaining qubits in the register will be used as accessory qubits and may also contain some part of the algorithm result. And this goes only with logical qubits. We've seen before that quantum error correction is using a lot of ancilla qubits.

Black boxes and oracles

A black box based algorithm is a classical operation encoded with qubit gates that is applied simultaneously to various computational basis states. It's used in the famous Deutsch-Jozsa, Simon and Grover search algorithms. A black box contains reversible quantum equivalents of Boolean and arithmetic functions. It works on n entry qubits x in superposed states and merges its result with m ancilla qubits y, that are usually initialized at 0. It leverages quantum parallelism with input initialized with Hadamard gates. If m = 1, the black box outputs a yes or no (1 or 0) and is branded as an "oracle"[1540].

There are many ways to implement an oracle. It can be entirely encoded with qubit gates or access some classical memory or functions, presumably through some qRAM addressing scheme. Presumably since the technology doesn't exist yet. Even the cost of implementing an entirely quantum oracle is unknown. For instance, just some complicated arithmetic functions can be highly costly in quantum gates since it may require implementing several QFTs (quantum Fourier transforms).

[1538] There are some ways to optimize amplitude encoding. See Quantum Resources Required to Block-Encode a Matrix of Classical Data by B. David Clader, William J. Zeng et al, Goldman Sachs, Caltech, AWS and Imperial College London, July 2022 (31 pages) also described in Goldman Sachs and AWS examine efficient ways to load data into quantum computers by Grant Salton et al.

[1539] See On nonlinear transformations in quantum computation by Zoë Holmes et al, December 2021 (10 pages) that describes another technique to introduce the support of nonlinearity in gate-based quantum computing.

[1540] See Inverse Problems, Constraint Satisfaction, Reversible Logic, Invertible Logic and Grover Quantum Oracles for Practical Problems by Marek Perkowski, May 2020 (62 slides).

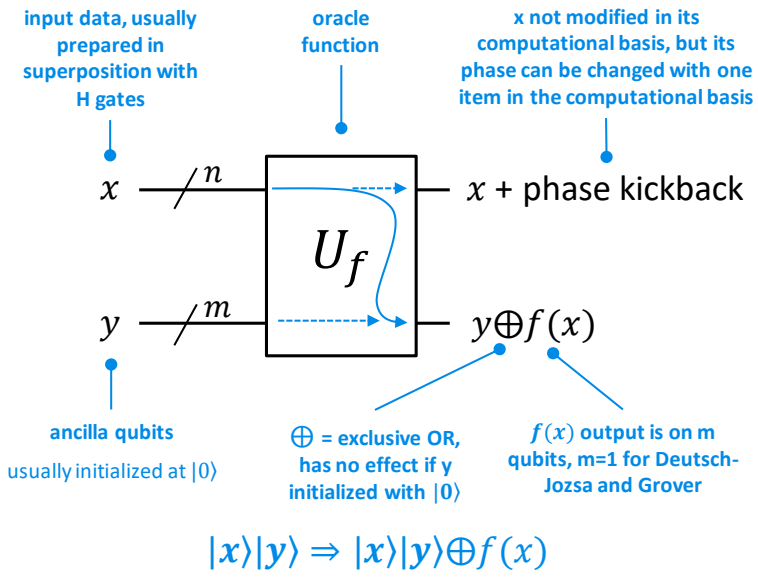


Figure 557: how an oracle function is used in an algorithm, in complement of a phase kickback. (cc) Olivier Ezratty, 2021.

Oracle-based algorithms speedup nearly never mention the potential computing overhead coming from the oracle itself. In an ideal world, the oracle implementation complexity should scale linearly and at worst polynomially with the number of handled qubits.

This overhead can be highly detrimental to any potential algorithm theoretical speedup. This is particularly concerning for Grover's algorithm that we'll look after later. This algorithm's speedup is only polynomial, before taking into account the oracle's cost, and of course, quantum error correction (although its cost is "only" polylogarithmic). In the end, Grover's algorithm may not bring any acceleration at all.

In other words, touting some oracle-based algorithm speedup is like saying that a car drives fast thanks to its aerodynamism, without mentioning anything about its engine specifications and power.

Output encoding

The literature covering quantum algorithms rarely explains the format of the results they are generating. There are as many variations as in data encoding. This section echoes the one that was dedicated on the various sorts of qubits measurement, page 184. The simplest outcome of a quantum algorithm should be a computational basis vector with a series of $|0\rangle$ and $|1\rangle$, generating a classical bit string like with Shor's factoring algorithm. In this case a single run and measurement provides full characterization of this outcome (modulo the error rate of the system). This is the case for many classical quantum algorithms as described in the table below.

However, some algorithms like HHL (linear equations) may generate data encoded in amplitude. Exploiting directly an amplitude encoded vector state doesn't make much sense since you lose any exponential advantage coming from the algorithm. Decoding a full vector state indeed requires running the algorithm several orders of magnitudes of an exponential of the number of qubits. But such an algorithm may be an intermediate one feeding another algorithm. If we keep using quantum data from end to end, then it makes sense to use and create algorithms that output amplitude encoded data[1541].

[1541] This is what is proposed in Quantum advantage for differential equation analysis by Bobak T. Kiani, Dirk Englund, Seth Lloyd et al, April 2022 (21 pages). The authors use the output of a quantum differential equation solver as the input for a quantum machine learning algorithm.

In some cases, though, like with VQE algorithms, some generalized measurement of the state vector must be done[1542]. Other algorithms like in computational chemistry output will take the form of expectation values that are real numbers computed with averaging the results of many qubit readout values obtained with many computing runs. Its overhead requires significant optimizations[1543].

algorithm	input	output
Deutsche-Jozzsa	oracle function	function is balanced if all output qubits are at ground state |0⟩
Bernstein-Vazirani	oracle function	(integer) secret string in basis encoding
Grover	oracle function	searched item index as integer in basis encoding
Simon	oracle function	parameters for a linear equation used to find a period, with average of basis encoding
Shor factoring	parametrized period finding function (quantum part)	integer in basis encoding
Shor dlog	integers in basis encoding	integer in basis encoding
QFT	series of complex amplitudes with amplitude encoding (any quantum input state)	Fourier coefficients in amplitude encoding, enabling the recovery of the main frequency
HHL	one vector and one matrix amplitude encoding	characteristics of inverted matrix x entry vector (= one vector) in amplitude encoding
VQE	cost function parameters encoded as an Hamiltonian with unitaries (quantum gates)	researched ground state in amplitude encoding
QML classification	object vector to classify encoded in amplitude	prediction result as an integer index in basis encoding

Figure 558: various algorithms and the format of their input and output data. (cc) Olivier Ezratty, 2021-2022

Quantum phase kickback

The role of an oracle is to change the phase of the found item in the computational basis state vector x. Instead of sending the phase to the ancilla qubit y, it is applied to the found result in the source x qubits thanks to the phase kickback mechanism. It is implemented for example in the Grover algorithm that we'll see later.

The Grover operator then amplifies the amplitude of the found item and attenuates the amplitude of the other items in the computational basis, leveraging this phase information injected in the x computational basis vector state. For this to work, the control qubits must be in a superposed state, created by Hadamard gates initialization, the target qubit $|\psi\rangle$ must be an eigenvector of the operator U applied to the target qubit $|\psi\rangle$ using the control qubits[1544].

This simple two qubit configuration explains what's happening. A control-phase gate ends up modifying the phase of the control qubit instead of the phase of the target qubit. It works in the example case since after the X gate being applied to the target qubit, the qubit state becomes an eigenvector of the control-S operation that is executed afterwards[1545].

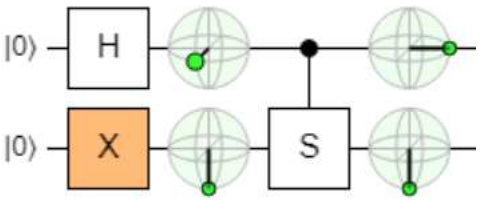


Figure 559: a two-qubit phase kickback.

[1542] See Learning to Measure: Adaptive Informationally Complete Generalized Measurements for Quantum Algorithms by Guillermo García-Pérez et al, PRX, November 2021 (18 pages) that proposes a POVM -based technique to undertake such measurement.

[1543] See Nearly Optimal Quantum Algorithm for Estimating Multiple Expectation Values by William J. Huggins, Ryan Babbush et al, Google AI, PNNL, Stanford and University of Toronto, November 2021-October 2022 (18 pages).

[1544] As explained in Phase Kickback by Eduard Smetanin, November 2019 (4 pages).

[1545] This is explained in A clever quantum trick by Emilio Peláez, January 2021. See also Quantum Phase Kickback - What I told you was true… from a certain point of view by Frank Zickert, March 2021.

It is not changed by a phase rotation. Since a control-phase changes the global phase of both qubits, the phase modification can only happen on the control qubit. Despite the entanglement created by the control-S gate, the qubits remain separable.

In a general case, when the target qubit $|\psi\rangle$ is an eigenvector of the unitary U (here, a S gate), the target qubit doesn't change after the control-U gate. Literally: $U|\psi\rangle = e^{i\phi}|\psi\rangle$. The control qubit changes and one of its computational state vector amplitudes gets multiplied by the eigenvalue of the eigenvector of U.

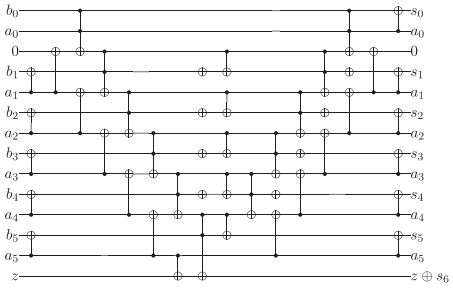
Arithmetic

Arithmetic functions can be implemented in a quantum algorithm. It's mostly used in oracles. There are many quantum algorithms around that implement various arithmetic functions: adders, multipliers, dividers and even transcendental functions (exponential, logarithm, and trigonometric functions)[1546].

arithmetic operations can be useful in many algorithms

quantum reversible adders/multipliers can be derived from their classical counterparts (ripple-carry adders) or use a QFT and IQFT (inverse QFT) to reduce the need for ancilla qubits

Adder type	Toffoli/T depth	Toffoli/T gates	Qubits required
Majority ripple [12]	$2n$	$2n$	$2n+1$
Prefix-ripple [Section A.1]	n	$3n$	$2n+1$
Carry look-ahead [13]	$4log_2(n)$	$10n$	$4n - log_2(n) - 1$
Fourier transform basis [33]	$3log_2(1/\epsilon)$	$3nlog_2(1/\epsilon)$	n



The ripple-carry adder for $n = 6$.

6-bit ripple-carry addition adder

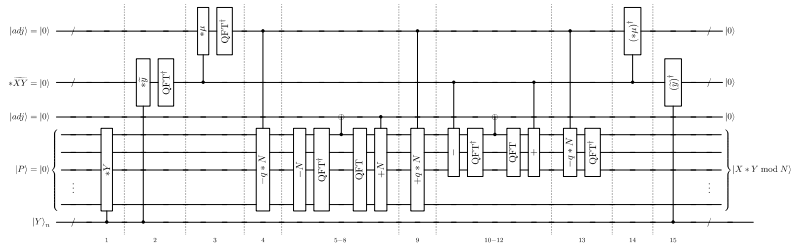


Figure 12: Barrett multiplication circuit using Fourier arithmetic. The numbers in the figure correspond to the steps of Algorithm 2.

Barrett multiplication circuit using QFT

Figure 560: various arithmetic computing can be implemented with quantum algorithms, mostly using a QFT. Sources: A new quantum ripple-carry addition circuit by Steven A. Cuccaro, Thomas G. Draper, Samuel A. Kutin and David Petrie Moulton, 2008 (9 pages) and High performance quantum modular multipliers, Rich Rinesy and Isaac Chuang, 2017 (48 pages).

Quantum reversible adders and multipliers can be derived from their classical counterparts like with ripple-carry adders, or use a QFT and IQFT (inverse QFT) to reduce the need for ancilla qubits.

Amplitude amplification

Amplitude amplification is a gate combination that is frequently connected to the phase kickback mechanism. It consists in amplifying one particular amplitude of the computational state vector of the control qubits that are submitted to an oracle function, at the expense of all the other amplitudes. It is used for example in the Grover operator from the Grover search algorithm as we'll see later.

In 2021, a researcher from the Fermi Lab at the DoE found a way to create an amplitude amplification working on a non-Boolean oracle[1547].

[1546] See A new quantum ripple-carry addition circuit by Steven A. Cuccaro, et al, 2008 (9 pages), High performance quantum modular multipliers, Rich Rinesyand and Isaac Chuang, 2017 (48 pages) and Quantum circuits for floating-point arithmetic by Thomas Haener, Mathias Soeken, Martin Roetteler and Krysta Svore, 2018 (13 pages) which were patented. See also Arithmetic on Quantum Computers: Addition, Faster by Sashwat Anagolum, October 2018, Arithmetic on Quantum Computers: Multiplication by Sashwat Anagolum, December 2018 and Everything You Always Wanted to Know About Quantum Circuits by Edgard Munoz-Coreas and Himanshu Thapliyal, August 2022 (18 pages) which provides a good overview of arithmetic algorithms among other topics.

[1547] See Non-Boolean Quantum Amplitude Amplification and Quantum Mean Estimation by Prasanth Shyamsundar, February 2021 (36 pages).

Qubitization was introduced by Low and Chuang in 2016 to facilitate the quantum computing of a time evolutive Hamiltonian e^{iHt} to a given error ϵ for particular types of Hamiltonian resulting from the projection of an unitary oracle onto a state created by another oracle [1548].

It enables the creation of optimized amplitude amplification techniques. It led to the creation of the singular value transformation algorithm (QSVT) that brings an exponential speedup with applying polynomial transformations to the singular values of a block of a unitary[1549]. This is related to the notion of SVD (singular value decomposition) of matrices to find the values in their diagonal matrix[1550].

Quantum Signal Processing is a technique also created in 2016 to compute and analyze a Hamiltonian that depends on a value θ that can be viewed as an angle in some signal. The QSP is a simulation algorithm with potential exponential speedup. It is based on a linearization of the operator of a quantum walk using eigenvalue transformation using a constant number of queries[1551].

Quantum Fourier Transform

Classical Fourier transforms are used to decompose a signal into its compound frequencies. In signal theory, this allows to identify the basic components of some sound by breaking it down into frequencies. In astrophysics, the atomic composition of stars is determined by a decomposition of the light spectrum, but this is done by an optical prism and not by Fourier transform. The same is true for Scio-type near-infrared sensors that determine the composition of food. A prism and the principle of diffraction therefore allow an optical Fourier transform to be performed.

The quantum Fourier transform was invented by **Don Coppersmith** (USA) in 1994.

A QFT is a quantum equivalent of a DFT or a FFT (Fast Fourier Transform). Its inverse operation, an inverse QFT is a QFT executed backwards, with its gates serialized in reverse order.

QFT is everywhere in the algorithm zoo as shown in red in Figure 553, page 587! Many known quantum algorithms are using it, including QPE (quantum phase estimation), HHL (linear equations), Shor's factoring algorithm and most QML algorithms. QFT helps find periodicity in a series of numbers, which is particularly helpful in Shor's algorithm.

A QFT is decomposing a series of qubits computational base states complex amplitudes in frequencies[1552]. The complex amplitude data encoding sits in the prepared register of qubits $|x_i\rangle$ with i=0 to n, as shown below.

These qubits contain a set of $N=2^n$ amplitudes α_j of the computational state basis orthogonal vectors $|j\rangle$, with j=0 to N-1.

The QFT implements a Discrete Fourier Transform (DFT) on these discrete amplitudes and converts it into a new computational state vector with amplitudes being the result of the QFT. The initial vector state can be written as in the formula on the right.

$$|\psi\rangle = \sum_{j=0}^{N-1} \alpha_j |j\rangle$$

[1548] See Hamiltonian Simulation by Qubitization by Guang Hao Low and Isaac L. Chuang, 2016-2019 (23 pages).

[1549] See Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics by András Gilyén, Yuan Su, Guang Hao Low and Nathan Wiebe, 2018 (67 pages).

[1550] See Everything about matrix factorizations by Tivadar Danka, 2022 which explains well what is SVD and visually.

[1551] See Optimal Hamiltonian Simulation by Quantum Signal Processing by Guang Hao Low and Isaac L. Chuang, 2016 (6 pages), Methodology of Resonant Equiangular Composite Quantum Gates by Guang Hao Low, Theodore J. Yoder and Isaac L. Chuang, PRX, 2016 (13 pages) and the tutorial A Grand Unification of Quantum Algorithms by John M. Martyn, Zane M. Rossi, Andrew K. Tan and Isaac L. Chuang, May 2021 (39 pages).

[1552] See Quantum circuit for the fast Fourier transform by Ryo Asaka et al, 2020 (20 pages) which describes a QFT variant using a faster basis encoding for the input register.

The QFT creates a new state vector $\text{QFT}_N(|\psi\rangle)$ with N β_k amplitudes of the N computational basis vectors $|k\rangle$. It is a formula similar to the above starting point.

$$\text{QFT}_N(|\psi\rangle) = \sum_{k=0}^{N-1} \beta_k |k\rangle$$

The amplitudes β_k are computed with a big sum using all the amplitudes α_j with the coefficient ω^{jk}.

$$\beta_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{jk} \alpha_j$$

These coefficients $\omega^{jk} = e^{\frac{-2\pi i}{N} jk}$ explain the heavy use of R_n phase rotation gates in the QFT algorithm as described on the right. You can remove the minus sign to obtain a reverse QFT.

$$\beta_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2\pi i \frac{jk}{N}} \alpha_j$$

In the end, the QFT_N is a unitary matrix transformation $[\text{QFT}_\text{N}]$ with simple coefficients $[\text{QFT}_\text{N}]_{jk}$, as in a DFT.

$$[\text{QFT}_\text{N}]_{jk} = \frac{1}{\sqrt{N}} \omega^{jk}$$

When n=1 and N=2, the QFT becomes a Hadamard gate transform. The QFT is indeed presented as a generalization of the Hadamard operation, applied to dimensions N>2.

Since preparing such an arbitrary vector could take an exponential time with regards to the number of qubits, it is usually done through some faster preparation mechanism like in Shor's algorithm.

What are we really getting out of a QFT? Let's say we have 4 qubits and complex amplitudes with a rotating phase by 45° steps. It means we'll have a full phase periodic rotation for each 8 amplitudes and 2 full rotations for the whole state vector. The QFT will then output a register with the third qubit at $|1\rangle$ and all the others at $|0\rangle$.

This third qubit corresponds to the value 2, which is the frequency of the phase rotation. But we could have a more complex QFT with several added frequencies in the signal.

Getting all the β_k coefficients and frequencies still wouldn't make much sense. Indeed, recovering a whole computational basis state would require running the QFT at least one or two orders of magnitudes of 2^N. We'd lose any quantum speedup. What is usually done is to directly reuse this vector in the remainder of another quantum algorithm like Shor. Otherwise, after running the QFT a limited number of times, we can extract the computational basis state with the highest frequency. In other words, it means we'll have the main frequency extracted from the QFT, but not all of them.

The QFT relies on two types of logic gates: Hadamard gates to perform an overlay and two-qubit phase-controlled R gates whose phase is inversely proportional to 1 up to N. This creates a huge problem of accuracy in the calculation: the larger N is, the smaller the angle of rotation of the qubit in its Bloch sphere will be and the more impacting the phase errors will be. This requires a very precise control of the activation of the qubits.

In practice, phase-controlled R gates are generated by a combination of H, Z and T gates, plus a CNOT for the entanglement of the control qubit with the target qubit.

And it takes a lot! For example, for an R_{15} gate, 127 H/Z/T gates must be used to obtain an accuracy of 10^{-5}, which is enormous[1553]. This can be optimized with auxiliary qubits. And of course, we must integrate the associated error correction codes that add a good order of magnitude to the number of quantum gates in the depth of the calculation. This mainly impacts the calculation duration since the error correction codes are supposed to lengthen the duration of the qubit coherence.

[1553] See Efficient decomposition methods for controlled-R n using a single ancillary qubit by Taewan Kim et Byung-Soo Choi, 2018 (7 pages) and Approximate quantum Fourier transform with O(n log(n)) T gates by Yunseong Nam et al, 2020 (6 pages).

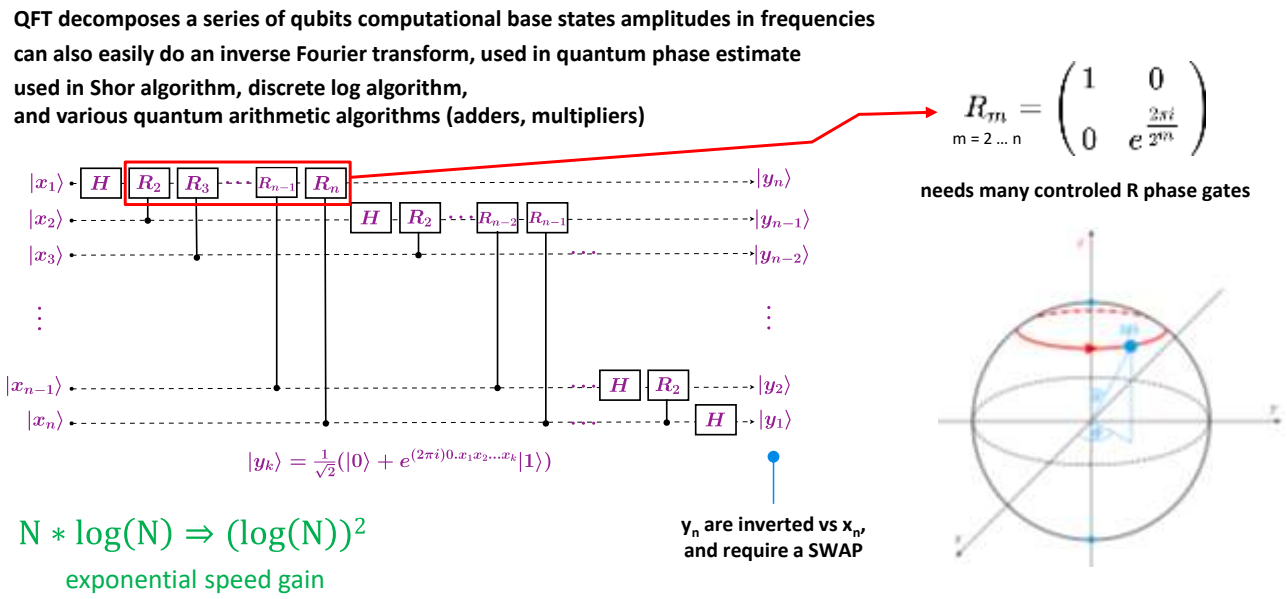


Figure 561: the quantum gates resource constraint with a QFT are enormous as its size grows. It requires controlled R phase gates that are very costly to generate, using in many cases a long combination of tens of H and T gates. (cc) Olivier Ezratty and various sources.

How about an R_{2048} gate decomposition, the last of a long series of R phase gates to break a 2048-bit RSA key? That's about the same number of gates. This comes from the Solovay-Kitaev theorem according to which this decomposition depends only on the targeted error rate[1554]. In the case of superconducting qubits, the generation of variable phase gates is achieved by sending a shorter microwave pulse.

Quantum phase estimation

Quantum phase estimation is an algorithm used to find the phase of an eigenvector of a unitary operator U. This operator can be implemented as an oracle function applied to a quantum state $|\psi\rangle$ that is decomposed in n controlled-unitaries operating on m qubits from $|\psi\rangle$. We are then looking for the phase angle θ according to $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$.

This algorithm is based on an inverse QFT. Practically speaking, the QPE can estimate the angle θ with a precision ϵ with executing U for $O(1/\epsilon)$ times (meaning, with a high probability within an error ϵ). The angle θ is encoded over n classical bits at the exit of the inverse QFT.

This algorithm was proposed by Alexei Kitaev in 1995[1555]. It is used among other domains in quantum chemistry and in Shor's factoring algorithm.

Quantum amplitude estimation

Quantum amplitude estimation was proposed by Gilles Brassard et al in 2000. In simple terms, it is used to evaluate the average value of a quantum oracle. The original version is a combination of a quantum phase estimation and Grover's algorithm. Some newer versions avoid the quantum phase estimate step and are more suitable to NISQ architectures[1556].

[1554] The main method of R_n gate decomposition is documented in Optimal ancilla-free Clifford+T approximation of z-rotations by Neil J. Ross and Peter Selinger, 2016 (40 pages). It's cotton!

[1555] New versions appear from time to time like Quantum Algorithm for the Direct Calculations of Vertical Ionization Energies by Kenji Sugisaki et al, University of Osaka, March 2021 (6 pages).

[1556] See Quantum Amplitude Amplification and Estimation by Gilles Brassard, Peter Hoyer, Michele Mosca and Alain Tapp, 2000 (32 pages) and Amplitude estimation without phase estimation by Yohichi Suzuki et al, 2019-2022 (13 pages).

Alexei Kitaev

finds the phase of an unitary operator

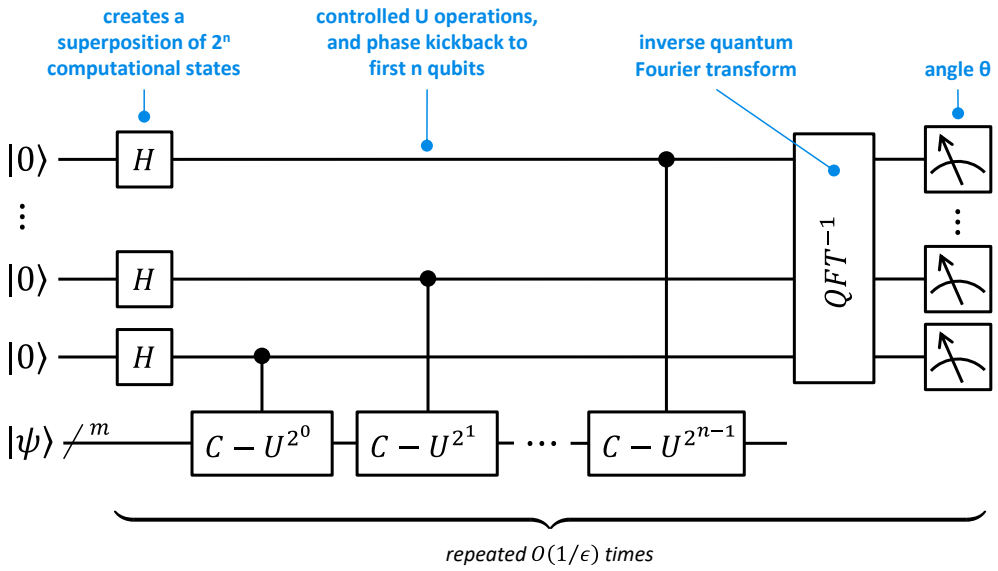


Figure 562: the quantum phase estimate algorithm explained. The probed unitary U must be decomposed beforehand into components. (cc) Olivier Ezratty with various sources.

Uncompute trick

The uncompute trick was created by Charles Bennet in 1989. It is used to rewind some parts of an algorithm affecting ancilla or input qubits. It cleans up the state of a qubits register without requiring a qubit reset that may damage the stored values in the qubits with the algorithm results. It is also used to disentangle the ancilla qubits from the input qubits. It then makes it possible to go on using these ancilla qubits for the remainder of the algorithm. In a word, it cleans up the qubits register garbage at the end of some computing. The transformation works if the unitary U_f is a reversible circuit which is the case for any combination of quantum gates (without any measurement done in between).

uncomputing U_f will:

disentangle ancilla qubits

make it available for subsequent computation

leave x and f(x) intact

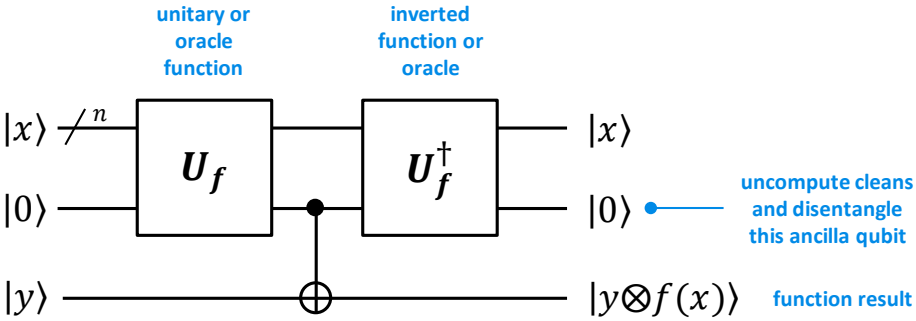


Figure 563: the uncompute trick algorithm cleans up a register and its ancilla qubits with disentangling them from the data qubits while preserving the function result from the computed algorithm. (cc) Olivier Ezratty with various sources.

The uncompute trick is often used when the algorithm is running an oracle function. But it presumes we are a working with "clean" qubits with no error. In a NISQ setting, an oracle inversion would generate so many errors that it would invert nothing.

Linear equations

Many other quantum algorithms exist that allow complex mathematical operations such as solving differential equations, inverting matrices, or processing various linear algebra problems. They are then used elsewhere as in QML.

The best-known algorithm is the **HHL**, named after its creators Harrow, Hassidim and Lloyd, and created in 2009. It allows to solve linear equations, with an exponential performance gain.

The HHL algorithm input is a combining a 2^Nx2^N sparse Hermitian matrix A (or is prepared to be Hermitian, see the schema below in Figure 564) and an input state $|b\rangle$ with 2^N amplitudes. Its output is $|x\rangle = |A^{-1}b\rangle$. Namely, it inverts matrix A and multiplies it by $|b\rangle$. The processing is done in time O(N) with an exponential speed-up. But the state $|b\rangle$ must be prepared in some sort of qRAM that doesn't exist yet or be prepared quantumly. Also, input matrix A must follow a lot of constraints, with a having only a few nonzero values (sparsity).

Harrow, Hassidim and Lloyd developed the HHL algorithm in 2009 which quantum mechanically inverts a system of linear equations. solves the system of equations $A\vec{x} = \vec{b}$ where:

- **A** : sparse square hermitian matrix nxn
- $\vec{b}$: vector with n values
- $\vec{x}$: solution vector to be characterized

requires inverting a matrix and uses a quantum phase estimate.

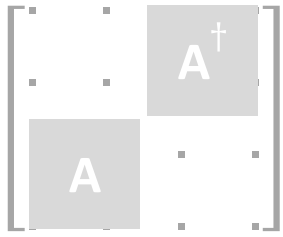
part of the QBLAS algorithms family
(Quantum Basic Linear Algebra Subroutines)

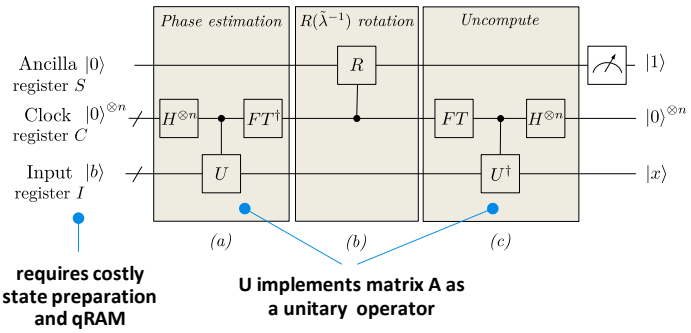
used in many QML algorithms.

$$N * \log(N) \Rightarrow (\log(N))^2$$

exponential speed gain, but finding the full $\vec{x}$ vector requires O(N) repetitions!

if matrix A is not hermitian, we construct another matrix with A that is hermitian





requires costly state preparation and qRAM

U implements matrix A as a unitary operator

Figure 564: the HHL linear equation solving algorithm. But its output is a quantum state that is costly to decode and should ideally be used with a subsequent quantum algorithm. The computed matrix must be Hhermitian. If it is not, it can be prepared to become Hermitian as explained on the top right. This preparation is named "block-encoding" or "standard-form" preparation.

There's a caveat, that Scott Aaronson explained well in 2015[1557]. The HHL output is a quantum state $|x\rangle$ that can't be read right away. The vector can be read to get some statistical information about it or, among other stuff, an evaluation of a dot product between $|x\rangle$ and another vector $|z\rangle$. If you want to know everything about $|x\rangle$, you'll need to repeat the operation 2^N times and lose any exponential advantage gained in the first place. In the end, HHL is not really inverting the matrix A with a real exponential speedup.

Still, HHL is an algorithm that can be piggybacked by other algorithms to solve interesting problems. It is mostly used with quantum machine learning algorithms. It can also be used to solve physics and engineering problems involving Poisson's equation[1558].

Hamiltonian simulation

Literally, as we've seen when describing Schrödinger's wave equation, a Hamiltonian of a quantum system is its description and evolution of its total energy, including kinetic and potential energy, over time. It's hard to evaluate for a given single quantum object and even harder for a multi-objects system. That's what Hamiltonian simulations are all about. One of their goals is to find the total energy of a system and its approximate ground state configuration which usually corresponds to its natural lowest-energy equilibrium state. It is particularly important in condensed matter physics and in organic chemistry.

[1557] See Read the fine print by Scott Aaronson, Nature Physics, 2015 (3 pages).

[1558] See Advanced Quantum Poisson Solver in the NISQ era by Walter Robson et al, September 2022 (4 pages) which shows however that such an algorithm doesn't work on an IBM 65-qubit system. A conclusion that shouldn't be generalized given future NISQ QPUs from various vendors including IBM could show up with better fidelities.

In that later case, it makes it possible to find the way molecules are naturally organized in three dimensions, from simple peptides to large proteins. It could also theoretically help simulate the interactions between different molecules.

Simulating a Hamiltonian was at the core of Richard Feynman's idea coined in 1981 when he wondered whether a quantum system could simulate another quantum system more efficiently than a classical computer, breaking down the fatal exponential growth of computing resources required to implement this kind of simulation on classical computers.

Such a simulation problem is described by a Hamiltonian which is a Hermitian matrix H of size 2^Nx2^N, when working with N qubits or N two-states quantum objects like spin-1/2 particles. This is based on the hypothesis of a constant H or a slowly evolving one, as in the adiabatic theorem. The quantum system evolves over time according to (1), given e^{itH} is the exponential of H (times i and t), is a unitary matrix. It is a solution to the Schrödinger equation (2):

$$(1) \quad |\psi(t)\rangle = e^{itH}|\psi(0)\rangle \qquad (2) \quad i\hbar\frac{\partial\psi(t)}{\partial t} = E\psi(t).$$

Simulating a Hamiltonian consists in finding matrix H or some characteristics of H. That simple. Or not.

The technique of the local Hamiltonian problem is a simplification of a Hamiltonian simulation. Thanks to special and general relativity, a Hamiltonian evolves according to local interactions. All Hamiltonian evolutions with only local interactions can be simplified as a combination of Hamiltonians acting on a limited space with at most ℓ of the total of N variables[1559].

Finding a system ground state of a local Hamiltonian is a QMA-complete class problem that can theoretically be efficiently solved on a quantum computer (QMA is defined later...)[1560]. Efficiently means with a polynomial instead of exponential growth in qubits. It mandates the usage of some quantum certificate or quantum proof, a validation technique used with QMA problems processing[1561].

There are of course many variations of Hamiltonian simulations depending on the type of quantum system to emulate and the characteristics we want to extract from H. It includes hybrid solutions associating classical and gates-based quantum computing including the quantum adiabatic algorithms.

If the Hamiltonian is of the family of an Ising model, it can be simulated using quantum annealers or quantum simulators. There are other families of Hamiltonians that can be simulated on quantum simulators or coherent quantum annealers with more than one degree of freedom (see Qilimanjaro).

Quantum teleportation

One of the most intriguing quantum gate-based quantum algorithms is qubit teleportation. It was created by Charles H. Bennett (USA), Gilles Brassard (Canada), Claude Crépeau (Canada), Richard Jozsa (USA), Asher Peres (Israel) and William K. Wootters (USA) in 1993[1562] .

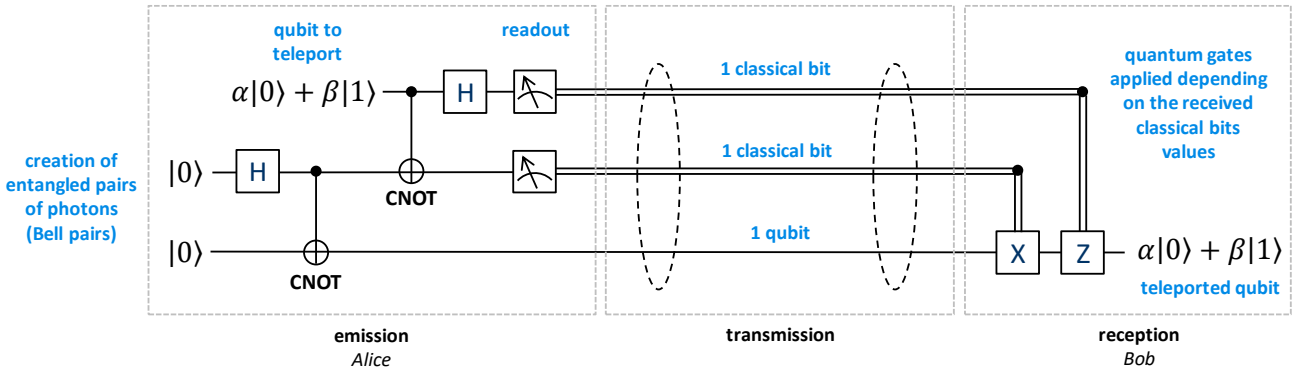
It allows to teleport the state of a qubit from one place to another. The principle of this algorithm consists in exploiting a pre-existing quantum entanglement channel to transmit the state of a qubit from one end of this channel to the other. Teleportation involves the transmission of two classical bits in the protocol that are used to reconstitute the qubit sent on arrival. As a result, the transmission of the latter cannot be faster than light.

[1559] See Using Quantum Computers for Quantum Simulation by Katherine L. Brown et al, 2010 (43 pages).

[1560] See QMA-completeness: the Local Hamiltonian Problem by Paul Fermé, based on lecture notes by Umesh Vazirani and lecture notes by Thomas Vidick, 2015 (6 pages).

[1561] See Lecture 20: Local Hamiltonian ground state problems by Richard Kueng, on a course from John Preskill, December 2019 (17 pages).

[1562] See Teleportation as a quantum computation by Gilles Brassard, 1996 (3 pages).



(cc) Olivier Ezratty, 2020

Figure 565: the quantum teleportation algorithm and its two classical channels. (cc) Olivier Ezratty with various sources.

Due to the quantum no-cloning theorem, this teleportation is a "move" and not a "copy" (or a "cut & paste" instead of a "copy & paste" to use an easy to understand analogy). The state of the transferred qubit is thus destroyed at its origin[1563]. The main use case of this algorithm and its many variants are in quantum cryptography and telecommunications systems that we will discover later.

It could also be used in distributed quantum computer architectures. Note that this algorithm can be tested locally in a quantum computer, as proposed by IBM in its Q Systems with Qiskit.

Higher level algorithms

We'll now cover higher level algorithms which are based on the algorithm's toolbox described in the previous part[1564]. Quantum software engineering requires three main set of skills: having an understanding of both low and high-level algorithms, then some know-how about the way these algorithms can be assembled and also coupled with classical algorithms, and then, above all, how to find the ways to translate "business problems" into these algorithms.

Oracle-based algorithms

One of the first quantum algorithms invented comes from David Deutsch, with its derivative called **Deutsch-Jozsa,** co-invented with Richard Jozsa and created in 1992. This algorithm makes it possible to characterize a function $f()$ called an "oracle" for which we know in advance that it will return for all its inputs, either always the same value, 0 or 1, or the values 0 and 1 in equal parts. The algorithm makes it easy to determine if the function $f()$ is balanced or not. It is working to a set of qubits n. Function $f()$ is making some classical computing on each 2^N values from the computational basis of n qubits.

The input qubits are all initialized to $|0\rangle$ except one which is initialized to $|1\rangle$. They are then all superposed between $|0\rangle$ and $|1\rangle$ with Hadamard gates. The qubits are thus said to have simultaneously all possible 2^{N+1} combinations of values.

It is easy to understand why this quantum algorithm is much more efficient than its traditional version: in traditional computation, more than half of the possible input values would have to be scanned sequentially, whereas in the quantum version, they are all analyzed at the same time by the oracle function working on all 2^N values of the first N qubits. The result is obtained with a few series of quantum gates, almost instantaneously, and it is perfectly deterministic.

[1563] See Quantum Teleportation in a Nutshell by Fabian Kössel, 2013 (35 slides).

[1564] See Quantum Algorithms by Ashley Montanaro, July 2016 (62 slides), Quantum algorithms: an overview by Ashley Montanaro, 2015 (16 pages), Quantum Algorithm Implementations for Beginners, 2020 (94 pages).

These superposed qubits are processed by the oracle which contains a set of gates implementing function $f()$ to be evaluated. The output is then measured to see if the function is balanced or not thanks to other Hadamard gates.

David Deutsch

Richard Jozsa

checks if oracle function f is balanced or not

has no known use case

$O(2^{N-1}) \Rightarrow O(1)$

exponential speed gain

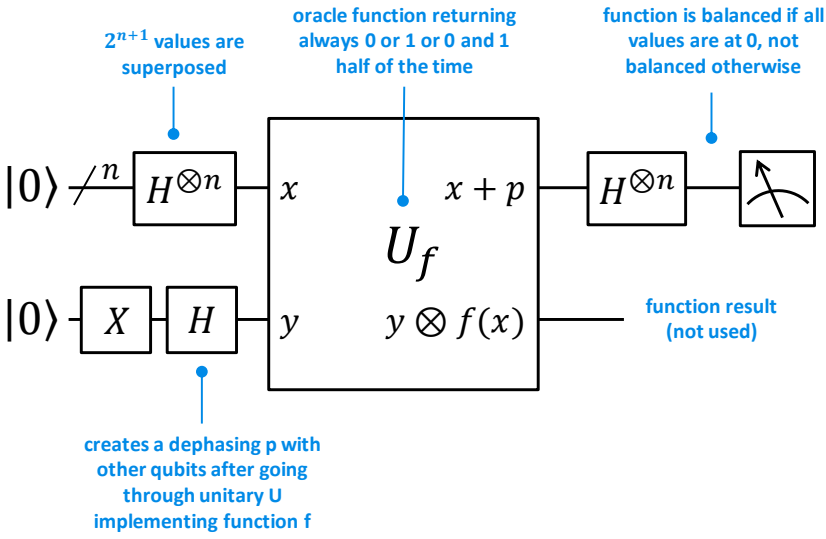


Figure 566: the famous Deutsch-Jozsa algorithm which says if a function is balanced or not and doesn't have any known practical application as far as I know. (cc) Olivier Ezratty with various sources.

The initialization of the last qubit to $|1\rangle$ is used to generate an interference with the other qubits that will impact the values leaving the H gates after passing through the oracle. The function $f()$ is constant if the final measurement gives $|000 \ldots 0000\rangle$ and unbalanced otherwise[1565].

What is the practical interest of such an algorithm given there are rather few functions $f()$ of this kind? This is an example of an ultra-powerful algorithm that has no known practical use to date. On top of that, there are very efficient classical probabilistic algorithms that are fast and cancel a good part of the quantum power gain coming from the Deutsch-Jozsa algorithm.

This is particularly the case with the Monte Carlo search algorithm which evaluates the oracle function on a limited number of randomly selected inputs.

The probability of errors depends on the number of evaluations and decreases very quickly[1566].

So, quantum computing is useless? Of course not. Other algorithms, less powerful but much more useful, have emerged since this patient zero of quantum algorithmics!

Bernstein-Vazirani's algorithm is less talked-about in textbooks. This algorithm created by Ethan Bernstein and Umesh Vazirani in 1992 is a variant of the Deutsch–Jozsa algorithm. Instead of using two different classes of functions, it tries to learn a secret string encoded in an oracle function. The algorithm was designed to prove an oracle separation between complexity classes BQP and BPP. The speedup of this algorithm is polynomial but a derivative recursive version of the algorithm has an exponential speed gain[1567]. The algorithm has not much practical use cases although it could be used in some cryptography cases[1568].

[1565] To find out how it works in detail, you can see the associated mathematical formulas as well as Eisuke Abe's Deutsch-Jozsa Algorithm presentation, 2005 (29 slides). But it is not that obvious!

[1566] See on this subject the document Quantum Computation Models (30 pages).

[1567] The algorithm is well explained in the Qiskit documentation.

[1568] See Using Bernstein–Vazirani algorithm to attack block ciphers by Huiqin Xie et al, 2019 (22 pages).

Ethan Bernstein and Umesh Vazirani - 1992

learns a secret string encoded in an oracle function

$O(n) \Rightarrow O(1)$

exponential speed gain

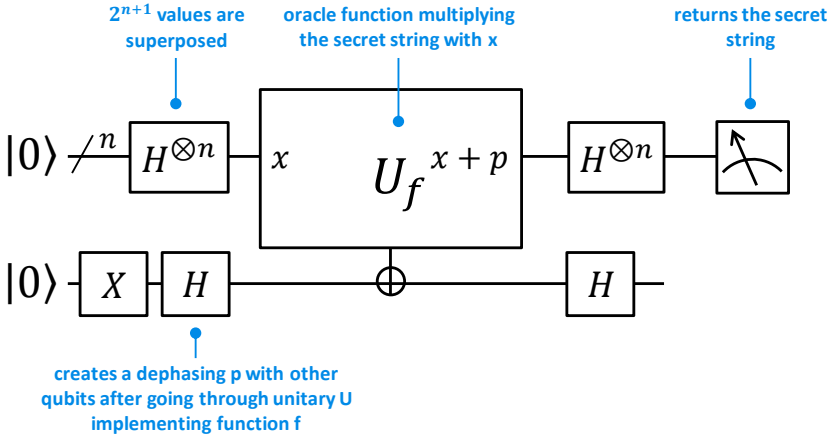


Figure 567: Bernstein-Vazirani algorithm. (cc) Olivier Ezratty with various sources.

Simon's algorithm is a more sophisticated variant of the Deutsch-Jozsa algorithm[1569]. It consists in finding the combinations of values that verify a condition imposed by the oracle function. It solves the so-called hidden subgroup problem (HSP). Its performance gain is very interesting and, this time, the algorithm is useful, particularly to solve path problems in graphs like with quantum walks. The gain in performance is typical of what quantum computing can bring: we go from a classical calculation which is exponential time ($2^{N/2}$) to a linear time in N.

Daniel Simon

search a subset of numbers matching a condition imposed by unknown oracle function f, so that f(x')=f(x) if x'=x⊕s

indirectly used in QFT and Shor

$2^N \Rightarrow N$

exponential speed gain

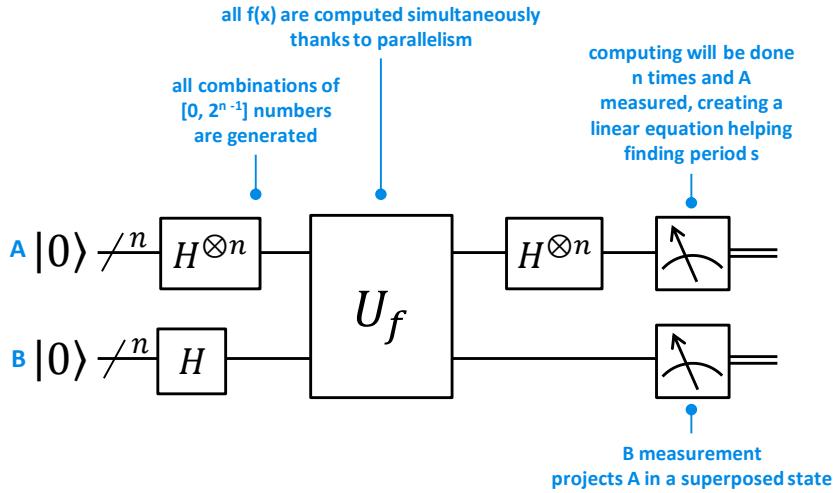


Figure 568: Simon algorithm. (cc) Olivier Ezratty with various sources.

The other best-known algorithm in this category is **Grover**'s algorithm, created in 1996 by Lov Grover. It allows to perform a fast quantum search in a database. It's however more generic: it can find an item in a long list that matches some specific criteria specified by an oracle function like finding the minimum item of an unsorted list of N integers, determining if a graph of N vertices is connected, or doing pattern matching searches, which can be useful in genomics.

The Grover oracle function is supposed to return 1 only for one combination of 0 and 1 with N bits. It also uses qubit state superposition to speed up processing compared to a traditional sequential search in an unsorted and non-indexed database. The performance improvement is significant compared to an unsorted database, except that in real life, we usually use indexed databases!

The question is to know if a 1 is yielded once and to which input combining 0 and 1s it corresponds. To do this, again with Hadamard gates, the algorithm will gradually amplify the combination of qubits

[1569] It is documented in On the power of quantum computation by Daniel Simon, 1997 (10 pages).

of the result to an amplitude approaching 1 and make the other combinations of qubits converge to 0. This amplification operation is nicknamed the "global diffusion operator" and is repeated $\sqrt{N}$ times, N being the number of qubits. It explains why Grover's algorithm has only a quadratic speedup.

It will then be possible to measure the result and obtain the combination of qubits with the desired value (still, with repeating the algorithm several times and making an average of the results). This is well explained in Figure 569.

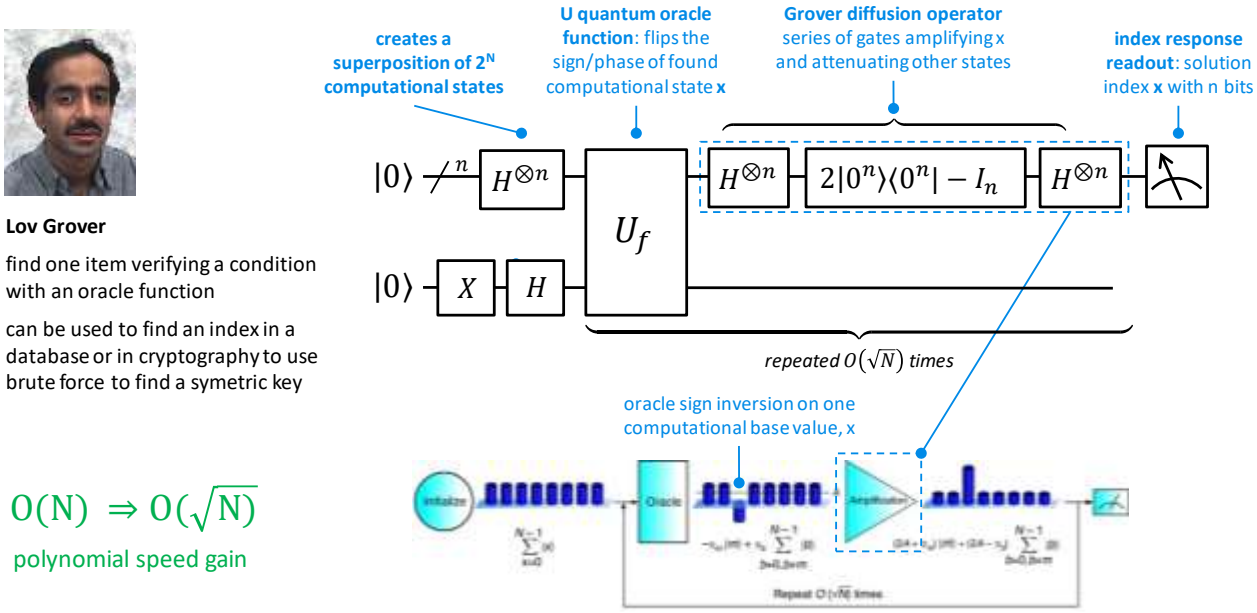


Figure 569: Grover algorithm. (cc) Olivier Ezratty with various sources. And "Quantum Computing Explained for Classical Computing Engineers" by Doug Finke, 2017 (55 slides), broken link.

The computing time is proportional to the square root of the base size and the storage space required is proportional to the logarithm of the base size. A classical algorithm has a computation time proportional to the size of the base. Going from a time N to √N is therefore an interesting gain, but it will not transform an exponential size problem into a polynomial size problem (2^N to N power M).

On the other hand, this algorithm can be exploited to be integrated into other algorithms such as those that allow the discovery of the optimal path in a graph or the minimum or maximum number of a series of N numbers. Grover's algorithm is also used in some quantum machine learning algorithms like for measuring min/max/mean distances or other metrics between sets of data points and for automatic clustering. The settings are in the oracle, that encodes a constraint function or a function cost for which we are searching a minimum.

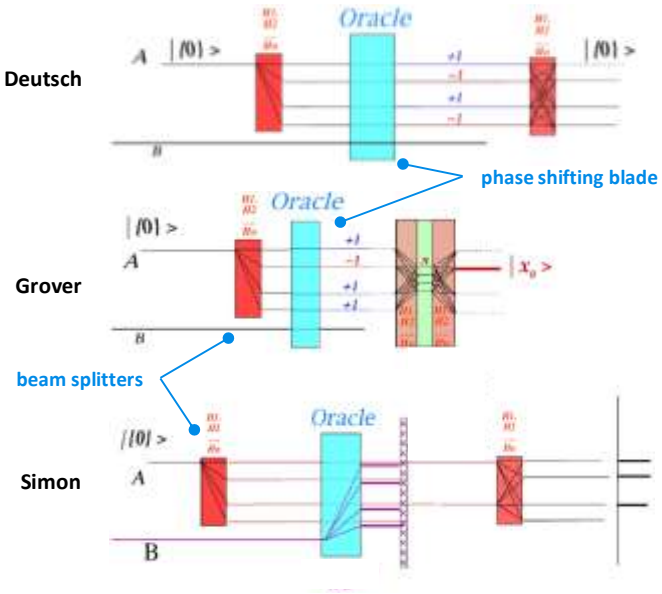
Note that Grover's search algorithm requires the use of quantum memory (qRAM) to "load" the related database in memory, in the oracle function[1570]! There are however some available optimization techniques available for quantum state preparation in the Grover oracle that could remove this qRAM requirement[1571].

In a 2002 lesson, **Serge Haroche** points out the known fact that these search algorithms have quantum optical interference equivalent implementations, as described in Figure 570 with 4 qubits. This has been described for a while, even trying to use only classical optical elements.

[1570] This is notably documented in Quantum algorithms for linear algebra by Anupam Prakash, 2015 (92 slides).

[1571] See Black-box quantum state preparation without arithmetic by Yuval R. Sanders et al, UNSW and Microsoft Research, 2018 (5 pages).

Various papers argue that, from a practical standpoint, these implementations don't scale well with a growing number of qubits, but they remind us that quantum algorithms are toying with waves and interferences and that optical analogies are well suited to understand their underlying processes[1572].



Deutsch algorithm can be described as a quantum interference process using 2^n paths: the Hadamard gates H_1 to H_n play the role of beam splitters decomposing and recomposing the states of register A. Oracle O is an analog to a phase shifting blade that modifies the relative phase of superposed states in A.

Grover algorithm optical equivalent would combine two beam splitters with a phase shifting blade. In both Deutsch and Grover, the sought-after effect is to favor in the final state a state analog to a shiny interference fringe.

Simon algorithm uses entanglement and projective measurement. The oracle creates some entanglement betwen input registers A and B, then measurement of B projects A in a superposition of two states. Then, after a mix in the beam splitter, the final interference signature provides an information on the separation between these two states, then on the searched period.

from: Serge Haroche, Chaire de Physique quantique. Année 2001-2002. 8 ème leçon. 26 Février 2002. Les algorithmes quantiques.

Figure 570: quantum algorithms explained with interferences when implemented with quantum optics, by Serge Haroche.

At last, let's remind again the reader that an oracle-based algorithm is efficient if the oracle itself is efficient, which depends on its implementation. If it is accessing some classical data or function, the algorithm's efficiency may be questionable in the end.

Shor integer factoring

Shor's factoring allows you to decompose integers into prime numbers much faster than with a traditional computer. It works in two stages as described in the diagram below in Figure 571 [1573]:

- A **classical part** which reduces the factoring problem to and order-finding problem and produces a function f(x) implemented as a unitary in the quantum part of the algorithm.
- A **quantum part** itself made of three sub-stages with a set of Hadamard gates, repeated squaring for a modular exponentiation transformation (which could be replaced by a QFT), and an inverse QFT that extracts the solution using the periods found in the classical part. The QFT is responsible for the exponential speedup of Shor's factoring algorithm.

The gain in speed generated by Shor's algorithm compared to conventional calculation? The computation time goes from N*log(N) for the best simple Fourier transforms to $\log_2(N)$ for the QFT. We thus go from a linear order of magnitude to a logarithmic order of magnitude. But the state of the art of classical integers factoring is much better than the usual $O(\sqrt{N}/2)$ pointed out in textbooks, like:

$$\exp((1.923 + o(1))(\log N)^{1/3}(\log \log N)^{2/3})$$

[1572] See Grover's search algorithm: An optical approach by P. G. Kwiat et al, 1999 (6 pages), Implementation of quantum search algorithm using classical Fourier optics by N. Bhattacharya and al, 2002 (4 pages) and Classical wave-optics analogy of quantum information processing by Robert J. C. Spreeuw, 2001 (9 pages).

[1573] See On Shor's algorithms, the various derivatives, their implementation and their applications by Martin Ekera, 2019 (135 slides) which describes in detail how Shor's algorithm works.

One of the first implementations of Shor's algorithm took place in 2001 at IBM with an experimental quantum computer of 7 qubits, to factorize the number 15. Since then, we have just moved to a 5-digit number, 56153[1574], but with a different factoring algorithm than Shor's algorithm. It is in fact an optimization algorithm that was running on a D-Wave quantum annealer! A record was reached in 2016 with the factorization of 200,099 with 897 qubits on a D-Wave but with yet another algorithm than Peter Shor's[1575].

It is important to remember that Shor's algorithm theoretically allows to break the public keys of the RSA cryptography that is commonly used in Internet security. Public keys work by sending a very long integer number to a recipient who already has its divisor.

He just has to divide the large number received by his divisor to retrieve the other divisor and use it to decipher the encrypted message. Whoever does not have the divisor cannot exploit the complete key unless he has enormous traditional computing power to find his divisors.

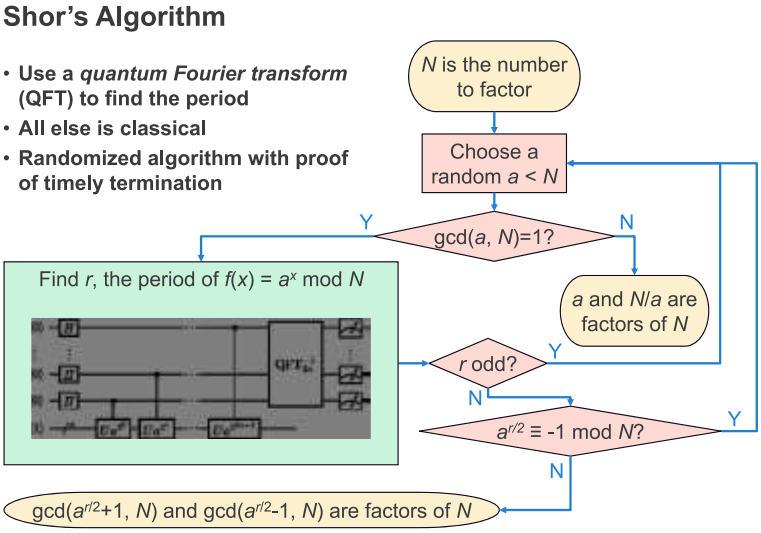


Figure 571: Shor's algorithm high-level components. Source: Quantum Annealing by Scott Pakin, NSF/DOE Quantum Science Summer School June 2017 (59 slides).

Until now, only NSA supercomputers have officially been able to break reasonably sized keys in the 256 to 800 bits range. But at 1024 bits and beyond, the task is inaccessible in a reasonable amount of time for these supercomputers. As far as we know!

In theory, this would become accessible someday to scalable quantum computers. To break a good 2048-bit RSA public key, one will still have to be patient because it requires to create quantum computers with a very large number of corrected qubits. It takes about twice as many logical qubits as there are bits in an RSA key. To factorize a 2048-bit RSA key, a minimum of 4098 logical qubits are required[1576]. Because of qubit noise, it is estimated that hundreds to tens of thousands of physical qubits per logical qubit would be needed.

Thus, such a RSA key break would require about 20 million qubits according to a famous Google algorithm from 2019. This algorithm based on a distance-27 surface code with about 10,000 logical qubits would require a bandwidth of 7.3 TBit/s per logical qubit for error processing[1577]. Another option would be to use some addressable quantum memory and reduce the qubits count to 13436[1578].

[1574] This is documented in Quantum factorization of 56153 with only 4 qubits, 2014 (6 pages).

[1575] The record was beaten in 2019, it was beaten by engineers from Zapata Computing and IBM with the factoring of 1,099,551,473,989 into 1,048,589 * 1,048,601, but using a variational hybrid algorithm on a few qubits, and with an undocumented speedup. See Analyzing the Performance of Variational Quantum Factoring on a Superconducting Quantum Processor by Amir H. Karamlou et al, 2019 (14 pages).

[1576] The formula is 2xN+2 qubits. See Factoring using 2n + 2 qubits with Toffoli based modular multiplication by Thomas Haner et al, 2017 (12 pages) and Circuit for Shor's algorithm using 2n+3 qubits by Stephane Beauregard, 2013 (14 pages).

[1577] See Hierarchical decoding to reduce hardware requirements for quantum computing by Nicolas Delfosse, January 2020 (8 pages).

[1578] See Factoring 2048 RSA integers in 177 days with 13436 qubits and a multimode memory by Élie Gouzien and Nicolas Sangouard, March 2021 (18 pages). It requires some quantum memory of 2 hours storage time and qubits with a 10^{-3} error rate. The authors suggest realizing such an architecture with a microwave interface between a superconducting qubits processor and some multiplexed addressable quantum memory using the principle of photon echo in solids doped with rare-earth ions like Erbium or NV centers. Their physical qubits would use some 3D gauge color error correction codes.

factors an integer in prime numbers

algorithm relies on a period funding algorithm and an inverse quantum Fourier transform

breaking RSA 2048 bits key requires 20 millions qubits with an error rate of 0.1% and 8 compute hours.

$$O(\frac{\sqrt{N}}{2}) \Rightarrow O(\log(N)^3)$$

exponential speed gain

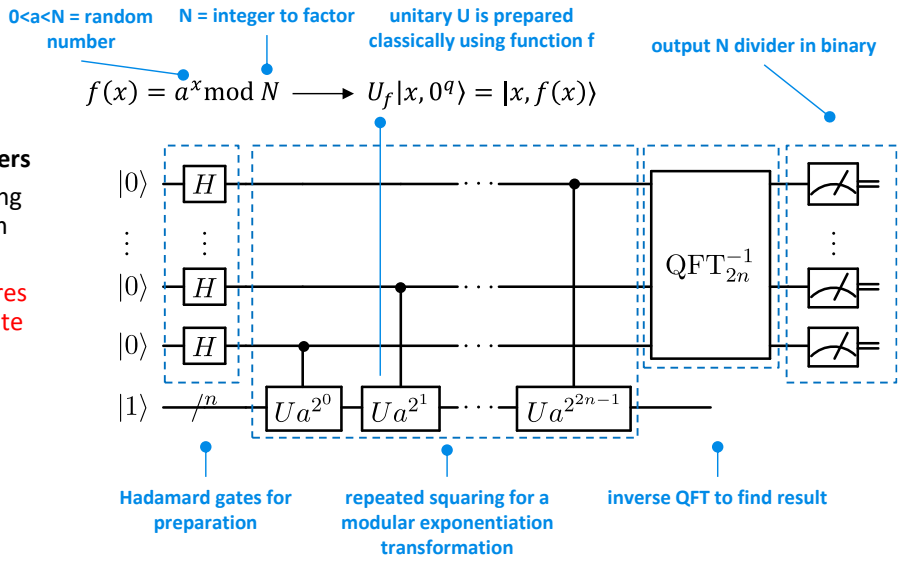


Figure 572: Shor's algorithm with all its qubits. Source: Wikipedia description of Shor's factoring algorithm.

Yet, another option would be to rely on qubits like cat-qubits for which the physical/logical qubits ratio would be much lower, in the 10-100 range.

Note that Shor's algorithm also allows to break cryptography using elliptic curves, which competes with RSA cryptography. By the way, some of the cryptography used in the Bitcoin protocol would also be broken by Shor integer factoring, which we will see later in this document, page 807.

In any case, Shor's algorithm has been terrorizing security specialists for a couple decades. This explains the interest in exploiting quantum keys distribution, which are supposed to be tamper-proof because their interception can be detected by their legitimate recipient, as well as post quantum cryptography, consisting in classical cryptographic algorithms and methods to make them (theoretically) tamper-proof by quantum computers using Shor's or any other algorithm.

But Shor's factoring is not the only quantum factoring algorithm created so far. Several other options are investigated like the **Variational Quantum Factoring** algorithm alternative that maps the factoring problem to the ground state of an Ising Hamiltonian that could be solved in a hybrid manner using the quantum approximate optimization algorithm (QAOA), running on a gates-based NISQ processor[1579]. But so far, the scalability of this algorithm with a large number of qubits and integer numbers is not proved.

Shor dlog

Peter Shor did create his quantum dlog (*aka* discrete logarithm) algorithm simultaneously with his factoring algorithm in 1994 and solves another classically intractable problem. The discrete logarithm $k=\log_b(a)$ (or logarithm of a in base b) is an integer k such that $b^k = a$, where a and b are given integer numbers. You understand that this problem is intractable with digging in group isomorphisms logic, which I won't cover.

The dlog algorithm can help break Diffie-Hellman signatures, including those using elliptic curves.

Integer factoring and finding a dlog are both special cases of the hidden subgroup problem for finite Abelian groups (as seen just below).

[1579] See Variational Quantum Factoring by Eric R. Anschuetz, Alán Aspuru-Guzik et al, 2018 (18 pages).

Hidden subgroup problems

The hidden subgroup problem is a generic problem which encompasses Shor's order finding, Simon's, the discrete log and the graph isomorphism problems. The definition of this problem is the following: let G be a group and H⊆G one of its subgroup. Let S be any set and f: G→S a function that distinguishes cosets of H, meaning that for all g_1 and g_2 in G, $f(g_1)=f(g_2)$ means $g_1H=g_2H$ (left cosets of H are equal). The hidden subgroup problem (HSP) is about determining the subgroup H using calls to function f with any combinations of g's in G.

Verstanden? Well, not really if you have no idea what's a group, a subgroup, a set and a coset. So let's define these:

- **Set**: arbitrary ensemble of elements.
- **Subset**: ensemble of some elements from a set.
- **Group**: a set coupled with an operation on the elements in the set, where any combination of two elements with this operation gives another item from the group. One example is the group ℤ of all integers associated with the addition. Any addition of integers yields an integer. A group also has an identity element (0 for integers) and all elements have an inverse element (inverse of integer a is -a). Operations are also associative: the order in which the operation is done is not important. For example, with integers: a+(b+c)=(a+b)+c.
- **Subgroup**: subset of the group G being also a group with regards to its associated operation. For example, with integers, the even set is a subgroup with addition since adding even numbers always give even numbers. It's however not true with uneven numbers given adding two uneven numbers gives an even number.
- **Coset**: set or ensemble of elements from G that contains all elements of H multiplied by a given item g from G. If you multiply all elements of H on the left by one element g of G, the set of products is a left coset. If multiplied by the right, it's a right coset (these operations may be non-commutative with some non-integer elements like matrices). A subgroup H of a group G may be used to decompose G into disjoint equal-size cosets. H cosets have the same number of elements as H.

Another definition of the hidden subgroup problem is: given a function f that is constant with all cosets of some subgroup H, find the subgroup H.

In its quantum version, the function f is usually implemented as an oracle. Solving HSP takes an exponential time classically with the size of log(|G|) whereas it can be solved efficiently for certain types of groups with quantum versions if done in a polynomial time of log(|G|), given log(|G|) is the logarithm of the number of elements in the group G[1580].

There are HSPs for Abelian and non-abelian groups given a group G is Abelian if xy = yx for all x, y in G. There is actually not a single quantum HSP algorithm but many of these that are applicable to different classes of groups and subgroups. It's a whole specialized field in itself.

One famous HSP problem is Pell's equation, a quadratic Diophantine equation of the form $x^2 - ny^2 = 1$ with n being a positive nonsquare integer, and x, y being integer solutions to the equation. A quantum algorithm to Pell's equation was created by **Sean Hallgren** at Princeton in 2002. It is based on a QFT[1581]. It has the particularity to be applied to an infinite group given we don't know in advance what are the bounds for x and y.

[1580] See a good overview of various HSP algorithms in The Hidden Subgroup Problem Master's Project by Frédéric Wang, 2010 (99 pages).

[1581] See Polynomial-Time Quantum Algorithms for Pell's Equation and the Principal Ideal Problem by Sean Hallgren, 2006 (21 pages).

Is solving that equation useful? It may be for some cryptographic purposes. The Hallgren algorithm finds one solution to the Pell equation, who has many. It has a (roughly) polynomial time vs an exponential time for its classical version, so we're in for some exponential speedup.

Fluid mechanics

Fluid mechanics simulations are mostly based on solving Navier-Stokes equations. These are nonlinear partial differential equations, whose solution is essential to the aerospace industry, weather forecasting, plasma magneto-hydrodynamics and astrophysics. The problem with Navier-Stokes is nonlinear and quantum computing is implementing linear algebra. But there are some tricks available to turn nonlinear equations into linear ones.

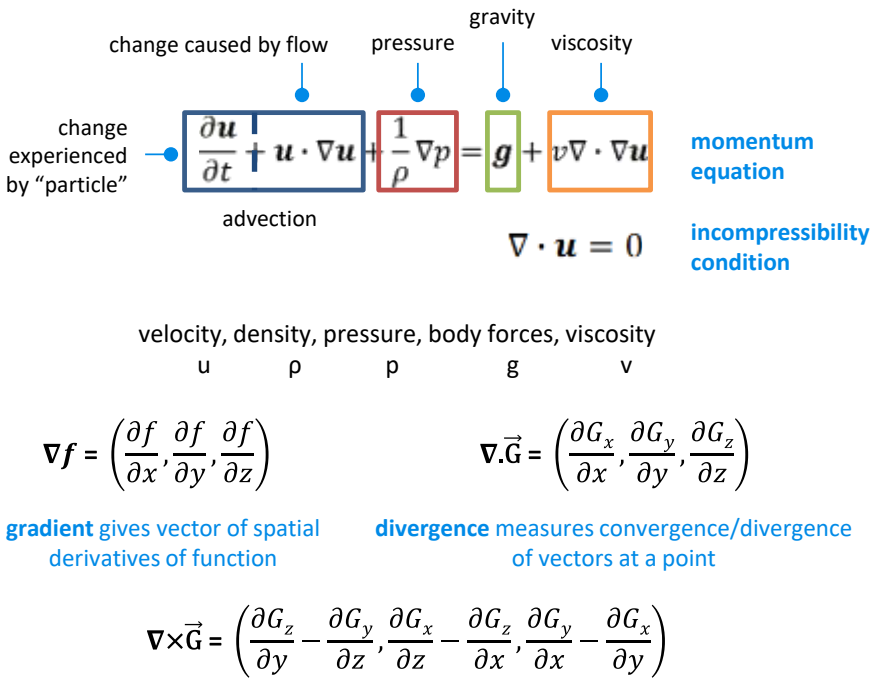


Figure 573: Navier-Stoke equation explained. (cc) Olivier Ezratty with various sources.

Various quantum algorithms have been designed to solve Navier-Stokes equations:

- **Hybrid computing** which makes use of a quantum nonlinear processing unit (QNPU) that is a unitary transformation implementing nonlinear operations[1582].
- **Continuous variable qubits** which implements nonlinearities with using multiple copies of the vector representing the state of the system to be investigated[1583]. Polynomial values are obtained with creating tensor products of all or part of these multiple copies of the vector state. It can simulate the dynamics of the nonlinear Schrödinger equation with quantum linear differential equation solvers.
- **Differentiable quantum circuits** to solve differential equations[1584].

[1582] See Variational quantum algorithms for nonlinear problems by Michael Lubasch et al, 2019 (15 pages).

[1583] See Quantum algorithm for nonlinear differential equations by Seth Lloyd et al, 2020 (17 pages).

[1584] See Solving nonlinear differential equations with differentiable quantum circuits by Oleksandr Kyriienko et al, 2020 (22 pages)

- **Converting a nonlinear system into a linear one** with transforming nonlinear problems into an array of linear equations[1585].
- **Quantum annealing for laminar plane channel flow problem** with a solution using a D-Wave quantum annealer[1586].

Worth mentioning, **Vorticity** (2001, USA) is developing custom (classical) DSA (domain specific accelerators) to solve Navier-Stokes equations with a 10^5 speed gain over classical methods. They don't provide any technical information on their technology (FPGA, ASIC?).

Quantum walks

Quantum walks are yet another weird beast of the quantum protocols zoo, based on sophisticated mathematical grounds. All in all, quantum walks are search algorithms in graphs. The concept was introduced in 1993 by Yakir Aharonov et al[1587]. They have many applications like searching a triangle in a graph or even Hamiltonian simulations[1588].

Andrew Childs demonstrated that quantum walks can be viewed as a universal quantum programming primitive, showing that an arbitrary set of qubit gates could be reduced to solving a quantum walk, which could be interesting with quantum systems implementing quantum walks at the hardware level one with photonic settings or even superconducting qubits[1589].

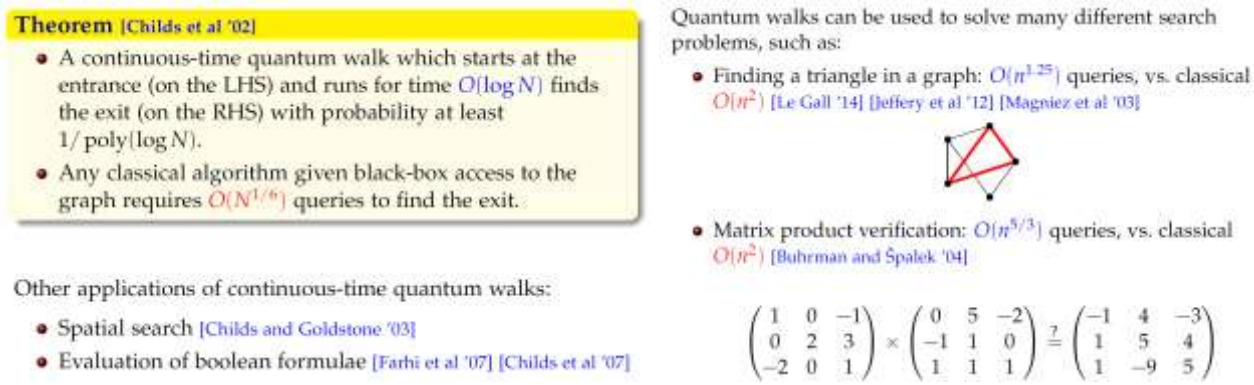


Figure 574: quantum walks and their applications.

That was the case with a 62 qubits system presented in China in 2021 that was dedicated to implementing a random quantum walk. The project was driven by Jian-Wei Pan. The processor is based on a 8x8 matrix of transmon superconducting qubits. It simulates a Mach-Zehnder interferometer. The matrix uses a nearest-neighbor connectivity like with Google Sycamore. Like Google's processor, two qubits were malfunctioning and disactivated, thus we have 62 instead of 64 qubits plus a non-functioning coupler. It runs at 10 mK and used 186 control lines, including 16 readout output lines with lines shared by 4 qubits[1590]. Quantum walks can also be implemented with photon qubits[1591].

[1585] See Efficient quantum algorithm for dissipative nonlinear differential equations by Jin-Peng Liu, Andrew M. Childs et al, March 2021 (36 pages) and New Quantum Algorithms Finally Crack Nonlinear Equations by Max G Levy, Quanta Magazine, January 2021.

[1586] See Towards Solving the Navier-Stokes Equation on Quantum Computers by N. Ray et al, April 2019 (16 pages).

[1587] See Quantum random walks by Yakir Aharonov (father of Dorit Aharonov), L. Davidovich and N. Zagury, 1993 (4 pages). See also this overview in Quantum walks by Martin Štefanák, 2020 (44 slides).

[1588] See On the relationship between continuous- and discrete-time quantum walk by Andrew M. Childs, 2008 (22 pages).

[1589] See Universal computation by quantum walk by Andrew M. Childs, 2008 (9 pages).

[1590] See Quantum walks on a programmable two-dimensional 62-qubit superconducting processor by Ming Gong et al, 2021 (18 pages).

[1591] See Two-dimensional quantum walks of correlated photons by Zhi-Qiang Jiao et al, 2021 (22 pages).

In classical computer science, random walk or Markov chain are a algorithmic tools applied to search and sampling problems. Their quantum walks equivalent provide a framework for creating fast quantum algorithms. Quantum walks are based on the simulated coherent quantum evolution of a particle moving on a graph. Quantum walk algorithms use faster hitting (the time it takes to find a target vertex from a source vertex) and faster mixing (the time it takes to spread-out over all vertices after starting from one source vertex) [1592]. The quantum time gain can be exponential for hitting and quadratic for mixing. Since quantum walks are efficient ways to evaluate Boolean formulae, it can be used to solve satisfaction problems (MaxCut, SAT, 3-SAT).

In gate-based systems, quantum walks can be solved using a Grover search with an oracle function using an adjacency matrix for the searched walk. It can help find the shortest path in a graph (we're back at the traveling salesperson's problem), finding if a graph is bipartite (with all edges in one vertex connected to the edges in the other), finding subgraphs such as a triangle and solving maximal clique problems (used for example in social networks to find groups of people who know each other).

Then, you have quantum random walks that help reduce quantum walks query complexity to search and find graph properties, with the discrete time and continuous time variations[1593]. These are equivalent of the famous Galton's board.

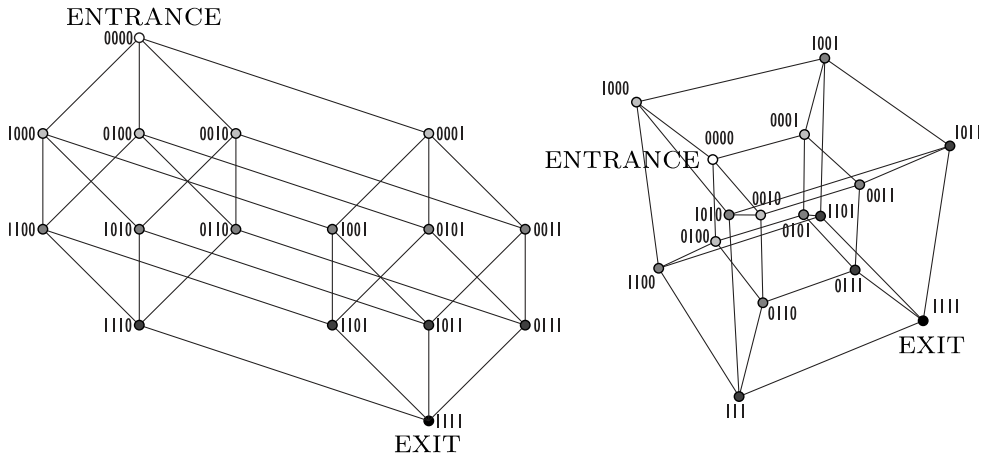


Figure 575: Source: Quantum Walks by Daniel Reitzner, Daniel Nagaj and Vladimir Buzek, 2012 (124 pages), page 13

On top of Andrew M. Childs, let's mention three great contributors to the quantum walk domain: **Stacey Jeffery**[1594], **Julia Kempe** and **Frédéric Magniez**.

Quantum machine learning

What if quantum computing could accelerate machine learning and deep learning training and inferences? This is one of its potential domains of applications, but it is not that obvious. First, quantum computing does not seem to enable machine learning tasks that are impossible to implement with classical computing, including the many specialized hardware (tensors processing units, spiking neurons).

Second, their benefits are still hard to evaluate, particularly given all quantum machine learning are hybrid in nature.

[1592] I'm summarizing here the quantum walks description from Quantum algorithms an overview by Ashley Montanaro 2015 (16 pages).

[1593] See Quantum Algorithm Implementations for Beginners by Abhijith J. et al, 2020 (98 pages) provides many references related to quantum walks and quantum random walks algorithms.

[1594] See her thesis: Frameworks for Quantum Algorithms by Stacey Jeffery, 2014 (166 pages) and a lot of subsequent work in quantum walks algorithms.

In many cases, benchmarks tend to favor a comparison in the quality of the results like minimizing an error function and error rates more than proving a quantum speedup[1595].

Various quantum algorithms have been created in the last decades that cover the field of classical machine learning and with some variations in neural networks and deep learning[1596]. Many are based on linear algebra algorithms like the foundational HHL algorithm.

The literature on QML defines four models that connect how the data is fed into the model (classically, quantumly) and how the process is handled (classically or at least partially quantumly) as described in Figure 576 [1597]:

CC with classical data that are processed by classical algorithms. This is classical machine learning.

CQ with classical data that is encoded in quantum states and processed by quantum algorithms, which may need the use of a quantum RAM (qRAM). This is the most common method in NISQ systems.

QC with quantum data that is converted in a classical form and processed by classical algorithms, a solution implemented to analyze quantum physics and sensors measurement statistics, like for doing a qubit tomography.

QQ with quantum data that is processed by quantum algorithms which could be implemented with feeding a QML algorithm directly with quantum data coming from a quantum sensor.

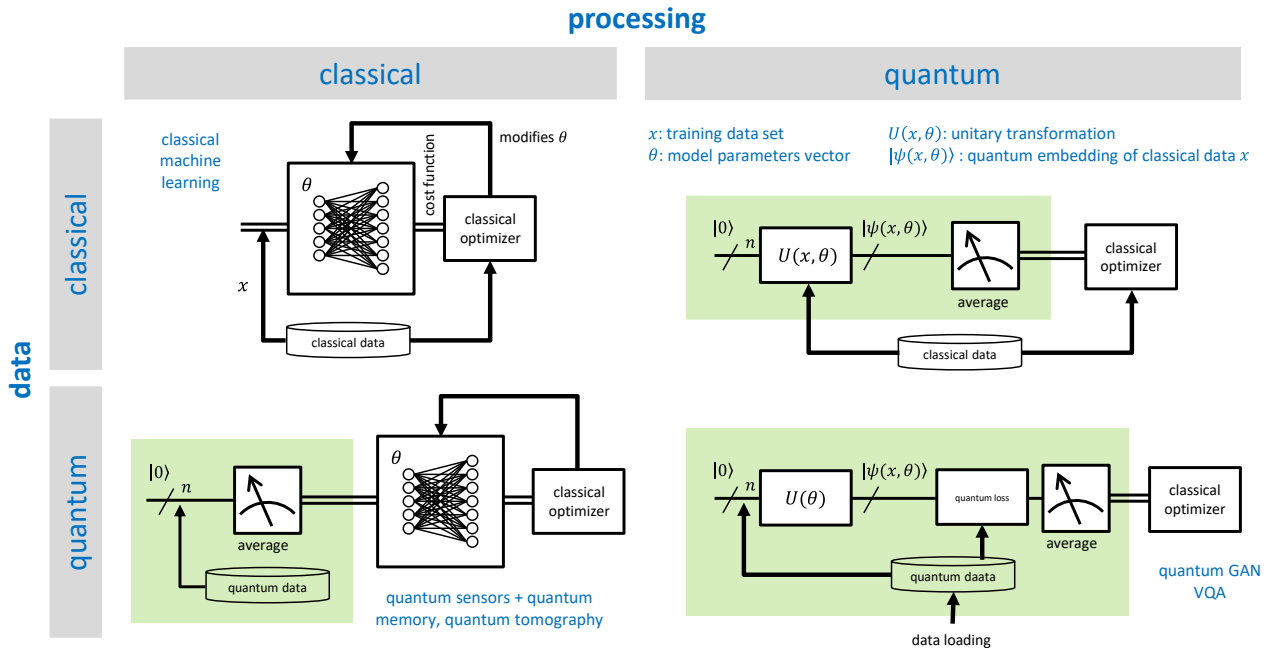


Figure 576: the four main types of QML depending on whether data loading is classical or quantum and part of the processing is classical or quantum. Source: schema inspired by An Introduction to Quantum Machine Learning for Engineers by Osvaldo Simeone, July 2022 (229 pages).

[1595] See Is quantum advantage the right goal for quantum machine learning? by Maria Schuld and Nathan Killoran, March 2022 (10 pages) and Why measuring performance is our biggest blind spot in quantum machine learning by Maria Schuld, Xanadu, March 2022, which provides an interesting perspective on why QML is not an obvious near-term candidate for some quantum advantage vs classical methods. And Quantum machine learning: a classical perspective by Ciliberto et al, 2020 (26 pages). It concludes with: "*Despite a number of promising results, the theoretical evidence presented in the current literature does not yet allow us to conclude that quantum techniques can obtain an exponential advantage in a realistic learning setting*".

[1596] See Machine Learning in the Quantum Era - Machine Learning unlocks the potential of emerging quantum computers by Loïc Henriet (Pasqal), Christophe Jurczak (Quantonation) and Leonard Wossnig (Rahko), November 2019. It highlights the potential of cold atom-based qubits for QML.

[1597] See An Introduction to Quantum Machine Learning for Engineers by Osvaldo Simeone, July 2022 (229 pages).

QML makes use of PQC, aka **parametrized quantum circuits** or parametric quantum circuits (not to be confused with post-quantum cryptography)[1598]. These are also labelled as "ansatz". These circuits contain rotation gates that contain the parameters of the problem to encode. A PQC model is usually defined by a classical optimizer. There are several types of data preparation ansatzes: with only single-qubit gates ("mean field ansatz") which require only N gates for N qubits and is simple and fast, then "hardware efficient ansatz" that also use a fixed number of entangling gates and then parametrized 2-qubit gates that are entirely tailored for the problem. These three models are presented below in Figure 577[1599].

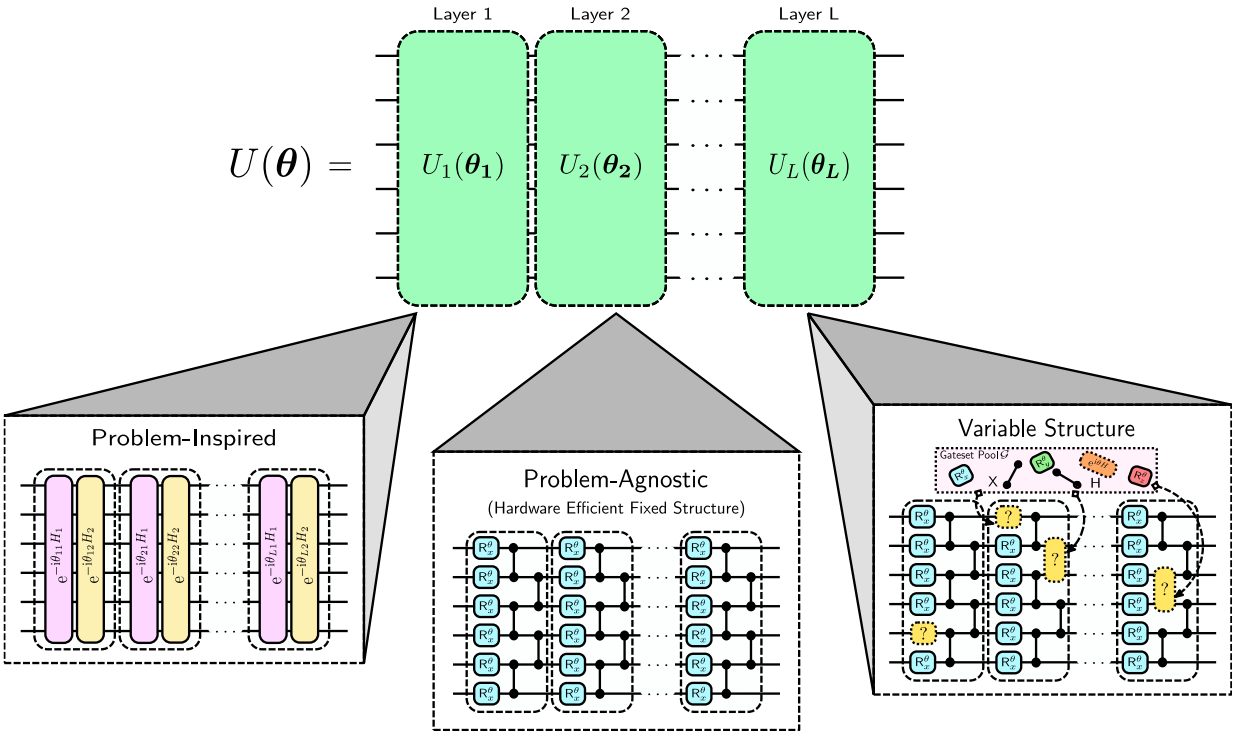


Figure 577: various ways of preparing a QML ansatz or model, problem inspired, problem agnostic and with a variable structure. Source: Machine learning applications for noisy intermediate-scale quantum computers by Brian Coyle, University of Edinburgh, May 2022 (263 pages).

Generically, QML algorithms from the CQ category rely on **variational circuits**, a family of hybrid algorithms that combine a quantum algorithm and a traditional algorithm that drives the latter[1600]. VQE and VQA are some of them[1601]. It allows finding global minimums. These algorithms are adapted to NISQ QPUs but their true quantum acceleration is not proven yet.

These algorithms are characterized by a cost function defining the problem, the quantum ansatz, how is the cost function optimized, the data encoded as the input to the VQA and the desired output.

[1598] See the review paper on PQCs Parameterized quantum circuits as machine learning by Parameterized quantum circuits as machine learning models by Marcello Benedetti, Erika Lloyd, Stefan Sack and Mattia Fiorentini, Quantum Science and Technology, 2019 (18 pages).

[1599] See the thesis Machine learning applications for noisy intermediate-scale quantum computers by Brian Coyle, University of Edinburgh, May 2022 (263 pages), done under the supervision of Elham Kashefi.

[1600] See Universal Variational Quantum Computation by Jacob Biamonte, 2019 (5 pages).

[1601] See Accelerated Variational Quantum Eigensolver by Daochen Wang, Oscar Higgott, and Stephen Brierley, 2019 (11 pages) which proposes a machine learning method to reduce the depth of the quantum circuits used (number of quantum gates to be executed). See also Quantum advantage with shallow circuits by Robert König et al, 2018 (97 slides). This list of quantum machine learning algorithms can be found in Quantum Machine Learning What Quantum Computing Means to Data Mining by Peter Wittek, 2014 (178 pages).

The breadth of QML algorithms is vast, covering all categories of classical machine learning and deep learning with supervised machine learning (to classify items or make predictions on time series), unsupervised machine learning (for automatic clustering), up to all sorts of neural networks (convolutional networks, recurrent networks, generative networks):

- Hybrid **quantum nonlinear regression** algorithm, one of the basic quantitative value prediction methods of the learning machine[1602].
- **SVM** (Support Vector Machine), a traditional method of segmentation that often relies on matrix inversions, based on its use of HHL[1603]. It can be used for text sentiment analysis.
- **PCA** (Principal Component Analysis) is used to determine the key variables in a data set[1604]. This is similar to searching for eigenvectors of a data set. Again, HHL is behind it.
- **Recommendation** systems useful in marketing or content[1605].
- **Gradient descent** used during training phase of neural network[1606].
- Unsupervised learning algorithm for **automatic data clustering**[1607].

Now onto deep learning algorithms:

- The implementation of **Perceptrons** which is the original neural network architecture designed by Franck Rosenblatt in 1957[1608].
- Quantum **convolutional neural networks**, still modest in size for the moment[1609]. These are now named **Quanvolutional Neural Network** algorithms[1610].

[1602] See Nonlinear regression based on a hybrid quantum computer, 2018 (7 pages), from researchers in several laboratories in China.

[1603] See Support Vector Machines on Noisy Intermediate-Scale Quantum Computers by Jiaying Yang, 2019 (79 pages) which discusses the use of SVM on NISQ computers, Quantum Machine Learning with Support Vector Machines by Anisha Musti, April 2020 and a practical example with Quantum support vector machines for aerodynamic classification by Xi-Jun Yuan et al, August 2022 (12 pages).

[1604] See Quantum principal component analysis by Seth Lloyd, Masoud Mohseni and Patrick Rebentrost, from MIT and Google, July 2013 (9 pages) which lays the groundwork on the matter.

[1605] See Quantum Recommendation Systems by Iordanis Kerenidis and Anupam Prakash, 2016 (22 pages, and video) is a proposed quantum machine learning algorithm for recommendation. The quantum algorithm of Iordanis Kerenidis had been challenged by a classical algorithm proposal by Ewin Tang in 2018. She "dequantized" Kerenidis's algorithm, meaning, she found a classical efficient equivalent. But Iordanis pointed out that with certain recommendation parameters, the quantum algorithm was still clearly superior. Always, as long as a machine is there to execute it. Both these algorithms are investigated in Exponential Advantages in Quantum Machine Learning through Feature Mapping by Andrew Nader et al, December 2020 (16 pages).

[1606] See Quantum algorithms for feedforward neural networks by Jonathan Allcock, Iordanis Kerenedis et al, 2018 (18 pages) and Quantum Circuit Parameters Learning with Gradient Descent Using Backpropagation by M Watabe et al, 2020 (15 pages).

[1607] See Quantum spectral clustering by Iordanis Kerenidis and Jonas Landman, April 2021 (20 pages). The method named spectral clustering consists in building a similarity graph with using distances between data vectors, extracting the eigenvectors from a matrix built with this graph and projecting the data onto this new orthogonal space and applying a classical k-means clustering method. But as seen frequently with QML algorithms, the best acceleration requires using some qRAM.

[1608] See An Artificial Neuron Implemented on an Actual Quantum Processor by Francesco Tacchino et al, 2018 (8 pages).

[1609] See Quantum Convolutional Neural Networks by Iris Cong et al, May 2019 (12 pages), Quantum Neurons: analyzing the building blocks of quantum deep learning algorithms by Zachary Cetinic et al, December 2019 (12 pages) and Quantum Algorithms for Deep Convolutional Neural Networks by Iordanis Kerenidis, Jonas Landman and Anupam Prakash, 2019 (31 pages). Also, Advances in Quantum Deep Learning: An Overview by Siddhant Garg and Goutham Ramakrishnan, May 2020 (17 pages) is focused on quantum neural networks including quantum convolutional neural networks and contains a good introduction to classical neural networks. And Realizing quantum convolutional neural networks on a superconducting quantum processor to recognize quantum phases by Johannes Herrmann et al, Nature Communications, 2022 (7 pages) which implements a QCNN algorithm on a 7-qubit QPU from IBM for a narrow problem (recognizing quantum phases) with some superiority in the results quality (and of course, not with a speedup given the low number of qubits).

[1610] See Predict better with less training data using a QNN by Barry D. Reese, Marek Kowalik, Christian Metzl, Christian Bauckhage, and Eldar Sultanow, Capgemini, June 2022 (23 pages).

They seem to have the advantage of avoiding the ill-fated barren plateaus that make it difficult to converge a network[1611]. Variations of QCNN algorithms also exist for D-Wave quantum annealers[1612].

- Quantum **graph neural networks** have many applications, particularly in chemistry and biology[1613].
- **Feature mapping** in deep learning and convolutional neural networks, to detect patterns efficiently[1614].
- **Recurrent Neural Networks** used for MNIST handwriting recognition, an existing common task for classical OCR (optical character recognition)[1615].
- **Equivariant Neural Networks** (ENN) with better geometrical robustness and a better resistance to adversarial attacks[1616].
- **Generative Machine Learning** models, including the models based on so-called quantum circuit Born machines (QCBM). It can be used to create (quantumly generated) synthetic training data sets used in classical machine learning models[1617].
- **Quantum Generative Adversarial Networks** (qGAN) algorithms that generate synthetic content from existing content by checking its plausibility via a network of recognition neurons[1618].

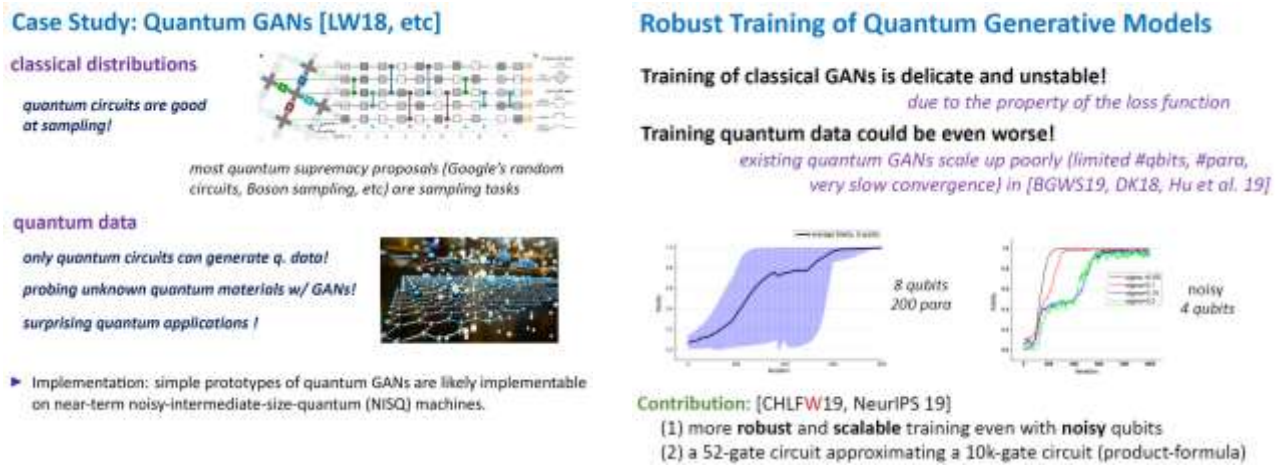


Figure 578: quantum generative neural networks. Source TBD.

[1611] See Absence of Barren Plateaus in Quantum Convolutional Neural Networks by Arthur Pesah et al, PRX, DoE Los Alamos Lab and UCL, November 2021 (26 pages).

[1612] See Adiabatic Quantum Computation Applied to Deep Learning Networks by Jeremy Liu et al, May 2018 (28 pages).

[1613] See Quantum Graph Neural Networks by Guillaume Verdon et al, 2019 (10 pages).

[1614] See Supervised learning with quantum enhanced feature spaces by Aram Harrow et al, 2018 (22 pages) which describes the use of quantum to detect complex shapes, far beyond what convolutional neural networks ("feature mapping") can do.

[1615] See Recurrent Quantum Neural Networks by Johannes Bausch (12 pages) and Quantum reservoir computing using arrays of Rydberg atoms by Rodrigo Araiza Bravo et al, Harvard and IBM Research, November 2021-July 2022 (10 pages).

[1616] See Introduction to Robust Machine Learning with Geometric Methods for Defense Applications by Pierre-Yves Lagrave and Frédéric Barbaresco, Thales, July 2021 (9 pages)

[1617] See Quantum versus Classical Generative Modelling in Finance by Brian Coyle, Elham Kashefi et al, August 2020 (17 pages) and The Born Supremacy: Quantum Advantage and Training of an Ising Born Machine by Brian Coyle, Daniel Mills, Vincent Danos and Elham Kashefi, April 2021 (47 pages).

[1618] This is well documented in Quantum generative adversarial learning by Seth Lloyd and Christian Weedbrook, 2018 (5 pages), Quantum generative adversarial learning in a superconducting quantum circuit, 2018 (5 pages) and Synthetic weather radar using hybrid quantum-classical machine learning by Graham R. Enos, Chad Rigetti et al, Rigetti, November 2021 (8 pages).

- **Reservoir Networks**[1619].
- **Graph Neural Networks**[1620].
- **Active Learning** algorithms which select the training data set to make learning more efficient and saves up to 85% of training time. It consists in labeling unlabeled data using an iterative supervised learning[1621].
- **Capsule Networks**, which can recognize features in images with taking into account their relative positioning[1622].
- **Various image analysis algorithms**[1623] with different use cases like improve satellite imaging interpretations[1624], improved edge detection[1625].
- Hybrid **transfer learning** which trains a quantum neural network using an already trained classical network[1626].
- **Federated machine learning** algorithms, which distributes training on several quantum computers to improve the training time while preserving privacy, with distributing and sharing the learned model instead of the training data[1627].
- **Spiking neurons** emulation although its speedup is not obvious[1628].
- And other fundamental advances like **group-invariant QML**[1629].

The table in Figure 579 positions the different quantum accelerations associated with various algorithms used in machine learning and deep learning[1630]. Accelerations in log(N) are more important than those expressed as the square root of N[1631].

[1619] See the review paper Opportunities in Quantum Reservoir Computing and Extreme Learning Machines by Pere Mujal et al, February-July 2021 (14 pages) and Time Series Quantum Reservoir Computing with Weak and Projective Measurements by Pere Mujal et al, May 2022 (19 pages).

[1620] See the thesis Quantum neural networks by Kerstin Beer, May 2022 (189 pages)

[1621] See Active Learning on a Programmable Photonic Quantum Processor by Chen Ding et al, August 2022 (17 pages).

[1622] See Quantum Capsule Networks by Zidu Liu and al, January 2022 (15 pages).

[1623] See the review paper Quantum Image Processing by Alok Anand et al, Carnegie Mellon, March 2022 (10 pages) and Processing Images in Entangled Quantum Systems by S.E. Venegas-Andraca and J.L. Ball, 2010 (11 pages).

[1624] See Towards Bundle Adjustment for Satellite Imaging via Quantum Machine Learning by Nico Piatkowski, Thore Gerlach, Romain Hugues, Rafet Sifa, Christian Bauckhage and Frederic Barbaresco, Thales and Fraunhofer IAIS, April 2022 (8 pages) which proposes keypoints extraction and objects alignment in pattern recognition applied to satellite imaging.

[1625] See A hybrid quantum image edge detector for the NISQ era by Alexander Geng et al, Fraunhofer ITWM, March 2022 (19 pages).

[1626] See Classical-to-quantum convolutional neural network transfer learning by Juhyeon Kim et al, August 2022 (15 pages).

[1627] See Federated Quantum Machine Learning by Samuel Yen-Chi Chen and Shinjae Yoo, Brookhaven Lab, March 2021 (25 pages) and Federated Quantum Natural Gradient Descent for Quantum Federated Learning by Jun Qi, GeorgiaTech, August 2022 (9 pages).

[1628] See An artificial spiking quantum neuron by Lasse Bjørn Kristensen, Alán Aspuru-Guzik et al, April 2011 (7 pages).

[1629] See Group-Invariant Quantum Machine Learning by Martin Larocca et al, Google Brain, University of Waterloo, May 2022 (28 pages).

[1630] The table is from The prospects of quantum computing in computational molecular biology by Carlos Outeiral, April 2020 (23 pages) which covers both QML algorithms and quantum simulation ones. It also mentions protein structures predictions. See also Quantum Machine Learning by Jacob Biamonte et al, May 2018 (24 pages).

[1631] Also see Application of Quantum Annealing to Training of Deep Neural Networks (2015), Machine learning &... artificial intelligence in the quantum domain, 2017 (106 pages), On the Challenges of Physical Implementations of RBMs, 2014, with Yoshua Bengio and Ian Goodfellow among the authors, illustrating the interest of AI specialists for quantum and Quantum Deep Learning, 2014, all extracted from Near-Term Applications of Quantum Annealing, 2016, Lockheed Martin (34 slides). See also Quantum machine learning for data scientists, 2018 (46 pages).

TABLE 1 Overview of the main quantum machine learning algorithms that have been reported in the literature, and complexities

Algorithm	Classical	Quantum	QRAM
Linear regression	$\mathcal{O}(N)$	$\mathcal{O}(\log\ N)^*$	Yes
Gaussian process regression	$\mathcal{O}(N^3)$	$\mathcal{O}(\log\ N)^\dagger$	Yes
Decision trees	$\mathcal{O}(N\ \log\ N)$	Unclear	No
Ensemble methods	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$	No
Support vector machines	$\approx\mathcal{O}(N^2)$-$\mathcal{O}(N^3)$	$\mathcal{O}(\log\ N)$	Yes
Hidden Markov models	$\mathcal{O}(N)$	Unclear	No
Bayesian networks	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$	No
Graphical models	$\mathcal{O}(N)$	Unclear	No
k-Means clustering	$\mathcal{O}(kN)$	$\mathcal{O}(\log\ kN)$	Yes
Principal component analysys	$\mathcal{O}(N)$	$\mathcal{O}(\log\ N)$	No
Persistent homology	$\mathcal{O}(\exp\ N)$	$\mathcal{O}(N^5)$	No
Gaussian mixture models	$\mathcal{O}(\log\ N)$	$\mathcal{O}(\text{polylog}\ N)$	Yes
Variational autoencoder	$\mathcal{O}(\exp\ N)$	Unclear	No
Multilayer perceptrons	$\mathcal{O}(N)$	Unclear	No
Convolutional neural networks	$\mathcal{O}(N)$	$\mathcal{O}(\log\ N)$	No
Bayesian deep learning	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$	No
Generative adversarial networks	$\mathcal{O}(N)$	$\mathcal{O}(\text{polylog}\ N)$	No
Boltzmann machines	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$	No
Reinforcement learning	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$	No

Figure 579: main quantum machine learning algorithms. Source: The prospects of quantum computing in computational molecular biology by Carlos Outeiral, April 2020 (23 pages).

Note the need for quantum memory for many of these algorithms, a type of memory that doesn't yet exists. None of these algorithms have been tested on a large scale, due to the absence of a quantum processor with more than fifty qubits.

QML is also one of the fields of application of D-Wave's quantum annealers. Annealers work well to find minimum energy of complex systems which is equivalent to searching for a minimum level of errors in the adjustment of the weight of neurons in a neural network[1632]. So far, they have tested an RBM (Restricted Boltzmann Machine) model[1633].

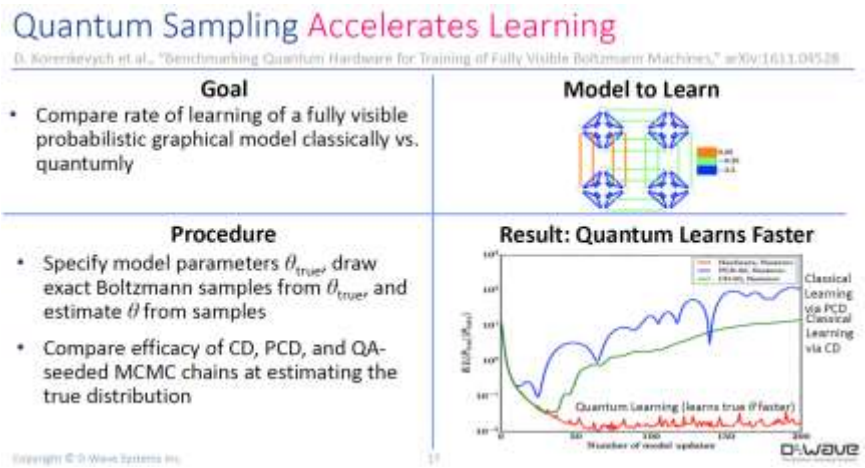


Figure 580: Source: D-Wave Quantum Computing - Access & application via cloud deployment by Colin Williams, 2017 (43 slides).

[1632] Examples source: D-Wave Quantum Computing - Access & application via cloud deployment by Colin Williams, 2017 (43 slides).

[1633] See Benchmarking Quantum Hardware for Training of Fully Visible Boltzmann Machines by Dmytro Korenkevych et al, Kindred AI et D-Wave, 2016 (22 pages).

They also did it with a hybrid algorithm for image recognition in a neural network, based on a variational circuit and a hybrid algorithm. But with very low-resolution images! D-Wave offers machine learning services in its Leap quantum cloud computing offering. But they are not the only ones. Many startups are specialized in Quantum Machine Learning, such as **QC Ware**.

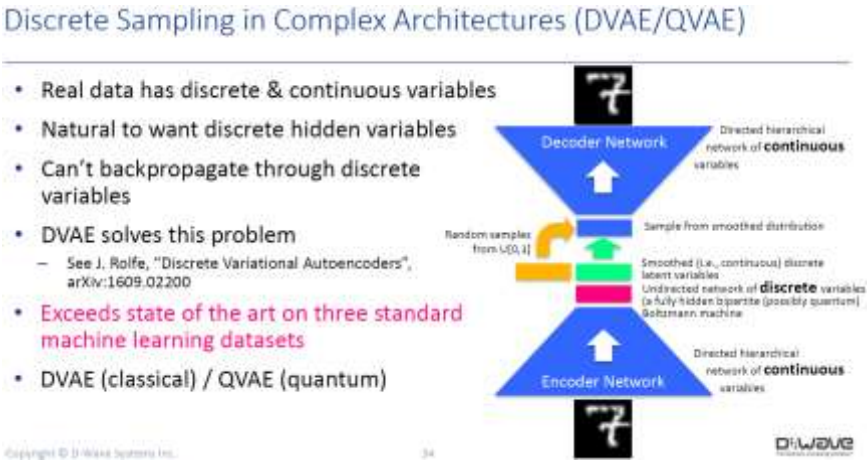


Figure 581: Source: D-Wave Quantum Computing - Access & application via cloud deployment by Colin Williams, 2017 (43 slides).

Many challenges remain to be addressed to operationalize QML beyond the emergence of sufficiently powerful and reliable quantum processors[1634]:

- **Loading training data** may take time and have a negative impact on the acceleration provided by QML. It also requires quantum random access memory (qRAM) which does not yet exist, even if some Quantum Data Loaders are proposed to circumvent this need[1635]. Some specific methods have to be created to load images efficiently[1636]. Other methods are developed that could require fewer training data than with classical machine learning[1637].
- **Avoiding the barren plateau** phenomenon which limits the efficiency of QML algorithms as the problem scales[1638].
- **Reading the results** of QML algorithms, particularly when they are classical data that take the form of real numbers.
- **Compressing** the neural networks to save quantum resources[1639].
- **Nonlinear activation functions** such as sigmoids used in classical neural networks are difficult to implement in quantum algorithms since quantum gates all apply linear transformations[1640].

[1634] See Quantum machine learning: a classical perspective by Ciliberto et al, 2020 (26 pages). It concludes with: "*Despite a number of promising results, the theoretical evidence presented in the current literature does not yet allow us to conclude that quantum techniques can obtain an exponential advantage in a realistic learning setting*".

[1635] See Quantum embeddings for machine learning by Seth Lloyd, January 2020 (11 pages). In Nearest Centroid Classification on a Trapped Ion Quantum Computer by Sonika Johri, Iordanis Kerenidis et al, December 2020 (15 pages), the QML algorithm "Nearest Centroid Classification" is implemented on a 11 trapped ions IonQ processor with an efficient amplitude data loader. See also Data compression for quantum machine learning by Rohit Dilip et al, April 2022 (8 pages) and the thesis Quantum Algorithms for Unsupervised Machine Learning and Neural Networks, by Jonas Landman, November 2021 (192 pages).

[1636] See A Novel Quantum Image Compression Method Based on JPEG by Jian Wang et al, 2017 (30 pages).

[1637] See Generalization in quantum machine learning from few training data by Matthias C. Caro et al, Nature Communications, 2022 (11 pages).

[1638] See Quark: A Gradient-Free Quantum Learning Framework for Classification Tasks by Zhihao Zhang et al, October 2022 (19 pages) which circumvents this problem with a quantum model and quantum optimizer.

[1639] See Quantum Neural Network Compression by Zhirui Hu et al, July 2022 (11 pages) and Experimental Quantum End-to-End Learning on a Superconducting Processor by Xiaoxuan Pan et al, March 2022 (10 pages).

[1640] The trick is explained in Quantum Neuron: an elementary building block for machine learning on quantum computers by Yudong Cao, Gian Giacomo Guerreschi and Alán Aspuru-Guzik in 2017 (30 pages).

There are workarounds, on which Iordanis Kerenidis has worked[1641] and some others[1642]. For example, quantum measurement can create the sough-after activation function nonlinearity in neural networks. There are also suggestions to use continuous variables qubits architectures to handle neural networks with nonlinearity provided by non-Gaussian qubit gates[1643], photonic quantum neural networks using Kerr nonlinearities[1644] and even other techniques not requiring measurement[1645].

- QML can take advantage of the **errors and noise** generated by quantum computation rather than be subjected to them. Work is going on in this direction.
- QML must prove that it brings a real **gain in computing time** compared to today's most advanced processors[1646].
- QML must also address the quest for **algorithms explicability**. The decomposition of the training and inference process of these quantum neural networks will probably be different from their implementation in more traditional processors[1647].

IBM published in 2021 a mathematical proof of a potential quantum advantage for a **quantum machine learning classification** task done with a quantum kernel method based on the Shor dlog algorithm. There was no actual experiment done due to the inexistence of sufficiently powerful quantum computers[1648]. We'll probably be stuck in this situation for several years from now.

On the other hand, QML's algorithm developments have served as a source of inspiration to improve algorithms that work with classical computation. As we will see in the section on quantum software vendors, page 740, there is no shortage of those who have specialized in QML. In general, they provide development tools and means to create QML proofs of concept.

In the AI domain, the European project H2020 **Quromorphic** launched in July 2019 aims to create a quantum processor dedicated to the execution of neural networks inspired by the brain[1649].

[1641] See Quantum Algorithms for Deep Convolutional Neural Network by Iordanis Kerenidis et al, 2020 (36 pages) which is discussed in Deep Convolutional Neural Networks for Quantum Computers by Jonas Landman, 2020.

[1642] See for example Continuous-variable quantum neural networks by Nathan Killoran et Al, June 2018 (21 pages).

[1643] See Continuous-variable quantum neural networks by Nathan Killoran, Maria Schuld, Seth Lloyd et al, 2018 (21 pages).

[1644] See Realistic quantum photonic neural networks by Jacob Ewaniuk et al, August 2022 (20 pages).

[1645] See Quantum activation functions for quantum neural networks by Marco Maronese et al, January 2022 (28 pages).

[1646] See Quantum Machine Learning: Algorithms and Practical Applications by Iordanis Kerenidis, QC Ware, Q2B Conference, December 2019 (34 slides) which makes an inventory of some potential gains with QML algorithms.

[1647] These techniques will be challenged by future memristor-based neuromorphic processors that will allow networks to converge more rapidly with backpropagation. Memristors will make it possible to place the neuron's computational functions and the associated memory in the same location in a semiconductor circuit, accelerating access to memory by several orders of magnitude during computations. This is another area of research, operated notably by Julie Grollier of the CNRS laboratory located at Thales TRT in Palaiseau.

[1648] See IBM shows quantum computers can solve these problems that classical computers find hard by Daphne Leprince-Ringuet, ZDNet, July 2021 that refers to Quantum kernels can solve machine learning problems that are hard for all classical methods, IBM Research, July 2021, itself referring A rigorous and robust quantum speed-up in supervised machine learning by Yunchao Liu, Srinivasan Arunachalam and Kristan Temme, Nature Physics, July 2021 (27 pages).

[1649] See Quantum computer: We're planning to create one that acts like a brain by Michael Hartmann and Heriot-Watt leads on next-gen computers, November 2018. The project is led by Michael Hartmann of IPaQS (Institute of Photonics and Quantum Sciences) at Heriot-Watt University in the UK, together with ETH Zurich, Delft University (Netherlands), Basque University (Spain), IBM Zurich and Volkswagen (Germany). 2.2M€ from the FET Open program were allocated to the project by the European Commission (details). My interpretation? The objective of the project has been adapted to the sauce of science fiction in order to recover community funding. The rest is about photonics.

It reminds us of the very controversial European flagship Human Brain Project led by Henri Markram from Switzerland. Quromorphic involves IBM Zurich, ETH Zurich, TU Delft, Volkswagen and Spanish and German Universities. Given the participants, we can guess that this will be based on superconducting qubits. The project got a funding of 2.9M€ in 2019 and is scheduled to end in 2022[1650]. This is quite reasonable.

We'll probably discover new fancy claims combining artificial intelligence and quantum computing and the devil will always be in complicated details[1651]. For instance, how about using these QML algorithms in robotics? Not so fast[1652]! It's still science fiction and *click-bait*.

On the other end, classical learning machine can be useful for quantum physics and quantum computing. We saw that Google used a deep learning algorithm to optimize the microwave frequency plan of the Sycamore processor's qubit control. Machine learning can also be used to model and simulate condensed matter, with an impact on the development of various qubits, especially superconducting qubits[1653].

Let us note finally the existence of an association promoting the field of AI and quantum computing, the **IAIQT** foundation based in Switzerland.

Quantum physics simulation

Quantum simulation algorithms are used to reproduce matter at the quantum level in a computer. It can be used to simulate the interaction between atoms in molecules for the creation of new materials.

They can also simulate physical phenomena related to magnetism or the interaction between photons and matter. This amounts to solving "N-body problems", i.e. calculating the interaction between several particles according to the physical laws governing their interaction. Quantum simulation also helps studying how superconducting materials behave, particularly at (relatively) high temperature, superfluids at low temperature, the temperature-dependent magnetism of certain materials and the interactions between graphene and light[1654].

These algorithms run in qubit-based universal quantum computers as well as on quantum simulators and quantum annealers although we still lack data to compare their respective performance.

Starting with 50 electrons in a molecule, classical computers can no longer simulate their dynamics, which corresponds to just a few atoms. For simple molecules, the applications are in the field of materials physics: carbon or nitrogen capture, new batteries, discovery of superconducting mechanisms that can then be used in medical scanners, ideally operating at room temperature.

[1650] See Quantum computer: we're planning to create one that acts like a brain, January 2019.

[1651] Here is one good example with Using Pioneering Quantum Machine Learning Methods, CQC Scientists Offer Bright Forecast For Quantum Computers That Can Reason par Matt Swayne, 2021 referring to Variational inference with a quantum computer by Marcello Benedetti, April 2021 (17 pages) which is about apply some quantum version of MCMC (Markov-Chain Monte Carlo) algorithm using Born machines. These are described in The Born Supremacy: Quantum Advantage and Training of an Ising Born Machine by Brian Coyle, Elham Kashefi et al, April 2021 (10 pages).

[1652] As described in Daniel Manzano's The Rise of Quantum Robots, April 2018. And with Qubit or Qubot? Quantum Technology May Help Robots Learn Faster par Matt Swayne, 2021, Robots learn faster with quantum technology by University of Vienna, March 2021 pointing to Experimental quantum speed-up in reinforcement learning agents by V. Saggio et al, Nature, March 2021 (10 pages).

[1653] See some review papers like Machine learning & artificial intelligence in the quantum domain by Vedran Dunjko and Hans J. Briegel, 2017 (106 pages), Artificial Intelligence and Machine Learning for Quantum Technologies by Mario Krenn, Jonas Landgraf, Thomas Foesel and Florian Marquardt, August 2022 (23 pages) and Modern applications of machine learning in quantum sciences by Anna Dawid et al, April 2022 (283 pages).

[1654] See this interesting lecture by Jacqueline Bloch at the Academy of Sciences which makes an excellent overview: Quantum Simulators: Solving Difficult Problems, May 2018 (29 mn).

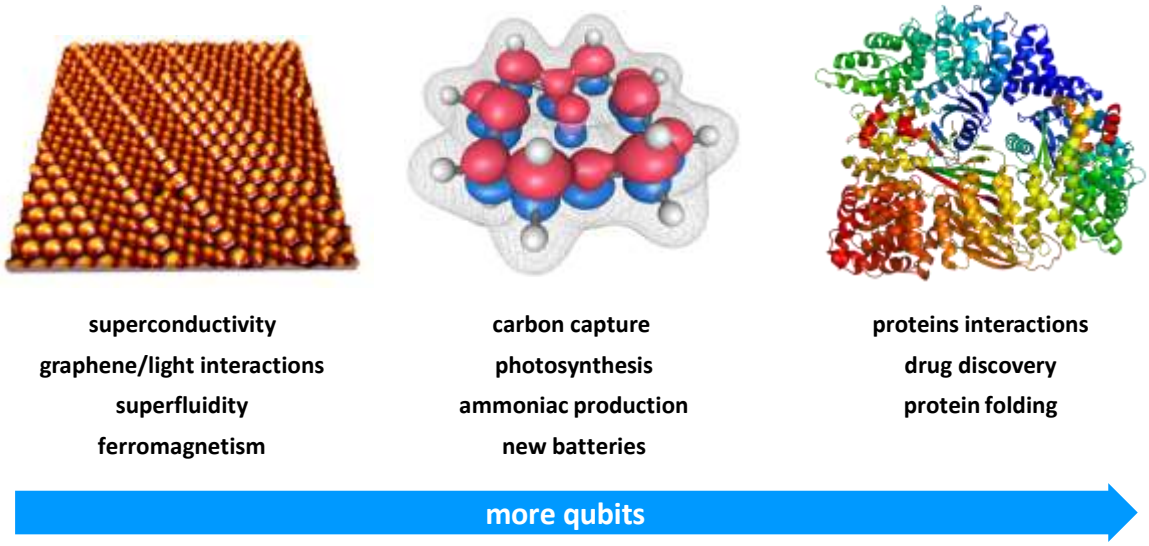
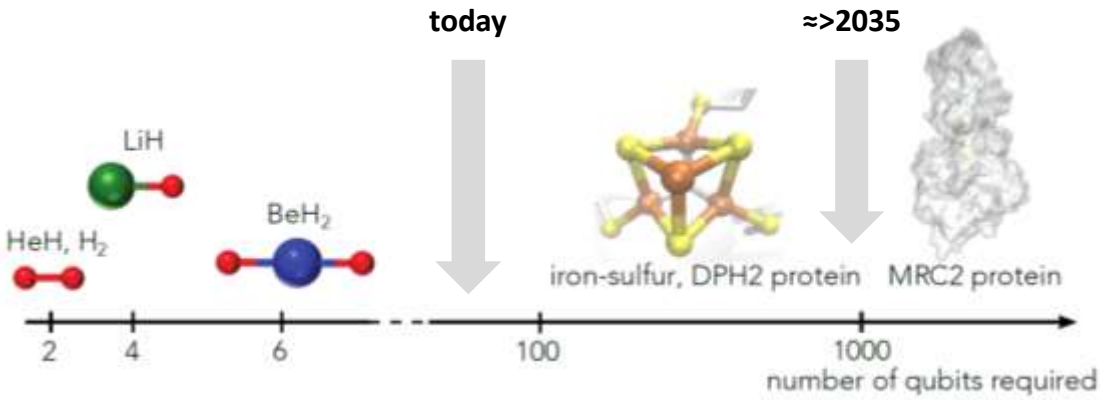


Figure 582: quantum physics simulation applications and a grade of complexity. (cc) Olivier Ezratty, 2020.

This should be accessible with universal quantum computers with 50 to a few hundred corrected logical qubits. For molecular biology simulations, it will probably take much longer before this is possible. We may need thousands or even hundreds of thousands of corrected qubits, which is far away in time. The diagram in Figure 583 positions the number of qubits needed to simulate the functioning of a mitochondrial protein, MRC2, in a fairly optimistic way.



source: Quantum optimization using variational algorithms on near-term quantum devices, 2017

Figure 583: another grade of complexity, for molecular simulations, in logical qubits. Source: from Quantum optimization using variational algorithms on near-term quantum devices by IBM researchers in 2017 (30 pages).

Here are some examples of quantum simulation algorithms:

- Simulation of **quantum field theory** as reviewed by John Preskill[1655].
- Simulation of **hydrogen atoms** in superconducting qubits computers[1656].
- Simulation of **simple molecules** by Alán Aspuru-Guzik, one of the world's leading authorities in the field[1657]. It's centered around the H_2 molecule.

[1655] Simulating a quantum field theory with a quantum computer by John Preskill, 2018 (22 pages).

[1656] Computation of Molecular Spectra on a Quantum Processor with an Error-Resilient Algorithm, 2018 (7 pages).

[1657] See Simulation of Electronic Structure Hamiltonians Using Quantum Computers by James Whitfield, Jacob Biamonte and Alán Aspuru-Guzik, 2010 (22 pages)

- Hybrid simulation of a **simple CaH^+ ion** also using two superconducting qubits[1658].
- Simulation of a **three atoms molecule**, beryllium hydride (BeH_2) with 6 qubits by IBM[1659].
- Determination of the **equilibrium state of simple molecules**[1660].
- Simulation of **water electrolysis** caused by light with use cases for the production of storable energy, particularly in fuel cells (hydrogen-based)[1661].
- Simulation of **semiconductor dynamics** using quantum annealing[1662].
- Simulation of the **cytochrome molecule**. With error rates of 0.1%, the run time would be 73 hours and require 4.6M physical qubits. With an error rate of 0.001% which is currently way out of reach, computing time could be down to 25 hours with 500K physical qubits. The equivalent classical computing is 4 years and requires 348 GB RAM and 2TB of storage[1663].
- Hybrid **molecular simulations** combining classical and quantum algorithms[1664].
- Simulation of **catalytic chemical processes** proposed by researchers from Microsoft and ETH Zurich with a requirement of about 4000 logical qubits[1665].
- Simulating organic molecules of medium complexity such as **cholesterol** would require about 1500 logical qubits and, above all, the ability to use billions of quantum gates[1666]. VQE algorithms can also be used there with a universal gate-based quantum computer using a reasonable depth of quantum gates (number of steps in the algorithm) [1667].
- Simulating **periodic solids**, which would require tens to hundred million of qubits[1668]!

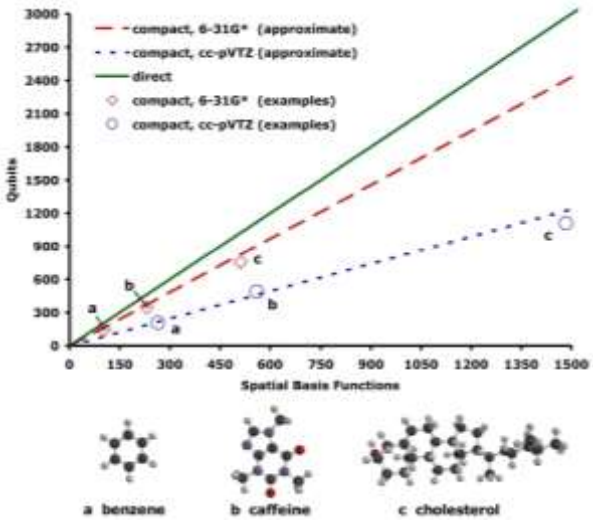


Figure 584: how many logical qubits are actually necessary to simulate relatively simple molecules. Source: Simulated Quantum Computation of Molecular Energies by Wiebe, Wecker and Troyer, 2006 (21 pages).

[1658] See Researchers succeed in the quantum control of a molecule by Román Ikonicoff, May 2017 (38 pages), pointing to Preparation and coherent manipulation of pure quantum states of a single molecular ion, 2017 (38 pages).

[1659] See Tiny Quantum Computer Simulates Complex Molecules by Katherine Bourzac, IEEE Spectrum, 201

[1660] See Simulated Quantum Computation of Molecular Energies by Wiebe, Wecker and Troyer, 2006 (21 pages).

[1661] This is one of the many examples from the presentation Enabling Scientific Discovery in Chemical Sciences on Quantum Computers, December 2017 (34 slides) by Ber De Jong from Berkeley

[1662] See Solving strongly correlated electron models on a quantum computer by Wecker, Troyer, Hastings, Nayak and Clark, 2015 (27 pages)

[1663] See Reliably assessing the electronic structure of cytochrome P450 on today's classical computers and tomorrow's quantum computers by Joshua J. Goings, Craig Gidney et al, Google, February 2022 (24 pages)

[1664] See Quantum Machine Learning for Electronic Structure Calculations, October 2018 (16 pages).

[1665] See Quantum computing enhanced computational catalysis by Vera von Burg, Matthias Troyer et al, July 2020 (104 pages).

[1666] See Quantum Computation for Chemistry and Materials by Jarrod McClean, Google 2018 (36 slides).

[1667] See An adaptive variational algorithm for exact molecular simulations on a quantum computer by Sophia Economou et al, 2019 (9 pages) which indicates in particular that "*VQE is much more suitable for NISQ devices, trading in the long circuit depths for shorter state preparation circuits, at the expense of a much higher number of measurements*".

[1668] See Quantum Computation for Periodic Solids in Second Quantization by Aleksei V. Ivanov et al, Oct 2022 (29 pages).

One of the applications of molecular quantum simulation is to better understand how photosynthesis works in order to improve or imitate it, the involvement of different forms of ferredoxin, relatively simple iron and sulfur-based molecules that serve to transport electrons from the photoelectric effect used in photosynthesis in plants. Algorithmic research on this molecule simulation have downsized the duration of quantum theoretical simulation from 24 billion years to one hour in a few years! The simulation of photosynthesis can pave the way for better carbon capture, among others to produce synthetic fuel. Research is also advancing in this field, without quantum computation for the moment[1669].

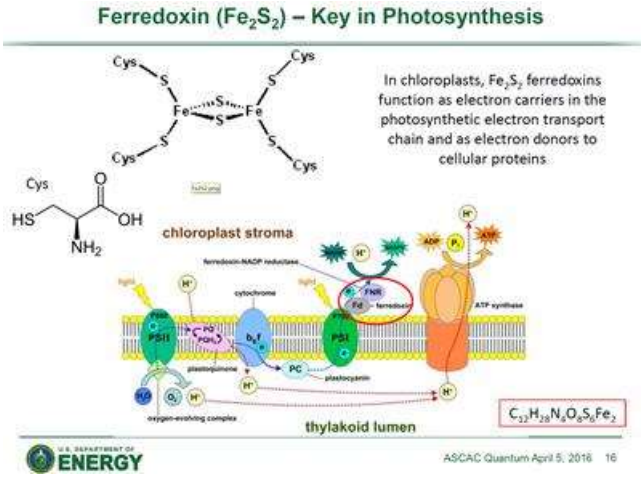


Figure 585: Source: Quantum Computing (and Quantum Information Science) by Steve Binkley, US Department of Energy, 2016 (23 slides).

Matthias Troyer explains how this algorithm has been optimized[1670].

At a higher abstraction level sits the simulation of atomic interactions in organic chemistry and molecular biology, going progressively from the smallest to the largest molecules: amino acids, peptides, polypeptides, proteins and perhaps much later, ultra-complex molecules such as ribosomes that fabricates proteins with amino acids using messenger RNA code.

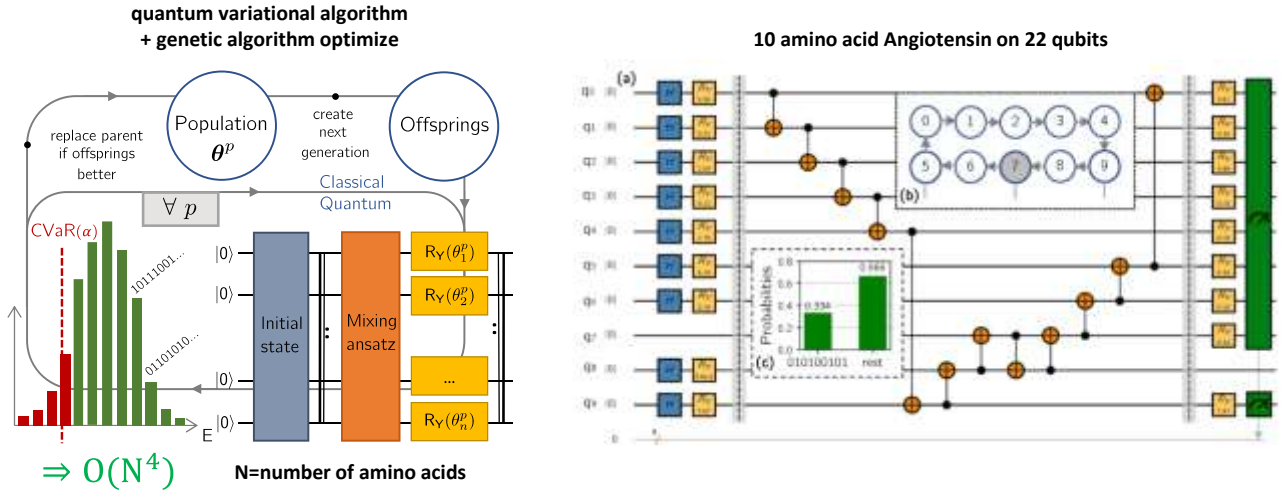


Figure 586: a hybrid classical and quantum algorithm to fold proteins. Source: Resource-efficient quantum algorithm for protein folding, Anton Robert et al, 2020 (5 pages).

Like classical algorithms, quantum simulation algorithms use approximation models based on known molecules, like what AlphaFold 3 from DeepMind does to predict the 3D structure of folded proteins. It works well for proteins which are close to those proteins used to train the model. For entirely new proteins (*aka* "de-novo proteins"), quantum simulation seems to be required[1671].

[1669] As seen in Semi-Artificial Photosynthesis Method Produces Fuel More Efficiently Than Nature, September 2018.

[1670] In What Can We Do with a Quantum Computer, Matthias Troyer, ETH Zurich, 2016 (41 slides), source for the illustration on the right.

[1671] See Evolution, energy landscapes and the paradoxes of protein folding by Peter Wolynes, 2015 (13 pages).

Various quantum algorithms have already been created for this purpose, including the Aspuru-Guzik algorithm in 2012, which was tested at a small scale on a D-Wave One[1672]. In 2020, researchers from IBM Zurich and from Institut Pasteur in France created an algorithm able to predict the 3D structure of a peptide, angiotensin, made of 10 amino acids and on just 22 qubits as shown above in Figure 586. Algorithms even exists to simulate RNA folding[1673].

The orders of magnitude of the quantum computers needed to solve these organic chemistry problems for large proteins have yet to be evaluated. It is not impossible that they are either impossible or extremely long-term even with the various optimizations that are proposed[1674]!

Hybrid algorithms

Hybrid algorithms are another branch of quantum algorithms that has been steadily growing in recent years. These algorithms combine a classical and a quantum part. Any quantum algorithm requires the support of a classical computer for the control of the quantum computer and the activation of its quantum gates [1675]. Hybrid algorithms distribute actual computing on both sides and ensure that the quantum part of the algorithm only covers what cannot be executed efficiently as classical computing. Eventually, it is likely that a majority of quantum algorithms will be hybrid [1676].

These hybrid algorithms can be implemented in development tools and languages capable of controlling both the classical and the quantum part of a supercomputer or a distributed system.

This is particularly the case with the **XACC** (eXtreme-scale ACCelerator) programming model[1677]. It enables the development of hybrid code that takes into account the characteristics of the quantum computer, and in particular its error rate. It interfaces with IBM and Rigetti quantum accelerators programming models.

Variational Quantum Eigensolver

One of the most pre-eminent hybrid algorithm class is the VQE (**Variational Quantum Eigensolver**), invented in 2013 by Alán Aspuru-Guzik[1678]. It allows the discovery of an energetic minimum of a complex equation[1679].

[1672] See D-Wave quantum computer solves protein folding problem by Geoffrey Brumfiel, 2012.

[1673] See A QUBO model of the RNA folding problem optimized by variational hybrid quantum annealing by Tristan Zaborniak et al, University of Victoria, August 2022 (12 pages).

[1674] See Quantum Information and Computation for Chemistry, 2016 (60 pages), which provides a good inventory of the various algorithmic works on quantum simulation of organic chemistry, A Comparison of the Bravyi–Kitaev and Jordan–Wigner Transformations for the Quantum Simulation of Quantum Chemistry by Andrew Tranter et al, 2018 (14 pages) that provides some solutions to reduce the gates count for quantum chemistry simulation with gate-based quantum computers and Creating and Manipulating a Laughlin-Type ν=1/3 Fractional Quantum Hall State on a Quantum Computer with Linear Depth Circuits by Armin Rahmani et al, November 2020 (7 pages).

[1675] See A Hybrid Quantum-Classical Approach to Solving Scheduling Problems, Tony T. Tran et al, (9 pages), Hybrid Quantum Computing Apocalypse 2018 (6 pages) according to which some Chinese team supposedly succeeded in running a Majorana fermion qubit, The theory of variational hybrid quantum-classical algorithms by Jarrod McClean et al (23 pages).

[1676] As such, the quantum algorithm patents filed by Accenture are worrying because they are at the limit of *troll patents*. See for example the Multi-state quantum optimization engine patent, USPTO 10,095,981B1, validated in October 2018 (20 pages). A second patent validated in April 2019 deals with a machine learning solution that helps an algorithm to decide which part to execute as classical and which part to execute as quantum. It is USPTO 10,275,721.

[1677] See Hybrid Programming for Near-term Quantum Computing Systems by A. J. McCaskey et al, Oak Ridge Laboratory, 2018 (9 pages).

[1678] VQE now belong to a broader category of hybrid algorithms, Variable Quantum Algorithms (VQA). See Variational Quantum Algorithms by M. Cerezo et al, Nature Reviews Physics, August 2021 (29 pages).

[1679] See an history timeline on Towards an experimentally viable variational quantum eigensolver with superconducting qubits, 2016 (18 slides). See also Variational Quantum Eigensolver explained, November 2019,

It is typically used to simulate the structures of molecules in inorganic and organic chemistry. It combines a classical part that determines an approximate starting point and a quantum part that refines the result. More precisely, the classical part prepares a so-called ansatz which is a set of parameters defining a quantum state, with using some nonlinear optimization techniques.

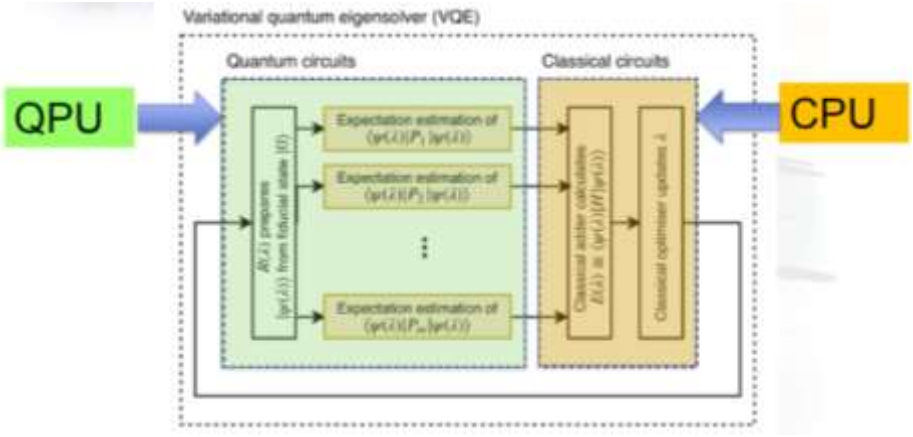


Figure 587: Source: Accelerated Variational Quantum Eigensolver by Daochen Wang, Oscar Higgott and Stephen Brierley, 2019 (11 pages).

The quantum side of the algorithm is used to compute a cost function outputting a real number that we seek to minimize with varying the parameters of the ansatz in the classical part.

This type of algorithm has the advantage of being able to be processed in distributed architectures with several classical and quantum processors. The gain in VQE comes from the ability of quantum computing to explore the space of possibilities in parallel. The approach is iterative and the speed of convergence depends on factors related to the simulated physical system, the digital modeling and the desired quality of the result.

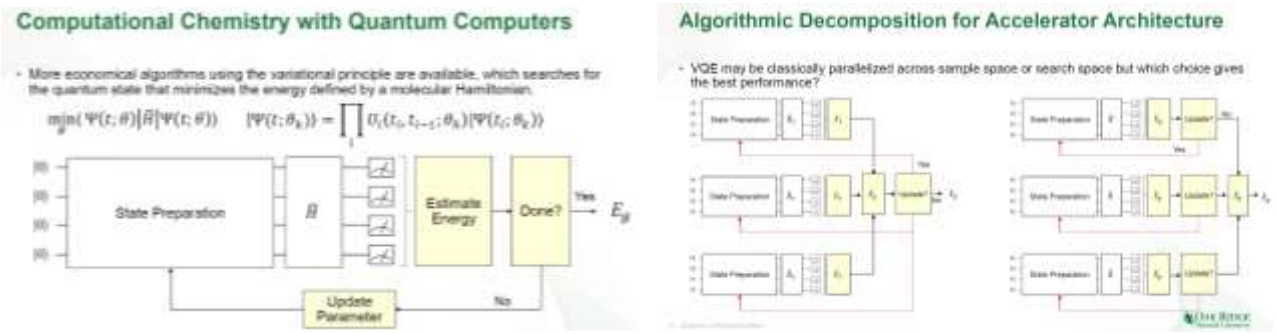


Figure 588: Source: Quantum Computing for Scientific Discovery: Methods, Interfaces, and Results by Travis Humble du Quantum Computing Institute, Oak Ridge National Laboratory, March 2018 (47 slides).

VQE can also be used to train a machine learning model[1680].

Quantum Approximate Optimization Algorithm

Another famous hybrid algorithm is the Quantum Approximate Optimization Algorithm **(QAOA)**, created by Edward Farhi in 2014. It is a combinatorial optimization algorithm used in particular in graph and slice management problems (MaxCut).

[1680] It is now possible to get rid of the classical part of the algorithm as explained in An adaptive variational algorithm for exact molecular simulations on a quantum computer, by Sophia Economou et al, 2019 (9 pages).

It has the advantage of requiring a low depth of quantum gates[1681].

Hybrid quantum algorithms

I'd put in this category hybrid algorithms using different quantum computing paradigm. Given there are three main paradigms, it adds up to four combinations, by pairs and the 3 altogether. One of these is about mixing quantum annealing and gate-based quantum computing. It is proposed by a team of Taiwan researchers with their large-system sampling approximation (LSSA) algorithm that solves Ising problems more efficiently than quantum annealers alone[1682].

Distribute quantum algorithms

In a section dedicated to distributed quantum computing using entanglement resources starting page 847, we have seen how quantum computer quantum interconnect could help create large QPUs. This is a rather long-term option and difficult to put in place.

Another sought option is to distribute some problem on several QPUs that are interconnected classically, using another form of hybrid algorithm. Such algorithms are designed for problems that can be split to run on several QPUs, with many constraints. This won't necessarily bring any exponential computing advantage but is an interesting path to work with NISQ QPUs[1683]. Among other scenarios, it is proposed to distribute some separable quantum neural network classification tasks to several QPUs[1684] and even more generic tasks[1685].

Tensor networks

In our presentation of basic linear algebra, we have described the notion of tensor products to mathematically represent a qubit register (page 147). It's a multiplication of matrices and a qubit register is represented by an exponentially growing vector state of 2^N complex numbers. Tensor products are also heavily used with neural networks programming in classical deep learning, including with the famous TensorFlow SDK from Google.

Describing a many-body quantum system is making use of these exponentially large tensor products and they are hard to compute classically. So here comes the notion of tensor networks which helps factorize very large tensors into networks of smaller tensors. It can be viewed as techniques that "zips" the tensor representation of these many-body systems, providing up to an exponential gain in the number of computing parameters[1686]. One of the reason these systems can be compressed relies on the so-called area-law that says that entangled quantum systems are connected only to their

---

[1681] See Quantum Approximate Optimization Algorithm explained, May 2020, An Introduction to Quantum Optimization Approximation Algorithm by Qingfeng Wang and Tauqir Abdullah, December 2018 (16 pages), QAOA: Quantum Approximate Optimization Algorithm by Peter Shor (25 slides), Quantum Approximate Optimization Algorithm: Performance, Mechanism, and Implementation on Near-Term Devices, by Leo Zhou, Mikhail Lukin et al, 2019 (23 pages) and Quantum approximate optimization of non-planar graph problems on a planar superconducting processor by Matthew P. Harrigan et al, 2021 (19 pages) which uses a QAOA algorithm on Google's 53 qubits Sycamore.

[1682] See Hybrid Gate-Based and Annealing Quantum Computing for Large-Size Ising Problems by Chen-Yu Liu et al, August 2022 (14 pages).

[1683] See Quantum Divide and Conquer for Combinatorial Optimization and Distributed Computing by Zain H. Saleem et al, Argonne Lab, Princeton, University of Colorado Boulder and SuperTech/ColdQuanta, July 2021 (13 pages).

[1684] See Scalable Quantum Neural Networks for Classification by Jindi Wu, Zeyi Tao and Qun Li, Department of Computer Science William & Mary, Williamsburg, August 2022 (11 pages).

[1685] See Enabling multi-programming mechanism for quantum computing in the NISQ era by Siyuan Niu and Aida Todri-Sanial, LIRMM, March 2022 (23 pages).

[1686] I found the zip analogy in Tensor network states to compress the many body problem by Antoine Tilloy, Inria, November 2021 (15 slides).

neighborhood, thus enabling the split of many-body systems into separable smaller body systems[1687].Tensor networks have various use-cases in many-body quantum physics digital simulations, for classical simulations of quantum computers, in chemistry, as well as in machine learning and applied mathematics.

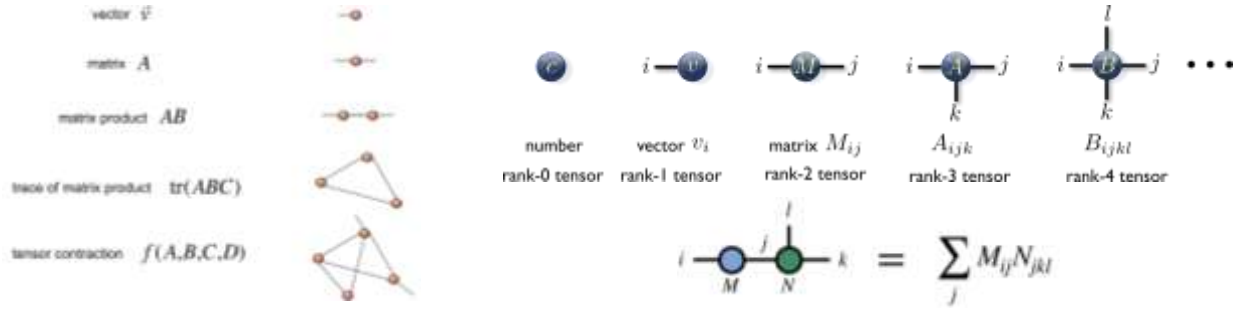


Figure 589: Sources: Introduction to Tensor Network States and Methods by Román Orús, DIPC & Multiverse Computing, 2020 (229 slides) and Lecture 1: tensor network states by Philippe Corboz, Institute for Theoretical Physics, University of Amsterdam (56 slides).

This is an entire new world of mathematics. How is it connected to quantum computing? The frontier is fuzzy.

Most of the tensor network literature deals with classical computing but tensor flow optimization techniques are also applicable to quantum computing. Some companies like Multiverse Computing make a lot of use of tensor networks techniques, sometimes embedded in the fuzzy concept of quantum inspired algorithms.

In typical graphical representations shown in Figure 589, tensor networks use graph notation connecting matrices (mid-points in graphs), vectors (line endpoints), traces of matrix products (triangles), and tensor contraction. Then, tensor network techniques are represented with these graphical views. As shown in Figure 590, the three main techniques are **MPS** (matrix product state represented in a 1D series of link with the preeminent DMRG variant [1688]), **PEPS** (Projected Entangled Pair States, used with graphs), **TPS** (Tensor Product States), and **MERA** (Multiscale Entanglement Renormalization Ansatz.

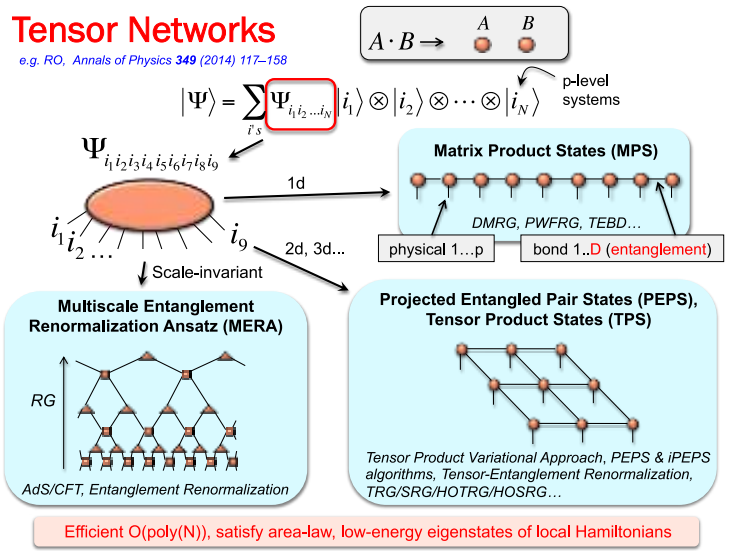


Figure 590: how tensor networks are graphically represented using the above notation. Source: Same as above.

[1687] For more on the area law, see Colloquium: Area laws for the entanglement entropy by J. Eisert, M. Cramer and M. B. Plenio, 2010 (28 pages) and Area Laws for Entanglement by Fernando G.S.L. Brandão and Michal Horodecki, Stanford University, 2014 (56 slides). To some extent, this law has indirect implications on the real scalability of quantum computers since on one hand, it seems to depend on the size of maximally entangled systems and in practice, these systems mays not exist due to the area law… !!!

[1688] Here are some key researchers behind tensor networks: Steven R. White, who created DMRG in 1992 and who's group at UCI in California maintains the ITensor software library for tensor network, Edwin Miles Stoudenmire who was his PhD and Ulrich Schollwöck from LMU München who also contributed to the development of DMRG.

The graphical representation of gate-based quantum circuits happens to be a special case of tensor networks[1689]! The ZX Calculus graphical language is also derived from the tensor network formalism[1690]. About 80 classical tools implement Tensor networks like Google TensorNetwork which relies on TensorFlow and was released in 2019[1691].

After you'll have spent some time understanding how tensor networks work[1692], you may wonder where quantum computing plays a role here. It seems mainly used as design tools to create quantum error correction codes, topological computing, solve condense matter physics problems[1693] and quantum machine learning algorithms[1694].

Tensor networks are also used in the creation of quantum code emulation software since these need various tensor contraction tools to save memory in storing the large quantum vector states if not density matrices of a number of qubits as large as possible[1695]. Xanadu's PennyLane framework contains tensor network circuit templates[1696].

Zapata Computing is also working on using tensor networks to prepare parametrized quantum circuits used in hybrid algorithms[1697].

Quantum inspired algorithms

Quantum inspired algorithms are classical algorithms whose design is inspired by quantum algorithms and interference management, but not programmed as quantum algorithms run through a classical emulator. Quantum inspired algorithms can be helpful in solving linear algebra problems[1698], simulating quantum systems[1699], with portfolio optimization, recommendation systems (like with the famous solution from Ewin Tang), images classification[1700] and machine learning[1701].

[1689] The Basics of Tensor Network - An overview of tensors and renormalization by Samuel Desrosiers, Glen B. Evenbly and Thomas E. Baker (5 pages) explain how we build tensor network algorithms using these representations. This graphical representation was created by Roger Penrose in 1971.

[1690] See a use-case of ZX Calculus in the creation of a tensor network for the classical part of a variational circuit Barren plateaus in quantum tensor network optimization by Enrique Cervero Martín, September 2022 (26 pages).

[1691] See The landscape of software for tensor computations by Christos Psarras et al, March 2021-June 2022 (16 pages) and Google TensorNetwork Library Dramatically Accelerates ML & Physics Tasks, 2019.

[1692] See Tensor Networks in a Nutshell by Jacob Biamonte et al, 2017 (34 pages), Lectures on Quantum Tensor Networks by Jacob Biamonte, January 2020 (178 pages), Hand-waving and Interpretive Dance: An Introductory Course on Tensor Networks Lecture Notes by Jacob C. Bridgeman and Christopher T. Chubb, 2017 (62 pages), Tensor Network Contractions by Maciej Lewenstein et al, 2020 (160 pages), the review paper Tensor Network Algorithms: a Route Map by Mari Carmen Bañuls, May 2022 (14 pages) and Hand-waving and Interpretive Dance: An Introductory Course on Tensor Networks by Jacob C. Bridgeman and Christopher T. Chubb, 2017 (62 pages).

[1693] See Applications of Tensor Networks: Machine Learning & Quantum Computing by Edwin Miles Stoudenmire, 2018 (142 slides).

[1694] See Towards Quantum Machine Learning with Tensor Networks by William Huggins, Edwin Miles Stoudenmire et al, Berkeley and Flat Iron Institute, July 2018 (12 pages).

[1695] See TensorCircuit: a Quantum Software Framework for the NISQ Era by Shi-Xin Zhang et al, May 2022 (43 pages).

[1696] See Tensor-Network Quantum Circuits, June 2022.

[1697] See Synergy Between Quantum Circuits and Tensor Networks: Short-cutting the Race to Practical Quantum Advantage by Manuel S. Rudolph et al, August 2022 (12 pages).

[1698] See An improved quantum-inspired algorithm for linear regression by András Gilyén et al, January 2022 (23 pages).

[1699] See one example in Classical algorithms for many-body quantum systems at finite energies by Yilun Yang, J. Ignacio Cirac and Mari Carmen Banuls, April 2022 (11 pages).

[1700] See AutoQML: Automatic Generation and Training of Robust Quantum-Inspired Classifiers by Using Genetic Algorithms on Grayscale Images by Sergio Altares-López et al, August 2022 (13 pages) which improves medical imaging grey images classification using a quantum inspired machine learning algorithm.

[1701] See the review paper Quantum inspired algorithms in practice by Juan Miguel Arrazola, Seth Lloyd et al, 2020 (24 pages).

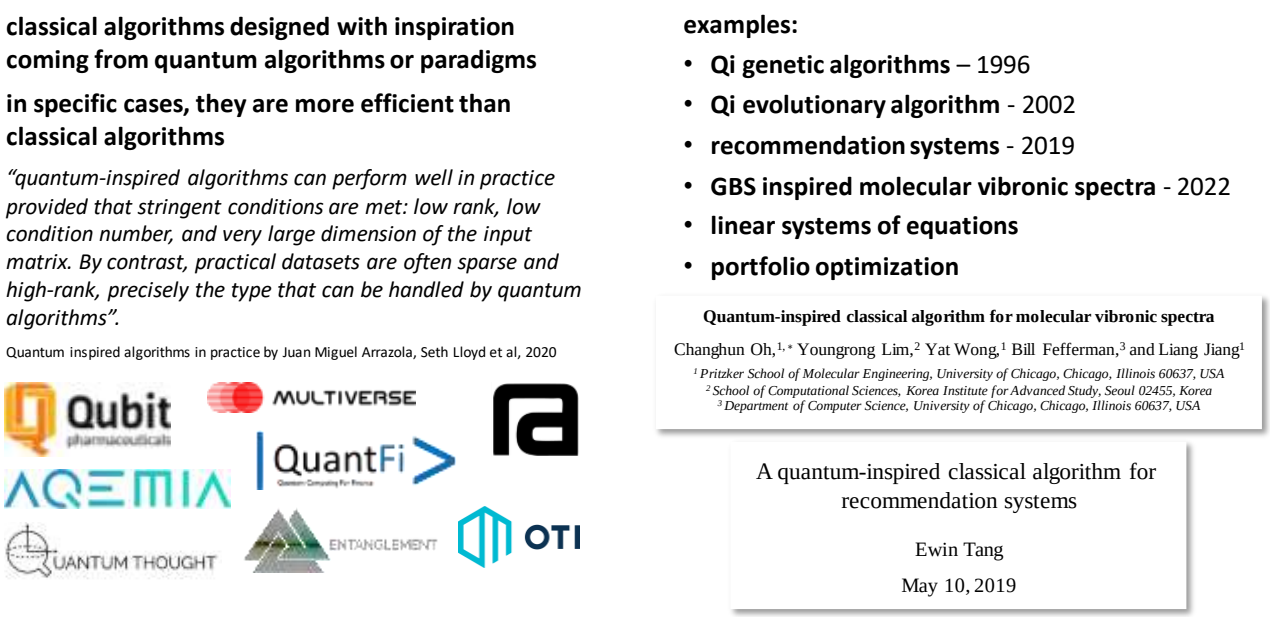


Figure 591: quantum inspired algorithms examples. (cc) Olivier Ezratty and various sources.

Creating a quantum inspired algorithm is sometimes said to rely on "dequantizing" or the "de-quantization" of a quantum algorithm[1702].

As Alastair Abbott and Cristian S. Calude wrote in 2010, "*de-quantization helps formulate conditions to determine if a quantum algorithm provides a real speed-up over classical algorithms. These conditions can be used to develop new quantum algorithms more effectively (by avoiding features that could allow the algorithm to be efficiently classically simulated), as well as providing the potential to create new classical algorithms (by using features which have proved valuable for quantum algorithms)*".In their paper, they also found that any algorithm in which entanglement is bounded is de-quantizable[1703].

Quantum inspired algorithms even exist that transposes the complicated gaussian boson sampling photonic based technique to simulate molecular vibronic spectra. Molecular vibronic spectra come from its light absorption that depends on the transitions between its different electronic states and changes in its vibrational energy[1704].

Quantum inspired algorithms are used in finance, healthcare and by many startups like Qubit Pharmaceuticals, Aqemia and Rahko in chemical simulations or QuantFi and Multiverse Computing in financial optimization. Quantum software startups find in quantum inspired algorithms a way to monetize their know-how while waiting for sufficiently powerful quantum computers.

Complexity theories

So far, we have reviewed a lot of the most common quantum algorithms and their theoretical acceleration.

[1702] See one example in Sampling-based sublinear low-rank matrix arithmetic framework for dequantizing quantum machine learning by Nai-Hui Chia, Ewin Tang et al, October 2019 (79 pages).

[1703] See Understanding the Quantum Computational Speed-up via De-quantisation by Alastair Abbott and Cristian S. Calude, 2010 (12 pages).

[1704] See Quantum-inspired classical algorithm for molecular vibronic spectra by Changhun Oh, Liang Jiang et al, University of Chicago, February 2022 (19 pages).

Quantum computing is sometimes presented as a miracle solution to extend computing capacities beyond the limits of classical supercomputing. It allows solving so-called "intractable" problems on conventional computers.

But what is the nature of the problems that can be solved with a quantum computer and that cannot be solved with classical computers? And above all, what are the limits of quantum computers? Do we still have computational limits?

We will see that these limits are rather blurred and shifting over time. This deals with **complexity theories**, a rather cryptic field of science and mathematics. It is a very abstract world involving a cryptic semantic made of P, NP, BQP and other complexities classes. Mathematicians have been discussing for half a century whether **P = NP** or not. This is the science of problem complexity classes. Behind these mathematics of complexity lie key technical but also philosophical considerations that are fundamental to Man and his omnipotence and control desires.

Problem complexity classes are Russian dolls more or less nested with each other that describe the range of time it takes to solve a problem, to verify given solutions and also on the associated required memory space, with regards to the problem size. The size of a problem is often formulated as an integer N, giving the number of items in the problem.

As far as time scales are involved, there are many ways in which this problem solving time scale can grow with N. The key ones are: constant, logarithmic, linear, polynomial and exponential. In this time scale, a time is considered reasonable if it is polynomial or below polynomial in the growing scale. A polynomial time is proportional to a given power of N.

Quantum computing allows under certain conditions to solve certain exponential problems in a polynomial time. It must be translated in: a given problem that would require an exponential time to be solved on a classical computer would require a polynomial time to be solved on a quantum computer.

But what lies beyond exponential time? There are still various inaccessible problems with, for example, exponential of exponential time scales. And we have also exponential memory space which can add another complexity dimension. Quantum computers will not be able to solve all these problems, even when we will be able to align gazillions of logical qubits.

These limitations have an indirect impact on predictions about the creation of some omniscient artificial intelligences capable of transcending human reasoning and solving all problems. This hypothetical AGI (Artificial General Intelligence) will be limited by the data and concepts that feed it and by the impossibility of solving all complex problems.

Mankind will continue to confront impossible computing tasks. It will not be able to solve all the complex problems around! Quantum computing does not allow us to dominate nature, to put the whole Universe in equations and to predict how it will run with quantum precision. Chance and the unexpected will continue to play a role in a very indeterministic world, and for the better. It is a small lesson in humility for Mankind.

Problem Complexity Classes

To dive into complexity classes, you need to define the main classes of problems by level of complexity. Here I am trying to simplify complexity, this time in the literal sense of the word.

Complexity classes often describe problems that are solved by using brute force with testing several combinations to find the ones matching some criteria (like with the so-called SAT problems) or with using mathematical equations defining complex systems (differential equations, Schrödinger's equation, ...).

Problem classes use the notion of Turing's deterministic and non-deterministic machines. Turing machines are conceptual models of computers created by Alan Turing before the Second World War.

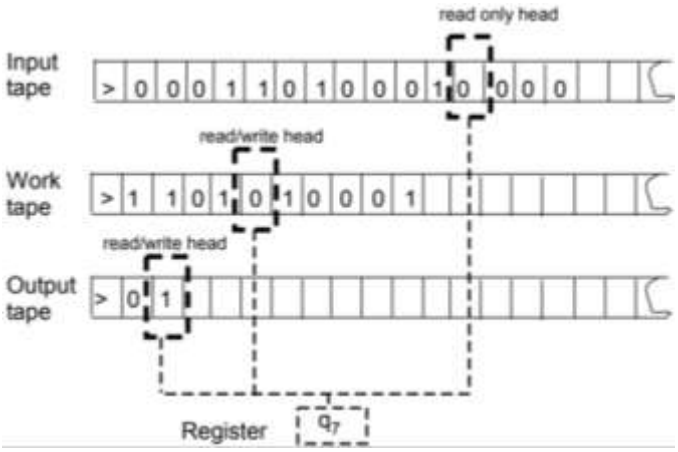


Figure 592: the famous Turing machine. Source: Computational Complexity: A Modern Approach by Sanjeev Arora and Boaz Barak, 2007 (489 pages).

They model computer processing based on the notion of programs and data, embodied by continuous and infinite rolls of paper, the first for the program, the second for the input data and the third for generating the results. Turing's theoretical model has long been used to define classes of problems that can or cannot be solved by a computer[1705].

Computers are all metaphorically Turing machines, reproducing this logic by reading program instructions and managing data in random access memory (RAM) or persistent storage (hard disk, SSD, ...). Associated with the notion of Turing machine is the notion of **Church-Turing's thesis**, named after Alonzo Church and Alan Turing, according to which there is an equivalence between computational problems that can be solved manually and with unlimited resources, those that can be handled with a Turing machine and those that can be solved with so-called recursive functions.

In a deterministic machine, the sequence of actions to be performed is predetermined and sequential. In the non-deterministic Turing conceptual machine model, computational rules can lead to execute several different operations for each evaluated situation. Basically, by exploring several paths in parallel and looking for a positive response to an algorithm component and closing parallel test loops once the sub-solutions are found.

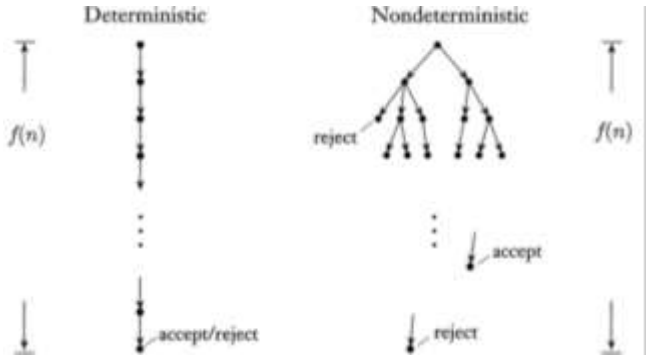


Figure 593: deterministic and non-deterministic Turing machines.

A non-deterministic machine increases the computational combinatorics compared to a deterministic machine. And this combinatorics usually jumps from polynomial to exponential.

Generic complexity classes

The level of complexity refers to the computing time and memory space required for these calculations. We are usually limited by computing time long before being limited by the available memory. However, some problems such as scheduling reach memory limits before computation limits.

[1705] See Computational Complexity: A Modern Approach by Sanjeev Arora and Boaz Barak, 2007 (489 pages) which is a good reference document on complexity theories. Students of a master's degree from ENS Lyon made a Turing machine in Lego in 2012 to celebrate the centenary of Alan Turing's birth (video) and it wasn't the only one of its kind (video)! Another one was made with wood in 2015 (video).

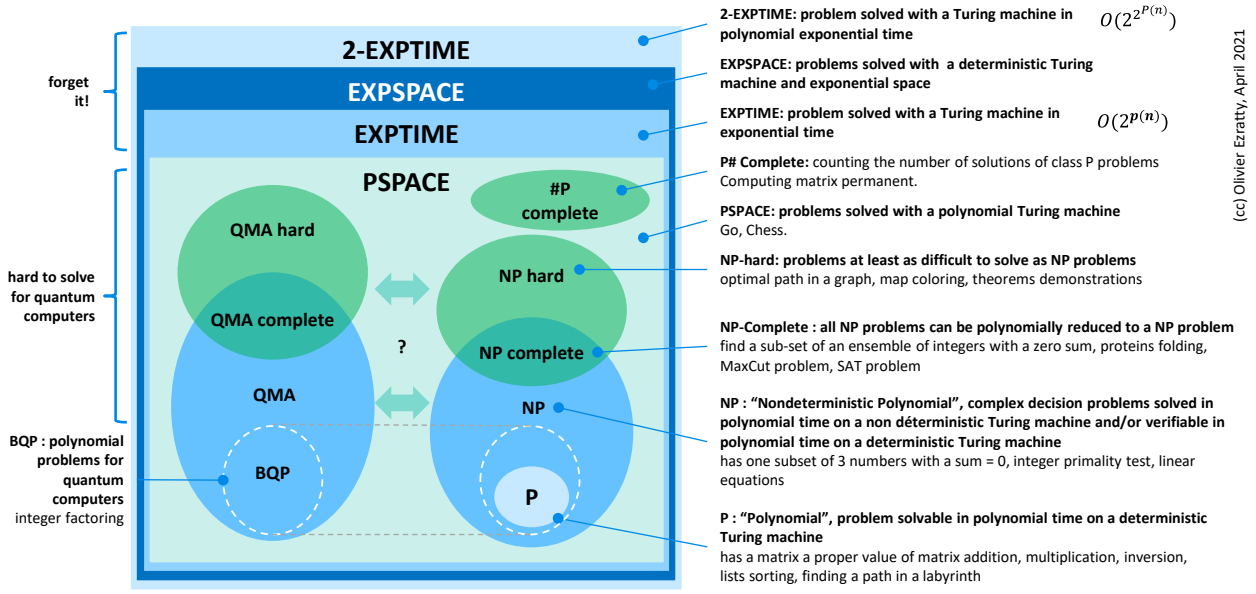


Figure 594: quantum and classical complexity classes, compilation (cc) Olivier Ezratty, 2021.

The association of a problem to a complexity class is related to the performance of the best-known algorithms to solve problems in that class.

Problem class levels in complexity theories are often based on black box or oracle models to which a system asks questions and gets answers based on the data provided. This is a logic of "brute force" and hypothesis scanning. The scale of the tested combinations depends on problem class.

So here are these classes by increasing level of complexity knowing that we will spend more time on NP related classes.

L or LSPACE, or DLOGSPACE, defines the class of problems that can be solved on a logarithmic scale of consumed memory and on a deterministic Turing machine, that is, on a traditional computer. Computational complexity increases slowly with the size of the problem. Unfortunately, very few complex problems sit in this class. These include queries in previously indexed relational databases, searches for DNA sequences, and generally speaking, search techniques that use pointers and optimize the use of computer memory.

NL is the class of problems solved on a logarithmic time scale on a non-deterministic machine. Complexity theory specialists are still trying to figure out whether L=NL or not! But they are less busy here than on determining whether P<>NP.

P covers problems that can be solved with a time growing polynomially with data to process and on a deterministic machine. If N is the size of the problem, the processing time is proportional to N^M, with M being an integer, preferably 2. It's an easy problem to solve and said to be "tractable". This includes sorting lists, validating the existence of a path in a graph, searching for a minimum path in a graph, multiplying matrices or evaluating a number to see if it is prime.

BPP is a class of problems that can be solved by random approaches ("Bounded-Error Probabilistic Polynomial-Time"). It would seem that BPP=P but this has not yet been demonstrated.

NP describes the class of problems for which it is easy to check the validity of a solution, i.e., that it can be realized in polynomial time by a deterministic machine. The other definition of the class is that it contains problems whose solution time is polynomial on a non-deterministic machine. These more complex problems have a computing time that is at least exponential when the method used is said to be naive, testing all possible combinations. These are "intractable" problems. In practice, these are problems particularly suited to quantum computers because of their ability to evaluate in parallel 2^N combinations of some classical computation.

Some examples of NP problems are the Steiner tree to determine whether an electrical network can connect a number of houses at a certain price, checking that a DNA sequence is found in several genes and the distribution of tasks to different agents to minimize the time it takes to complete them.

These problems have very concrete equivalents in logistics, planning, production, transportation, telecom, utilities, finance and cryptography. Note that a "decidable" problem, i.e., one that requires exploring a finite space of options, is not necessarily feasible from a practical point of view. Even if it can be solved in a finite amount of time, its resolution may take too long. An exponential problem has an elegant solution if one can find one solution that has a polynomial or, at best, linear duration. Polynomial times scale better than exponential times!

A big debate has been going on since 1956 (Kurt Gödel) as to whether class P equals class NP. If P = NP, it would be as simple to find a result when one can also simply verify it. The general consensus is that P is not equal to NP[1706]. The demonstration of whether or not P<>NP is part of one of the seven Clay Mathematics Institute mathematical challenges launched in 2000, each with a prize of $1M (Figure 595)[1707].

Among these challenges are the demonstration of the Navier-Stokes fluid mechanics equations and of Riemann's hypothesis on the distribution of prime numbers.

On the P vs NP side, the wording of the challenge provides an example of such a problem: you have to allocate 50 rooms of two students to 400 candidates but some candidates do not need to live in the same room[1708].

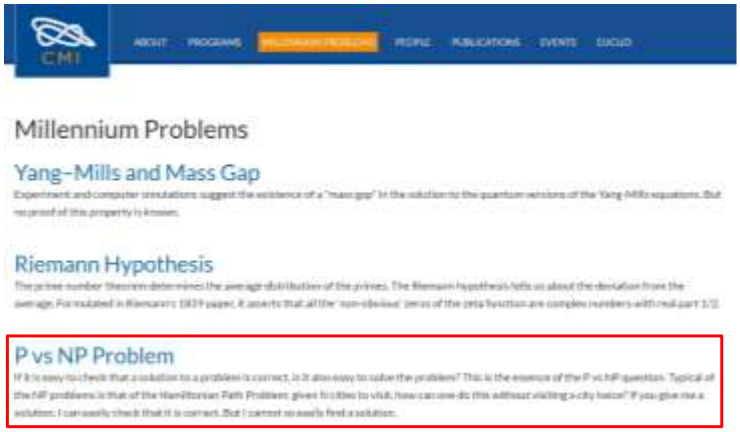


Figure 595: the Millennium challenge and P vs NP problem. Source: Clay Mathematics Institute mathematical challenges.

The combinatorial choice of 100 students among 400 is huge, so the problem is not easily handled with a supercomputer and brute force. It is indeed an NP problem because a given solution is easy to verify because it is simple to check that none of the rooms contains a forbidden pair of individuals. It is a bit like an all-or-nothing theory because if P = NP, all NP problems have an efficient polynomial solution. If P ≠ NP, none of the NP problems have a "pure" efficient solution[1709]. The definition of the problem classes NP and NP-Complete is relatively recent[1710].

[1706] See Fifty Years of P vs. NP and the Possibility of the Impossible by Lance Fortnow, 2021 (11 pages).

[1707] A Brazilian researcher, André Luiz Barbosa, published in 2010 his P ≠ NP Proof (25 pages) as well as a paper invalidating Cook's theorem that a Boolean SAT problem is NP-Complete, The Cook-Levin Theorem Is False, 2010 (11 pages). But this work seems ignored by specialists.

[1708] See The P versus NP problem by Stephen Cook (12 pages).

[1709] The classical method for solving these problems is to use heuristics allowing to obtain a satisfiable approximate solution, therefore not necessarily optimal, and in particular via probabilistic approaches.

[1710] It is derived from The complexity of theorem-proving procedures by Stephen Cook of the University of Toronto, 1971 (8 pages), best popularized in An overview of computational complexity (8 pages) and Reducibility among combinatorial problems by Richard Karp, 1972 (19 pages) and in Complexity and calculability by Anca Muscholl of the LaBRI, 2017 (128 slides).

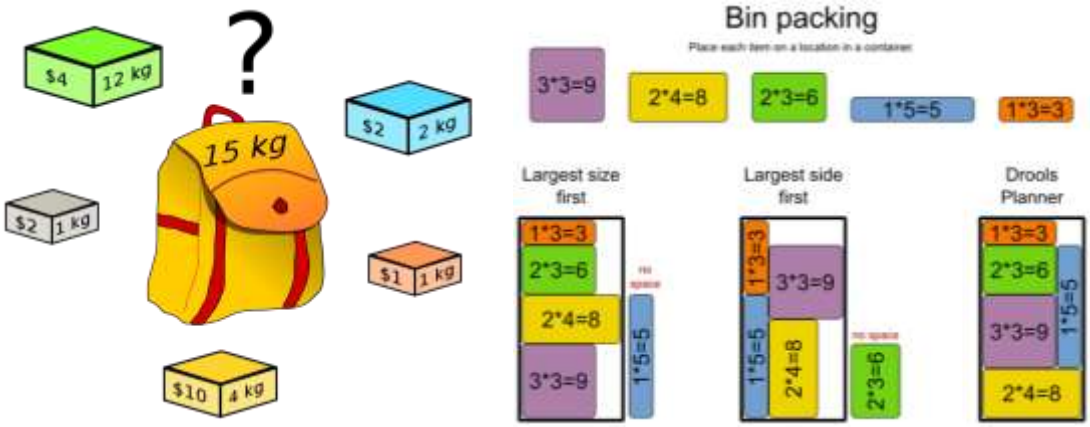


Figure 596: the famous bin-packing problems. Ever filled your car's trunk when going to vacation? Sources: Wikipedia and Stackoverflow.

Complete NP corresponds according to Richard Karp to problems in which other NP problems can be polynomially reduced. They have no known P (polynomial) solution. They are not accessible to quantum computers. It is in this class that we find the SAT or 3SAT type Boolean logic problems! More than 3000 NP-Complete problems are identified to date (list).

One of the typical problems is filling up the trunk of a car when you go on vacation or when you come back from Christmas with a bunch of presents for your family. And then the **bin packing** problem consisting in filling a backpack in an optimal way with a set of objects, to obtain the largest load and without exceeding a maximum weight (*aka* "bin packing" or "knapsack" problems).

It also includes the **subset sum problem of** finding a subset of a set of integers whose sum is equal to an arbitrary integer.

The **deminer's problem** consists in locating hidden mines in a field with only the number of mines in adjacent areas and the total number of mines in the field as an indication. All this without detonating them. It is a game well known by Windows users, launched in 1989!

The simulation of complex protein folding is also a NP-Complete problem[1711].

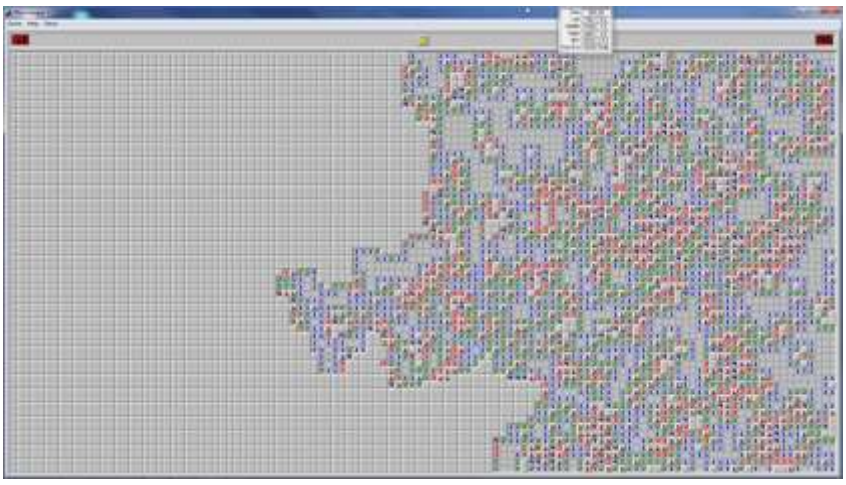


Figure 597: the deminer's problem is also an NP complete problem. Source of the illustration.

So, this would be a potentially very difficult problem to solve with a quantum computer with large proteins.

It is demonstrated that if an optimal solution to an NP-Complete problem could be found, all the solutions to problems in this class would be found. This is the important notion of problem reduction.

Graphs coloring with different colors for knots, branches or surfaces is part of the NP, NP-Complete and NP-Hard problems. The first two cases requiring a number of colors depending on the maximum number of connections between elements of the graph and the last case, relating to the coloring of

[1711] See Is protein folding problem really a NP-complete one? First investigations, 2013 (31 pages).

maps in different adjacent colors which requires a maximum of four, thanks to the computer demonstration of the four-color theorem done in 1976 by Kenneth Appel and Wolfgang Haken.

- **Graph nodes** coloring has applications in the placement of mobile antennas and in the allocation of memory registers for a compiler. The problem is NP-Complete for its resolution and NP-Difficult to find its optimal solution.
- **Branch** coloring has applications in the frequency allocation of multimode fiber optic networks. It also allows to optimize the placement of objects or persons according to their compatibility or incompatibility (*aka* the wedding tables problem). Optimum coloring is a NP-Hard problem.
- **Area map** coloring is used to define the coverage areas of mobile radio antennas or telecommunications satellites. It can even be used to allocate microwave frequencies for the activation of superconducting qubits. The coloring with three colors is an NP-Complete problem.

In general, many C problem classes have a subclass C-Complete and C-Hard. A problem is C-Hard if there is a type of reduction of problems from class C to this problem. If the problem C-Hard is part of class C, then it is said to be "C-Complete"[1712].

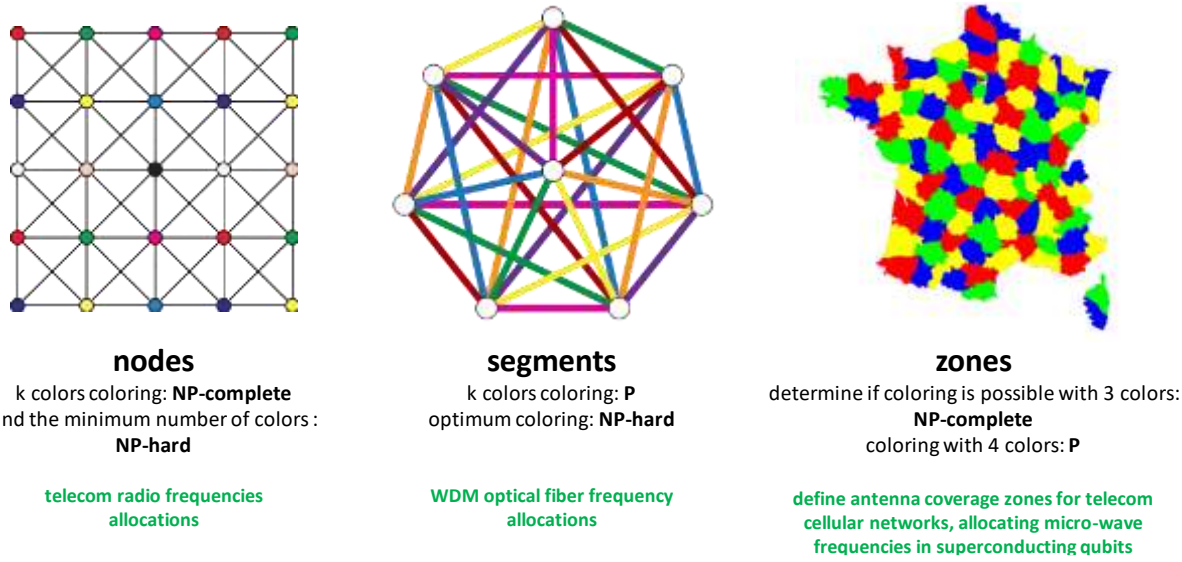


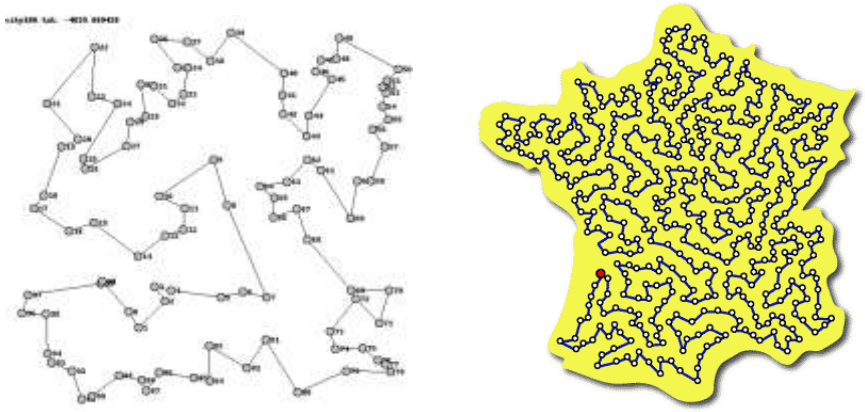
Figure 598: graph problems with nodes, segments and zones coloring.

NP Hard covers optimization problems where a minimum or a maximum is sought with a large combinatorics. A problem is NP-Hard if all NP-Complete problems can be reduced by polynomial simplification to this problem. It is the case of the solution of the **traveling salesperson problem** where one must test a large combination of routes to find the quickest one passing through a fixed number of cities. In this case, all solutions must be tested.

If a traveler has to go through 125 cities in less than 30 days, if there is a solution that works in that time frame, then the problem is NP.

[1712] For more information, see in particular Complexity Theory Part I (81 slides) and Part II (83 slides), which is part of a Stanford course on Complexity Theories, Calculability and Complexity- Some Results I Know by Etienne Grandjean of the University of Caen, 2017 (43 slides) as well as this video by Olivier Bailleux (2017, 20 minutes).

But nothing says that all the solutions have been found. Solving the problem below an arbitrary travel time with a return to the starting point is an NP-complete problem. This is called a Hamiltonian circuit: a path running a graph passing once and only once through each of the nodes and returning to its starting point. The determination of the shortest travel time is NP Hard.



what is the shortest possible route that visits each place exactly once and returns to the origin place : **NP-hard**

Figure 599: the TSP (traveling salesperson problem).

The brute force algorithm to solve it has a time that depends on N! where N is the number of nodes in the network. The known optimum time is $N^2 2^N$. The problem is difficult to solve beyond 20 steps[1713]!

The NP-Hard problem class also contains a number of **Nintendo** games like Super Mario Bros, The Legend of Zelda and Pokemon[1714]. Quantum computing would not be able to solve the most complex NP-Hard problems.

PSPACE is the class of problems that can be solved in polynomial space on a deterministic machine. NPSPACE is the class of problems that can be solved in polynomial space on a non-deterministic machine. And NPSPACE = PSPACE according to Savitch's theorem.

EXPTIME is the class of problems decidable in exponential time by a deterministic machine. Precisely, the computation time of these problems is $2^{p(N)}$ where p(N) is a polynomial of N, N being the level of complexity of the problem. They are intractable with traditional machines. Some of these problems can be converted into problems that can be treated polynomially by quantum computers. Chess and Go games on arbitrarily sized grids belong to this category. In size-limited grids, the exponential effect has limits. These were exceeded for Deep Blue's chess game in 1996 and for DeepMind's AlphaGo game of Go in 2016 and 2017.

NEXPTIME is the class of problems decided in exponential time by a non-deterministic machine with unlimited memory space.

EXPSPACE is the class of problems that can be solved in exponential space. In other words, they are difficult to access on today's and even tomorrow's machines.

2-EXPTIME is a class including the previous ones that covers decision problems that can be solved by a deterministic Turing machine in double exponential time with an order of magnitude of $O(2^{2^{P(n)}})$where P(n) is a polynomial of n. In other words, it's an exponential of an exponential problem.

We should add the class **#P** of problems for counting the number of solutions of class P problems, which are solved in polynomial time. Proposed in 1979 by Leslie G. Valiant, it obviously has its associated classes **#P Hard** and **#P Complete**.

[1713] See The Traveling Salesman Problem site which provides some examples of such problems such as the itinerary of all 49,687 English pubs or 49,603 tourist places in the USA.

[1714] See Classic Nintendo Games are (Computationally) Hard, 2012 (36 pages).

The computation of the permanent of a square matrix filled with 0 and 1 is a complete #P problem according to Ben-Dor and Halevi's theorem demonstrated in 1993. In 2011, Scott Aaronson demonstrated that the calculation of the permanent of a matrix is a #P Difficult problem[1715]. All this is related to the numerical simulation of the boson sampling which is compared to its resolution by photon-based systems that we study in a section on photon qubits, page 434.

The classes PSPACE, EXPTIME, NEXPTIME, EXPSPACE and 2-EXPTIME do not correspond to practical problems that are easy to identify in everyday life. They cover the problems of predicting the behavior of ultra-complex systems with strong interactions. If it is possible that modeling the folding of a protein is an NP problem, what would be the class of problem to simulate the functioning of a whole living cell, or even a multicellular organism? There are so many interactions at the atomic, molecular and cellular level that the class of this kind of problem is probably well beyond NP-Hard level.

There are many other problem complexity classes that won't be described here: EXP, IP, MIP, BPP, RP, ZPP, SL, NC, AC0, TC0, MA, AM and SZK! You can find them in the Complexity Zoo site which inventories the zoo of problem complexity classes. There seems to be over a hundred of them[1716].

Figure 600: there is even a zoo website for complexity classes! Source: the Complexity Zoo.

Quantum complexity classes

Let's now discuss the classification of problems that are theoretically addressable by quantum computers, the correspondence with the *above* classes being still a problem that is not entirely solved!

The classification is different because quantum computers can parallelize processing in an exponential way while classical computers like Turing machines cannot do it.

This is still very theorical since it doesn't take into account known constraints of quantum computers: their short coherence time and creates constraints on the number of quantum gates that can be chained together to solve a problem. This is a constraint that traditional computers do not have. But again, theoretically, this computation time constraint could be removed with using correction error codes.

[1715] In A Linear-Optical Proof that the Permanent is #P-Hard par Scott Aaronson, 2011 (11 pages).

[1716] To learn more about the subject of complexity theories, you can read the well-documented Computational Complexity A Modern Approach by Sanjeev Arora and Boaz Barak of Princeton University, 2007 (489 pages).

PH is a class of problems that generalizes the NP class. PH means "Polynomial Hierarchy".

BQP defines a class of problem that is solvable in polynomial time on a quantum computer with a constrained error rate of 1/3. This may in some cases correspond to P problems. The class was defined in 1993, when the first quantum algorithms appeared.

Whether the BQP class is really different from the P class is an ongoing debate. It has already been shown that the P class of polynomial problems is in BQP. But is NP in BQP? Seems not. It is however difficult to prove it in a generic way. The exact relationship between BQP and NP is still unknown.

The key point is to find algorithms that are part of BQP (processable in quantum) and that are not in PH (processable with any present and future classical architecture). This uncertainty has been removed only very recently[1717]. Oracle-based algorithms were found that are in BQP but not in PH.

NISQ is a class proposed by researchers from UC Berkeley, Harvard, Catltech and Microsoft in a paper published in 2022[1718]. It describes the class of problems that could be processed by a hybrid system using a NISQ quantum computer. It is showing that this class is in between BPP and BQP but it seems closer to BPP (problems accessible to classical computers) than BQP (problems accessible only to quantum computers) for Grover algorithm and farther for Bernstein-Vazirani algorithm. It doesn't include problems that are solvable by quantum annealers and simulators.

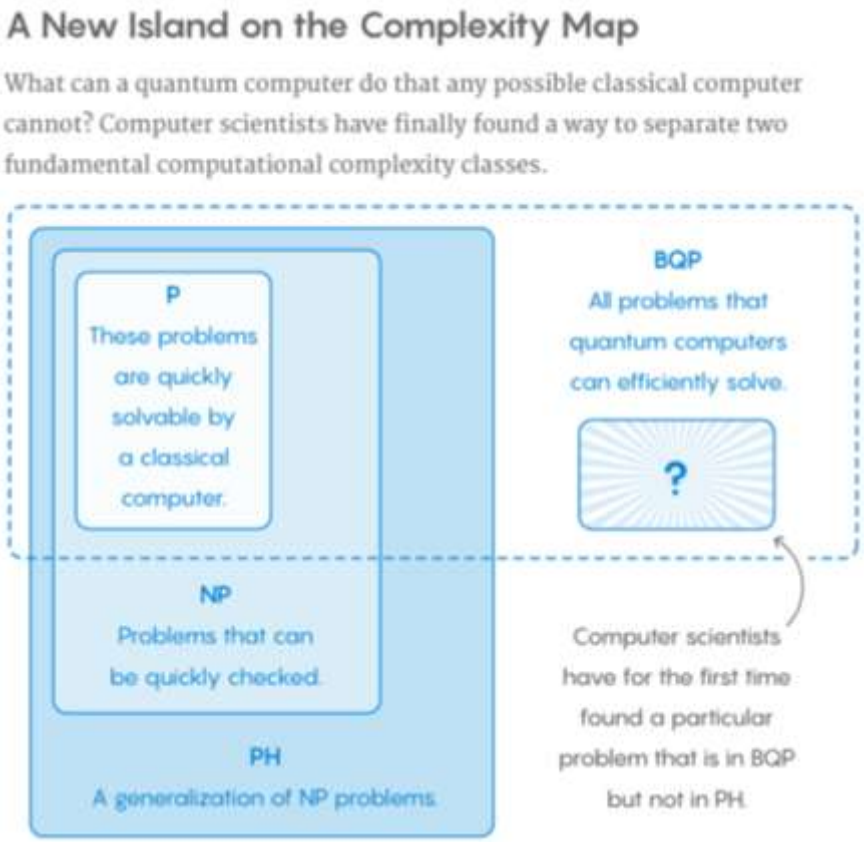


Figure 601: how BQP relates to the P and NP complexity classes. Source: Finally, a Problem That Only Quantum Computers Will Ever Be Able to Solve by Kevin Hartnett, 2018.

Therefore, these algorithms have a polynomial resolution time on quantum computers which remains exponential on their equivalent crafted for classical computers.

[1717] See Finally, a Problem That Only Quantum Computers Will Ever Be Able to Solve by Kevin Hartnett, 2018, referring to Oracle Separation of BQP and PH by Ran Raz and Avishay Tal, May 2018 (22 pages), presented in the Electronic Colloquium on Computational Complexity conference. This is the source of the illustration on this page.

[1718] See The Complexity of NISQ by Sitan Chen, Jordan Cotler, Hsin-Yuan Huang, Jerry Li, October 2022 (52 pages).

By the way, what about a possible complexity difference for problems manageable with universal gate quantum accelerators vs. quantum annealing accelerators? According to several researchers, there is no difference[1719]. Various theorems show that a problem that can be solved with universal quantum gates can also be solved with a D-Wave quantum annealing architecture and vice versa with only a polynomial time difference.

QMA (for Quantum Merlin Arthur) defines a class of problems that is verifiable in polynomial time on a quantum computer with a probability greater than 2/3. It is the quantum analog of the "traditional" NP complexity class. The QMA class contains the classes P, BQP and NP[1720]. Like the NP class, the QMA class has two derived subclasses, QMA Complete and QMA Hard. In practice, these are difficult problems to solve with quantum computers. Unfortunately, the literature on the subject does not describe its nature or provide examples. This is a pity for those who appreciate a practical sense of things!

QCMA is a hybrid problems class situated between QMA and NP. The proof is provided in classical polynomial time, but the resolution is at the QMA level and is performed in a quantum way.

Many publications point out the limitations of quantum algorithms and computers. A BQP problem that is not in PH gives the advantage to quantum computing. But exponential intractable problems for which the improvement brought by quantum computing is only a square root of classical time do not change their exponential nature. This is what Scott Aaronson points out[1721]. Complete NP problems and beyond remain inaccessible to quantum computers. Brute force has limits that even quantum computing cannot overcome in theory! This partly explains the difficulty of creating efficient quantum algorithms.

Finally, **NEEXP** is a class of problems that requires a double exponential computation time for its verification. Recent work shows that a result can be verified with several quantum computers with entangled qubits. This does not however enable us to solve this type of problems[1722]!

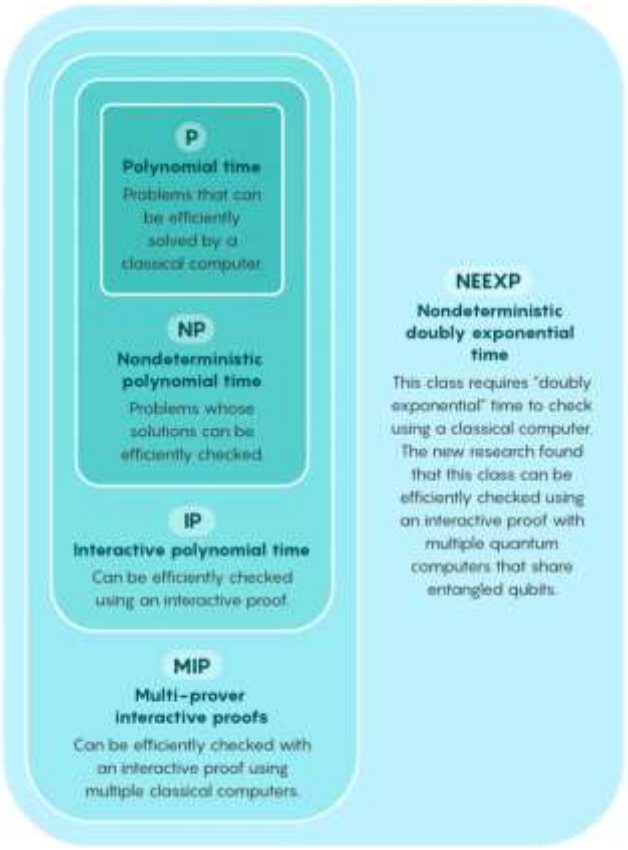


Figure 602: the NEEXP complexity class. Source: Computer Scientists Expand the Frontier of Verifiable Knowledge, 2019.

Some problems are undecidable, i.e., they cannot be solved by an algorithm, no matter how much time you have.

This is the case for the determination of the end of a Turing machine program.

[1719] See Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation by Dorit Aharonov, Wim van Dam and Julia Kempe (from CNRS), 2008 (30 pages).

[1720] See QMA-complete problems by Adam Bookatz, 2013 (18 pages).

[1721] See The Limits of Quantum Computers (16 pages) and NP-complete Problems and Physical Reality (23 pages).

[1722] See NEEXP in MIP* by Anand Natarajan and John Wright, 2019 (122 pages) and Computer Scientists Expand the Frontier of Verifiable Knowledge, 2019.

In other words, there is no program that can determine whether any program written in a common programming language will stop or loop for an infinite amount of time.

However, in 2020, there was some progress with a demonstration that the classes MIP* and RE were identical [1723].

In the same order, **Rice's theorem** demonstrates that no non-trivial property of a program can be decided algorithmically. All this is to say that there is no automatic method to detect bugs in a program or to certify that it runs well. There are, however, formal methods of proof that can be used to certify the execution of specific programs. This involves the use of formal program specifications that serve as a reference for assessing how well a program is running. This is already widely used, without quantum, in industrial information technology and in critical systems such as aerospace.

Quantum speedups

The chart in Figure 603 summarizes the theorical performance gains of some of the deterministic algorithms we have just seen. Complexity levels (exponential, polynomial, linear, ...) are generic.

The precise levels of complexity of each algorithm are roughly associated with these classes. Nlog(N) is the complexity of a classical Fourier transform and is nearly linear since N grows much faster than log(N) and $\log(N)^3$ is a log level complexity for the Shor algorithm and a QFT.

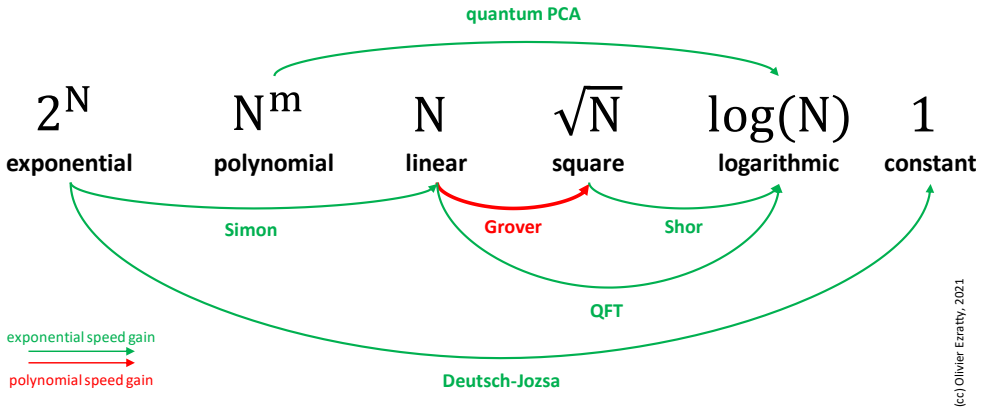


Figure 603: how do O() compare for complexity classes in quantum computing. The arrows show how their classical and quantum solution compare. (cc) Olivier Ezratty, 2021.

You can also visualize graphically the way computing time grows according to the big O() scale of problems below. A quantum algorithm's main goal is to move your problem's computation time from the red zone to the orange, or better, the yellow and green zones.

[1723] The MIP* class of problems that can be verified by quantum entanglement is equal to the RE class of problems that are no more difficult than the problems of program termination. See A quantum strategy could verify the solutions to unsolvable problems - in theory by Emily Conover, 2020 which refers to MIP*=RE by Zhengfeng Ji et al, January 2020 (165 pages) and seen in Mathematicians Are Studying Planet-Sized Computers With God-Like Powers by Mordechai Rorvig, 2020. See Landmark Computer Science Proof Cascades Through Physics and Math by Kevin Hartnett, March 2020.

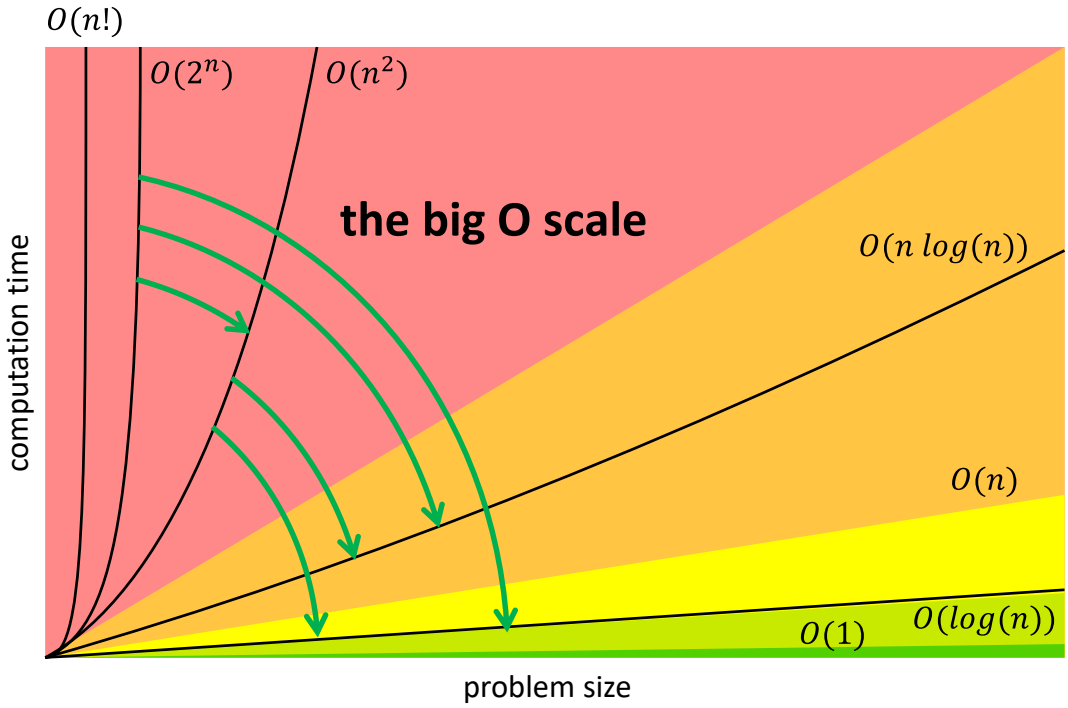


Figure 604: another view of the big O() scale. Source: Wikipedia, reformatted.

An exponential gain is also obtained when we move from N or √N to log(N). A QFT thus generates a theoretical exponential gain. The time scales are more meaningful in the table from Figure 605.

Complexité	n	$n \log_2 n$	n^2	n^3	1.5^n	2^n	$n!$
$n = 10$	< 1 s	< 1 s	< 1 s	< 1 s	< 1 s	< 1 s	4 s
$n = 30$	< 1 s	< 1 s	< 1 s	< 1 s	< 1 s	18 min	10^{25} ans
$n = 50$	< 1 s	< 1 s	< 1 s	< 1 s	11 min	36 ans	∞
$n = 100$	< 1 s	< 1 s	< 1 s	1s	12, 9 ans	10^{17} ans	∞
$n = 1000$	< 1 s	< 1 s	1s	18 min	∞	∞	∞
$n = 10000$	< 1 s	< 1 s	2 min	12 jours	∞	∞	∞
$n = 100000$	< 1 s	2 s	3 heures	32 ans	∞	∞	∞
$n = 1000000$	1s	20s	12 jours	31, 710 ans	∞	∞	∞

Figure 605: complexity classes and times scales. Heures = hours. Jours = days. Ans = years. Source: Complexity in time, Ecole Polytechnique (25 pages).

The ideal performance gain consists in traversing several complexity scales, and particularly for an exponential problem. In practice, the main algorithms skip one or two complexity classes, but not necessarily from the exponential problem class. But my scheme is misleading. N can also grow exponentially depending on the size of a problem. The classic example is Shor's algorithm.

The starting point is an N which is actually a RSA key size which itself is evaluated in power of 2. A 1024-bit key is 2^{1024}. If we move from 2^{256} to 2^{1024}, the growth of the key size is exponential. With Shor's algorithm, we get an exponential performance gain by going from a square root of 2^{1024} to $\log(2^{1024})$, that is to say 1024 (in log base 2)! So, the time scale moves from 2^{512} to 1024, which is a perfectly exponential gain. Deutsch-Jozsa's algorithm has the particularity of traversing all levels of this scale, from an exponential time to a fixed time. We have unfortunately seen that it has no known practical application.

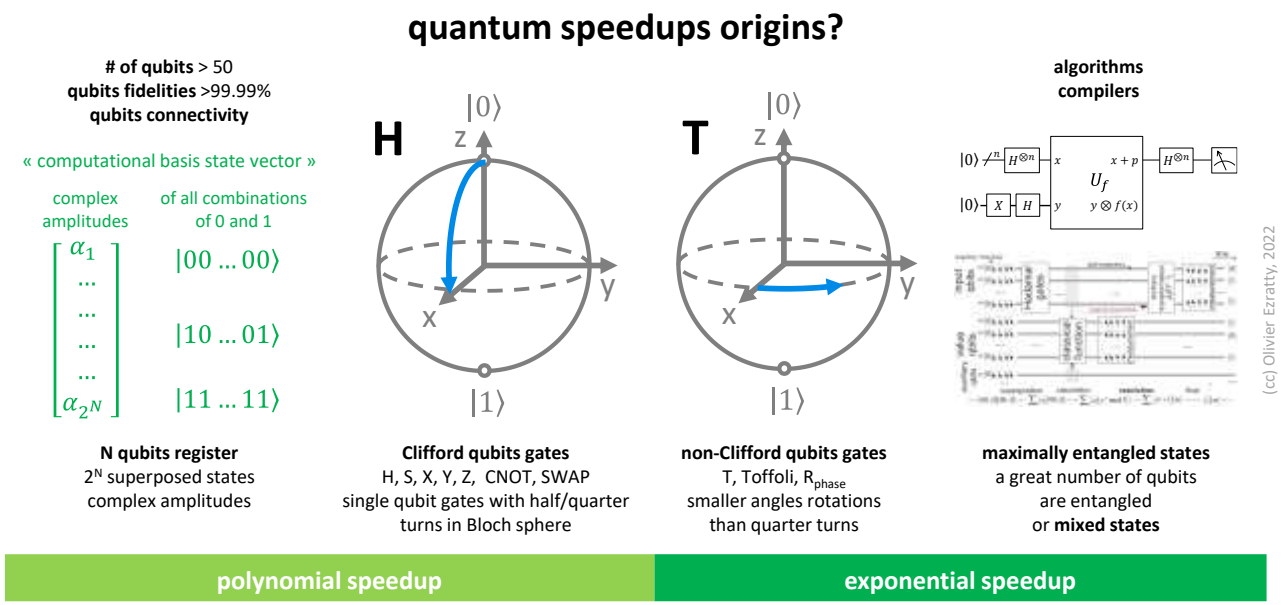


Figure 606: the origins of quantum speedups are not obvious. It may be counter-intuitive but the exponential size of the computational vector space of N qubits doesn't explain any potential exponential gain in quantum computing. You need to have at least two other conditions: use non-Clifford qubit gates and have a N-qubit maximally entangled space. (cc) Olivier Ezratty, 2022.

The speedup gain from an algorithm depends on the gates it's using. Shor's algorithm and any QFT based algorithm provide an exponential gain since it uses phase-controlled R gates. Grover's algorithm is providing a polynomial gain since it uses only Hadamard gates. But Deutsch-Jozsa's algorithm has an exponential gain although it is using only Clifford's group gates like the Hadamard gate.

Why so? Because it uses an Oracle function that may use non-Clifford's group gates[1724].

On top of using non-Clifford quantum gates, a quantum algorithm is also having an exponential speedup if it handles **maximally entangled states**[1725]. It means that there's a correlation of states between a maximum number of qubits in the register until the end of computing. If an algorithm handles islands of disconnected sets of qubits in the register, the speed-up will be constrained by the size of these islands.

The bigger the island, the bigger the Hilbert space managed by the algorithm. Let's explain this simply with a register of N qubits. If the algorithm is split into 4 different subspaces of N/4 qubits, you'll end-up managing a space with $4x2^{N/4}$ amplitudes, or $2^{2+N/4}$. That number is way smaller than 2^N, starting with N=3. For N=50, the difference is between $2{,}3x10^5$ and 10^{15}!

Studies on maximally entangled states and multipartite entanglement are numerous and accessible only to specialists[1726]. They deal with the theory, like with absolutely maximally entangled states (AME) that are multipartite quantum states and carry absolute maximum entanglement for all possible

[1724] See Focus beyond quadratic speedups for error-corrected quantum advantage, by Hartmut Neven et al , 2021 (11 pages) that also explain why quadratic speedups are not efficient due to the error correction overhead.

[1725] On maximally entangled states, see On the role of entanglement in quantum computational speed-up by Richard Jozsa and Noah Linden, 2003 (22 pages), Review on the study of entanglement in quantum computation speedup by ShengChao Ding and Zhi Jin, 2007 (6 pages) and Necessity of Superposition of Macroscopically Distinct States for Quantum Computational Speedup by Akira Shimizu et al, University of Tokyo and NTT, 2013 (16 pages). It refers to an indice p defined in Macroscopic entanglement of many-magnon states by Tomoyuki Morimae et al, 2005 (12 pages).

[1726] See A brief introduction to multipartite entanglement by Ingemar Bengtsson and Karol Zyczkowski, 2016 (38 pages).

subsystem partitions[1727], with how much entanglement is required for quantum algorithms[1728] and with how it can be checked with quantum measurement[1729].

As of 2022, the largest set of entangled quantum object was achieved with 3,000 atoms, but not for doing any computing and without a characterized quality of their entanglement[1730].

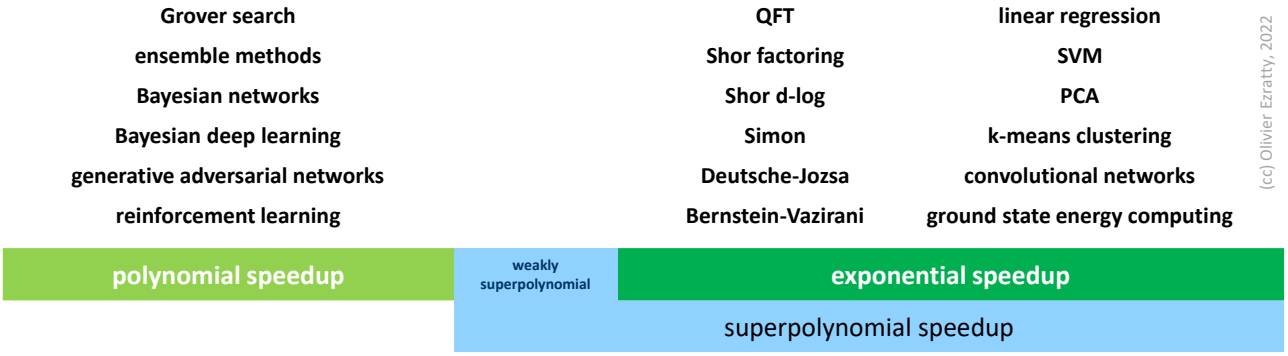


Figure 607: polynomial, superpolynomial and exponential speedups and their corresponding most common quantum algorithms. (cc) Olivier Ezratty, 2022.

We should here introduce the notion of superpolynomial speedup. A superpolynomial time is not bounded above by any polynomial. An exponential speedup is naturally superpolynomial but some superpolynomial speedups are not exponential, and said "weakly superpolynomial". Most common quantum algorithms showcase either a polynomial or an exponential speedup (*aka* strong superpolynomial speedup).

Other exponential speedups have been found for various algebraic algorithms like **estimating Gauss sums**[1731], **approximating Jones polynomial** that is not based on a QFT and still brings some exponential speedup, with some applications in topological quantum computing[1732] or counting solutions of **finite field equations**[1733].

It is also necessary to boil in the fact that the complexity of some problems can be addressed on conventional computers with probabilistic or heuristic approaches that also allow a significant reduction of the computing time of exponential problems. Practically, when moving from this kind of solution to a quantum algorithm, we replace one probabilistic approach with another since quantum computing is also highly probabilistic and prone to many computing errors.

All in all, quantum algorithms are interesting, but they are not always the only solution to cleverly solve a complex problem. This is amplified by the emulation going on between algorithms designers. Each and every new quantum performance challenge the classical supercomputers algorithms designers to improve the performance of their own tools.

[1727] See the thesis Symmetry and Classification of Multipartite Entangled States by Adam Burchardt, September 2021 (126 pages).

[1728] See How Much Entanglement Do Quantum Optimization Algorithms Require? by Yanzhu Chen, Linghua Zhu, Chenxu Liu, Nicholas J. Mayhall, Edwin Barnes and Sophia E. Economou, May 2022 (12 pages).

[1729] See Quantifying multiparticle entanglement with randomized measurements by Sophia Ohnemus, Heinz-Peter Breuer and Andreas Ketterer, July 2022 (17 pages) and Scalable estimation of pure multi-qubit states by Luciano Pereira, Leonardo Zambrano and Aldo Delgado, npj, May 2022 (12 pages).

[1730] See Entanglement with negative Wigner function of almost 3,000 atoms heralded by one photon by Robert McConnell, Hao Zhang, Jiazhong Hu, Senka Ćuk and Vladan Vuletić, Nature, March 2015 (11 pages).

[1731] See Efficient Quantum Algorithms for Estimating Gauss Sums by Wim van Dam and Gadiel Seroussi, 2008 (11 pages).

[1732] See A Polynomial Quantum Algorithm for Approximating the Jones Polynomial by Dorit Aharonov, Vaughan Jones and Zeph Landau, 2006 (19 pages).

[1733] See Quantum computing and polynomial equations over the finite field by Christopher M. Dawson et al, 2004 (7 pages).

This is what Toshiba did in 2019 with a classic optimization algorithm that was 10 times more powerful than the state of the art. That was fine even though a linear x10 gain is still not an exponential progress[1734].

This also explains why some are proposing to create a notion of "strong quantum speedup" using complexity classes instead of algorithms speeds[1735]. This being said, even if a polynomial gain is considered as a minor gain in complexity theories, it can still have a non-negligible practical value and make quantum computing attractive, without going through the Holy Grail of some fancy exponential acceleration.

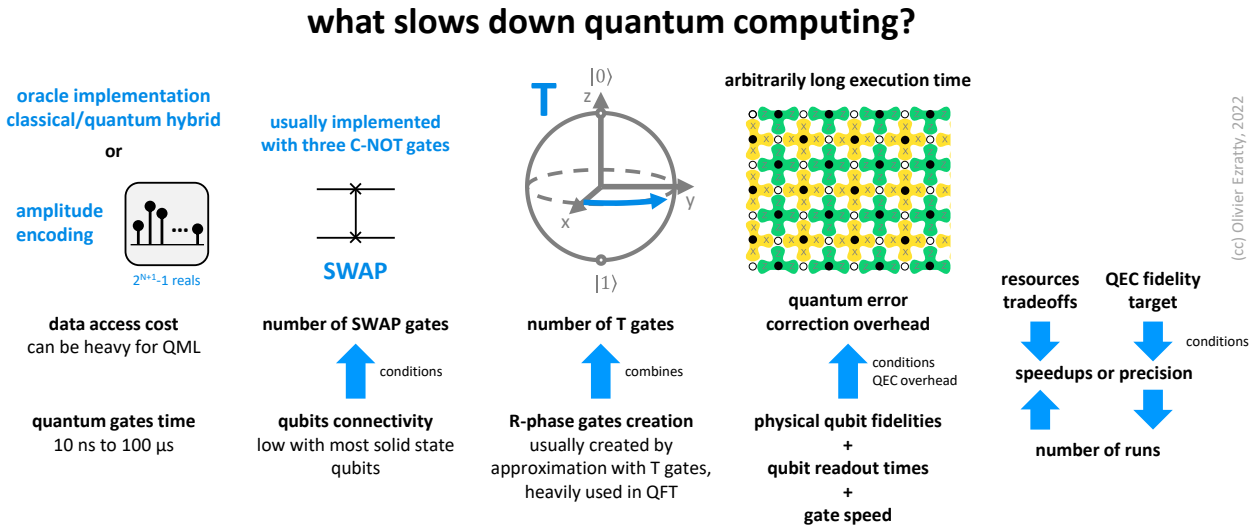


Figure 608: quantum computing speedup must also include faces sources of slowdowns, which have to be known by algorithms developers. (cc) Olivier Ezratty, 2022.

But the devils in the details must be cared about[1736] :

- First, the quantum speedup will be affected by the number of times the algorithm must be run. It's considered in some of the speedups like with Grover's algorithms but not always. These repetitions are also named shot count or shots. It depends on the problem, the number of qubits and the algorithm output (integers, real numbers). With Google's supremacy and its 53 qubits, it was 3 million shots. With IBM Quantum System One using from 5 to 28 qubits, the typical proposed shots number ranges from 1000 to 8000 shots.
- The quantum advantage is also depending on the number of qubits in your register that are put in superposition using Hadamard gates. Other qubits might be used elsewhere in the algorithm such as ancillas.
- Data preparation must also be handled, which is of particular importance for quantum machine learning algorithms[1737].
- The same should be said of oracle-based algorithms, particularly when they rely on some classical data access.

[1734] See Toshiba Promises Quantum-Like Advantage on Standard Hardware by Tiffany Trader, 2020, which references Combinatorial optimization by simulating adiabatic bifurcations in nonlinear Hamiltonian systems by Hayato Goto et al, April 2019 (9 pages).

[1735] See Measures of quantum computing speedup by Anargyros Papageorgiou and Joseph F. Traub, 2013 (4 pages). Proposing that "strong quantum speedup" is measured by a ratio between quantum complexity class and classical complexity class for a particular problem instead of comparing just cost of best-in-class classical algorithm vs cost of quantum algorithm "quantum speedup".

[1736] This is well explained in What Is the Quantum Advantage of Your Quantum Algorithm? by Jack Krupansky, February 2020.

[1737] See Information-theoretic bounds on quantum advantage in machine learning by Hsin-Yuan Huang, Richard Kueng and John Preskill, April 2021 (34 pages) which describes the conditions when QML algorithms provide a real speedup.

- Then, with large scale quantum computing, quantum error correction will add some additional burden. Using concatenation codes, you may lose polynomially on your speedup. Meaning that an initial polynomial speedup may be lost at this stage[1738].

So, as mentioned before, appreciating the real speedup of any quantum algorithm requires adopting an end-to-end approach considering all the parameters of the quantum algorithm execution time.

I would summarize the kinds of benefit coming from quantum computing over time like this:

Better. Some algorithms running on NISQ systems may bring a quality advantage in the solution they provide, like with quantum machine learning or various optimization tasks. This is due to the ability of quantum systems to better explore the problem computational space. For a QML problem, the better is expressed in precision %[1739].

Faster. We may then create solutions that are running faster than their best equivalent on classical computers. This may happen between the NISQ and the FTQC/LSQ era.

Beyond. In the longer term, and pending unlocking many showstoppers, large scale quantum computing with over 100 logical qubits may then be able to solve problems that are entirely not accessible by classical supercomputers, like in the quantum physics simulation realm.

Quantum algorithms key takeaways

- Quantum algorithms have been created since the early 1990s, over ten years before any quantum computer was working out of a research laboratory.
- Quantum algorithms use very different concepts than classical programming, even including artificial intelligence development tools or object oriented programming. It's based on the manipulation of large matrices and using interferences.
- The main algorithms classes are oracle based and search algorithms, optimization algorithms, quantum physics simulation algorithms and quantum machine learning algorithms.
- A quantum algorithm is interesting if it provides some quantum speedup compared to their equivalent best-in-class classical version, including those that are heuristics based. These problems are said to be intractable on classical hardware. Most of the time, quantum speedups are theorical and do not incorporate the costs of quantum error corrections and of creating non-Clifford quantum gates. These gates are implementing small phase changes and are used in quantum Fourier transforms and implemented in many other algorithms. A quantum speedup that is not exponential is highly questionable. All of this requires some understanding of complexity classes like P, NP and BQP.
- Another key aspect of quantum algorithms is data loading and/or preparation. It is often overlooked and can have a significant time cost, on top of frequently requiring some form of not-yet-available quantum memory hardware. As a consequence, quantum computing is not adequate for big-data computations.
- Gate-based computers, quantum annealers and quantum simulators can exploit hybrid algorithms, combining a classical (preparation) part and a quantum part interacting with each other. This is particularly true with quantum machine learning.
- Quantum inspired algorithms are running on classical computers and are using some form of quantum mathematical models like interferences and signals decomposition (Fourier series/transforms).

[1738] See Focus beyond Quadratic Speedups for Error-Corrected Quantum Advantage by Ryan Babbush, Craig Gidney, Hartmut Neven et al, March 2021 (11 pages). Quadratic speedups requires more than 1M physical qubits!

[1739] See The Complexity of NISQ by Sitan Chen, Jordan Cotler, Hsin-Yuan Huang, Jerry Li, October 2022 (52 pages) which casts serious doubts on real quantum speedups that could be obtained with NISQ QPUs. In that case, we are left with better quality results as a potential quantum advantage.

Quantum software development tools

We now need to explore quantum computing software to implement the various algorithms we've just uncovered. It is a completely new world with very different paradigms.

Quantum algorithms still require programming, programming languages and development environments.

As shown in Figure 609, quantum software is organized in layers with, starting from the bottom, the physical qubits followed by low-level machine language to drive them at the physical level (microwaves length and frequencies, readouts, etc).

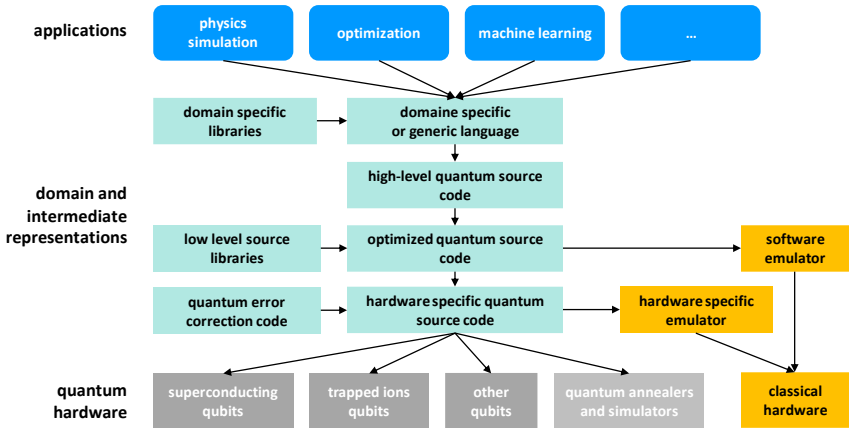


Figure 609: classification of quantum software engineering tools. (cc) Olivier Ezratty, 2021.

Next comes high level quantum source code which is in fact a kind of macro-assembler, able to take advantage of function libraries with ready-to-use algorithms (quantum Fourier transforms, phase estimates, etc.) and finally, high-level languages or libraries tailored to specific business needs.

In the lower layers between machine language and macro-assembler are functions for converting quantum gates into a set of universal quantum gates supported by the quantum hardware as well as error correction code systems that may require the execution of a large number of quantum gates.

A quantum compiler also implements many optimizations by for example removing quantum gate sequences that do not change the state of a qubit, such as two consecutive Hadamard or X (NOT) gates.

It also arranges these quantum gates to minimize the number of quantum gate steps in the solution. Quantum software architectures are generally hybrid. They manage side by side the execution of classical and quantum code, as shown in this diagram from Rigetti.

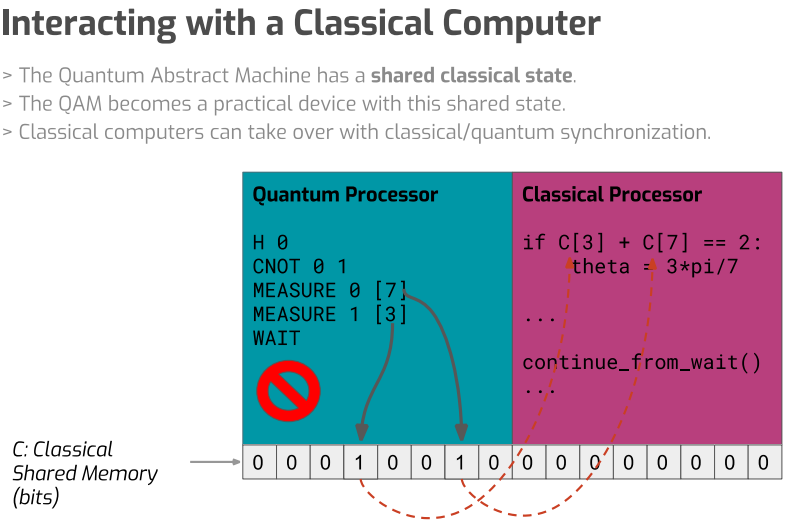


Figure 610: Source: Quantum Cloud Computing by Johannes Otterbach, January 2018 (105 slides).

At the very least, the classical computer is used to control the execution of quantum algorithms, if only to trigger the quantum gates at the right time, sequentially.

Development tool classes

We can identify some major classes of tools for creating quantum software: graphic programming tools, scripting languages, intermediate languages, machine languages, compilers and application libraries.

Graphical programming tools

They allow to visually define the sequence of quantum gates to create algorithms and execute it on quantum accelerators.

These tools can also emulate, run and visualize the status of qubits when their number is reasonable with various methods: Bloch sphere, register state and density matrix.

One example of such tools is the IBM Quantum Experience IBM Composer that is available online since 2016. Code can be executed on an IBM emulator or on one of the many IBM quantum systems available in the cloud, and for free up to 15 operational qubits.

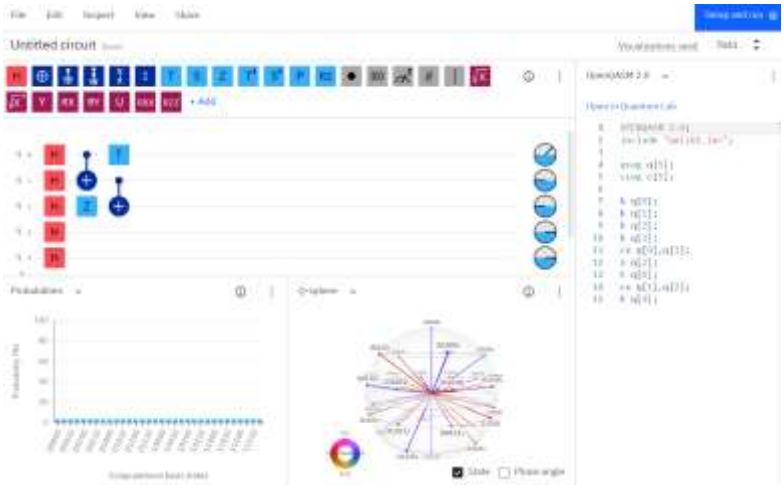


Figure 611: IBM Quantum Experience visual interface. Source : IBM.

There are also graphical simulators of qubits that can be used to understand how to chain quantum gates on a few qubits and visualize the result visually. The most open one is the open source tool Quirk which can simulate up to 16 qubits. It works online and can be downloaded to run on your own computer locally. Below is an example of a quantum Fourier transform performed in Quirk. It was developed by **Craig Gidney**, now a Google engineer specialized in algorithms and error correction codes.

Figure 612: Quirk's visual open sourced quantum programming tool, working in any browser. Source: Quirk Algassert.

Finally, let's pay some attention to **ZX-calculus**, a graphical programming language that uses topological composition rules. It was created in 2008 by Bob Coecke and Ross Duncan[1740]. It visualizes the modifications made to a set of qubits and is based on transformations applicable to the geometric representation of quantum gates that simplify models.

[1740] See Interacting Quantum Observables: Categorical Algebra and Diagrammatics by Bob Coecke and Ross Duncan, 2009 (80 pages).

It is particularly useful for programming a quantum computer in MBQC (measurement base quantum computing) and for visually model error correction codes. It can also help optimize quantum code compiling[1741].

Contributors to the ZX-Calculus work include researchers from Loria under the responsibility of Simon Perdrix, a research laboratory located in Nancy and Dominic Horsman then at UGA LIG in Grenoble and now at Oxford University[1742].

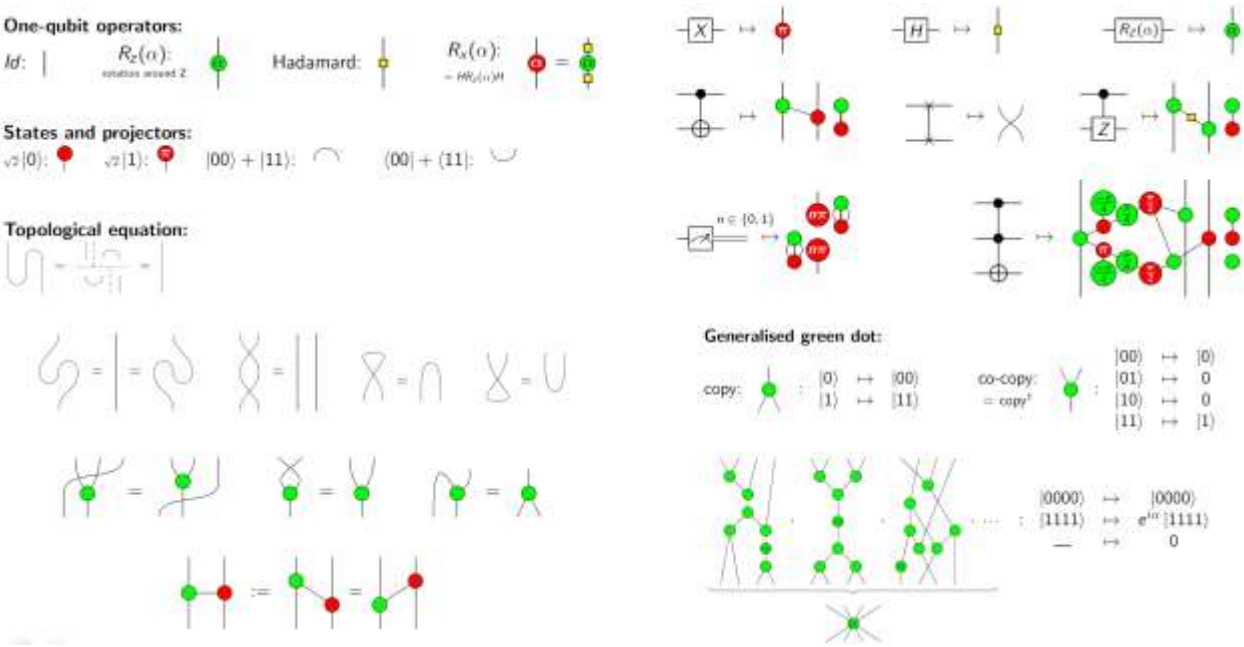


Figure 613: ZX calculus graphical language key operations. Source: Completeness of the ZX-Calculus by Renaud Vilmart, 2018 (123 slides).

ZX has its own zoo of extensions:

- **PyZX** is a Python tool created in 2019 that implements ZX-Calculus principles for the creation, visualization, and automated rewriting of large-scale quantum circuits.
- **SZC-calculus** (Scalable ZX-calculus) is a high-level extension of ZX-calculus for the design and verification of quantum computations with qubits registers. Among other things, it can be used to describe graph states used in MBQC and error correcting codes[1743].
- **ZXH-calculus** is a graphical language based on ZX-calculus helps modelize many-body states[1744].
- **ZW-calculus** is a variant that allows better entanglement modeling and **ZH-calculus** is used for the generalization of MBQC programming models thanks to the addition of a box implementing the Hadamard gate and an easier integration of Toffoli gates in its diagrams. It is associated with a development tool, **Quantomatic**, created by Aleks Kissinger and Vladimir Zamdzhiev then at of Oxford University and now at Inria in France [1745].

[1741] See Effective Compression of Quantum Braided Circuits Aided by ZX-Calculus by Michael Hank et al, November 2020 (13 pages).

[1742] See Completeness of the ZX-Calculus by Renaud Vilmart, 2018 (123 slides) and Completeness of the ZX-Calculus by Emmanuel Jeandel, Simon Perdrix and Renaud Vilmart (73 pages) which explains them.

[1743] See SZX-calculus: Scalable Graphical Quantum Reasoning by Titouan Carette, Dominic Horsman and Simon Perdrix, April 2019 (29 pages).

[1744] See AKLT-states as ZX-diagrams: diagrammatic reasoning for quantum states by Richard D. P. East et al, December 2020 (22 pages).

[1745] See Quantomatic: A Proof Assistant for Diagrammatic Reasoning, 2015 (11 pages).

They organize their own international conference, the **QPL** (Quantum Physics and Logic) but it covers broader topics than ZX calculus.[1746]

- **DisCoPy** (Distributional Compositional Python) is an open source toolbox for computing with string diagrams and functors[1747]. Its diagram data structure allows to encode various kinds of quantum processes, with functors for classical simulation and optimization, as well as compilation and evaluation on quantum hardware. It supports ZX calculus and its variants and linear optical quantum computing. Its photonics module that was under development as of May 2022 will allow to build linear optical circuits and interface with the quantum simulator **Perceval** from Quandela. DisCoPy encodes arbitrary string diagrams and interprets these for computation on various classical (NumPy, JAX, TensorFlow, PyTorch, Sympy) and quantum systems (Perceval, PyZX). DisCoPy is of particular use with quantum natural language processing (QNLP) and quantum machine translation applications[1748].

Scripting languages

They are used to program a quantum algorithm in text mode. These tools allow to associate classical programming with the chaining of quantum functions conditioned by the state of variables in classical memory.

There are two main types of quantum scripting languages: imperative and functional languages:

- **Imperative languages** are procedural programming languages where step-by-step algorithms are described. They include the usual languages such as C, C++, PHP or Java.
- **Functional languages** are used by defining various functions that are called on an ad-hoc basis by the program. The loops (for, while) are replaced by recursive functions and there are no modifiable variables. It uses high-level abstract data types that are manipulated by functions. It creates more concise code.

Many traditional programming languages can be used for imperative or functional programming, especially if they use function pointers or support event-driven logic.

To some extent, JavaScript and jQuery can be used as functional languages via their call-back functions. This is also the case with C++.

With quantum computer vendors such as IBM or Rigetti, two types of languages are sometimes offered: an intermediate language (Quil at Rigetti, openQASM with IBM) and a higher-level language in the form of extensions to the Python programming language (pyQuil at Rigetti, IBM Qiskit). A conversion tool converts the second one into the first one.

The most common programming language used with quantum libraries is Python. It provides language constructs, data types, for-loops code branching, modularity and classes. It can help build repetitive code structures, which would be harder than with graphical circuit design. It can also be used to create automatic testing tools.

[1746] See SZX-calculus: Scalable Graphical Quantum Reasoning by Titouan Carette, Dominic Horsman and Simon Perdrix, April 2019 (29 pages).

[1747] See DisCoPy for the quantum computer scientist by Alexis Toumi et al, CQC and University of Oxford, May 2022 (6 pages). A functor is "*a design pattern inspired by the definition from category theory, that allows for a generic type to apply a function inside without changing the structure of the generic type*" (Wikipedia).

[1748] See Towards Machine Translation with Quantum Computers by Irene Vicente Nieto, 2021 (48 pages).

Table 1: A selection of some quantum programming languages.

Name	Style	Notes
QCL	Imperative	Has classical sublanguage, multiple high-level programming features.
qGCL	Imperative	Emphasis on algorithm derivation and verification.
LanQ	Imperative	Full operational semantics, proven type soundness.
Quipper	Functional	Focus on scalability, plans to include linear types for static checks (currently done at run-time).
QPL	Functional	Statically typed, denotational semantics in terms of CPOs of superoperators.
QML	Functional	Linearly typed, focused on weakening - not contraction. Quantum control and quantum data.
Qumin	Functional	Two sublanguages (untyped and linearly typed). Focus on ease of use and clean, functional style of programming.

Figure 614: imperative and functional quantum programming languages. Source: Qumin, a minimalist quantum programming language, 2017 (34 pages).

Machine languages

These are the lowest level programming languages of the quantum computer, which program the initialization of qubits and drive the physical signals sent to the qubits to implement universal gates and qubit readouts. They are generally specific to each type of quantum computer, or even to each quantum computer. Most quantum algorithms developers never use this type of low-level language.

Compilers

Quantum compilers translate your code into the low-level sequences of qubit electronic controls for the target quantum accelerator expressed in a sort of machine language. It can also integrate quantum error correction codes (QEC). These compilers transform the program gates into universal physical gates operated by the quantum computer and then into control pulses of the qubits.

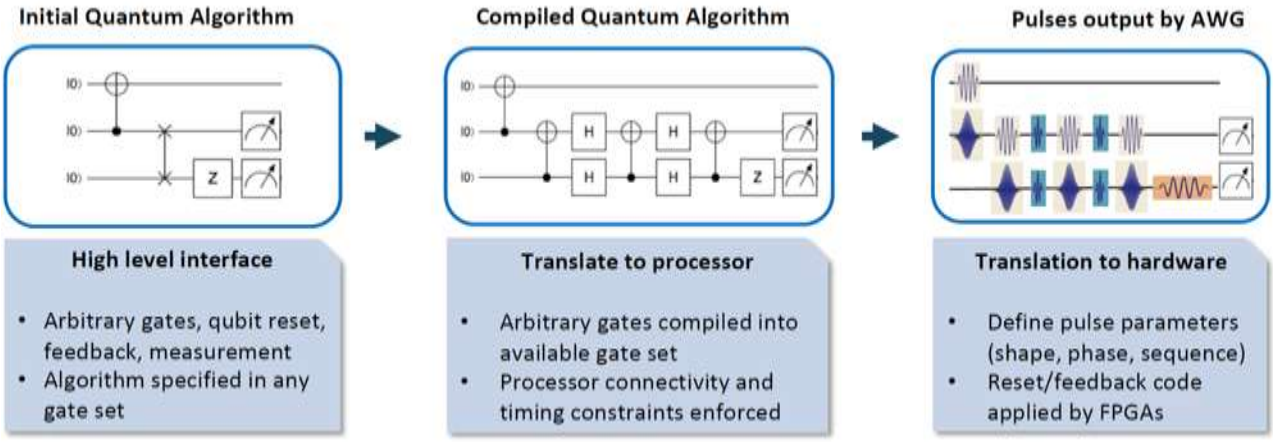


Figure 615: the various roles of a quantum code compiler, first to translate high-level gate codes into primitive gates supported by the quantum processor, and then to turn these gates into low-level electronic controls driving qubit gates and readout. Source: How about quantum computing? by Bert de Jong, June 2019 (47 slides).

It will also compute the gates activation times and verify that the accumulation of these activation times is within the range of the target accelerator's qubits coherence time.

Compilers can also carry out optimizations specific to certain types of algorithms and also hardware specifics[1749]. Many advances can reduce the number of gates used and create shallower circuits. It can be done with qubit mapping which optimizes SWAP insertion techniques that are used heavily when qubits connectivity is poor, like with converting SWAP gates into 3 CNOTs and removing redundant combinations of CNOTs[1750], with optimizing CNOT circuits generation[1751], optimizing the balance between CNOTs and T gates, particularly for fault-tolerant schemes that are very costly with T gates (it's about minimizing the T-count, the number of T gates used in the algorithm or its constituent parts like with quantum Fourier transforms)[1752] and also recycling unused qubits with automated uncompute set of gates[1753]. There are even strategies available to optimize the compilation of a VQE algorithm for NISQ QPUs[1754] and to distribute computing across multiple quantum computers[1755].

Like Atos' aQASM, these compilation tools can be cross-platform and support different gate-based quantum computer architectures. Quantum programming languages are generally able to combine classical procedural programming with quantum registers and gates programming. They allow parallel management of classical memory with quantum registers.

All these programming tools come from either research labs or from quantum computer vendors such as IBM, Rigetti and D-Wave[1756].

Application specific frameworks

On top of scripting languages used to program quantum computers, annealers or simulators sit a wealth of application specific frameworks aimed at solving particular problems. The bulk of these frameworks are proposed by the many software vendors we inventory in a special part of this book, starting page 740. They usually support various underlying hardware architectures from classical digital emulators to QPUs running on-premises or in the cloud, the best ones being able to support heterogeneous classical and quantum platforms for the test and implementation of hybrid algorithms.

[1749] This is the case of Partial Compilation of Variational Algorithms for Noisy Intermediate-Scale Quantum Machines by Pranav Gokhale et al, 2019 (13 pages) which deals with a two-pass compiler optimized for Variational Algorithms (VQE). See also Spacetime tradeoffs when optimizing large quantum computations by Craig Gidney (Google AI Quantum, USA), IQFA 2020, December 2020 (60mn) and slides. He is turning serialized circuits into parallelized ones. With T state distillation, he gains three orders of magnitude in fidelities. At last, see Full-stack quantum computing systems in the NISQ era: algorithm-driven and hardware-aware compilation techniques by Medina Bandic et al, QuTech, April 2022 (6 pages) which summarizes well the full-stack architecture thinking influencing compilers designs.

[1750] See Architecture aware compilation of quantum circuits via lazy synthesis by Simon Martiel and Timothée Goubault de Brugière, Atos, December 2020 (31 pages), Not All SWAPs Have the Same Cost: A Case for Optimization-Aware Qubit Routing by Ji Liu et al, North Carolina State University, May 2022 (17 pages) and See Qubit Mapping Toward Quantum Advantage by Chin-Yi Cheng et al, October 2022 (14 pages).

[1751] And Decoding techniques applied to the compilation of CNOT circuits for NISQ architectures by Timothée Goubault de Brugière, Marc Baboulin, Benoît Valiron, Simon Martiel and Cyril Allouche, January 2022 (31 pages).

[1752] And Gaussian Elimination versus Greedy Methods for the Synthesis of Linear Reversible Circuits by Timothée Goubault de Brugière, Marc Baboulin, Benoît Valiron, Simon Martiel and Cyril Allouche, January 2022 (27 pages) and Reducing the Depth of Linear Reversible Quantum Circuits by Timothée Goubault de Brugière, Marc Baboulin, Benoît Valiron, Simon Martiel and Cyril Allouche, January 2022 (22 pages). On a way to reduce the T-count with a QFT: Halving the cost of quantum Fourier transform by Byeongyong Park et al, July 2022 (19 pages).

[1753] See Recycling qubits in near-term quantum computers by Galit Anikeeva et al, PRA, April2021 (11 pages).

[1754] See Policy Gradient Approach to Compilation of Variational Quantum Circuits by David A. Herrera-Martí, November 2021-September 2022 (17 pages).

[1755] See Qurzon: A Prototype for a Divide and Conquer Based Quantum Compiler by Turbasu Chatterjee et al, November 2021 (11 pages).

[1756] See this presentation which describes some of the tasks performed by quantum compilers: Opportunities and Challenges in Intermediate-Scale Quantum Computing by Fred Chong, 2018 (34 slides).

The most common proposed frameworks cover generic optimization problems (mostly using variational techniques mixing classical and quantum computing like QAOA and VQE/VQA), and others for chemical simulations and financial optimizations, which have been identified as the first go-to-markets for quantum computing so far.

Some application specific frameworks are also proposed by the large vertically integrated quantum computing vendors like IBM (with their Qiskit frameworks). Others can also be proposed by research labs like Q^2 Chemistry which comes from USTC in China[1757].

Emulators

Emulators are software and/or hardware tools that emulate the execution of quantum algorithms on classical computers. Their qubits emulation capacity is closely related to the amount of memory available and the emulation mode that is implemented[1758]. These emulators are also labelled "simulators" or "quantum classical simulators", which is creating some confusion with quantum simulators which are quantum systems simulating quantum physics systems.

Quantum code emulation serves multiple purposes: learning how to code, visualize a quantum algorithm internal data (which can't be done with a real quantum computer), develop quantum algorithms and test them at a low scale. It can also be used to simulate how quantum hardware behaves at a low level, with reproducing digitally their defects like noise and other imperfections. Some emulators are even able to simulate the inner physics of the underlying physical qubits, like Perceval from Quandela (for photon qubits).

The required classical computing capacity grows more or less exponentially with the number of supported qubits. On a laptop equipped with 16 GB of memory, you can simulate about 20 qubits. Specialized server appliances such as Atos' QLM fits in a datacenter rack, are designed to manage a very large amount of memory and can support the emulation of up to 40 qubits. More than 40 qubits can be emulated on massively parallel architectures and supercomputers or on a large number of clusters.

There are various methods for emulating a circuit of N qubits and a certain level of depth of quantum gate sequences which will resonate with what we've learned about registers computational basis and density matrices[1759]. We'll cover some of them from the hardest to the simplest with regards to computational resource requirements.

- **Density matrix** computing which requires $2^N x 2^N$ complex numbers, so 2^{2N+1} floating point numbers. It is the most memory-hungry method and is not used with a large number of qubits. It can be necessary if you need to emulate imperfect qubits with their noise and decoherence and their impact on quantum algorithm's execution.
- **Quantum state vector** which handles the complex amplitudes of all the Hilbert space managed by N qubits in memory. It requires 2^N complex numbers representing 2^{N+1} floating point numbers and 2^{N+5} bytes with double precision floating point numbers using 16 bytes. The action of quantum gates on this large vector consists in applying to it the quantum gates unitary matrices to one, two or three qubits which are respectively made of 2x2, 4x4 or 8x8 complex numbers. This method is implemented on supercomputers with huge memory capacities of the order of several Po. It is currently limited to about 50 qubits.

[1757] See Q^2 Chemistry: A quantum computation platform for quantum chemistry by Yi Fan et al, August 2022 (32 pages).

[1758] See the list of quantum algorithm simulation tools at https://quantiki.org/wiki/list-qc-simulators.

[1759] See Classical Simulation of Intermediate-Size Quantum Circuits, Alibaba, 2018 (12 pages). See also What limits the simulation of quantum computers? by Yiqing Zhou, Edwin Miles Stoudenmire and Xavier Waintal, March 2020 (14 pages) which provides a theoretical and practical framework for the optimization of quantum code emulation. Noteworthy is the work on the emulation of superconducting qubit modules with ... superconducting qubits. See Quantum computer-aided design: digital quantum simulation of quantum processors by Thi Ha Kyaw et al, 2020 (23 pages).

- **Tensor network** compression techniques are used to simplify emulation and ease its distribution across multiple classical computing nodes[1760]. It was used for example in September 2019 by Alibaba on a cluster of 10,000 servers with 96 CPUs. They simulated Google Bristlecone's 70 qubits (which never really run practically) over a depth of 34 quantum gates with 1449 instances of their Cloud Elastic Computing Service (ECS), each comprising 88 Intel Xeon chipsets with 160 GB of memory. So, a total of 127,512 processors[1761]! This method can be implemented with many compression techniques providing a lower accuracy[1762]. It was improved in October 2021, again by Alibaba, to classically simulate the Google Sycamore on the new Sunway supercomputer in 304 seconds[1763]. The chart below from this team shows the extent of tensor network compression capabilities as compared to state vector emulation.

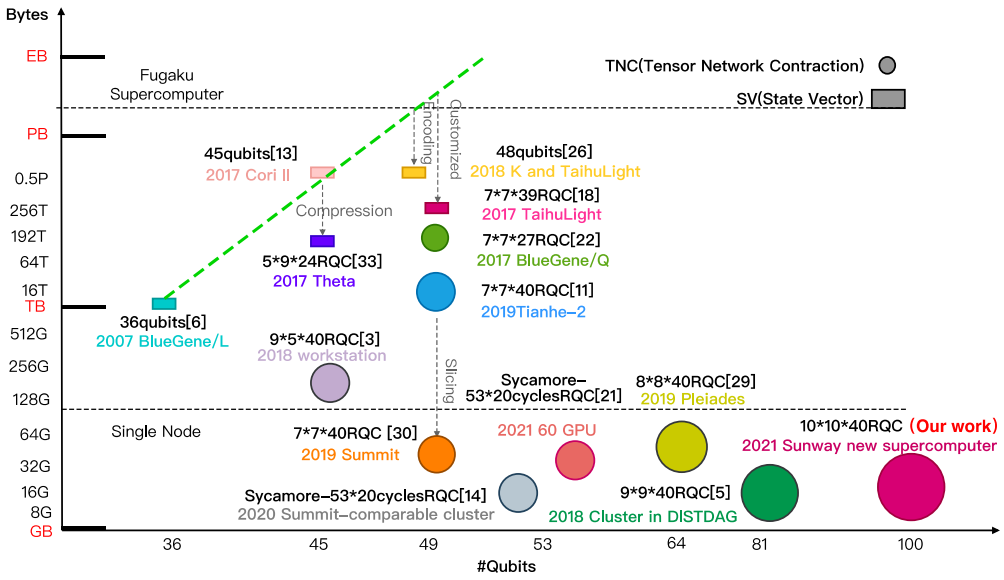


Figure 2: A summary of major classical RQC simulations. The x-axis denotes the number of qubits, while the y-axis shows the corresponding memory space required. The size of the circle/rectangular corresponds to the complexity (depth) of the circuit.

Figure 616: the capacities of various quantum emulators in number of qubits (X) and memory capacity (Y). Source: Closing the "Quantum Supremacy" Gap: Achieving Real-Time Simulation of a Random Quantum Circuit Using a New Sunway Supercomputer by Yong (Alexander) Liu et al, October 2021 (18 pages).

- **Weak simulation** which manages quantum state vector amplitudes without the phase, with 2^N floating point numbers and thus 2^{N+4} bytes, representing output measurement probabilities in the $|0\rangle$ and $|1\rangle$ computational basis[1764]. The method is easier to distribute over several servers. It is however not widely used.

[1760] Partitioning methods for quantum simulation are well described in Distributed Memory Techniques for Classical Simulation of Quantum Circuits, Ryan LaRose of the University of Michigan, June 2018 (11 pages).

[1761] See Alibaba Cloud Quantum Development Platform: Large-Scale Classical Simulation of Quantum Circuits, September 2019 (5 pages).

[1762] See Full-State Quantum Circuit Simulation by Using Data Compression by Xin-Chuan Wu et al, 2020 (29 slides).

[1763] See Closing the "Quantum Supremacy" Gap: Achieving Real-Time Simulation of a Random Quantum Circuit Using a New Sunway Supercomputer by Yong (Alexander) Liu et al, October 2021 (18 pages). The China team behind this was awarded the 2021 ACM Gordon Bell Prize. Their work was later contradicted by ORNL researchers who had developed Google's supremacy classical simulation in 2019. See China's exascale quantum simulation not all it appears by Nicole Hemsoth, NextPlatform, November 2021.

[1764] See Just Like the Real Thing: Fast Weak Simulation of Quantum Computation by Stefan Hillmich et al, July 2020 (6 pages).

- **Hybrid quantum computing emulation** which emulates the quantum part, and executes the classical part as developed in China on a Sunway supercomputer[1765].

The main limitations of supercomputers for emulating quantum algorithms are more related to their memory (RAM) than to their processing capacity. It would take 16 Po of memory to fully simulate 50 qubits. How about 96 qubits? The memory requirement would be multiplied by $2^{46}*2$. Moore's law with memory cannot therefore keep pace with a linear increase in the number of used qubits in a quantum computer.

Nevertheless, the number of emulated qubits on supercomputers is still constantly increasing. China research teams have been the most active in this emulation race, particularly at Alibaba and Huawei, with several records set in 2018 up to 2021.

Origin Quantum, a Chinese multi-role (hardware, software) startup in partnership with the Guang-Can Guo team from the **University of Science and Technology of China**, emulated 64 qubits with a 22-depth algorithm on a cluster of 128 nodes in 2018[1766]. They used a method to transform combinations of CZ gates (conditional Pauli Z gates) and single-qubit gates into simpler sub-circuits that do not need to be interleaved. They also thought they could simulate 72 qubits over a depth of 23 gates on a supercomputer running for 16 hours. This work shows that two key parameters condition the emulation capabilities in classical computers: not only the number of qubits but also the number of quantum gate sequences. The larger the number of qubits emulated, the fewer quantum gate sequences we can simulate.

A second 2018 record coming from **Alibaba** was achieved with 81 qubits and 40 quantum gate sequences[1767]. Their Taizhang simulation exploited a method created by Igor Markov and Shi Yaoyun in 2005 that allows a quantum algorithm to be distributed over a farm of thousands of servers[1768]. The Alibaba Quantum Laboratory is managed by the same Shi Yaoyun, a professor at the University of Michigan. Their simulations included 100 qubits over 35 layers (10x10x35), 121 qubits over 31 layers (11x11x31) and 144 qubits over 27 layers (12x12x27). Another 2018 record came from **Huawei** and its "HiQ Cloud" service, capable of emulating 42 to 169 qubits[1769]. The method was similar to the one used by **Alibaba**. The 42 qubits were simulated in "full amplitude" mode. 81 qubits were simulated with "a single amplitude" and 169 qubits with a single amplitude and a small number of quantum gates. Other records have been broken in the USA in 2019, such as **Google's** record with NASA, the University of Illinois and the Oak Ridge laboratory with 49 to 121 qubits on the IBM Summit[1770].

IBM broke a record of 56 qubits emulation in 2017 on a classic supercomputer of their own, the Vulcan BlueGene installed at the Lawrence Livermore National Laboratory in California. The same Oak Ridge laboratory is at the origin of **XAAC** (eXtreme-scale ACCelerator programming framework), a framework for Eclipse that manages hybrid calculations combining quantum computers and supercomputers such as the Titan equipped with Nvidia GPUs installed in Oak Ridge[1771] .

[1765] See Large-Scale Simulation of Quantum Computational Chemistry on a New Sunway Supercomputer by Honghui Shang et al, July 2022 (13 pages).

[1766] See Researchers successfully simulate a 64-qubit circuit, Science China Press, June 2018.

[1767] See Alibaba Says Its New "Tai Zhang" Is the World's Most Powerful Quantum Circuit Simulator, May 2018 et Alibaba announced that it has developed the world's strongest quantum circuit simulator "Taizhang", May 2018.

[1768] See Simulating quantum computation by contracting tensor networks by Igor Markov et Shi Yaoyun, 2005 (21 pages).

[1769] See Huawei Unveils Quantum Computing Simulation HiQ Cloud Service Platform, October 2018.

[1770] See Establishing the Quantum Supremacy Frontier with a 281 Pflop/s Simulation, May 2019 (11 pages). This Summit must have consumed a good part of the production of Nvidia V100! Here is also the list of qubit and qubit simulation records in https://quantumcomputingreport.com/scorecards/qubit-count/.

[1771] See Eclipse Science and Open Source Software for Quantum Computing, 2017 and the article describing XAAC: A Language and Hardware Independent Approach to Quantum-Classical Computing, July 2018 (15 pages).

It can transform quantum code for computers with quantum gates or quantum annealing models into executable code on any quantum architecture.

Many other IT players want to jump on the quantum emulation bandwagon. It was the case with **Dell** which announced in 2021 its hybrid solution combining classical computing and quantum emulation using its Dell EMC PowerEdge R740xd server appliance and IBM's Qiskit Runtime.

In March 2022, **Fujitsu** created "*the world's fastest quantum computer simulator*" supporting 36 qubits on a cluster system using Fujitsu PrimeHPC FX 700 and the in-house A64FX CPU that powers their supercomputer Fugaku. They run the quantum simulator software **Qulacs** from Kyoto University.

Atos (France) sells since 2017 an Intel-based quantum emulator appliance, the Atos Quantum Learning Machine (QLM).

It's been widely adopted worldwide, such as by the US DoE's ORNL, by the CEA, at the University of Reims, at the cybersecurity research department of the University of Applied Sciences of Upper Austria in Hagenberg, by the Hartree Science and Technology Facility Centre (STFC) in the UK, at the C-DAC (Centre for Development of Advanced Computing) in India, in its Quantum Computing Experience Center[1772], in Japan, in Finland at the CSC IT Center for Science Kvasi in collaboration with IQM, in the new Quantum Integration Centre (QIC) from LRZ (Leibniz Supercomputing Centre) of the Bavarian Academy of Sciences and in Spain (CESGA). A QLM was also sold to CERN in 2021.

Atos is also working with Total to develop quantum solutions to identify new materials and molecules in the energy transition.

In June 2020, Atos launched the QLM E, a new version of this emulator integrating from 2 to 32 Nvidia V100 GPUs, and multiplying computing power by 12 compared to the Intel-based initial version. This system was first delivered in December 2020 to the Irish HPC center (ICHEC). This was completed in early July 2020 with the support of a limited form of quantum annealing emulation.

Figure 617: Atos QLM customers. Source: Atos.

In May 2019, Atos launched myQLM, a quantum programming tools for researchers, students and developers. It is a Python-based development environment that allows users to simulate quantum programs on their own computer. Programming is carried out in AQASM (Atos Quantum Assembly Language) and pyAQSM. To access a number of qubits that exceeds the current capacity of PCs, i.e. more than 20 qubits, developers can run their code on an Atos Quantum Learning Machine simulator in the cloud, but at a charge. Atos also enables the sharing of quantum practices, libraries and application codes. Atos offers one of the open source translators of myQLM code to other quantum programming environments. In September 2020, this software offer became free of charge to all audiences[1773].

[1772] See Atos and C-DAC sign a cooperation agreement to accelerate the development of quantum and exascale computing and Artificial Intelligence in India, August 2019.

[1773] See Atos roadmap in The Atos Quantum Program - Paving the way to quantum-accelerated HPC by Jean-Pierre Panziera, June 2021 (10 slides).

Atos announced in 2020 that they would launch a NISQ quantum accelerator by 2023. They are looking at several tracks such as superconductors (with IQM), trapped ions (with the University of Innsbruck and AQT), cold atoms (with Pasqal) and in the longer-term silicon qubits (with CEA-Leti). They participate in the European Flagship projects **AQTION** (quantum accelerator), **PASQuanS** (analog quantum simulator) and **NEASQC** (NExt ApplicationS of Quantum Computing, which they coordinate).

Atos is also heavily involved in the EuroHPC project, which includes the **European Processor Initiative**, an initiative to develop a processor adapted to the needs of supercomputers and on-board as well as autonomous vehicles[1774]. And, of course, in the $\langle HPC|QS \rangle$ project which will deploy in Finland, Germany and France three hybrid quantum solutions combining a supercomputer and a quantum computer.

Nvidia (USA) developed the cuQuantum SDK running on top of their GPGPUs. It implements gates-based programming emulation, announced in April 2021, beta in November 2021[1775] and released in March 2022[1776].

Thanks to the GPGPU tensors implementing matrix multiplications and fast HBM2E memory, the acceleration provided is clear, making it possible to emulate Google Sycamore processor with a depth of 20 gates in less than 10 minutes[1777]. It is to be supported by various cloud offerings from JUQCS-G (Julich), Qgate (NVAITC), Qiskit-AER (IBM), QuEST (Oxford), SV1 (Amazon Web Services) and Vulcan (QC Ware).

The cuQuantum SDK supports both state-vector emulation with 10s of qubits (**cuStateVec**) and a less resources-hungry tensor-network based emulation (**cuTensorNet**) that supports up to thousands of qubits. They integrated cuStateVec into qsim, Google Quantum AI's state vector simulator that can be used through Cirq. cuStateVec can also be used with Qiskit Aer, IBM's emulation framework.

Nvidia also proposes its quantum compiler **NVQ++** that targets the Quantum Intermediate Representation (QIR), a low-level machine language specification covering hybrid classical/quantum computing needs. It is supported by the Linux Foundation led **QIR Alliance** with contributions from ORNL, Rigetti, Quantinuum, Microsoft and Quantum Circuits Inc[1778].

Nvidia's software tools adopters include QC Ware (for quantum chemistry and QML using cuQuantum on the Nvidia A100-based Lawrence Berkeley National Laboratory Perlmutter supercomputer launched in 2021), ORNL (using cuQuantum in TNQVM, a framework for tensor network quantum circuit simulations), Xanadu (using cuQuantum in their PennyLane framework for QML and quantum chemistry), Classiq (in their Quantum Algorithm Design platform) and Zapata Computing (in Orquestra). Nvidia also works with Google Quantum AI, IBM, IonQ and Pasqal.

[1774] In July 2018, Atos also acquired Syntel for $3.4B in the USA, a $923M service provider specializing in the development and deployment of applications in the cloud with 22,500 employees, created in 1980 by Indo-Americans. This does not seem to have anything to do with quantum.

[1775] See NVIDIA Teams With Google Quantum AI, IBM and Other Leaders to Speed Research in Quantum Computing by Sam Stanwyck, Nvidia, November 2021.

[1776] See Nvidia Unveils Onramp to Hybrid Quantum Computing by Timothy Costa, March 2022.

[1777] See What Is Quantum Computing? by Dion Harris, April 2021 and Nvidia entangled in quantum simulators by Nicole Hemsoth, April 2021.

[1778] See https://github.com/qir-alliance.

In 2022, Pasqal (France) deployed an on-premises Nvidia DGX POD to run digital simulations of its quantum simulator using cuQuantum. In July 2022, Nvidia announced its quantum software emulation and hybrid computing, the Quantum Optimized Device Architecture (**QODA**) platform. It helps develop software that can run on both GPU-based classical emulation and on QPUs, including hybrid quantum/classical solutions.

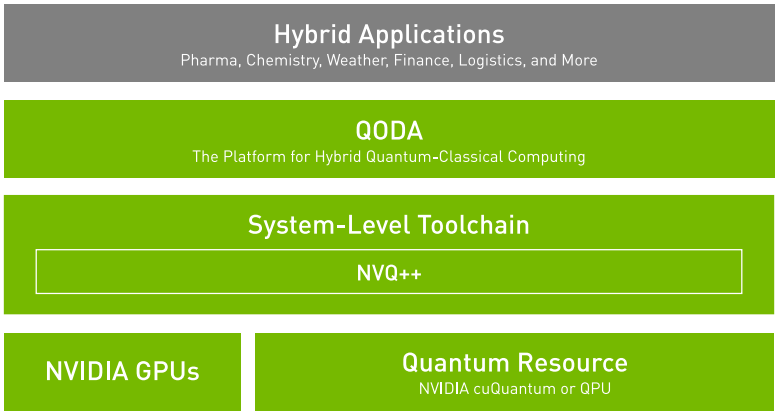


Figure 618: Nvidia QODA architecture. Source: Nvidia.

Beyond the solutions mentioned above, many software emulation tools are available and are mostly always open source [1779]:

Quantum Circuit Simulator runs under Android and was developed in 2013.

Quirk runs in your browser and even on your smartphone. It was developed in 2016 by Craig Gidney before he joined Google in 2017.

Intel IQS (formerly qHiPSTER) created by Intel in 2016[1780]. It supports up to 42 qubits pure states in state vector simulation mode.

SimulaQron from QuTech can run on their **Quantum Inspire** platform with two quantum processors using 2 spin qubits (Spin-2) and 5 superconducting qubits (Starmon-5) and two hardware emulators supporting 26, 31 and 34 qubits.

Psitrum is a software emulator developed in Saudi Arabia in Matlab. It computes the algorithm matrix, the density matrix of the simulated qubit register and the output state vector. It can simulate quantum noise and has a graphical circuit designer. It provides density matrices visualization tools[1781].

QuEST (Quantum Exact Simulation Toolkit) is a quantum emulator developed in C language and supporting QUDA APIs (not CUDA) and Nvidia's GPUs, created in 2017 by Simon Benjamin's Quantum Technology Theory Group from Oxford University and distributed in open source. The system can simulate 26 to 45 qubits depending on the available memory, respectively 2 GB and 256 GB.

myQLM was created by Atos in 2020. It supports the emulation of the three quantum computing paradigms: quantum annealing, quantum simulation and gate-based programming. myQLM is a freely available subset of the full QLM software simulation suite which can work in several modes: perfect state vectors, with using various compression methods (stabilizers, binary decision diagrams, tensor networks MPS), and with simulating qubit noise.

Google's emulator qsim can simulate 30 qubits on a laptop and up to 40 qubits in Google Cloud.

Qiskit Aer is IBM's emulation software solution launched in December 2018. It supports simulations in state vector mode and density matrix mode as well as in the more exotic matrix product state (adapted to weakly entangled states) and stabilizer modes (supporting only Clifford group gates).

[1779] See this long list of emulators.

[1780] qHiPSTER stands for quantum High Performance Software Testing Environment. See qHiPSTER: The Quantum High Performance Software Testing Environment by Mikhail Smelyanskiy et al, 2016 (9 pages).

[1781] See Psitrum: An Open Source Simulator for Universal Quantum Computers by Mohammed Alghadeer et al, Saudi Arabia, March 2022 (27 pages).

staq : another emulator available as a GitHub repository, staq is a modern C++17 library for the synthesis, transformation, optimization and compilation of quantum circuits authored by softwareQ Inc. under the MIT License. It is usable either through the provided binary tools or as a header-only library that can be included to provide direct support for parsing & manipulating circuits written in the OpenQASM circuit description language. Inspired by Clang, staq is designed to manipulate OpenQASM syntax trees directly, rather than through an intermediate representation which makes retrieving the original source code impossible. In particular, OpenQASM circuits can be inspected and transformed (in most cases) without losing the original source structure. This makes staq ideally suited for source-to-source transformations, where only specific changes are desired. Likewise, this allows translations to other common circuit description languages and libraries to closely follow the OpenQASM source.

Qrack is a C++ quantum bit and gate simulator, with the ability to support arbitrary numbers of entangled qubits—up to system limitations. Suitable for embedding in other projects, the Qrack QInterface contains a full and performant collection of standard quantum gates, as well as variations suitable for register operations and arbitrary rotations. The developers of Qrack maintain a fork of the ProjectQ quantum computer compiler which can use Qrack as the simulator, generally. This stack is also compatible with the SimulaQron quantum network simulator. Further, it maintains a QrackProvider for Qiskit. Both ProjectQ and Qiskit integrations for Qrack support the PennyLane stack. For Qiskit, a fork of the Qiskit plugin provides support for a "QrackDevice".

QX Simulator is a universal quantum computer simulator developed at QuTech by Nader Khammassi. The QX allows quantum algorithm designers to simulate the execution of their quantum circuits on a quantum computer. The simulator defines a low-level quantum assembly language namely Quantum Code which allows the users to describe their circuits in a simple textual source code file. The source code file is then used as the input of the simulator which executes its content.

QuIDDPro is a fast, scalable, and easy-to-use computational interface for generic quantum circuit simulation. It supports state vectors, density matrices, and related operations using the Quantum Information Decision Diagram (QuIDD) data structure. Software packages including Matlab, Octave, QCSim, and libquantum, have also been used to simulate quantum circuits. However, unlike these packages, QuIDDPro does not always suffer from the exponential blow-up in size of the matrices required to simulate quantum circuits. As a result, we have found that QuIDDPro is significantly faster and uses significantly less memory as compared to other generic simulation methods for some useful circuits with many more than ten qubits.

LIQUi|> is a software architecture and tool suite for quantum computing. It includes a programming language, optimization and scheduling algorithms, and quantum simulators. LIQUi|> can be used to translate a quantum algorithm written in the form of a high-level program into the low-level machine instructions for a quantum device. LIQUi|> is being developed by the Quantum Architectures and Computation Group (QuArC) at Microsoft Research.

Quantum Programming Studio is a web-based graphical user interface designed to allow users to construct quantum algorithms and obtain results by simulating directly in the browser or by executing on real quantum computers. The circuit can be exported to multiple quantum programming languages/frameworks and can be executed on various simulators and quantum computers.

Quantum Computer Emulator (QCE) is a software tool that emulates various hardware designs of quantum computers. QCE simulates the physical processes that govern the operation of a hardware quantum processor, strictly according to the laws of quantum mechanics. QCE also provides an environment to debug and execute quantum algorithms under realistic experimental conditions. The software consists of a Graphical User Interface (GUI) and the simulator itself.

SimQubit is a GUI quantum circuit simulator, written on top of the Q++ (sourceforge.net/projects/qplusplus) quantum templates. It allows editing of quantum circuits and applying them to quantum states, with multiple ways to view the output probabilities.

Qubit101 simulator is a user-friendly quantum circuit editor and simulator. The tool helps users to create, modify and save the quantum circuits. Along with this, users can simulate its effect over a predefined quantum state, watch the evolution of the state stage by stage, together with the possible measurements results, use other quantum circuits as gates, so complex circuits can be easily created and finally, simulate an almost arbitrary number of qubits. Supported platforms include Rigetti Forest, IBM Qiskit, Google Cirq and TensorFlow Quantum, Microsoft Quantum Development Kit, Amazon Braket and more.

ScaffCC is a compiler and scheduler adapted to the Scaffold programming language supporting the LLVM infrastructure. It supports QASM.

Perceval is a photon qubits emulator and simulator developed by Quandela.

Pulser is a cold atoms emulators developed by Pasqal.

Research-originated quantum development tools

Here is an overview of the main quantum languages created to date, starting with languages that are independent of hardware architectures and that often originate from research laboratories.

They have the disadvantage that they are not generally linked to cloud quantum computer offerings. The related researchers are the equivalents of the Kernighan and Richie (creators of the C language) and Bjarne Stroustrup (creator of C++) in the quantum realm! A good number of these languages come from Europe.

- **QCL** or Quantum Computation Language has a syntax and data types close to those of the C language. This language is one of the first for quantum programming, created in 1998 by the Austrian researcher **Bernhard Ömer** from the Austrian Institute of Technology in Vienna. It is described in Structured Quantum Programming, 2009 (130 pages) which positions very well the conceptual differences between classical and quantum programming languages.

Classical concept	Quantum analogue
classical machine model	hybrid quantum architecture
variables	quantum registers
variable assignments	elementary gates
classical input	quantum measurement
subroutines	operators
argument and return types	quantum data types
local variables	scratch registers
dynamic memory	scratch space management
boolean expressions	quantum conditions
conditional execution	conditional operators
selection	quantum if-statement
conditional loops	quantum forking

Figure 619: classical and quantum programming concepts. Source: Structured Quantum Programming, 2009 (130 pages).

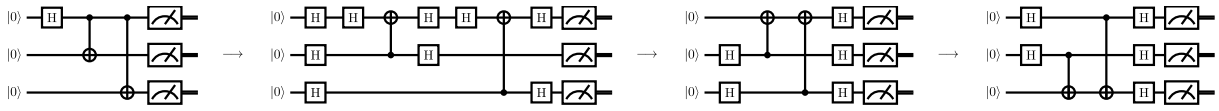
- **Q Language** is an extension of the C++ language that provides classes for programming quantum gates (Hadamard, CNOT, SWAP, QFT for quantum Fourier transform)[1782].
- **QFC** and **QPL** are two functional languages defined by Peter Selinger, from Canada, the first one using a graphical syntax and the second one using a textual syntax[1783].
- **QML** is a functional programming language created by Thorsten Altenkirch and Jonathan Grattage (UK)[1784].

[1782] It is documented in Toward an architecture for quantum programming, 2003 (23 pages), with as co-author, Stefano Bettelli from the Laboratory of Quantum Physics of the Paul Sabatier University of Toulouse.

[1783] They are described in Towards a Quantum Programming Language, 2003 (56 pages).

[1784] See A functional quantum programming language, 2004 (15 pages). The principles are well described in the presentation Functional Quantum Programming, (151 slides).

- **qGCL** or Quantum Guarded Command Language was created by Paolo Zuliani of the University of Newcastle[1785].
- **ProjectQ** is a scripting language from ETH Zurich that takes the form of an open source Python framework, released on GitHub since 2016. It includes a compiler that converts quantum code into C++ language for execution in a quantum simulator with a traditional processor[1786]. Launched in early 2017, it supports IBM's quantum computers via their OpenQASM language, which is normal since ETH Zurich is a partner of the latter, as well as simulation on a traditional computer via a C++ implementation that supports up to 28 qubits. ProjectQ is compatible with OpenFermion from Rigetti and Google.



(a) After decomposing. (b) After CNOT mapping. (c) After optimization. (d) After mapping to hardware.

Figure 5: Individual stages of compiling an entangling operation for the IBM back-end. The high-level Entangle-gate is decomposed into its definition (Hadamard gate on the first qubit, followed by a sequence of controlled NOT gates on all other qubits). Then, the CNOT gates are remapped to satisfy the logical constraint that controlled NOT gates are allowed to act on one qubit only, followed by optimizing and mapping the circuit to the actual hardware.

Figure 620: ProjectQ compiler entangling gates decomposition. Source: ProjectQ: An Open Source Software Framework for Quantum Computing by Damian Steiger, Thomas Häner and Matthias Troyer, 2018 (13 pages).

- **Quipper** is a language created in 2013 that builds on the classic Haskell language, created in 1990, to which it provides extensions in the form of data types and function libraries[1787]. It manipulates a software version of qRAM, an addressable quantum memory register, that is essential for the execution of algorithms such as Grover and QMLs. The language does not seem to have evolved since 2016. One of its creators is Benoît Valiron who teaches quantum programming at CentraleSupelec in France[1788].
- **QWire** is another quantum programming language close to Quipper, launched in 2018, from the University of Pennsylvania [1789]. It is associated with a formal proof solution.

```
bob :: Qubit -> (Bit,Bit) -> Circ Qubit
bob b (x,y) = do
    b <- gate_X b `controlled` y
    b <- gate_Z b `controlled` x
    cdiscard (x,y)
    return b

teleport :: Qubit -> Circ Qubit
teleport q = do
    (a,b) <- bell00
    (x,y) <- alice q a
    b <- bob b (x,y)
    return b

teleport_generic_labeled :: (QData qa) => qa -> Circ qa
teleport_generic_labeled q = do
    comment_with_label "ENTER: bell00" q "q"
    (a,b) <- bell00_generic (qc_false q)
    comment_with_label "ENTER: alice" (a,b) ("a","b")
    (x,y) <- alice_generic q a
    comment_with_label "ENTER: bob" (x,y) ("x","y")
    b <- bob_generic b (x,y)
    return b
```

Figure 621: example of Quipper code. Source: An Introduction to Quantum Programming in Quipper, 2013 (15 pages).

[1785] See Compiling quantum programs, 2005 (39 pages).

[1786] See ProjectQ: An Open Source Software Framework for Quantum Computing by Damian Steiger, Thomas Häner and Matthias Troyer, 2018 (13 pages) which explains how the compiler optimizes the code according to the gates available in the quantum computer.

[1787] It is documented in *An Introduction to Quantum Programming in Quipper, 2013 (15 pages).* Its creation was funded by IARPA.

[1788] See his presentation Programming a Quantum Computer, 2017 (38 slides) and Quantum Computation Model and Programming Paradigm, 2018 (67 slides).

[1789] See QWIRE: A Core Language for Quantum Circuits (13 pages) and A core language for quantum circuits by Jennifer Paykin et al, 2017 (97 slides).

- **Qubiter** is an open source language developed in Python that can be used on top of IBM's OpenQASM and Google's OpenFermion. It was created in 2017.
- **Scaffold** is a language developed at Princeton University[1790]. It is used to program traditional code which is then automatically transformed into quantum gates via its C2QG (Classical code to Quantum Gates) function. In particular, Scaffold can generate QASM. It can be interesting to develop oracles for search algorithms. Figure 622 contains a sample Scaffold code, almost easy to understand! Its development was also funded by IARPA.
- **Qumin** is a minimalist open source quantum language designed in Greece in 2017[1791].

```
// Pauli X, Pauli Y, Pauli Z, Hadamard, S, and T gates
gate X(qreg input[1]);
gate Y(qreg input[1]);
gate Z(qreg input[1]);
gate H(qreg input[1]);
gate S(qreg input[1]);
gate T(qreg input[1]);

// Daggered gates
gate Tdag(qreg input[1]);
gate Sdag(qreg input[1]);

// CNOT gate defined on two 1-qubit registers
gate CNOT(qreg target[1], qreg control[1]);

// Toffoli (CCNOT) gate
gate Toffoli(qreg target[1], qreg control1[1], qreg control2[1]);

// Rotation gates
gate Rz(qreg target[1], float angle);        //Arbitrary Rotation

// Controlled rotation
gate controlledRz(qreg target[1], qubit control[1], float angle);

// One-qubit measurement gates
gate measZ(qreg input[1], bit data);
gate measX(qreg input[1], bit data);

//One-qubit prepare gates: initializes to 0
gate prepZ(qreg input[1]);
gate prepX(qreg input[1]);

//Fredkin (controlled swap) gate
gate fredkin(qreg targ[1], qreg control1[1], qreg control2[1])
```

Figure 622: Scaffold code example. Source: Scaffold: Quantum Programming Language by Ali Javadi Abhari et al, 2012 (43 pages) page 15.

- **Q.js** is a graphical quantum emulator launched in 2019, running in JavaScript and thus running in a browser[1792].
- **QuTiP** (Quantum Toolbox in Python) is another open source quantum code emulation tool developed by Paul Nation of IBM, Robert Johansson of Rakuten and Franco Nori of RIKEN (Japan) and the University of Michigan. The project started in 2011. It targets superconducting qubits.
- **QNET** is a language from Stanford University created in 2012, which allows to simulate the operation of quantum networks.
- Quantum implementation languages of **lambda calculus**, conceptualized by Alonzo Church and Stephen Cole Kleene during the 1930s, followed. This type of computation makes it possible to solve very complex and NP-complete problems, the class of problems that can be verified in polynomial time and whose resolution requires exponential time on classical computers and potentially polynomial time on quantum computers[1793]!
- **OpenQL** is an open source quantum programming language created by TU Delft in 2020. It includes a high-level quantum programming language, its associated quantum compiler and a low-level assembly language, cQASM[1794].
- **eQASM** is an intermediate quantum machine language from Delft University and its subsidiary QuTech. It sits in between high-level programming tools (QASM) and the quantum accelerator. It is a compiled language, hence the "e" for executable. The compiler manages the dependencies with hardware implementation specifics. Tests have been carried out with a 7-qubit superconducting chipset.

[1790] See Scaffold: Quantum Programming Language by Ali Javadi Abhari et al, 2012 (43 pages).

[1791] See Qumin, a minimalist quantum programming language, 2017 (34 pages).

[1792] See Quantum Programming: JavaScript (Q.js) - a drag and drop circuit editor by Stewart, 2020. And https://quantumjavascript.app/.

[1793] See A lambda calculus for quantum computation with classical control by Peter Selinger and Benoît Valiron, 2004 (15 pages).

[1794] See OpenQL : A Portable Quantum Programming Framework for Quantum Accelerators by N. Khammassi et al, 2020 (13 pages).

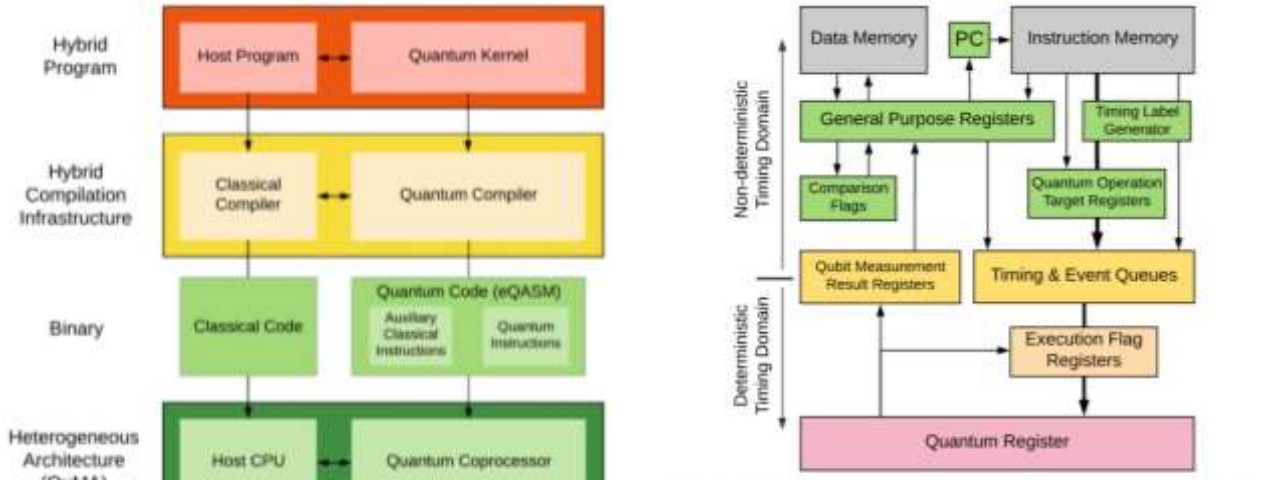


Fig. 1. Heterogeneous quantum programming and compilation model.

Fig. 2. Architectural state of eQASM. Arrows indicates the possible information flow. The thick arrows represent quantum operations, which read information from the modules passed through.

Figure 623: eQASM architecture, from Delft University. Source: eQASM: An Executable Quantum Instruction Set Architecture, March 2019 (14 pages).

- Researchers at the University of Chicago's Enabling Practical-scale Quantum Computation (**EPiQC)** laboratory proposed a compiler that can improve the speed and reliability of quantum computers by a factor of 10. Here again, the compiler has to adapt to the underlying hardware architecture[1795]. Their video explains the process. The team used Google's TensorFlow library to optimize the physical control parameters of the qubits.
- **Silq** is a concise and static quantum programming language proposed by a team from ETH Zurich[1796].
- **Yao.jl** is a package for the Julia language used for creating quantum circuits.
- **Qunity** is a language created in 2022 at the Universities of Maryland and Chicago, and at AWS[1797]. Its goal is to unify quantum and classical programming concepts in a single language. Its syntax uses familiar programming constructs that can have both quantum and classical effects like summing linear operators, using exception handling syntax with projective measurements and using aliasing to induce entanglement. It can also automatically construct reversible subroutines from irreversible quantum algorithms through the uncomputation of "garbage" outputs. It can for example create full quantum oracle functions for algorithms like Grover, Deutsch-Jozsa and Simon. Qunity is still being developed and will be compiled to generate OpenQasm lower level code.
- **MCBeth** is a language created at Yale University and Chicago tailored for MBQC (measurement based quantum computing) programming[1798]. It can represent, program and simulate measurement-based and cluster state computation. Its compiled code can be executed directly on MBQC hardware as well as on traditional gate-based QPUs. This language is based on the initial work by Vincent Danos, Elham Kashefi and Prakash Panangaden in 2007[1799].

[1795] See Research provides speed boost to quantum computers, April 2019.

[1796] See Swiss scientists launch high-level quantum computing language by ETH Zurich, June 2020.

[1797] See Qunity: A Unified Language for Quantum and Classical Computing by Finn Voichick et al, April 2022 (34 pages).

[1798] See MCBeth: A Measurement Based Quantum Programming Language by Aidan Evans et al, April 2022 (27 pages).

[1799] See The measurement calculus by Vincent Danos, Elham Kashefi and Prakash Panangaden, 2007 (46 pages).

- **TWIST** is a language created in 2021 by MIT's CSAIL lab that enforces how qubits are entangled or not, handles the notion of purity (a set of qubits not influenced by others) and enables the creation of safer programs. It introduces μQ, a small functional quantum language. Its creators plan to devise a higher-level abstraction language using TWIST[1800]. Although this project was jointly funded by IBM Research, it remains unclear whether IBM could reuse it in its quantum software toolbox.
- **QIRO** (Quantum Intermediate Representation for Optimization) is a two-dialect language proposal to enable quantum-classical co-optimizations[1801].
- **ScaleQC** is a framework developed by Princeton researchers for hybrid quantum and classical computing[1802].

Most quantum programming software tools are open sourced. Their differentiation is mainly concentrated on documentation and tutorials[1803]. However, in practice, few commercial application developers use the languages discussed in this section. Instead, they are hooked to the languages and toolkits provided by commercial quantum computer vendors listed afterwards. They are easily locked into "full stack" approaches that are proprietary in practice although also open sourced in principle.

The most interesting thing about all this is that many development tools allow us to get our hands on small-scale quantum algorithms before scalable and usable quantum computers are available. And most of them are also open sourced and free to install and use[1804].

Some optimization tools can also be mentioned here like **CutQC** which distributes in an optimized way a large quantum circuit onto several (non-connected) QPUs and classical platforms (CPU or GPU) for co-processing[1805]. It enables using NISQ QPUs at their optimum regime, when a small number of qubits have a sufficient fidelity. Obviously, it doesn't generate an equivalent system to the sum of the qubits of the used QPUs.

[1800] See Twist: Sound Reasoning for Purity and Entanglement in Quantum Programs by Charles Yuan, Christopher McNally and Michael Carbin, January 2022 (32 pages).

[1801] See Enabling Dataflow Optimization for Quantum Programs by David Ittah et al, Microsoft Research and ETH Zurich, January-August 2021 (15 pages).

[1802] See ScaleQC: A Scalable Framework for Hybrid Computation on Quantum and Classical Processors by Wei Tang and Margaret Martonosi, Princeton, July 2022 (12 pages).

[1803] As described in Open-source software in quantum computing, by Mark Fingerhuth, Thomas Babej and Peter Wittek, December 2018 (28 pages). It makes a detailed inventory of these different tools and gauges them against classical open source software features like source code documentation.

[1804] See on this subject the presentations of FOSDEM 2019 conference.

[1805] See Cutting Quantum Circuits to Run on Quantum and Classical Platforms by Wei Tang and Margaret Martonosi, Princeton University, May 2022 (11 pages).

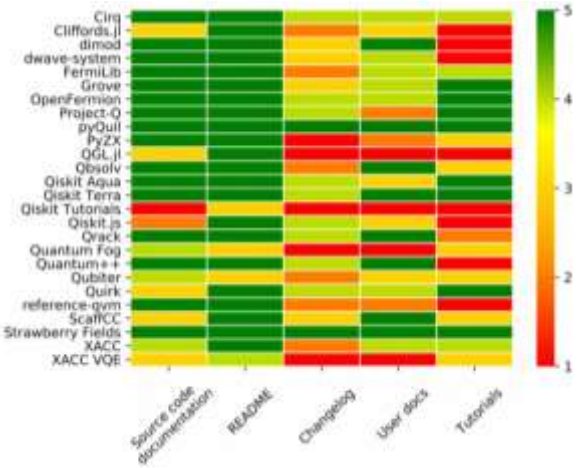


Figure 624: heatmap of various quantum coding tools and their quality figures of merits. Source: Open-source software in quantum computing, by Mark Fingerhuth, Thomas Babej and Peter Wittek, December 2018 (28 pages).

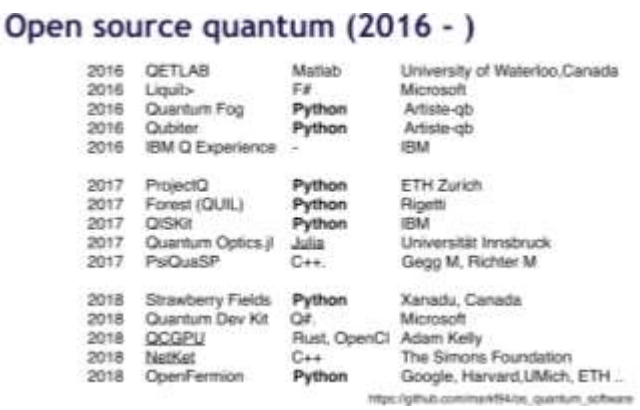


Figure 625: a summary timeline of the appearance of various quantum development tools. Source: Quantum Software Engineering Landscapes and Horizons by Jianjun Zhao, 2020 (31 pages) which provides an excellent overview of development tools covering the entire quantum software creation cycle, including the thorny issues of debugging and testing.

Year	Language	Reference(s)	Semantics	Host Language	Paradigm
1996	Quantum Lambda Calculi	[181]	Denotational	lambda Calculus	Functional
1998	QCL	[206–209]		C	Imperative
2000	qGCL	[241, 312–314]	Operational	Pascal	Imperative
2003	λ_q	[282, 283]	Operational	Lambda Calculus	Functional
2003	Q language	[32, 33]		C++	Imperative
2004	QFC (QPL)	[245–247]	Denotational	Flowchart syntax (Textual syntax)	Functional
2005	QPAlg	[141, 160]		Process calculus	Other
2005	QML	[10, 11, 113]	Denotational	Syntax similar to Haskell	Functional
2004	CQP	[102–104]	Operational	Process calculus	Other
2005	cQPL	[180]	Denotational		Functional
2006	LanQ	[188–191]	Operational	C	Imperative
2008	NDQJava	[298]		Java	Imperative
2009	Cove	[227]		C#	Imperative
2011	QuECT	[48]		Java	Circuit
2012	Scaffold	[1, 138]		C (C++)	Imperative
2013	QuaFL	[162]		Haskell	Functional
2013	Quipper	[114, 115]	Operational	Haskell	Functional
2013	Chisel-Q	[175]		Scala	Imperative, functional
2014	LIQUi|⟩	[292]	Denotational	F#	Functional
2015	Proto-Quipper	[234, 237]		Haskell	Functional
2016	QASM	[212]		Assembly language	Imperative
2016	FJQuantum	[82]		Feather-weight Java	Imperative
2016	ProjectQ	[122, 266, 272]		Python	Imperative, functional
2016	pyQuil (Quil)	[259]		Python	Imperative
2017	Forest	[61, 259]		Python	Declarative
2017	OpenQASM	[66]		Assembly language	Imperative
2017	qPCF	[213, 215]		Lambda calculus	Functional
2017	QWIRE	[217]		Coq proof assistant	Circuit
2017	cQASM	[146]		Assembly language	Imperative
2017	Qiskit	[4, 232]		Python	Imperative, functional
2018	IQu	[214]		Idealized Algol	Imperative
2018	Strawberry Fields	[147, 148]		Python	Imperative, functional
2018	Blackbird	[147, 148]		Python	Imperative, functional
2018	QuantumOptics.jl	[157]		Julia	Imperative
2018	Cirq	[271]		Python	Imperative, functional
2018	Q#	[269]		C#	Imperative
2018	$Q\|SI\rangle$	[174]		.Net language	Imperative
2020	Silq	[35]		Python	Imperative, functional

Figure 626: a timeline of quantum programming tools. Source: Quantum Software Engineering Landscapes and Horizons by Jianjun Zhao, 2020 (31 pages).

Quantum vendors development tools

Even before general-purpose quantum computers are operational on an exploitable scale, the software platforms battle has already begun. The major quantum computing players have almost all adopted an end-to-end vertical integration approach from quantum processors to development tools. This is particularly the case at IBM, Microsoft, Rigetti and D-Wave. This is well illustrated in the chart in Figure 627, which also describes the main development environments for quantum applications from Rigetti and IBM.

The vertical offering of the above-mentioned vendors often integrates a low-level quantum language, then a higher-level language similar to the macro-assembler of traditional computers, then an open sourced framework that can be most often used in Python with ready-to-use functions, a development environment, possibly a quantum gates graphical coding tool, and often some access to their cloud based quantum accelerators and simulators.

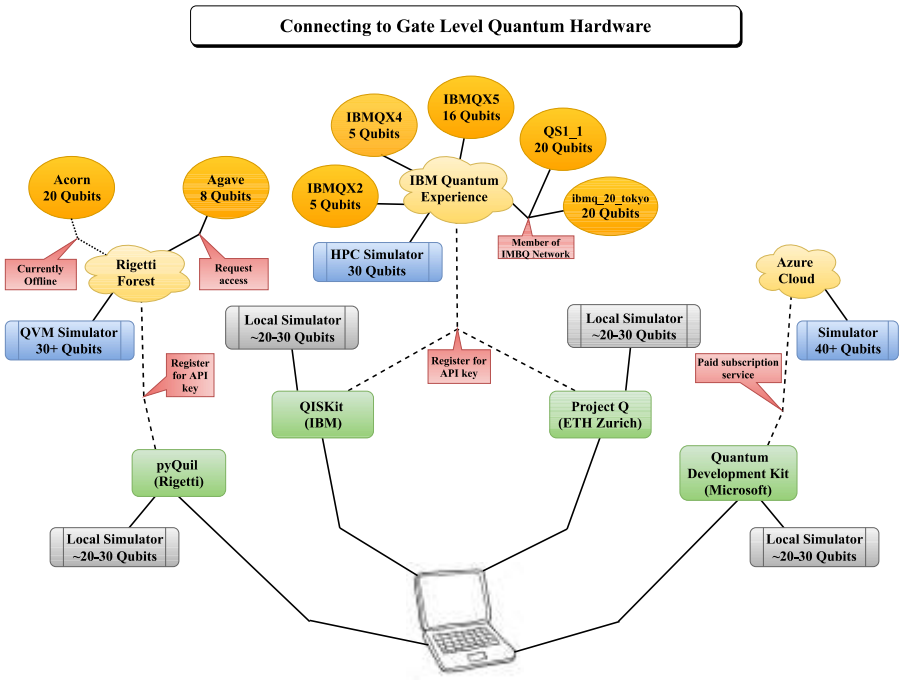


Figure 627: Source: Overview and Comparison of Gate Level Quantum Software Platforms by Ryan LaRose, March 2019 (24 pages).

One remaining tool to invent would be a higher level of abstraction tool to free developers from understanding the intricacies of quantum gates and interferences. Most recent supposed "higher level" languages are classical gate-based programming tools.

Another consolidation of these proprietary - although also open sourced - quantum software development platforms is shown in Figure 628.

	IBM	rigetti	D-Wave	XANADU	Google	Microsoft	aws	Atos
visual programming and integrated development environments	Q Experience	Forest			Quantum Playground	Visual Studio		
thematic quantum libraries (chemisty, finance, machine learning, ...)	QisKit Aqua	OpenFermion	Quadrant, Qsage, ToQ	PENNYLANE	OpenFermion	Quantum Chemisty PNNL	PENNYLANE	QLIB
generic quantum libraries / full-stack	QisKit	Grove QAOA	QUBO qbsolv	STRAWBERRY FIELDS	Cirq	Quantum Developer Kit	Braket SDK	pyAQASM
high level machine language (quantum circuits)	QisKit Terra	pyquil	QMASM			Q#		AQASM
low level machine language	Open QASM	quil	QMI	Blackbird	many machine languages		D-Wave rigetti	Cirq QPU
qubits and quantum gates	super-conducting	super-conducting	quantum annealing	photons	super-conducting	topologic, IonQ, Quantinuum	IONQ OQC	any

Figure 628: the various software stacks from large quantum vendors. (cc) Olivier Ezratty, 2022. Based on a schema found in Quantum Computing languages landscape by Alba Cervera-Lierta of the Quantum World Association, September 2018.

When all software tools are open source, it's not anymore a differentiating factor, or it is when you look at the fine prints. Is the open source software controlled by the vendor or by an independent third party?

Are all software tools really open sourced or just the lower layers with additional proprietary layers? Who are the main contributors to the open source tool? What is the exact open source license used?

D-Wave

D-Wave proposes a complete range of software tools that have evolved a lot since its creation[1806]. The latest iteration of D-Wave's software platform is called **Ocean**. It includes low- and high-level building blocks for the development of quantum applications[1807]. The lowest level language is **QMI**, a kind of machine language for defining the links between the qubits to prepare the related Hamiltonian for an Ising model. QMI is usable from C, C++ Python and even Matlab, via the SAPI (Solver API) interface. Above QMI is a higher level of abstraction tool, **qbsolv**, an open source library launched in 2017.

It allows you to solve optimization problems by converting a QUBO (Quadratic Unconstrained Binary Optimization) problem into an Ising model ready to be processed by a D-Wave or even a classical computer.

Developers can also use the open source **QMASM** (Quantum Macro Assembler) language, which is a low-level language suitable for programming on a D-Wave annealer. It is a third-party tool coming from a D-Wave partner. Like qbsolv, QMASM is used to describe a Hamiltonian made of coupler-based qubit relationships. This method has a drawback: it is preferable to initialize the system in a state close to the search solution and this state can only be determined by classical calculations. It is in any case a very different programming model from the universal quantum gate model, even if there is a theoretical equivalence between quantum annealing and gate-based models as we saw in the previous section.

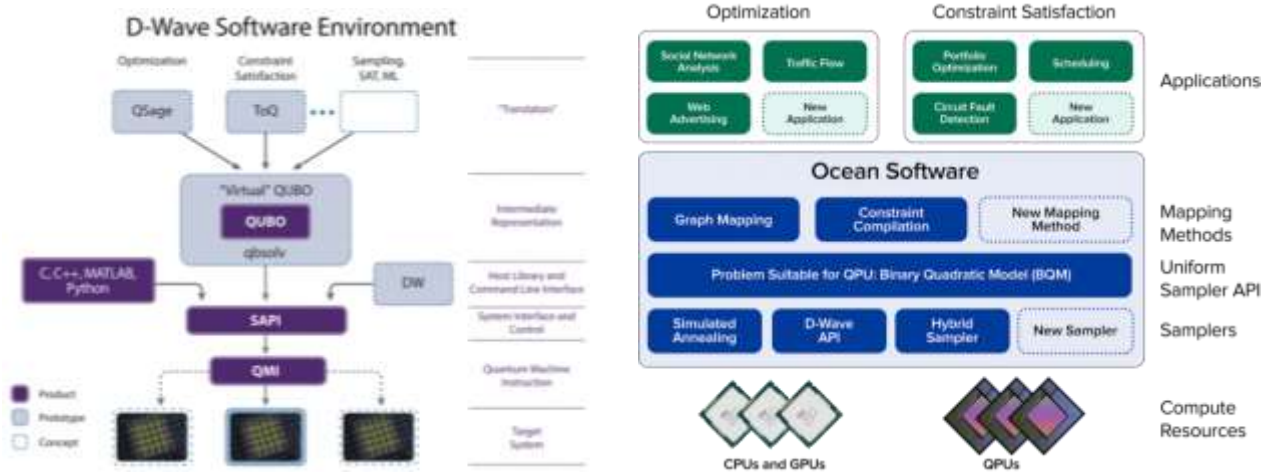


Figure 629: D-Wave's software architecture components around the Ocean platform. Source: D-Wave.

QMASM is also part of **Quadrant**, a comprehensive platform for the development of D-Wave's cloud-based solutions for machine learning launched by D-Wave in 2018[1808].

[1806] The source for the diagram on the left is D-Wave Initiates Open Quantum Software Environment, January 2017. And the one on the right is from: https://www.dwavesys.com/software.

[1807] D-Wave provides a very good document describing the problems that can be solved with their computers: D-Wave Problem - Solving Handbook, October 2018 (114 pages).

[1808] See D-Wave Announces Quadrant Machine Learning Business Unit, May 2018.

The D-Wave Ocean SDK also includes **Hybrid**, an open source framework for creating hybrid algorithms. We can add third party tools such as **QSage**, an optimization problems framework and **ToQ**, another framework for solving constraint satisfaction problems, as well as the SDK from **1Qbit**.

As of spring 2021, D-Wave, its partners and customers had prototyped over 250 algorithms and solutions. They have not necessarily generated any definite quantum advantage, but they do allow customers to learn quantum programming.

D-Wave's offering is mainly offered as a cloud-based resource, under the name **Leap**.

Leap V2 was launched in February 2020[1809].

It includes a new hybrid solver service that can handle optimization problems with up to 10,000 variables and a new interactive development environment using Python.

Prices range from $335 to $3000 per month for access to 10 to 90 minutes of quantum computing time.

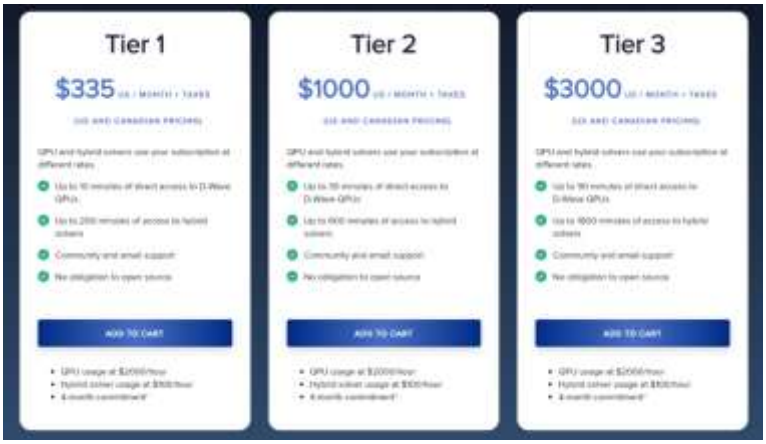


Figure 630: D-Wave's Leap pricing as of 2021.

IBM

IBM's quantum software development platform is built around Qiskit and OpenQASM.

OpenQASM is an open sourced programming language introduced in 2017 that complements IBM's online graphical programming tool Q Experience Composer[1810]. The current version of OpenQASM is v3 and was codeveloped with AWS and the University of Sussex in the UK[1811].

It added support for arbitrary control flow, calling external classical functions, a description of quantum circuits at multiple levels of specificity, and extensions to drive gates timing, modifiers and even pulse control.

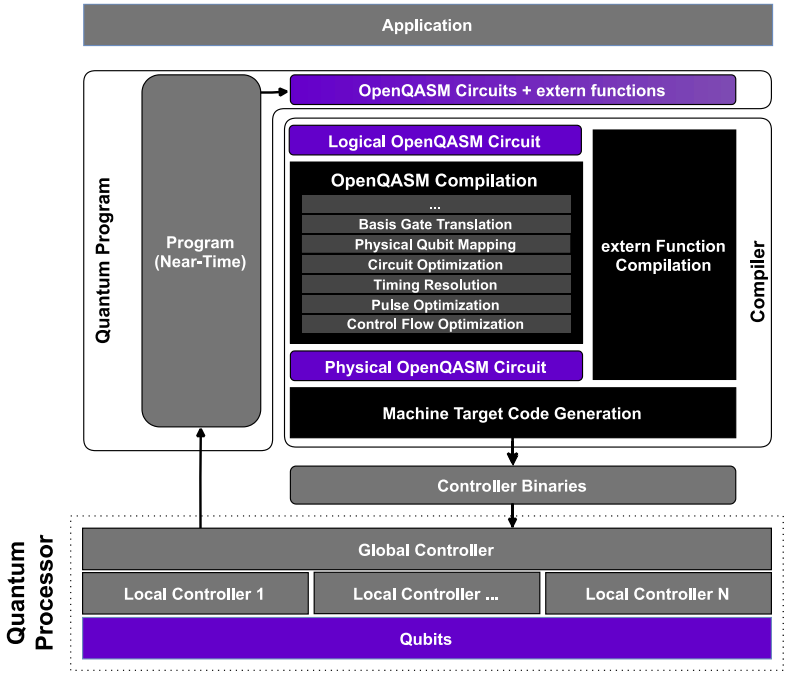


Figure 631: IBM software architecture. Source: IBM.

[1809] See D-Wave announces Leap2, its cloud service for quantum computing applications by Emil Protalinski, February 2020.

[1810] It is specified in Open Quantum Assembly Language, 2017 (24 pages), this document describing the many tasks performed by the associated compiler.

[1811] See OpenQASM 3: A broader and deeper quantum assembly language by Andrew W. Cross, Jay Gambetta et al, March 2022 (60 pages).

Qiskit is a high-level scripting library associated with OpenQASM. It can be used with Python, JavaScript and Swift (a general-purpose language from Apple) and on Windows, Linux and MacOS. It was launched in early 2017 and is also published in open source.

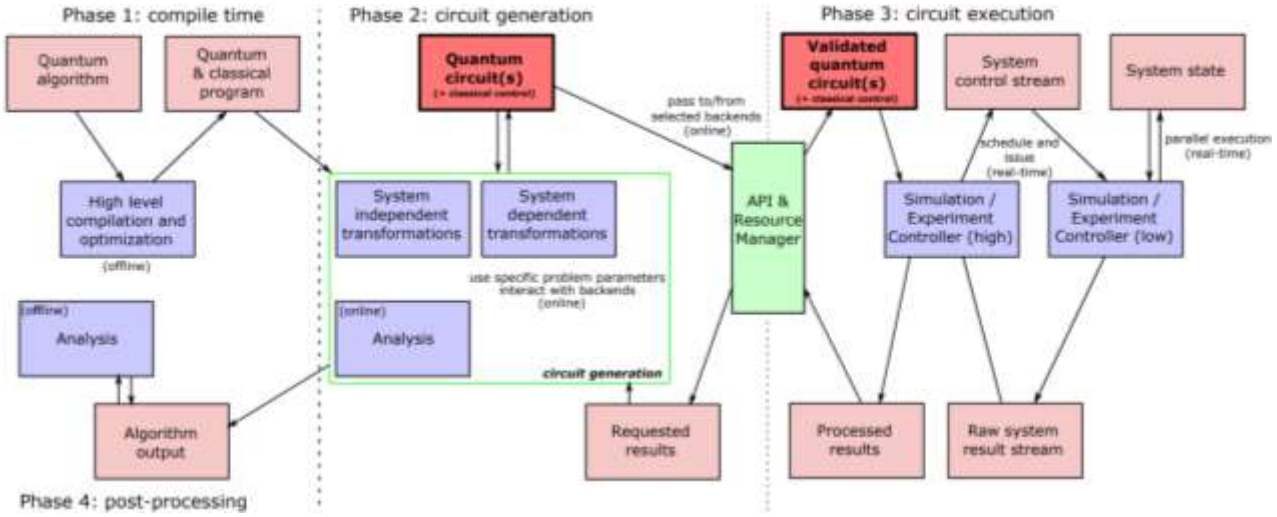


Figure 632: Qiskit block-diagram of processes (blue) and abstractions (red) to transform and execute a quantum algorithm. Source: Open Quantum Assembly Language, 2017 (24 pages).

Qiskit comes with numerous templates and sample codes to exploit a wide range of known quantum algorithms. These can be found in Qiskit documentation and Qiskit textbook on qiskit.org. It includes a graphical circuit-drawing function that generates a graphical visualization of quantum circuits using the open source document composition language LaTeX. Qiskit is or will be supported by other quantum computers vendors such as **IonQ** (USA) and **AQT** (Austria), both with trapped ions qubits, and **ColdQuanta** (USA) with cold atoms.

Qiskit is organized with modules around software building blocks:

- **Qiskit Terra** provides the circuit building and optimization functionalities and manages execution on the different backends like IBM's Qiskit Aer quantum simulator, and QPUs devices from various hardware providers including of course IBM.
- **Qiskit Aqua** is where use cases applications stood. It was deprecated to increase the library portfolio, with more specialized modules like Qiskit Finance, Qiskit Optimization, Qiskit Machine Learning and Qiskit Nature (for chemistry and materials science).
- **Qiskit Metal** is an open source EECAD (Electronic and Electrical Computer-Aided Design) used to design custom superconducting qubits chipsets and simulate their behavior and performance. It was launched in March 2021.
- **Qiskit Cold Atoms** supports quantum simulation models with fermionic modes and spins[1812].
- **Bosonic Qiskit** is a third-party extension which simulate bosonic qubits at the physical level, either purely photon based or in the quantum electrodynamic field, like with cat-qubits [1813].

Quantum code compilation takes place either on IBM's classic cloud-based HPC simulator or on a single quantum computer such as those from IBM that are available in the cloud with 5 and 7 qubits (free access), followed by 16, 27, 65 and 127 qubit versions (charged access) launched between 2019 and 2021.

[1812] See You Can Use Qiskit to Control Cold Atom Systems, May 2022.

[1813] See Bosonic Qiskit by Timothy J Stavenger, Eleanor Crane, Kevin Smith, Christopher T Kang, Steven M Girvin and Nathan Wiebe, DoE PNNL, NIST, Yale University, University of Toronto and University of Washington, September 2022 (8 pages).

The graphical **IBM Quantum Composer**, shown in Figure 634, is used to create quantum code graphically online and run it on a quantum emulator or on the various IBM quantum systems available online. It allows to interact indifferently with the text code on the right or with its graphical version in the middle. It shows vector states after running the code.

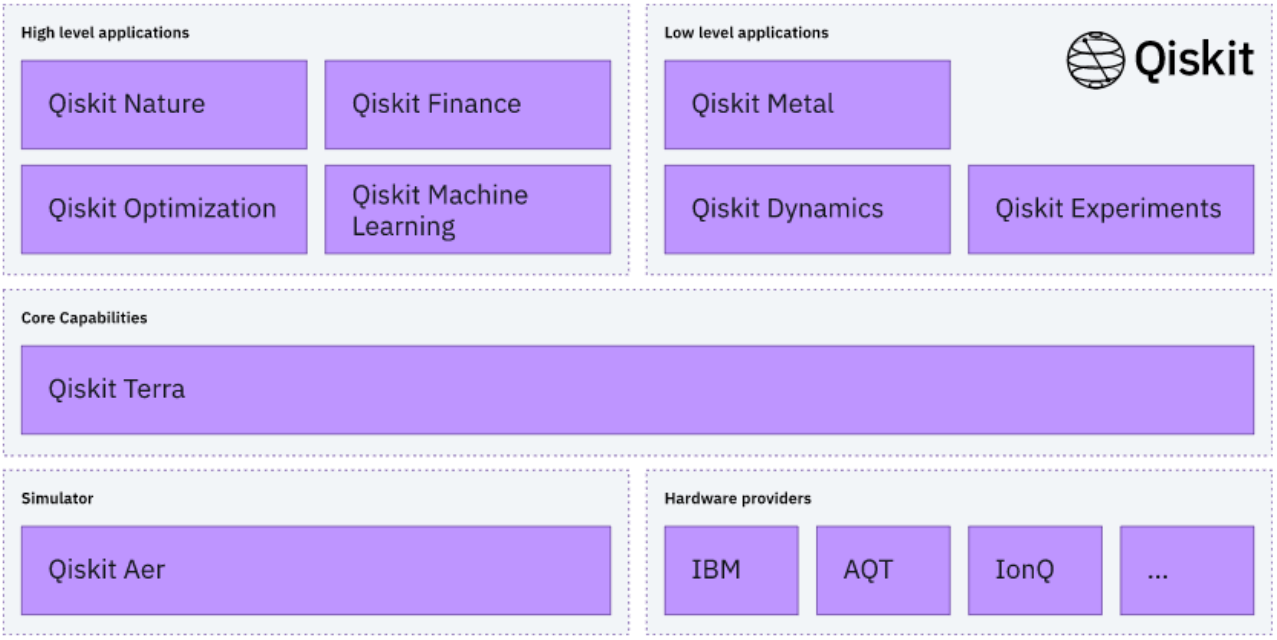


Figure 633. Qiskit components, source qiskit.org.

The 'ibm_qasm_simulator' emulates up to 32 qubits as if it was a real quantum device, including measurement pseudo-randomness, and also supports noise models injection. Circuits can be executed from 1 to 8192 shot(s). The local simulator included in Qiskit does not have this limitation but usually does not run efficiently above circa 15 qubits algorithms.

Figure 634: IBM Quantum Composer, the graphical tool to design your quantum circuit, interacting with the language version on the left. Source: IBM Quantum Experience.

Qiskit Aer also provides access to a 32 qubits state vector simulator, as well as 63, 100, 5000 qubit simulators, with some restrictions on the quantum gate sets. Since the batches are submitted one after the other, on the 9 open devices, and 400000+ registered users, one can wait up a long time, more than one hour for your code to be executed[1814].

Over the years since 2016, IBM has been building a user community, not only within the IBM Quantum Network with over 180 various partners, industry participants, startups and universities accessing premium devices and support, but also with a broad public, particularly students.

[1814] There's a legal caveat in the tool terms of use: *"You may not use IBM Q in any application or situation where failure could lead to death or serious bodily injury of any person, or to severe physical or environmental damage, such as aircraft, motor vehicles or mass transport, nuclear or chemical facilities, life support or medical equipment, or weaponry systems"*. Given that with the few qubits offered, you can wonder how you could risk doing any of these nasty things.

Beyond free access to the quantum devices and simulators, IBM organizes Quantum Challenges, public and free Quantum Global Summer Schools in August since 2020 with two weeks of lectures and workshops, as an online and worldwide event, provides online Qiskit documentation in many languages including Japanese, Spanish, German and French, and online textbooks for learning quantum computing, a Qiskit channel on Youtube with learning content and weekly "seminar series" featuring scientists and technologists of this field. Setting the tone, a mobile application ("Hello Quantum") was launched for learning and playing with qubits and gates, as shown in Figure 635.

Figure 635: Hello Quantum mobile app. Source: IBM.

In February 2021, IBM complemented its hardware roadmap announced in September 2020 with a five-year software roadmap[1815]. Its main item was **Qiskit Runtime** bringing a 120x improvement on the time needed to run variational algorithms (such as VQE, which uses a classical optimizer iteratively with a call to the quantum processor until an exit condition is reached). With Qiskit Runtime both parts are run in the cloud, within the same job submission, avoiding returning to the queue for each iteration.

This x120 improvement can be broken down as follows: x4 from Qiskit itself, then x1.8 for the algorithm, x1.5 for system software, x4.2 with electronics control systems enabling faster readouts and, at last, x2.8 thanks to device fidelities. The rest of the announcement covered the willingness to address vertical markets with partners. They plan to package off-the-shelf libraries for natural science, optimization, machine learning, and finance with partners like **Strangeworks**.

IBM launched in March 2021 a certification program and test for Qiskit developers based on 60-question exam running on the Pearson VUE electronic testing solution[1816]. This is a typical tactic used to build technical communities. It was implemented a long time ago by Novell (Certified Novell Engineers) and Microsoft (Certified Professionals and Most Valuable Professionals programs).

Other software announcements were made in May 2022[1817]. They cover further improvements with Qiskit Runtime thanks to using "dynamic circuits" enabling a reduction of circuit depth and adding "threads", allowing the control of parallelized quantum processors. In 2024 and 2025, IBM will introduce error mitigation and suppression techniques. IBM will also improve Qiskit Runtime Service's primitives and process distribution across classical and quantum processors.

IBM will introduce "Quantum Serverless" in 2023 which transparently allocates classical and quantum processor resources to the developer. It will also enable "circuit knitting" and "entanglement forging", their techniques distributing large quantum circuits onto smaller circuits and reconstructing the results with consolidating their respected results. One of these techniques is "entanglement forging".

It is used to double the size of the quantum systems we could address with the same number of qubits, but it was used just in a particular case for the simulation of a single water molecule on 5 qubits[1818]. And it works only for weakly entangled states, those who do not bring a real exponential speedup!

[1815] See IBM's roadmap for building an open quantum software ecosystem by Karl Wehden, Ismael Faro and Jay Gambetta, February 2021.

[1816] See IBM offers quantum industry's first developer certification by Abe Asfaw, Kallie Ferguson, and James Weaver, IBM, March 2021.

[1817] See Expanding the IBM Quantum roadmap to anticipate the future of quantum-centric supercomputing by Jay Gambetta, May 2022.

[1818] See Scientists double the size of quantum simulations with entanglement forging by Robert Davis, IBM, January 2022 and Doubling the Size of Quantum Simulators by Entanglement Forging by Andrew Eddins, Sarah Sheldon et al, January 2022 (15 pages).

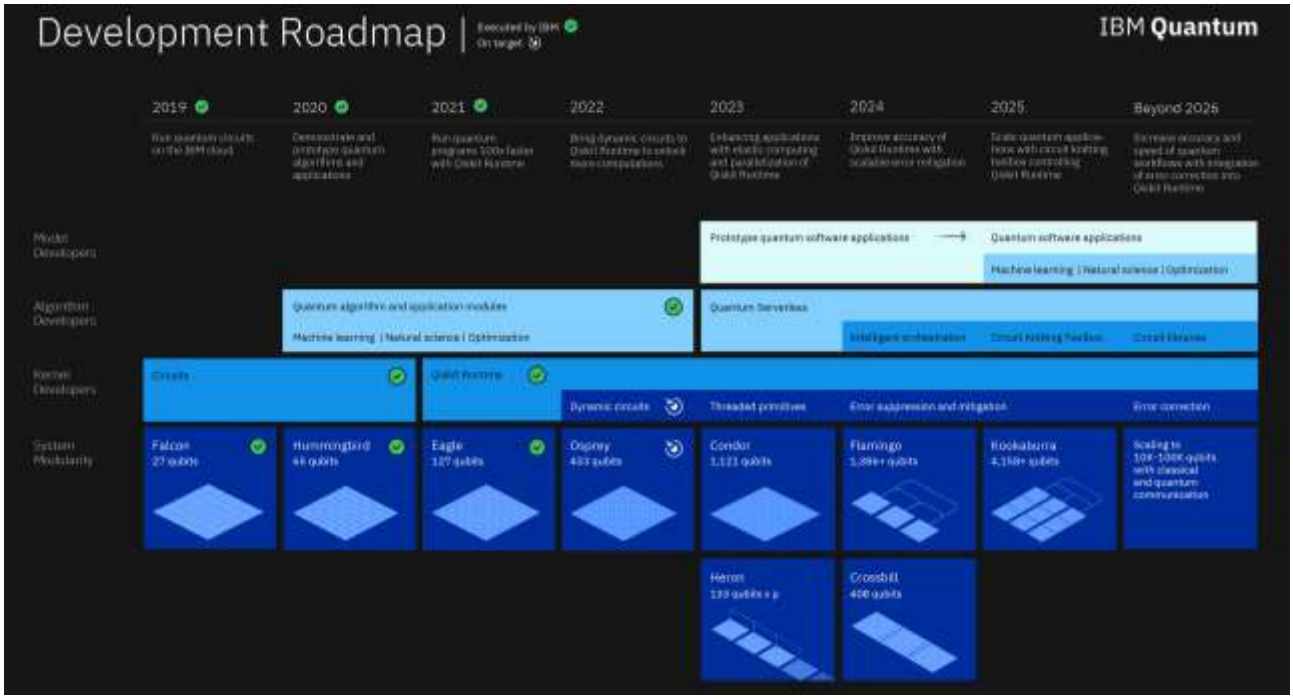


Figure 636: IBM software and hardware roadmap as of May 2022. Source: Expanding the IBM Quantum roadmap to anticipate the future of quantum-centric supercomputing by Jay Gambetta, May 2022.

Rigetti

Rigetti proposes an integrated software development platform with the low-level language **Quil** that supports a mixed classical and quantum memory model[1819]. It runs on Windows, Linux and MacOS. The language uses the gates class to describe operations to be performed on qubits, indexed from 0 to n-1, for n qubits and with quantum gates.

The language allows you to create conditional programming based on the qubits state. It is completed by the open source library **pyQuil** launched in 2017 which includes the Grove library of basic quantum algorithms (documentation). It can be used with the Python programming language. The high level pyQuil (assembler) generates the low-level Quil language (machine code). Figure 638 contains a simple example with a single qubit activated by a Hadamard gate that creates a superposition of |0⟩ and |1⟩ to create a quantum random number generator.

Figure 637: pyQuil language example and the lower level Quil language generated on the right. Source: Rigetti.

Used iteratively in a classical loop, the program can generate a random series of 0s and 1s with a 50% chance of having either one allowing to create a completely random single binary code.

[1819] It is documented in A Practical Quantum Instruction Set Architecture, 2017 (15 pages).

```
# random number generator circuit in pyQuil
from pyquil.quil import Program
import pyquil.gates as gates
from pyquil import api

qprog = Program()
qprog += [gates.H(0),
          gates.MEASURE(0, 0)]

qvm = api.QVMConnection()
print(qvm.run(qprog))
```

Hadamard gate on qubit 1

qubit readout on superposed state

readout output

Listing 2: pyQuil code for a random number generator.

Figure 638: Hadamard gate programmed with pyQuil. Source: Rigetti.

Rigetti offers the execution of quantum programs in its cloud systems and on conventional simulators via its QVMs, for **Quantum Virtual Machines**[1820]. Since 2020, it's also available on Amazon Braket cloud services. It is usable from the **Forest** development environment proposed by Rigetti. These tools are open source, but not cross-platform.

At the end of 2017, Google and Rigetti launched the open source initiative **OpenFermion**.

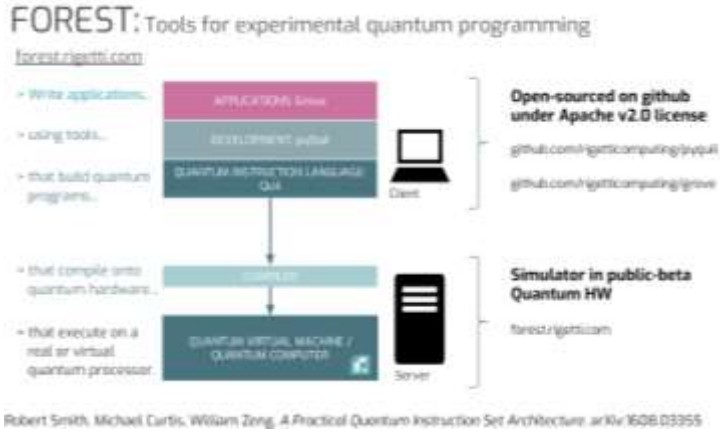


Figure 639: Rigetti Forest software platform. Source: Rigetti.

This framework developed in Python exploits research work from the Universities of Delft and Leiden in the Netherlands. It is a software solution for the creation of quantum algorithms for the simulation of chemical functions supporting any quantum computer, from Universal Quantum Computers to D-Wave annealers.

It complements Atos[1821]. In 2018, Rigetti finally launched a Quantum Algorithm Contest with a $1M prize, but with an interesting bias, comparing the creators of quantum algorithms with others seeking to create equivalents running on conventional computers.

The process could last 3 to 5 years and looks like the XPrize process[1822].

At last, Rigetti is also promoting **Quantum Programming Studio**, a web based interactive programming tool that can run your code on a Rigetti quantum computer in the cloud.

Google

In addition to OpenFermion which is a high-level framework, Google launched on July 19, 2018, its own quantum framework **Cirq**, of course also in open source. It is a Python framework.

[1820] This is documented in pyQuil Documentation, June 2018 (120 pages) which contains many code examples like the one *above*.

[1821] See the announcement in October 2017, OpenFermion: The Electronic Structure Package for Quantum Computers, 2018 (19 pages) and Openfermion documentation.

[1822] See Can You Make A Quantum Computer Live Up To The Hype? Then Rigetti Computing Has $1 Million For You by Alex Knapp, Forbes, October 2018.

Since Google's superconducting Sycamore systems are not available on the cloud, Cirq is mainly used on a cloud simulator provided by Google[1823]. A tool for compiling OpenFermion code in Cirq is also proposed. It also supports IonQ trapped ions qubits that are supported in Google Cloud since 2021. It supports also Pasqal cold atoms systems and Rigetti superconducting qubits.

In March 2020, Google launched **TensorFlow Quantum**, an extension of the famous open source machine and deep learning framework. It provides hybrid classical/quantum computing functions for machine learning[1824]. Of course, the library supports Cirq.

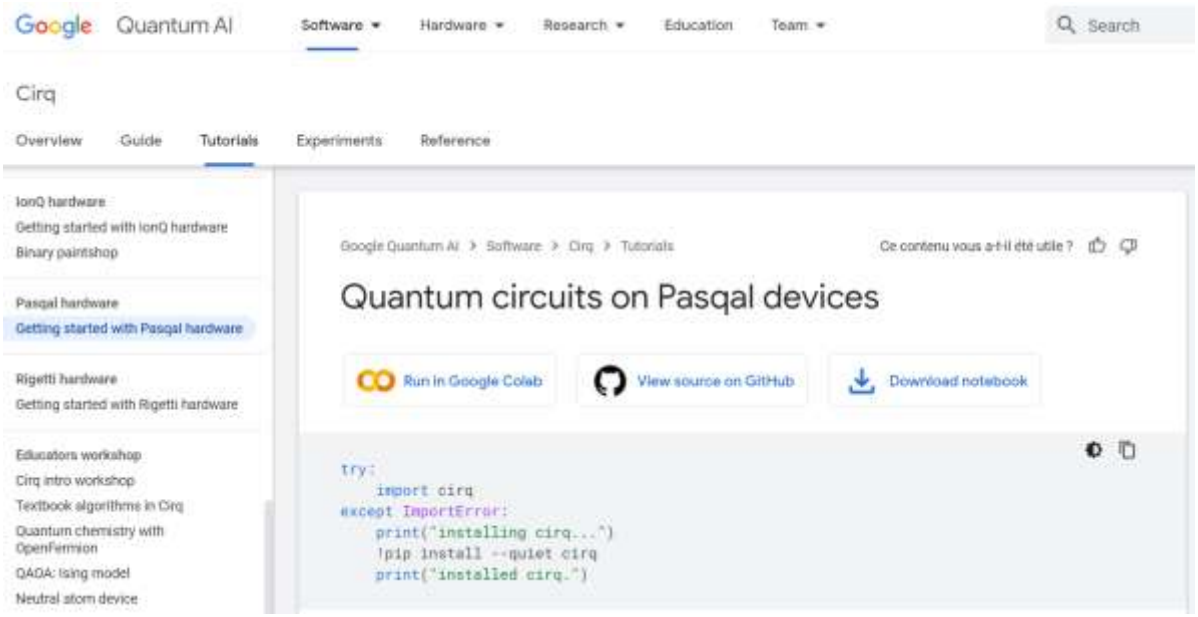


Figure 640: Cirq support Pasqal cold atoms computer circuits. Source: Google Cirq tutorials.

It is adapted to quantum simulators running on classical computers based on CPUs, GPUs and TPUs (Tensor Processing Unit, the specialized AI processors running in Google's data centers).

Eventually, QPUs (Quantum Processing Units) will be supported. Why doesn't Google use its 53-qubit quantum computer? Because it is a research object and not yet a production tool that could be integrated at this stage in a cloud offer. Meanwhile, you can access IonQ trapped ions in Google's cloud!

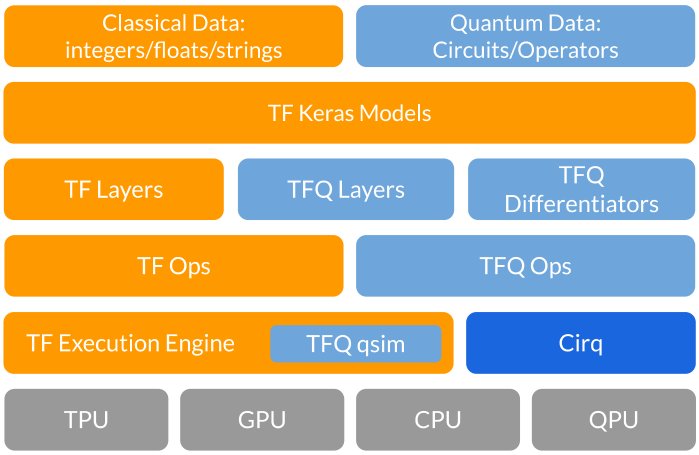


Figure 641: Google's hybrid quantum classical software architecture. Source: TensorFlow Quantum: A Software Framework for Quantum Machine Learning by M Broughton et al, 2020 (39 pages).

[1823] See explanations in Google Cirq and the New World of Quantum Programming by Jesus Rodriguez, July 2018.

[1824] See TensorFlow Quantum: A Software Framework for Quantum Machine Learning by M Broughton et al, 2020 (39 pages, and associated video).

Microsoft

Microsoft's quantum efforts are proposed under the umbrella of Azure Quantum. It embeds various efforts ranging from fundamental hardware research to commercial offerings. Research covers Majorana fermions. Commercial offerings contain a wealth of software development solutions and a cloud offering hosting emulation software and third party quantum hardware vendors QPUs.

Let's try to decompose the Microsoft quantum platform.

Q# language is their cornerstone open source quantum language[1825] given Azure Quantum also supports Qiskit and Circ frameworks. Development is usually done with VScode, a lightweight and extensible integrated development environment. It's using Python as a scripting language which calls various modules developed in various languages including Python.

Quantum Development Kit is a software kit for Q# that support the development cycle and execute quantum code either on quantum hardware or on quantum simulators, all supporting Jupyter Notebooks. The QDK can run on your local computer and run with your preferred interactive development environment (Visual Studio or another). It contains several libraries supporting Hamiltonian (gate-based) simulations, amplitude amplification (for Grover search), phase estimation, arithmetic and quantum error correction codes.

Quantum Katas is an open source project launched in July 2018 that contains examples of quantum Q# code integrated into interactive tutorials[1826]. In December 2018, Microsoft introduced a chemical simulation library co-developed with Pacific Northwest National Labs, an equivalent of OpenFermion, which is co-developed by Rigetti and Google[1827]. The library complements PNNL's NWChem quantum chemistry simulation software package.

QIR (Quantum Intermediate Representation) is an intermediate representation for quantum programs launched in September 2020, serving as a layer between gate-based quantum programming languages like Q# and target quantum computers. It's based on **LLVM** open sourced intermediate language that was created in 2000 at the University of Illinois and is handled by the LLVM Foundation run by Tanya Lattner. It can also be used to run code on an emulator. The support is done with a compiler extension supporting that QIR with Q# but it can support other languages and frameworks like Qiskit. It is used by Azure Quantum to support the various hardware platforms it serves (IonQ, Honeywell, QCI). But it seems, not yet by any other vendor. It became the **QIR Alliance** in November 2021, to promote the adoption of QIR. It is now part of the Linux Foundation. The Alliance founding members are Honeywell, Microsoft, the DoE Oak Ridge National Laboratory, Quantum Circuits Inc. and Rigetti Computing[1828].

[1825] There's a long history behind Q#. Microsoft's first forays in quantum software developments started with the **LIQUi|>** extension of the **F#** scripting language which allowed to simulate quantum programs. In December 2017 was launched **Q#**, using a syntax derived from Microsoft's C# language. See Q#: Enabling scalable quantum computing and development with a high-level domain-specific language, 2018 (11 pages). It involves Alain Sarlette, Anthony Leverrier, Eric Fleury, Hélène Robak and Laurent Massoulie from Inria and Nicolas Delfosse from Microsoft Research.

[1826] See Learn at your own pace with Microsoft Quantum Katas, July 2018.

[1827] See Simulating nature with the new Microsoft Quantum Development Kit chemistry library, December 2018. PNNL is a research laboratory co-funded by the US Department of Energy and operated by the non-profit foundation Battelle Memorial Institute. Battelle operates numerous US laboratories such as Lawrence Livermore National Laboratory, Los Alamos National Laboratory and Oak Ridge National Laboratory.

[1828] See New Quantum Intermediate Representation Alliance Serves as Common Interface for Quantum Computing Development, November 2021.

Quantum simulation is proposed in several fashions, with full state simulation (limited to 30 qubits, operating the full quantum state vector), sparse simulation (sparse matrices and quantum states), a Toffoli simulator limited to X, CNOT and multicontrol X operations) and a noise simulator. They also have a resources estimator that computes the quantum resources necessary to run some quantum code (number of qubits, gates, CNOT, T and R gates, measurements, code depth).

Quantum hardware access is provided in Azure Quantum with an ever increasing breath of QPUs, starting with IonQ, Quantinuum, Rigetti and Pasqal. Access pricing is calculated at the quantum gate level with a different formula for each hardware. A single qubit gate costs $0.00003 and two-qubit gates costing $0.0003 on IonQ systems.

Quantum Inspired software models are also proposed in Azure Quantum. They are implemented classically. It contains various software libraries: Parallel Tempering (sort of digital annealing), Simulated Annealing (stochastic simulation method that mimics annealing), Population Annealing (walker simulation), Quantum Monte Carlo (a quantum-inspired optimization) and Tabu Search (an heuristic search algorithm used to solve QUBO optimization problems).

All that is summarized below in Figure 642 in an outdated slide from 2021. Microsoft has a lot to improve in it marketing of the Azure Quantum Platform.

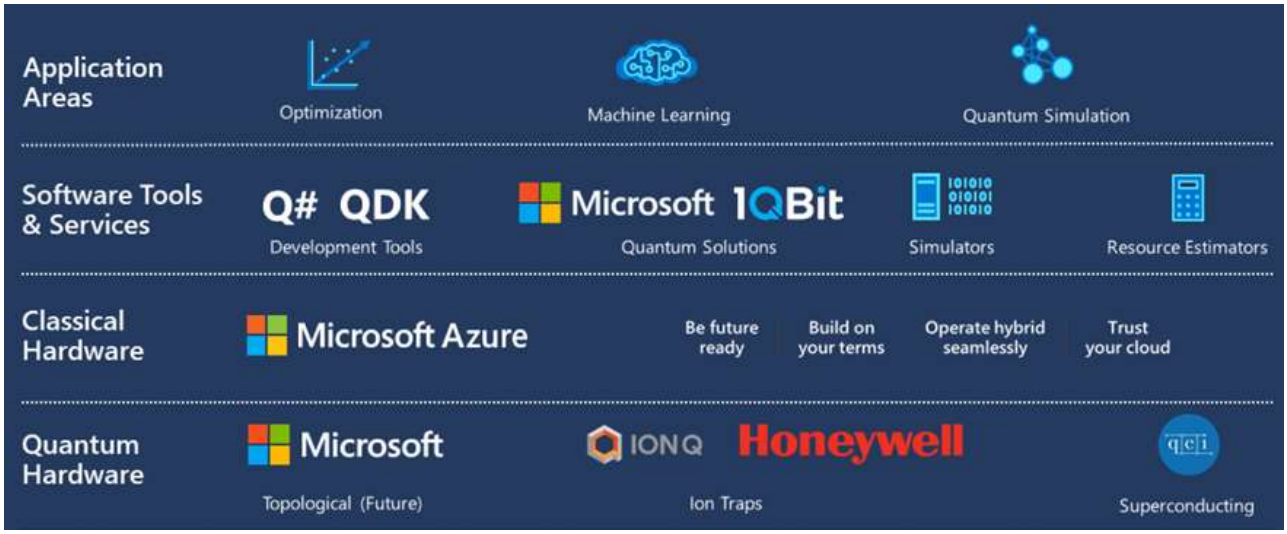


Figure 642: Microsoft Azure Quantum overview. Since then, some new hardware vendors have been added or announced like Rigetti and Pasqal. QCI that is in this slide was announced in 2019 but never delivered a functional QPU. Source: Microsoft, 2021.

Amazon

Amazon's quantum software offering is organized in their Braket platform. It contains both a custom hardware independent development framework as well as the PennyLane framework from Xanadu, and all the tools to submit quantum code to the various AWS supported systems (IonQ, D-Wave, Rigetti and soon OQC) as well as their own classical computing emulators for testing and learning purpose.

IonQ

Like Rigetti, IonQ also has its own "full stack" software offering adapted to their trapped ions quantum computer architecture and proposed in the cloud. It's also offered in Amazon and Microsoft's quantum cloud services.

Intel

At this stage, Intel is not very advanced in the development of quantum software. They have created a quantum emulation software for classical computers, IQS, the first two authors working at Intel and the last one at Harvard. It can simulate up to forty qubits[1829].

Huawei

At the end of 2018, Huawei launched its own quantum application development framework, compatible with ProjectQ, and including a graphical interface for algorithm creation. All this is integrated into their HiQ cloud-based quantum emulation service [1830]. It is provided free of charge for simulating up to 38 qubits. It can also simulate up to 81 qubits with a processing depth of 30 and 169 qubits with a computing depth of 20.

Atos

Atos is not a manufacturer of quantum computers. Their partnerships with various players such as Finland's IQM and France's Pasqal suggest that at some point, they will integrate hybrid solutions mixing their classical server nodes and HPCs and quantum accelerators.

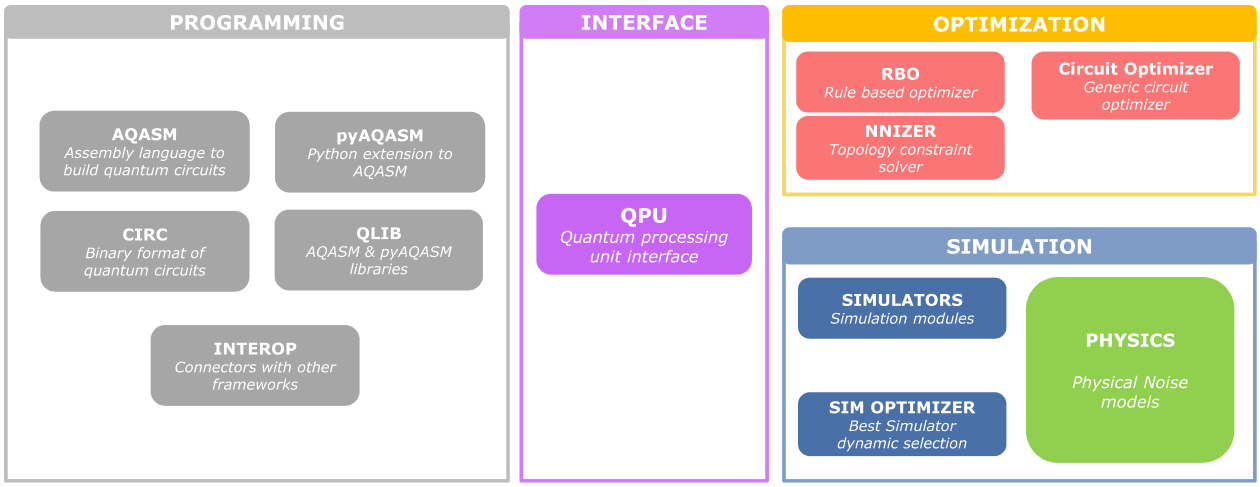


Figure 643: Atos software platform around pyAQSM.

For the time being, they are offering a quantum software emulation solution running on Intel processor machines and with their own optimized memory architecture, QLM.

They simulate 30 to 40 qubits depending on the QLM configuration and are agnostic regarding the physical qubit that are emulated. Since July 2020, they sell QLMe, a faster version of this emulator that runs Nvidia V100s GPUs. They can simulate a system's density matrix to model quantum noise up to 20 qubits.

aQASM (Atos Quantum Assembly Programming Language) is a programming language that complements Python to create quantum algorithms executable on QLM emulator or on any physical quantum computer architecture with universal gates. The language allows to define quantum gates using other quantum gates, equivalents of objects, functions or macros in traditional programming[1831].

[1829] Documented in qHiPSTER: The Quantum High Performance Software Testing Environment by Mikhail Smelyanskiy, Nicolas Sawaya, and Alán Aspuru-Guzik, 2016 (9 pages)

[1830] See Huawei Unveils Quantum Computing Simulation HiQ Cloud Service Platform, October 2018.

[1831] Source of the diagram: Atos QLM, a future-proof approach to quantum computing by Christelle Piechurski, Atos, March 2018 (26 slides).

Their compiler is also very efficient at optimizing code and removing useless combinations of quantum gates due to the addition of many SWAP and CNOT gates in relation to qubits connectivity limitations with their Lazy Synthesis feature[1832]. They can also interoperate with Qiskit, PyQuil and Cirq. A Qiskit code can be used to drive a QLM emulation backend and be used as a QPU by a QLM appliance.

aQASM is based on the OpenQASM standard language. It is completed by the PyAQASM Python library used to generate aQUASM files. The language helps programing the repetitive execution of looped gates and create reusable functions.

The aQASM code compiler generates CIRC binary code that is the low-level pivot language, which is then converted into the control language for specific universal quantum computers or for simulation supercomputers via the Quantum Processing Unit Interface (QPU). It is complemented by various optimization plugins that eliminates useless gates and tunes the generated low-level code for the targeted quantum accelerator hardware architecture.

Atos's QLM now support the three quantum computing paradigms: gate-based control, quantum simulations (with Pasqal) and quantum annealing (with D-Wave). They can classically simulate both noisy and noiseless hardware systems and at a low hardware level they call "below the gate".

At last, myQLM Power Access is a software tool that extends myQLM to submit quantum jobs to a QLM Appliance.

Cloud quantum computing

A large share of quantum computers is intended to be offered through cloud services. It's even got a specific name: **QCaaS** (Quantum Computing as a Service). There are various estimates for the cloud quantum computing market including a very optimistic one of $26B by 2030 by The Quantum Daily[1833].

Let's mention a few of the many technical and economic reasons behind the ineluctable cloudification of quantum computing access. Most quantum computers are relatively expensive devices, costing at least a couple $M. D-Wave systems are sold at a price of about $14M. These are rapidly changing devices with one generation cancelling the previous one nearly each and every year. Also, many quantum algorithms are hybrid in nature, requiring a nearby classical computer, if not an HPC or supercomputer. All of this mandates some mutualization. Making a quantum computer accessible in the cloud requires putting in place a software infrastructure reminiscent of the old mainframe days. Indeed, QPUs are not "multitasking" machines. They are fed by classical computers through a queueing system in "batch mode". The batches first compile the code, execute it several times, usually a couple thousand times, then the result is sent in asynchronous mode to the user[1834]. Cloud quantum solutions usually also provide access to emulation solutions. This can be found at IBM, Microsoft, Google, Alibaba and, Huawei to name a few. If the cloud is to run a hybrid algorithm, it must also provision classical datacenters or HPC resources and synchronize their availability with the related QPU (and right now, we're using only one QPU at a time).

[1832] See Architecture aware compilation of quantum circuits via lazy synthesis by Simon Martiel and Timothée Goubault de Brugière, December 2020 (32 pages).

[1833] See Report: Quantum Computing as a Service Market to Hit $26 Billion by End of Decade by The Quantum Daily, August 2021 and Quantum Computing as a Service Market Sizing - How We Did It by The Quantum Daily, August 2021. These forecasts are fairly inconsistent with other quantum computing forecasts mentioned in this document, page 526, planning a total $2B in 2030.

[1834] See Quantum Computing in the Cloud: Analyzing job and machine characteristics by Gokul Subramanian Ravi et al, University of Chicago and Super.tech, March 2022 (13 pages).

When would customers prefer to purchase a QPU and run it on-premises in their own datacenters? It would make sense when economies of scale are large within the customer or if he handles very sensitive data and processes. The first on-premises installations will probably be deployed for military and intelligence use cases.

The first company to launch a quantum cloud offering was **IBM**, which started to make its first QPUs online in 2016. Is now proposes cloud access to over 24 QPUs with 1 to 127 superconducting qubits as of September 2022. Half of their QPUs with fewer than 15 qubits are accessible for free. **D-Wave** launched its Leap cloud solution in 2018 with its quantum annealers.

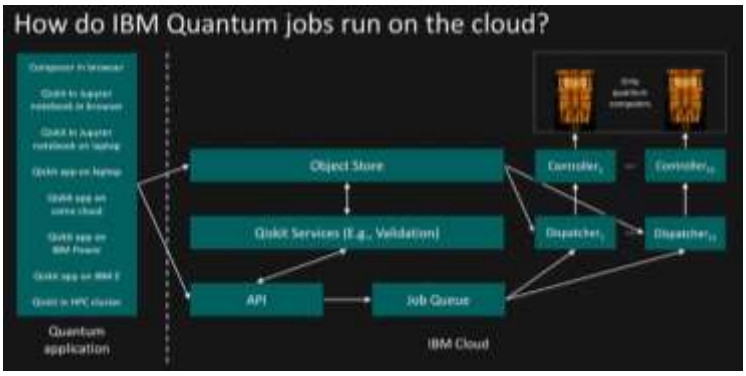


Figure 644: how IBM is running a quantum job in the cloud. Source: IBM.

Rigetti followed with its Cloud Services launched in 2019

Alibaba has a similar offer in China . We are here in the context of vertically integrated offers, the operator of the cloud service being the designer of the quantum computers.

Quantum cloud offering also started to be proposed in 2020 by cloud vendors selling access to third-party quantum computers, mixed with quantum emulation resources on conventional servers. This is what Amazon and Microsoft announced almost simultaneously at the end of 2019 and made available in 2020. Google followed-on in 2021.

Microsoft announced in November 2019 that it was integrating a quantum computing offering into the Azure cloud, and relying on **IonQ** and **Honeywell** (trapped ions qubits) as well as **QCI** (superconducting qubits). As of spring 2022, no QCI QPU was available online, seemingly since their qubits are not yet operational[1835]. **Rigetti** (superconducting qubits) was added to Azure Quantum in December 2021 (in "private previews" as of March 2022) and **Pasqal**'s quantum simulator in May 2022. Microsoft is associated among others with **1QBit** (Canada) to propose quantum software application layers[1836]. They promote quantum inspired algorithms that rely on traditional cloud resources, as in this case study of MRI scanner optimization at Case Western Reserve University[1837]. Microsoft and **KPMG** announced a partnership related to the development of quantum inspired algorithms in December 2022. Microsoft Azure Quantum also supports Qiskit and Cirq Python-based quantum code since October 2021. You can test Azure Quantum for free with a credit of $500 an even win a credit of $10K after submitting your applications. Microsoft is also selling the access to **Toshiba**'s Simulated Quantum Bifurcation Machine+ (SQBM+), a classical Ising model solver using quantum inspired models[1838].

[1835] Microsoft Azure Quantum was introduced step by step: announced in December 2019, released in limited preview in May 2020 and then in public preview in February 2021.

[1836] See Experience quantum impact with Azure Quantum, November 2019 and Microsoft Announces Azure Quantum with Partners IonQ, Honeywell, QCI, and 1QBit by Doug Finke, 2019. At the same time, Microsoft also announced that it has brought together many other quantum software partners: ProteinQure, Entropica Labs, Jij, Multiverse Computing, Qu&Co, QC Ware, OTI, Qubit Engineering, Qulab, QunaSys, Rahko, Riverlane, SolidStateAI, StrangeWorks, Xanadu, Zapata Computing. See the list here : Quantum Network- A community of pioneers by Microsoft, 2019.

[1837] See How the quest for a scalable quantum computer is helping fight cancer by Jennifer Langston, July 2019.

[1838] See Toshiba launches new SQBM+ quantum-inspired optimization provider on Azure Quantum, June 2022.

Amazon made its entrance in the quantum cloud market at the end of 2019 with the announcement of three components: Amazon Braket cloud services, AWS Center for Quantum Computing at Caltech University[1839], and Amazon Quantum Solutions Lab, a customer evangelization program reminiscent of IBM's Q initiative[1840]. Amazon also uses the brand Quantum Compute Cloud (QC2) for its offering. Braket is their whole quantum software infrastructure. It provides access to quantum computers from D-Wave (the 2000Q and Advantage annealers with respectively 2048 qubits and 5000 qubits), IonQ (it started with 11 qubits), Rigetti (16Q Aspen-4 with 16 superconducting qubits and their 31 qubits Aspen-9 version, and later, their 80 qubits system) and OQC (with 8 coaxmon qubits, in 2022). IonQ is thus proposed by both Microsoft and Amazon. Amazon announced in November 2021 that QuEra's cold atoms systems running in quantum simulation mode (*aka* "Hamiltonian simulation") would be added to AWS Braket in 2022. Late 2021, Amazon Braket Hybrid Jobs was added to their software portfolio with the capacity to run hybrid algorithms associating classical and quantum computation[1841]. Amazon also proposes software emulation of quantum algorithms on classical servers.

Amazon Braket is associated with an in-house SDK based on the classic Python language. Development is supported in the integrated open source environment Jupyter. It also includes support for the OCL (Object Constraint Language) constraint programming language. Like Microsoft, Amazon is also a partner of quantum software vendors. We find almost the same players with Xanadu, Zapata Computing , Rahko, QC Ware, 1Qbit and Qsimulate.

Google didn't offer any access to its own quantum computers in its cloud offering. Its Sycamore QPUs are only available to a handful of US Universities in a sort of "private cloud" access. Google still has a digital emulation offering supporting up to 40 qubits. In June 2021, it also announced the integration of IonQ's 11 qubits processor in its Cloud Marketplace. IonQ becomes de-facto the most distributed solution in the cloud with Amazon, Google and Microsoft.

At last, let's mention France's **OVHcloud** who entered the cloud quantum space in May 2022 with announcing that its datacenter was handling the classical part of **Pasqal**'s first entry in the cloud with its 100-qubits cold atoms-based quantum simulator. This is to be extended with the support of other European QPU solutions. They also host Perceval, **Quandela**'s photon qubits classical emulator.

Below is a summary of these cloud-based quantum computing offerings, distinguishing between emulating quantum code on classical computers and executing quantum code on quantum computers.

In China, we can add **Baidu** and its Quantum Leaf cloud offering. It's provided with **Paddle Quantum**, a quantum machine learning development toolkit based on the PaddlePaddle programming language, **QCompute**, a Python-based open source SDK and **Quanlse**, a machine-level programming tools controlling the pulse sent to emulated superconducting qubits.

Other cloud offerings can be mentioned like **Quantum Inspire** in The Netherlands and one from **Xanadu**.

[1839] The AWS Center for Quantum Computing is headed by Brazilian Fernando Brandao (1983), who is both a professor at Caltech and director of this Amazon AWS laboratory. He was previously a researcher at Microsoft Research. He is a good generalist, initially a physicist and now a specialist in quantum algorithms. In June 2020, John Preskill, also a professor at Caltech, announced that he would spend one day a week at the research center.

[1840] See Amazon Braket-Get Started with Quantum Computing by Jeff Barr, December 2019 and the presentation of the announcement Introducing Quantum Computing with AWS by Fernando Brandao and Eric Kessler (video and slides, featuring the Eiffel Tower of Rydberg atoms from French startup Pasqal in slide 15). I discovered in the hundreds of presentations at the Amazon Reinvent conference in December 2019 where this Braket announcement took place that Amazon was also presenting the QLDB, or Quantum Ledger Database, a blockchain management software brick. But that doesn't seem to have anything quantum at all.

[1841] See Introducing Amazon Braket Hybrid Jobs – Set Up, Monitor, and Efficiently Run Hybrid Quantum-Classical Workloads, Amazon, November 2021. See also PennyLane on Braket + Progress Toward Fault-Tolerant Quantum Computing + Tensor Network Simulator by Jeff Barr, December 2020.

Let's finish this with the newly launched hybrid quantum solutions launched by public organizations, mostly in the European Union. These are associating QPUs and supercomputers. The European project **HPC-QS** (for quantum simulation) will be deployed in three sites: in Finland (CSC LUMI), Germany (Munich at the Jülich Supercomputing Centre) and France (Bruyères-le-Châtel at CEA). It will start with attaching an Atos QLM appliance to these sites' supercomputers, themselves all running classical CPUs and GPGPUs from Nvidia.

Figure 645: main quantum cloud emulation and QPU offerings worldwide. (cc) Olivier Ezratty, 2022.

Then, in 2023, they will be completed by a European QPU. Atos's QLM will both run quantum code emulation in the three paradigms (annealing, simulations, gates) and drive QPUs quantum code execution. In Germany and France, the first installed QPUs will be quantum simulators from Pasqal. In Finland, it will probably be superconducting qubits systems from IQM. In Germany, an IQM system will also be deployed with an Atos QLM at the Leibniz Supercomputing-LRZ center, as part of the project Q-EXA. These hybrid computing centers will mainly serve the needs of researchers and large companies.

Quantum software engineering

Certification and verification

The verification and certification of quantum algorithms and the results of their use is an important new topic. The factorization of integer numbers is obviously easy to verify. But when a quantum algorithm is used to simulate physical interactions such as those of atoms in molecules, it is less obvious.

Theoretical work shows that it is possible to prove polynomially that a result of a quantum algorithm is accurate[1842]. Unfortunately, we cannot explain in detail the origin of the result by breaking it down.

[1842] See How to Verify a Quantum Computation by Anne Broadbent, 2016 (37 pages) which demonstrates that all quantum algorithm results can be verified with classical polynomial algorithms by performing several tests and encrypting the input data. See also Verification of quantum computation: An overview of existing approaches by Alexandru Gheorghiu, Theodoros Kapourniotis and Elham Kashefi, 2018 (65 pages).

Nor can we prove that the result found, however valid it may be, is the best of all if there are several good ones[1843]. On top of that, we must make a distinction between error corrected hardware (LSQ) and noisy systems (NISQ). Surprisingly, while LSQ regimes will be inaccessible to classical hardware emulation and make verification difficult, verification is also complicated for noisy systems, particularly when they repeat some sequence of code iteratively.

The other key point is to make sure, in the case of the use of a remote quantum computer, that the recovered result corresponds to the submitted calculation and that an intruder did not interfere in the history nor was able to alter the calculation on the quantum computer side. Many research inroads have been made in the last 15 years for that respect.

One of the methods consists in relying on the concept of **blind computing** devised in 2009 by Anne Broadbent, Joseph. Fitzsimons and Elham Kashefi[1844].

CEA LIST announced in June 2020 that it had created **QBRICKS**, an environment for the specification, programming and formal verification of quantum algorithms. They used to do this for critical embedded systems where certification by formal proof is particularly important. They are now entering the field of quantum programming and have experimented their model with QPE, the quantum phase algorithm (QPE= that fits into Shor's model for integer factorization, the full Shor algorithm and Grover's algorithm. This work involves the joint LRI laboratory at the University of Paris-Saclay and CentraleSupelec[1845].

One of the major advances in the explicability of quantum algorithms comes from researcher **Urmila Mahadev,** whose work between 2012 and 2018 has led to the creation of a method for verifying quantum computer processing. She was a postdoc at Berkeley and supported by Scott Aaronson and Umesh Vazirani, two eminent researchers in quantum algorithmic research. Her work aims at proving that a quantum computer has indeed performed the treatments it has been asked to do. She shows that a classical computer coupled to a simple quantum computer can verify in a polynomial way the results of a quantum computer[1846] . The method exploits a technique of post-quantum cryptography that the verifier cannot break (LWE: Learning With Errors). LWEs are part of the Lattice-based cryptography (EN) or Euclidean networks (FR) class[1847]. The method was recently improved by an Austria team to work with an untrusted quantum computer[1848].

Other quantum programs verifiers[1849] from research laboratories include the **Path-sum** framework from the University of Waterloo[1850], **VOQC** (Verified Optimizer for Quantum Circuits) from the

---

[1843] See also Quantum cloud computing with self-check by Rainer Blatt et al, May 2019, which discusses quantum simulation calculations on 20 qubits of trapped ions with results controlled on the quantum computer as fast as on the PC.

[1844] See Universal blind quantum computation by Anne Broadbent, Joseph Fitzsimons and Elham Kashefi, 2008 (20 pages) and the associated presentation (25 slides) and A Framework for Verifiable Blind Quantum Computation by Theodoros Kapourniotis, Harold Ollivier, Elham Kashefi et al, June 2022 (33 pages) which shows a mathematical link between code verification and error correction.

[1845] See Toward certified quantum programming by Sébastien Bardin, François Bobot, Valentin Perelle, Christophe Chareton and Benoît Valiron, 2018 (4 pages) and An Automated Deductive Verification Framework for Circuit-building Quantum Programs by Christophe Chareton, Sébastien Bardin, François Bobot, Valentin Perrelle and Benoît Valiron, 2021 (30 pages).

[1846] See a description of the method in near-natural language in Graduate Student Solves Quantum Verification Problem, October 2018 and two reference publications: Classical Verification of Quantum Computations, September 2018 (53 pages) and Interactive Proofs For Quantum Computations, April 2017 (75 pages).

[1847] See this presentation describing the LWE protocol: An Introduction to the Learning with Errors Problem in 3 Hours (76 slides).

[1848] See Towards experimental classical verification of quantum computation by Roman Stricker et al, AQT and Innsbruck University, March 2022 (19 pages).

[1849] See the review paper Formal Methods for Quantum Programs: A Survey by Christophe Chareton, Sebastien Bardin, Dongho Lee, Benoit Valiron, Renaud Vilmart and Zhaowei Xu, September 2021 (66 pages).

[1850] See Towards Large-scale Functional Verification of Universal Quantum Circuits by Matthew Amy, University of Waterloo, 2018 (21 pages).

University of Maryland, itself based on **SQIR** (Small Quantum Intermediate Representation) supporting verification[1851] and QHL from Tsinghua University[1852].

Debugging

Like any computer software, quantum software requires a set of quality control processes. Like most human-originated creations, they are prone to bugs and errors. Some classical computing methods can be reused for this respect but many require some adaptation to the specifics of quantum computing, whether done on gate-based systems or on analog quantum simulators.

A quantum circuit is not easy to debug! It will certainly require new debugging tools and approaches. And a majority of quantum code bugs are "quantum" in nature and not easy to spot with traditional methods[1853].

For the moment, simple circuits can be analyzed and debugged with a quantum emulator running on a classical computer, to understand how the qubit register vector state evolves step-by-step. But when quantum circuits in the advantage regime, beyond any classical emulation capacity, other means will have to be used.

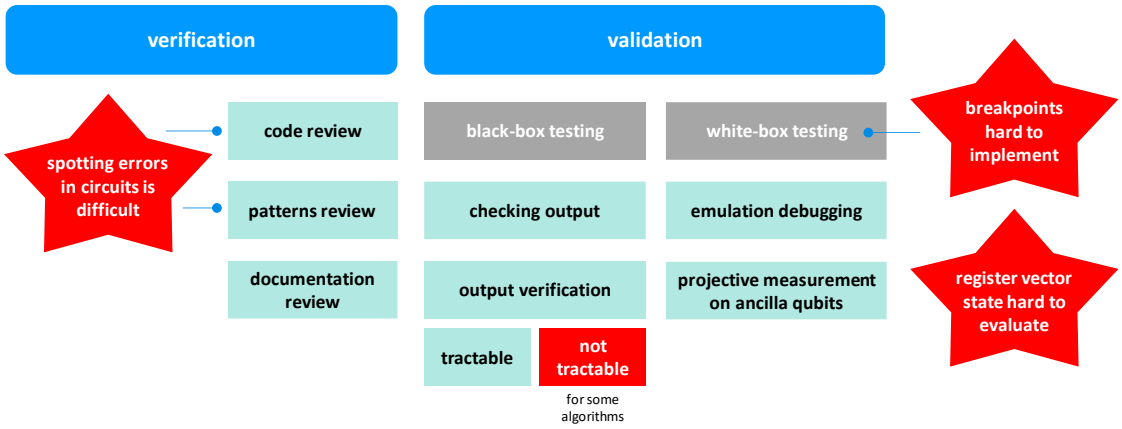


Figure 646: some of the challenges with quantum software engineering. (cc) Olivier Ezratty, 2022.

Software quality control usually goes through two main steps: verification and validation.

Verification deals with verifying that the code will run as expected. It includes checking code documentation, designs, circuits and the various software components or patterns that are used. Verification also deals with making sure that the specifications are correctly implemented by the system. It responds to the question: are we building the product right?

In classical programming, good programmers and code reviewers can spot an error with just looking at the code. Code inspection tools can also detect undeclared variables or variables used in the wrong context. These errors are way more difficult to detect visually on a quantum circuit, particularly with large ones. It may require the use of code decomposition in modules or patterns, like in object-oriented programming.

Validation concerns the program output and making sure it works as planned. It includes testing and validating the code against the user's needs. It responds to the question: are we building the right product?

[1851] See A Verified Optimizer for Quantum Circuits by Kesha Hietala et al, University of Maryland (36 pages).

[1852] See Quantum Hoare logic with classical variables by Yuan Feng et al, University of Technology Sydney, Australia, Chinese Academy of Sciences and Tsinghua University, China, April 2021 (44 pages).

[1853] As studied in A Comprehensive Study of Bug Fixes in Quantum Programs by Junjie Luo et al, January 2022 (8 pages).

Quantum computing results validation is usually fast like with integer factoring (it requires a simple classical multiplication) or a Grover search (it requires checking the Oracle once in a classical way).

But some circuit validations may need to be done on a quantum computer, like with a boson sampling or with a QMA prover (Quantum-Merlin-Arthur). On top of that, contrarily to classical computers, quantum computations errors can also come from hardware imperfections and the fateful quantum noise[1854]. Compiler, code optimizers and even error correction codes can also generate software bugs and amplify some errors.

Quantum software bugs can have various sources: errors in the data preparation (which is itself based on quantum gates), incorrect operations and transformations, incorrect compositions and iterations and also incorrect qubits deallocations (or "uncomputations").

During validation, testing use the white-box and black-box approaches. **White box** testing tests internal data structures and program flow, and may include some interactive debugging.

One solution is to decompose manually or automatically the quantum code into accumulated slices of code with its incremental different parts like data preparation, oracle execution and amplitude amplifications in the case of a Grover algorithm, as pictured below. The debugging tool with run each accumulated slice followed by a measurement one after the other[1855]. It's not a classical pause-play like in classical interpreters like JavaScript but "pause" and "play again from the start", a probably with several shots being run and their results averaged to get a sampled output.

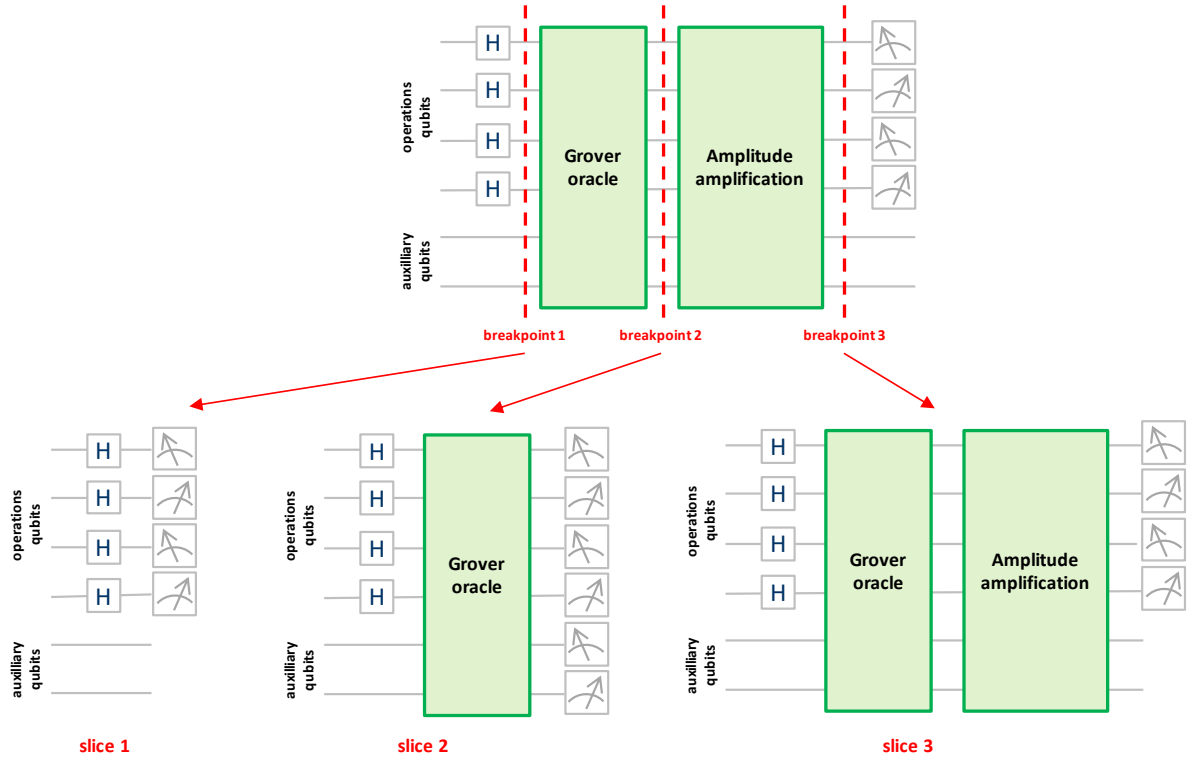


Figure 647: a quantum code debugging approach with code slicing. Source: A Tool For Debugging Quantum Circuits by Sara Ayman Metwalli and Rodney Van Meter, Keio University, May 2022 (11 pages).

Black-box testing looks at the functionality, ignoring the inner workings of the software, making sure the expected output is obtained with a given input?

[1854] See Formal Verification vs. Quantum Uncertainty by Robert Rand et al, University of Maryland, 2019 (12 pages) that pinpoints the role of hardware errors in quantum programs.

[1855] See A Tool For Debugging Quantum Circuits by Sara Ayman Metwalli and Rodney Van Meter, Keio University, May 2022 (11 pages).

How about using interactive debugging in the white-box approach? Right now, it can be done on quantum emulators but is limited by their computing/memory capacity. It can't exceed 40 qubits and practically 16 qubits. A state vector representation is quite difficult to visualize beyond 8 qubits.

On a real machine, implementing interactive breaking points in a quantum circuit is difficult due to the impact of measurement on the qubits register vector state and on the probabilistic nature of quantum computing. Let's say we'd like to implement a breaking point and line by line code execution. We'd need to run the quantum algorithm and stop it at the breaking point then make some measurement.

But good measurement, just to get a state in the computational basis would require running the code many times. And even way more times if we'd need to reconstitute the full vector state. Then, to move to the next series of gates, the circuit would have to be re-run the same number of times. And again and again and again. It would be worse if we were to check the entanglement within the register. Deciding if a register is separable is in itself an NP-hard problem. One way to proceed is to implement unit testing with splitting the code in trusted blocks and patterns. Other debugging tools can involve projective measurements on ancilla qubits or even gentle measurement techniques[1856]. And this deals just with classic gate-based quantum computing. Analog quantum computing and special techniques like MBQC or FBQC (from PsiQuantum) will mandate specific debugging techniques and tools.

At last, let's mention that many quantum algorithms are hybrid and aggregate classical and quantum algorithms, which requires another set of discipline and tools.

Research is going on in all these dimensions around the world. These are strategic components for quantum computing[1857].

Benchmarking

Benchmarking quantum computing is becoming a strategic tool for both vendors and users. In the IT space, vendors have continuously relied on benchmarking to showcase new hardware advances and customers rely on it to assess the cost/benefit ratio of emerging technologies. Benchmarks participate to fostering innovation with driving the competition between vendors and technologies[1858].

In classical computing, raw computing power is measured in **FLOPs** (floating point operations per seconds). **Linpack** is used in the HPC TOP500 ranking and is based on a linear equation solving task. **MLPerf** is used in machine learning and for comparing GPGPUs like those from Nvidia and their competitors. Personal computers processors can be compared with **Passmark Software** benchmarks or alternative from other vendors.

Quantum computing benchmarking can have several purposes:

- Comparing quantum computing with classical computing, which involves coupling best-in-class algorithms and software in both cases, all being moving targets given the steady progress of classical computing, particularly with so-called "domain specific architectures", the most famous one being the tensor-based GPGPUs and ASICs. This sort of benchmarking can be exploited to assess a potential quantum advantage, where a quantum solution is either solving a problem in a shorter time than classical computers or able to solve a problem that can't be solved with existing classical

[1856] See Debugging Quantum Processes Using Monitoring Measurements by Yangjia Li and Mingsheng Ying, 2014 (7 pages) describes the process of interim measurement process within code and Projection-Based Runtime Assertions for Testing and Debugging Quantum Programs by Gushu Li et al, 2020 (29 pages) proposes to use some ancilla qubits to indirectly detect vector state characteristics. It uses projective measurements on a different basis than the computational basis of each qubit.

[1857] It includes the study Program Verification, Debugging, and QC Simulation — EPiQC, a IARPA funded project on quantum program verification and debugging.

[1858] See The Race to Quantum Advantage Depends on Benchmarking by Matt Langione, Jean-François Bobier, Lisa Krayer, Hanl Park and Amit Kumar, February 2022.

computers. The archetypal such benchmark is the cross-entropy benchmark (XEB) used by Google in 2019 to showcase its quantum supremacy with Sycamore[1859].

- Comparing different quantum computers competing with each other to solve particular tasks. It can be done with quantum computers using the same programming paradigm like gate-based systems (e.g. IBM's quantum volume), or even, quantum computers solving a given problem with different paradigms (annealing, simulation, gate-based; e.g. Atos Qscore). An objective comparison can be made with solving one or a broader set of specific problems and assessing the maximum problem size addressable by competing solutions (e.g., Atos Qscore, QED-C and IonQ's algorithmic qubits).
- Comparing different characteristics. The most common is computing time, but other metrics will become important as well such as precision, energy spent, weight, environmental footprint and total cost (e.g. DARPA's benchmarking project RFP won by Raytheon BBN and the Quantum Energy Initiative's Green 500 benchmark proposal).
- Comparing different algorithms solving a given problem on similar or different quantum hardware. These are not yet there.

Benchmarking tools already abound and are very diverse.

Following a bottom to top system approach, there are benchmarks for spare system level features (number of qubits, qubits gates and readout fidelities, connectivity, gates speed aka CLOPS with IBM, all of which are not benchmark results per se, entanglement quality). These are the quantum equivalent of number of cores, CPU clock, RAM, storage size and speed and network specs in classical computing.

what and whom	what	pros	cons	timing / adoption
IBM quantum volume	breath/depth computing capacity, 2^#qubits	simple qualifier of qubits quality	doesn't work in advantage regime due to emulation needs requirements	published in 2019 IBM, Quantinuum
Cisco MBQC quantum volume	computing capacity for MBQC CV photon qubits	adapted to photon qubit using a different model than circuit based models	to be adapted to direct variable photons MBQC model	proposed in 2022 by Cisco
IBM CLOPS	circuit layers operations per seconds	complements QV for speed	N/A	announced in November 2021
cycle benchmarking	qubits entanglement evaluation	useful to benchmark qubits quality	limited to one low-level feature	2019, Canada, Denmark and Austria universities
scalable benchmarks for gate-based QC	six low-level structured circuits tests	tested 21 configurations from IBM, IonQ and Rigetti	low-level benchmark not usage based	published in 2021 QuSoft, Cambridge, Caltech
PQF (photonic quality factor)	assess performance of linear optics single photons multimode QPUs	covers many NISQ photon qubit implementations	limited to a specific photonic qubit configuration	published in 2022 by Quandela
entanglement-based volumetric benchmark	estimate size of maximum entangled qubit state	entanglement is a key feature of quantum acceleration	narrow and not usage oriented	proposed in 2022 par DoE Oak Ridge et al

Figure 648: low level benchmarking proposals. (cc) Olivier Ezratty, 2022.

Then, some are benchmarking hardware capabilities at a higher level and regardless of the use case (quantum volume from IBM). At last, others are assessing the capability to solve one or several typical use cases, and usually, their maximum size (QED-C, Atos Q-score, IonQ algorithmic qubits, SupermarQ). At some point, benchmarking will be even more tricky when mixing quantum and classical computers.

[1859] This benchmarking technique like the quantum volume is limited by the capacities of classical emulation. One proposed way to overcome this problem is to run only Clifford gates, which reduces the resources requirements in the classical computer. See Linear Cross Entropy Benchmarking with Clifford Circuits by Jianxin Chen et al, June 2022 (30 pages).

	what and whom	what	pros	cons	timing / adoption
multiple use cases	**scalable benchmarks for gate-based QC**	six low-level structured circuits tests	tested 21 configurations from IBM, IonQ and Rigetti	low-level benchmark not usage based	published in 2021 QuSoft, Cambridge, Caltech
	QED-C supported benchmark	set of low-level algorithms benchmarks	breadth of use cases	complicated visualization	published in 2021 QED-C, Princeton, HQS, QCI, IonQ, D-Wave, Sandia Labs
	IonQ Logarithmic Qubits	$\min(\#\text{qubits}, \sqrt{\#gates})$	run on different use cases	a bit complicated	published in 2020 and refined in 2022, IonQ
	SupermarQ from Super.tech	suite of applications benchmark	also handles error correction benchmarking		published in March 2022, Intel and Amazon
	Qpack by TU Delft	three sets of problems (Max-Cut, TSP, DSP)	measure différents metrics	Adoptions	proposed in April 2022
single use cases	**Atos Q-score**	maximum size of solvable MAXCUT problem size	application need oriented works in advantage regime hardware independant	limited to MAXCUT problems marketing & adoption	published in 2020 Atos, be be expanded to other algos
	DoE ORNL	chemical simulation	works on existing superconducting hardware	limited to three 2-atom molecules simulations	published in 2020 DoE
	Zapata benchmark for fermionic quantum simulations	one-dimensional Fermi Hubbard model (FHM) VQE running on NISQ	tested on Google Sycamore with its tunable couplers	narrow use case	proposed in March 2020

Figure 649: application level benchmarking proposals, either multiple or singe cases. (cc) Olivier Ezratty, 2022.

These tools are created by different kinds of players, sometimes working together: research laboratories (e.g. DoE Sandia Labs), software and hardware vendors (IBM, IonQ, Atos, Zapata Computing, …), industry consortium usually working with a combination of these players (USA's QED-C) and then standards bodies (e.g. IEEE). The combination of these players is important.

what and whom	what	pros	cons	timing / adoption
Unitary Fund Metriq	repository of benchmark results	N/A	N/A	announced in May 2022
DARPA project	SWAP (size-weight-application-power)	hardware-agnostic and resource estimates	N/A at this point	awarded in 2022 to Raytheon BBN
IEEE QC Perf Metrics & Perf Benchmarking PAR	gate-based QC benchmarking	ongoing standardization project		submission in Oct 2023 completion in Oct 2024
Quantum Energy Initiative	QC energetics benchmarking consolidated approach, QGreen500 proposal could consolidate cryogeny benchmarks	methodology (MNR) to optimize QC energetics, first analysis done with superconducting qubits	research and industry must build coordination around this goal	joint research/industry Quantum Energy Initiative launched in 2022

Figure 650: other benchmarks proposals. (cc) Olivier Ezratty, 2022.

Industry vendors have some biasing interest. They don't want to favor the adoption of benchmarks that would be unfavorable to their offerings. This is amplified by the wide spectrum and diversity of quantum computing technologies and qubits including aspects like gate-times, fidelities and topologies. Some benchmarks can also be misleading if improperly extrapolated in the future, given all technologies don't have the same upscaling potential. An equivalent to Moore's law can't be applied in a simplistic way to all these technologies roadmaps. In all cases, quantum computing benchmarking will be difficult to interpret without the right technical background. You can be easily fooled by vendors given the complexity of the matter.

Quantum Volume and CLOPs

Since late 2021, IBM uses three systems-level metrics and benchmarks to characterize its quantum computers: the scale with the number of qubits, the speed measured in CLOPS (circuit layer operations per second) and qubits quality measured with their homemade quantum volume metric.

The quantum volume was introduced in 2017 and was adopted by **Honeywell** in March 2020 and afterwards by **IonQ** in October 2020. Its use is also recommended by the **Gartner Group**.

Quantum volume is an integer that associates the quantity of qubits and the number of quantum gates that can be executed consecutively with a reasonable error rate. Indeed, having N qubits but being limited by the number of quantum gates that can be used can be detrimental to the execution of many quantum algorithms. Some are greedy for quantum gates, others are not[1860].

This quantum volume number is supposed to aggregate four performance factors:

- The **number of physical qubits of** the processor.
- The **number of quantum gates** that can be chained consecutively without the error rate being detrimental to the results.
- The **connectivity between these qubits**, which will impact the length of execution of an algorithm and potentially improve quantum volume for qubits with high connectivity such as with trapped ions. It reduces the number of SWAP gates that are required when connectivity is limited.
- The **number of quantum gates** that can be executed in parallel[1861].

The QV is evaluated using a random calculation benchmark consisting of chaining random quantum gates and which must give a correct result in two thirds of the cases. Why two thirds? Because quantum computing provides a probabilistic result. To obtain a deterministic result, the calculation is executed several times and the average of the results is evaluated, up to thousands of times as proposed by IBM in its cloud system. With an average of two-thirds good results, one can therefore statistically converge to a good result after a few measurements. The accuracy of the result will depend on this number, which is usually a few thousand.

In the first version in 2017, the quantum volume was the square of the maximum number of qubits on which the processor could perform this calculation[1862]. The definition then was changed in 2019 to become 2 to the power of this number of qubits[1863]. The following illustration explains how the 2017 and 2019 quantum volumes are evaluated.

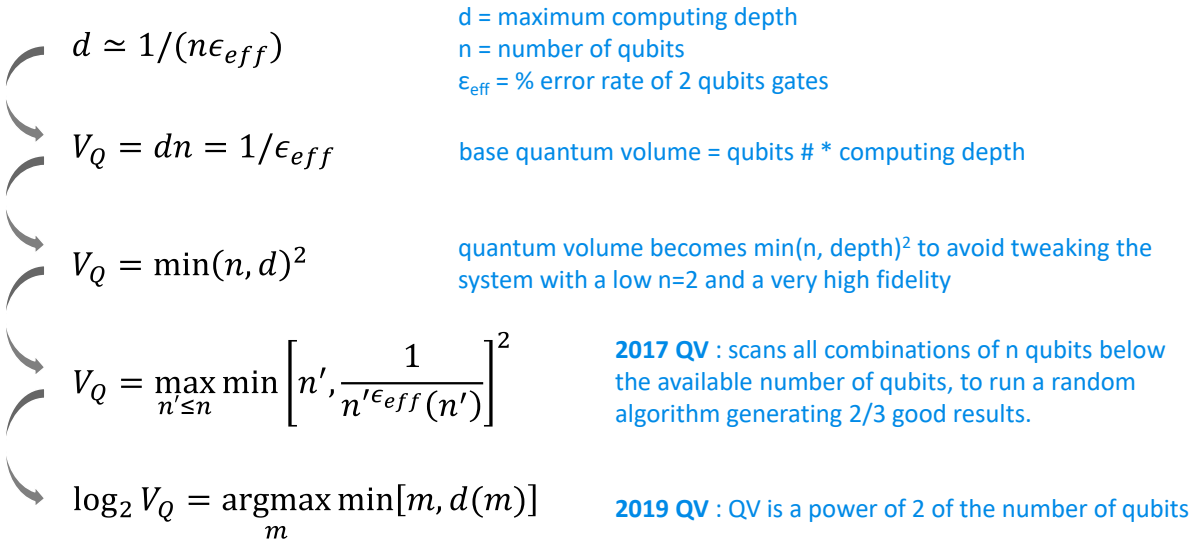


Figure 651: how is/was IBM's quantum volume calculated. (cc) Olivier Ezratty, 2021.

[1860] Some algorithms can thus be satisfied with a limited number of quantum gates, such as Deutsch-Jozsa's and is satisfied with only four series of quantum gates. Peter Shor's integer factoring algorithm requires a depth of quantum gates equal to the cube of the number of qubits used.

[1861] Trapped ions quantum computers can't do that with two-qubit gates.

[1862] See Quantum Volume by Lev Bishop, Sergey Bravyi, Andrew Cross, Jay Gambetta and John Smolin, 2017 (5 pages).

[1863] See Validating quantum computers using randomized model circuits by Andrew W. Cross et al, 2019 (12 pages).

The diagram below from a paper by Robin Blume-Kohout and Kevin Young specifies how the m (number of qubits) and the d (computational depth) are evaluated[1864].

The number of qubits obtained to evaluate the quantum volume is much lower than the total number of qubits available: 8 for 16 in this case. The benchmark allows only 8 series of quantum gates in a row over 8 qubits, for 38 with only two qubits. In its 2017 version, the quantum volume was the grey square area containing the red lined squares.

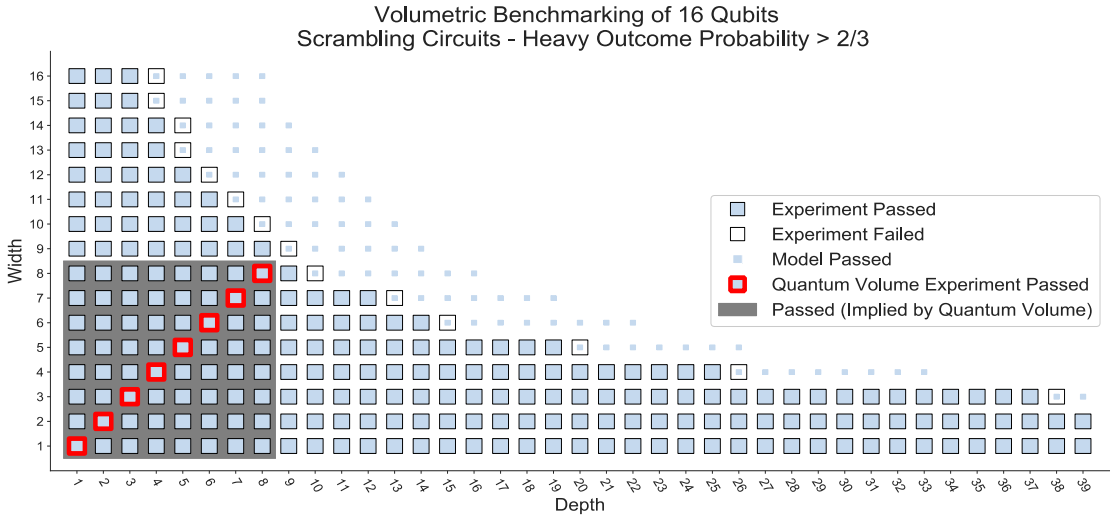


Figure 8(a). Volumetric benchmarking of a 16 qubit device using scrambling circuits. If at least 2/3 of the measurement results are heavy for a given width/depth pair, then the pair passes the test and is marked with a large, solid blue box. Using linear axes, the quantum volume experiments appear along the diagonal and are outlined with heavy, red lines. For this example, $\log_2(V_Q) = 8$. It is expected that scrambling circuits with both width and depth less than or equal to the quantum volume should succeed, and we highlight these with a gray background.

Figure 652: a better visualization of how a quantum volume is evaluated. Source: A volumetric framework for quantum computer benchmarks by Robin Blume-Kohout and Kevin Young, February 2019 (24 pages).

In its 2019 version, it became 2^8, or 256 instead of 64 (8^2). In the end, it is the dimension of Hilbert's vector space, i.e. the number of different superposed states that it is able to manage from a practical point of view with a depth of computation equal to the number of corresponding qubits.

When IBM states that their 27-qubit processor has a quantum volume equal to 128, it means that they only managed to validate their benchmark with 7 qubits among these 27 qubits.

IonQ announced in 2020 a quantum volume greater than four million corresponding to a QV of 4,194,304, representing 2^{22}. So, with the ability to run 22 sets of quantum gates on 22 of their 32 qubits, with two-thirds correct results on the used random benchmark. This record seems to be related to the good connectivity of trapped ion qubits. These can all be directly entangled with each other, unlike superconducting qubits, which are at best entangled with their immediate neighbors. This allows the benchmark to be achieved in fewer series of quantum gates than on superconducting qubits, which require a lot of SWAP gates generating rapidly accumulating errors.

[1864] In A volumetric framework for quantum computer benchmarks, February 2019 (24 pages), Robin Blume-Kohout and Kevin Young propose volumetric benchmarks to evaluate the performance of quantum computers based on IBM's quantum volume. The latter also proposes its own quantum volume evaluation code.

When you look at the relative progress of QV between IBM, IonQ and Honeywell/Quantinuum systems, you see a clear difference: IBM has a tougher time to use all its qubits while trapped ions do it better, although with a rather limited number of qubits[1865]. But if and when IBM fixes some scalability issues with their qubits, like with reducing qubit crosstalk, they can potentially increase their QV to higher levels than those from trapped ions vendors.

Year	Brand	Version	Hw Qubits	Log2(QV)	%
2017	IBM	Tenerife	5	2	40%
2018	IBM	Tokyo	20	3	15%
2019	IBM	Johannesburg	20	4	20%
2020	Honeywell		4	4	100%
2020	IBM	Raleigh	28	5	18%
2020	IBM	Montreal	27	6	22%
2020	Honeywell	H0	6	6	100%
2021	IBM	Montreal	27	7	26%
2020	Honeywell	H1-1	10	7	70%
2021	Honeywell	H1-1	10	9	90%
2021	Honeywell	H1-1	10	10	100%
2022	IBM	Manhattan	127	6	5%
2020	IonQ	Aria	32	22	69%
2022	Quantinuum	H1-2	12	12	100%
2022	Quantinuum	H1-1	22	13	59%

Figure 653: evolution of systems quantum volumes over time. (cc) Olivier Ezratty, 2022.

QV is limited to about 50 operational qubits because it can only be evaluated with a benchmark comparing the qubits with their simulation on a conventional computer. This emulation is constrained by memory size, which reaches its limits between 50 and 55 qubits[1866].

Quantum computing scientists are circumspect about the interest of this indicator which is too simplistic[1867]. This use is contested by Scott Aaronson, a specialist in complexity theories and quantum algorithms [1868]. He reminds us that current QVs are more than easily emulable in a simple classical computer, if not on an Apple Watch! This does not make it particularly powerful. And when the QV will get significant, beyond the threshold of 50, we won't be able to measure it!

Scott Aaronson believed that this quantum volume indicator, which is a marketing simplification tool from IBM, should be avoided. He prefers a description of systems characteristics like the number of qubits, their connectivity, their coherence time (T1, T2), their reset, one and two-qubit gates and readout fidelities. With most vendors, these indicators are generally found in the scientific publications of researchers but not always in the vendors marketing literature. However, IBM publishes most of these data on their quantum systems available on Q Experience.

In August 2022, a team from **Cisco** proposed a way to evaluate a quantum volume for a MBQC-based photonic quantum processor. It is based on using a continuous-variable cluster state and the Gottesman-Kitaev-Preskill (GKP) encoding. It computes the system quantum volume based on the logical gate error channels of cluster state GKP squeezing and photon loss rate[1869].

In November 2021, **IBM** added the CLOPS speed metric (circuit layers operations per seconds), an equivalent to the clock of a classical CPU, given the numbers are different for resetting qubits, operating quantum gates and measuring qubits[1870]. As of 2021, IBM's systems CLOPS where between 1,5 and 2,4K, so about 2.000 layers of qubit gates per seconds. CLOPS are calculated as M * K * S * D / time taken, where M is the number of templates, K the number of parameter updates, S the number

---

[1865] See Quantum Volume in Practice: What Users Can Expect from NISQ Devices by Elijah Pelofske et al, March 2022 (19 pages).

[1866] See Why Is IBM's Notion of Quantum Volume Only Valid up to About 50 Qubits? by Jack Krupansky, October 2020.

[1867] Imagine an indicator of the power of your laptop aggregating the processor clock frequency, its number of cores, the power of its CPU, the RAM memory, the storage capacity, its type (hard disk, SSD) etc? And there, to ask yourself if you will be able to efficiently use your video editing, photo derush or video game software on augmented reality headphones!

[1868] In Turn down the quantum volume, Scott Aaronson, published just after Honeywell's February 2020 announcement.

[1869] See Quantum Volume for Photonic Quantum Processors by Yuxuan Zhang et al, August 2022 (22 pages).

[1870] See Scale, Quality, and Speed: three key attributes to measure the performance of near-term quantum computers by Andrew Wack, Hanhee Paik, Ali Javadi-Abhari, Petar Jurcevic, Ismael Faro, Jay M. Gambetta and Blake R. Johnson, October 2021 (8 pages). With their Falcon R5 processor, qubit reset takes 450ns while qubits readout takes 750 ns. It's much longer than gates.

of shots and D, the number of quantum volume layers, or $\log_2$(QV). IBM published a methodology where M=100, K=10, S=100 and D was dependent on the quantum volume of each of the benchmarked systems[1871]. IBM plans to reach 10K CLOPS in 2022 with its 433 qubits Osprey processor, thanks to using "dynamic circuits" that handle feedback and feedforward of quantum measurements and help fasten quantum error corrections.

Algorithmic qubits

IonQ was initially supportive of IBM's quantum volume metric but now uses a QV variation denominated "algorithmic qubits". They wanted to create a more relevant single-number metric that is usage oriented and more telling for customers. They wanted to avoid using random circuits benchmarking as in IBM's QV.

It's not far from $\log_2$(IBM's QV) but not exactly. It was initially defined as the size of the largest circuit that could run with N qubits and N^2 two-qubit gates, but was then refined as $\min(\#\text{qubits}, \sqrt{\#gates})$ with algorithm success probability ≥50% (not the 66% from IBM's QV), assuming the algorithm requires N^2 two-qubit gates [1872].

Practically speaking, the #AQ benchmark is run on different algorithms, like the ones defined in the QED-C benchmark. You'll then get several numbers, one for each algorithm and for each tested machine. The #AQ must be represented in a 2D chart as shown in Figure 654, with these various algorithms' success probability represented as colored circles and two axis: on X, the 'depth' of the circuit represented by a log scale of number of two qubits entangling gates, and on Y, the number of qubits used.

IonQ touted in March 2022 having reached an algorithmic qubits record of 20 with its 32 bits Aria system. It was achieved with one of these algorithms, surprisingly, the most successful one, quantum phase estimation, which by the way, is very far from a practical "customer need". Other algorithms had #AQs of 4 to 16.

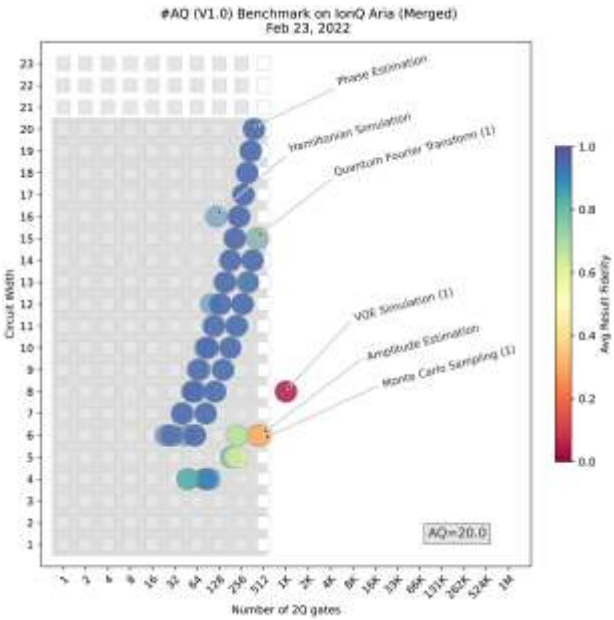


Figure 654: Source: Algorithmic Qubits: A Better Single-Number Metric by IonQ, February 2022.

With higher fidelities qubits, you could run an algorithm with a greater number of two-qubit gates and improve X. But in that case, your #AQ would still be constrained by the number of qubits used. However, with poor fidelities qubits, your #AQ could become much lower than this number of qubits, a bit like with IBM's quantum volume, but on a real algorithm and not with a randomized benchmark.

Since the suite of tested algorithms will change over time, IonQ will define release numbers for its #AQs.

Other systems level benchmarks and metrics

Other various low-level systems benchmarks are worth mentioning:

[1871] See Driving quantum performance: more qubits, higher Quantum Volume, and now a proper measure of speed by Jay Gambetta, Ali Javadi-Abhari, Blake Johnson, Petar Jurcevic, Hanhee Paik and Andrew Wack, November 2021.

[1872] The algorithmic qubits benchmark is described in details in Algorithmic Qubits: A Better Single-Number Metric by IonQ, February 2022 and in QIP 2022 | The application oriented benchmarks for quantum computing (Luming Zhao, IonQ), (1h video).

Cycle benchmarking from a team involving Canada, Denmark and Austria which assesses the low-level quality of qubits entanglement, created in 2019[1873].

A proposal made by a team from QuSoft (The Netherlands), the University of Cambridge (UK) and Caltech (USA) in April 2021 is bound to measure the performance of universal quantum computers in a hardware-agnostic way with six structured circuits tests (Bell test, Schrödinger's microscope, Mandelbrot, line drawing, matrix inversion and platonic fractals). It's quite complex to interpret and reading out the graphical results is not straightforward, nor connected to an application need[1874].

In 2021, **DARPA** launched a research RFP for the creation of benchmarks in two categories: application-specific hardware-agnostic benchmarks (TA1, with $1.45M for 18 months) for quantum computing and hardware resource estimates for quantum computers (TA2, with a funding of $1.5M over 18 months). In the end, the project was awarded in March 2022 to Raytheon BBN and University of Southern California. Their benchmark targets all sorts of quantum technologies, both computing and sensing, and are summarized with the **SWAP** nickname corresponding to (size, weight, application and power)[1875]. In July 2022, as part of these benchmarking programs, DARPA awarded a three-year contract of $2.9M to Rigetti, the University of Technology Sydney, Aalto University and the University of Southern California to create benchmarks for large-scale quantum computers.

Another similar approach, but a narrower one, was proposed by researchers from **Brookhaven** and **Pacific Northwest** National Laboratories from the DoE which estimates hardware resources needed for key algorithms[1876]. Another DoE lab, the **Sandia Labs**, proposed a variation of randomized benchmarking that works in the quantum advantage regime[1877]. In 2022, DoE's **Oak Ridge** lab and several US universities proposed a volumetric benchmark qualifying the quality of qubit entanglement, that was tested first on IBM QPUs[1878].

And to be complete, another team from Berkeley, HRL Labs and University of Chicago devised a randomized benchmark measuring noise in non-Clifford quantum gates (those gates that are needed for a QFT and for generating an exponential speedup), extending the work from Google on their 2019 supremacy experiment[1879]. Other extensions are proposed by Alibaba USA with their Universal randomized benchmarking (URB) that scales better than the cross-entropy benchmark used by Google[1880] and with a randomized benchmark supporting a universal gate set[1881].

In a different realm, there is even a proposal of benchmark for **MBQC-based** computing systems, mostly used in photonic qubits[1882].

[1873] Presented in Characterizing large-scale quantum computers via cycle benchmarking par Alexander Erhard et al., 2019 (7 pages).

[1874] See Scalable Benchmarks for Gate-Based Quantum Computers by Arjan Cornelissen et al, April 2021 (54 pages).

[1875] See DARPA asks Raytheon BBN and USC researchers to test limits of quantum computing for military applications by John Keller, Military+Aerospace Electronics, March 2022.

[1876] See On the importance of scalability and resource estimation of quantum algorithms for domain sciences by Vincent R. Pascuzzi, Ning Bao and Ang Li, May 2022 (5 pages). They notices that for a QFT, the number of gates and CNOT gates scale exponentially with an increased number of qubits

[1877] See Measuring the Capabilities of Quantum Computers by Timothy Proctor et al, Sandia Labs, August 2020/January 2022 (4 pages) and Scalable randomized benchmarking of quantum computers using mirror circuits by Timothy Proctor et al, Sandia Labs, December 2021 (8 pages).

[1878] See An entanglement-based volumetric benchmark for near-term quantum hardware by Kathleen E. Hamilton, Sophia Economou et al, September 2022 (21 pages).

[1879] See Benchmarking near-term quantum computers via random circuit sampling by Yunchao Liu et al, April 2022 (43 pages)

[1880] See Randomized Benchmarking Beyond Groups by Jianxin Chen et al, Alibaba USA, March 2022 (35 pages).

[1881] See Demonstrating scalable randomized benchmarking of universal gate sets by Jordan Hines, Robin Blume-Kohout, Irfan Siddiqi, Birgitta Whaley, Timothy Proctor et al, August 2022 (31 pages).

[1882] See Measurement-based interleaved randomised benchmarking using IBM processors by Conrad Strydom et al, Stellenbosch University, March 2022 (17 pages).

Q-score

Atos proposed its Q-score benchmark in December 2020. It's based on determining the maximum size of a standardized problem that can be solved on a given hardware on any quantum programming paradigm[1883]. The first selected problem is the classical combinatorial **MaxCut**. Its variations are used to solve the traveling salesperson problem or various graphs problems with applications in logistic, industry and finance. It can also be used to handle clustering in quantum machine learning. The Q-score benchmark is evaluated with using a hybrid classical+quantum algorithm like with QAOA (Quantum Approximate Optimization Algorithm).

This benchmark creates a simple metric (the number of variables that can be used in the optimization problem) and is independent from the computing paradigm used (gate-based or other) and it doesn't require a quantum computing emulation capacity like with the IBM Quantum Volume. And the algorithm solutions can be verified polynomially on a classical computer. The Q-Score software tools are also open source and published on Github.

Atos plans to publish the Q-scores of various QPU manufacturers. Right now, the record is at around 15Q. It could soon reach 20Q. And 60Q is needed to showcase a real quantum advantage. In August 2022, a Dutch team evaluated **D-Wave** 2000Q and Advantage annealers and obtained a record of 70Q and 140Q, which is much better than existing gate-based QPUs[1884]. But it's not yet sufficient to exceed the performance of classical computers. It seems however than hybrid solutions may under certain conditions outperform supercomputers. Another team, from **Pasqal**, implemented a Q-score benchmark on their neutral atoms simulator and obtained a Q-score of 80Q using a digital simulation of their system[1885]. They solved the benchmark MaxCut problem using a classical machine learning technique to reduce the number of runs on their QPU.

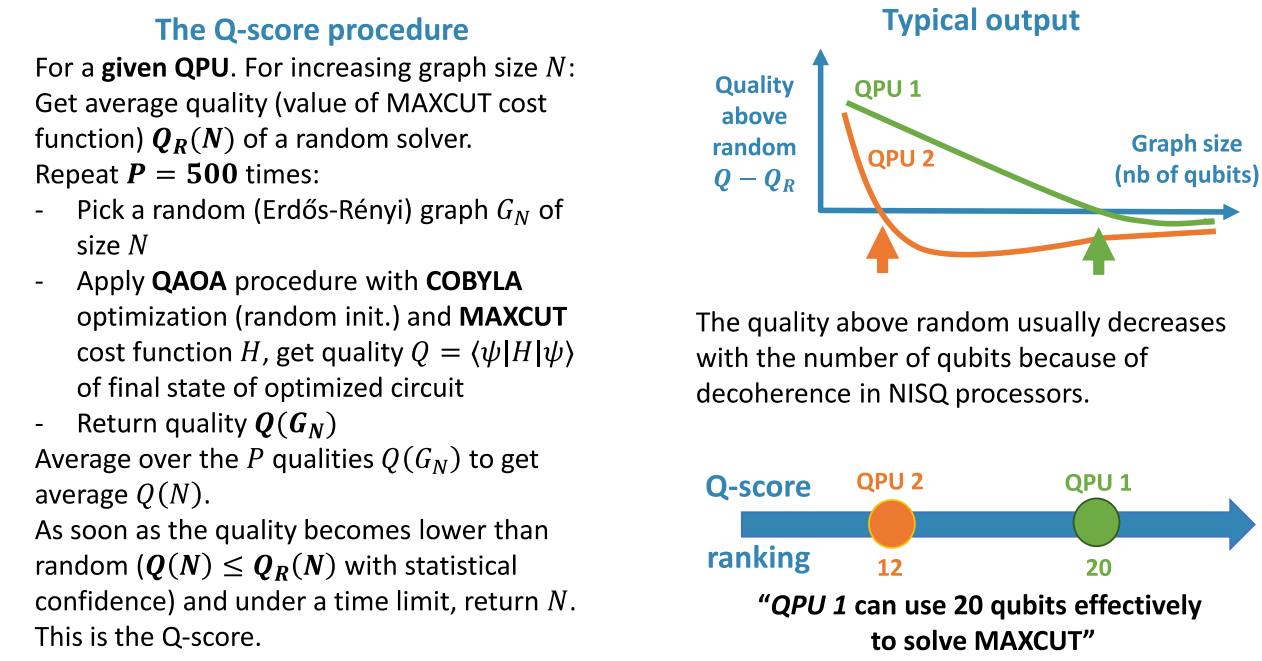


Figure 655: Atos Qscore calculation method. Source: Atos.

[1883] See Benchmarking quantum co-processors in an application-centric, hardware-agnostic and scalable way by Simon Martiel, Thomas Ayral and Cyril Allouche, IEEE Transactions on Quantum Engineering, February 2021 (11 pages).

[1884] See Evaluating the Q-score of Quantum Annealers by Ward van der Schoot et al, The Netherlands Organisation for Applied Scientific Research, August 2022 (8 pages).

[1885] See Efficient protocol for solving combinatorial graph problems on neutral-atom quantum processors by Wesley da Silva Coelho, Mauro D'Arcangelo and Louis-Paul Henry, August 2022 (23 pages).

This benchmark would need to be completed by other benchmarks such as one for quantum chemistry simulation (number of atoms in molecule) and another on the size of the maximum number that can be factorized (in power of 2).

Other use case benchmarks

QED-C is supporting a series of application oriented benchmarks proposed by researchers from Princeton, HQS, QCI, IonQ, D-Wave and Sandia Labs in the USA[1886]. It mixes the volumetric benchmarking method from IBM and a comparison of performance with various standard algorithms. They did some comparison on actual quantum hardware from IBM, Rigetti, HQS and IonQ. It was launched in October 2021.

SupermarQ is a benchmark proposed in 2022 by Super.tech (acquired in May 2022 by ColdQuanta) and supported by Amazon and Intel (both of which have no functional quantum computer yet). It is a suite of application benchmarks that covers use cases in finance, pharmaceuticals, energy, chemistry and other verticals. SupermarQ also contains an error correction benchmark[1887].

QPack is a benchmark based on the Max-Cut problem (like Atos's Q-score), the dominating set problem (DSP) and the traveling salesperson problem (TSP), and using the QAOA algorithm as a benchmarking tool, proposed by TU Delft researchers. It measures the maximum problem size a quantum computer can solve, the required computing runtime and the achieved accuracy[1888].

The DoE **ORNL** (Oak Ridge National Laboratory) proposed a benchmark for chemical simulation[1889]. It deals with the simulation of three 2-atoms molecules (NaH, KH et RbH) which can be simulated on existing IBM and Rigetti 20 and 16 qubits superconducting systems. It's not generic and can't go beyond these molecule sizes.

Other single use-cases benchmarks have also been created: **Agnostiq** created a benchmark dedicated to optimizing financial portfolio using the Quantum Approximate Optimization Algorithm (QAOA)[1890], scientists from New-York created a benchmark related to Grover's search algorithm[1891] and Zapata Computing created one benchmarking on fermionic simulations[1892].

IEEE and ISO

The **IEEE** has launched several benchmarking initiatives on its own with a standard to be submitted in 2024[1893].

[1886] See Application-Oriented Performance Benchmarks for Quantum Computing by Thomas Lubinski et al, October 2021 (33 pages).

[1887] See SupermarQ: A Scalable Quantum Benchmark Suite by Teague Tomesh et al, Princeton, University of Chicago, Super.tech and Intel, February 2022 (15 pages) and Applying classical benchmarking methodologies to create a principled quantum benchmark suite by Teague Tomesh et al, March 2022.

[1888] See QPack: Quantum Approximate Optimization Algorithms as universal benchmark for quantum computers by Koen Mesman et al, April 2022 (28 pages) and QPack Scores: Quantitative performance metrics for application-oriented quantum computer benchmarking by Huub Donkers et al, May 2022 (23 pages).

[1889] See ORNL researchers advance performance benchmark for quantum computers, January 2020.

[1890] See Wasserstein Solution Quality and the Quantum Approximate Optimization Algorithm: A Portfolio Optimization Case Study by Jack S. Baker et al, February 2022 (21 pages).

[1891] See Quantum search on noisy intermediate-scale quantum devices by Kun Zhang, Kwangmin Yu and Vladimir Korepin, February 2022 (12 pages).

[1892] See An application benchmark for fermionic quantum simulations by Pierre-Luc Dallaire-Demers et al, Zapata Computing, March 2020 (14 pages).

[1893] See P7131 - Standard for Quantum Computing Performance Metrics & Performance Benchmarking. It covers gate-based quantum computing. See also Metrics & Benchmarks for Digital Quantum Computing by Robin Blume-Kohout (18 slides) and Summary of the IEEE Workshop on Benchmarking Quantum Computational Devices and Systems, 2019. Also, see P2995 - Trial-Use Standard for a Quantum Algorithm Design and Development and P3120 - Standard for Quantum Computing Architecture.

They entertain several working groups with participating industry vendors and academic institutions.

- Trial-Use Standard for a Quantum Algorithm Design and Development (P2995, details).
- Standard for Quantum Computing Architecture (P3120, details).
- Software-Defined Quantum Communication (P1913).
- Standard for Quantum Computing Definitions (P7130).
- Standard for Quantum Computing Performance Metrics & Performance Benchmarking (P7131).

There is also an **ISO** working group working on quantum computing (ISO/IEC JTC 1/WG 14).

Benchmarking tools

Metriq from **Unitary Fund** announced in May 2022 is a repository of benchmarking results.

MQT Bench aka the Munich Quantum Toolkit is a multiple-abstraction level suite of benchmarking tools covering both low-level abstraction building blocks (QFT, QPE, amplitude estimation) and higher-level ones (Grover, Shor, HHL)[1894].

Arline (Germany) is also proposing its own benchmarking tools suite that is used to compare compiler optimizers[1895].

QUARK (Germany) is another industry application-centric benchmarking proposal based on an opt-source framework[1896].

Quantum supremacy and advantage

Quantum supremacy and advantage are two terms used to qualify the superiority of quantum computers as compared with the most powerful supercomputers.

Quantum supremacy was a term coined by John Preskill in a paper presented at the Solvay Congress in 2011[1897]. It is achieved when a problem, useful or not, is only solvable with a quantum algorithm running on a quantum computer, and there is no known classical algorithm for the most powerful supercomputers that could run in a reasonable human scale time[1898]. Quantum supremacy was a goal for researchers and vendors like Google and it became claims, with a peak in October 2019.

Quantum supremacy doesn't mean that a given quantum computer is supremely more powerful than all its contemporary supercomputers. The term is applicable to a combination of a specific problem and related quantum algorithm, a given quantum computer, and the best-in-class available classical algorithms adapted to the most powerful available supercomputers. The criteria are moving targets. Supercomputers have not said their last word and are classical algorithms are also improved[1899].

[1894] See MQT Bench: Benchmarking Software and Design Automation Tools for Quantum Computing by Nils Quetschlich et al, TUM Germany, Johannes Kepler University Linz, Austria and Hagenberg GmbH (SCCH), Austria, April 2022 (7 pages).

[1895] See Arline Benchmarks: Automated Benchmarking Platform for Quantum Compilers by Y. Kharkov et al, February 2022 (27 pages).

[1896] See QUARK: A Framework for Quantum Computing Application Benchmarking by Jernej Rudi Finžgar, Philipp Ross, Leonhard Hölscher, Johannes Klepsch and Andre Luckow, August 2022 (12 pages).

[1897] It is described in Quantum Computing and the Entanglement Frontier, 2011.

[1898] See Quantum supremacy: Some fundamental concepts by Man-Hong Yung, January 2019 (2 pages) according to which there are three ways to demonstrate quantum supremacy: boson sampling, PQI and chaotic quantum circuits.

[1899] See Quantum Algorithms Struggle Against Old Foe: Clever Computers by Ariel Bleicher, February 2018. This mentions the discovery of classical algorithms that are as powerful as their quantum equivalents, such as the one from Ewin Tang, already mentioned on page 61.

Robert König (Technical University of Munich), David Gosset (University of Waterloo, Canada) and Sergey Bravyi (IBM) demonstrated in October 2018 that quantum computers could perform operations inaccessible to conventional computers but based only on the case of a particular algorithm[1900].

Others are devising "*proofs of quantumness*", which are methods to demonstrate to a classical verifier that a quantum computer can perform some computational tasks that a classical computer with comparable resources cannot (meaning, the classical computer must achieve things in a tractable way, i.e. less than polynomial time)[1901].

Some D-Wave and Google benchmarks carried out in 2015 and showing the superiority of the quantum solution were then contradicted by the creation of algorithms optimized for supercomputers under certain conditions. In a few years' time, it will certainly come into play for a few algorithms that cannot have optimized supercomputer equivalents.

Google's quantum supremacy announced in October 2019 was touted as serious back then[1902]. It was later downgraded. It was based on a sort of *random numbers sampling* algorithm using 53 qubits. But there was only a 0,15% chance to get a good result, thus the need to run the algorithm 3 million times to compute an average. When Sycamore is used for useful algorithms, fewer than 20 qubits are used and we're far off any quantum supremacy or advantage.

Cristian and Elena Calude of the University of Auckland in New Zealand then argued that a high-performance limit, that of a precise quantum computer, is compared to a low limit which is the best performance in solving the same problem in a supercomputer[1903]. Quantum supremacy is thus a comparable between the existence of a quantum performance and the assumption of the non-existence of an equivalent performance in classical computing.

A 2020 paper from Yiqing Zhou (University of Illinois), Edwin Miles Stoudenmire (Flatiron Institute) and Xavier Waintal (CEA-IRIG) provided an interesting "reset" view on Google's quantum supremacy. It stated that emulating Sycamore's processes in a classical computing could use some compression technique to take into account the qubit's noise. With this compression, emulating Sycamore is much less costly and can be done on a simple microcomputer[1904]. But this corresponded to a 95% emulated gates fidelity. With a 99% fidelity matching Sycamore, it would still require a couple hundred cores and some TB of memory, fitting in a datacenter rack. There would be an energy advantage for Sycamore but going down from x500.000 vs the IBM Summit to about only x325 for a 500 core cluster server. A Chinese research team published an even better performance in 2021, using an improved tensor contraction technique and running for 15 hours on a cluster of 512 GPUs[1905].

In 2022, Xavier Waintal, Edwin Miles Stoudenmire and a team of Atos researchers including Thomas Ayral improved their classical simulation of Google's supremacy with a density-matrix tensor networks renormalization group (DMRG) algorithm. It did run on a few classical CPU cores from an Atos QLM and in a couple hours. The algorithm has a simulation cost scaling polynomially with the number of qubits and the depth of the circuit.

[1900] See First proof of quantum computer advantage, October 2018 and Quantum advantage with shallow circuits, April 2017 (23 pages).

[1901] See Simpler Proofs of Quantumness by Zvika Brakerski et al, May 2020 (12 pages).

[1902] See The power of random quantum circuits by Bill Fefferman, 2019 (25 slides) that explains the power behind the randomized benchmarking technique chose by Google.

[1903] In The road to quantum computing supremacy, 2017.

[1904] See What limits the simulation of quantum computers? by Yiqing Zhou, Edwin Miles Stoudenmire and Xavier Waintal, PRX, November 2020 (14 pages).

[1905] See Solving the sampling problem of the Sycamore quantum circuits by Feng Pan, Keyang Chen, and Pan Zhang, PRL, July 2022 (9 pages).

A consequence of this work is that to reach an exponential quantum computing advantage, it is more important to increase qubit fidelities than their number[1906].

In 2021, a Chinese team was even able to classically simulate the Google Sycamore cross-entropy benchmark with a single Nvidia A100 GPGPU running for 149 days with a fidelity of 73,9% while Sycamore's fidelity was only 0,2%[1907]. Another Chinese research team, from Alibaba, found a way to optimize Sycamore's emulation in September 2021 to reach only 20 days of computing on a system equivalent of the IBM Summit[1908]. And yet another one in October 2021 could simulate it on the new Sunway supercomputer in 304 seconds, using a tensor compression technique[1909]. At last, in October 2022, Gil Kalai et al produced an in-depth and well-crafted detailed analysis of Google's supremacy experiment and related protocoles[1910].

Likewise, and the other way around, a Google team did show that the 2021 Chinese gaussian boson sampling (GBS) supremacy experiment could be efficiently simulated classically (still, quadratically)[1911]. Another team, from the UK, achieved a similar feat in 2022, in which they did simulate a 100-mode and up to 60 click detection events GBS on a ~100,000-core supercomputer[1912].

In 2018, IBM researchers demonstrated that quantum supremacy was assured in the long run, even with quantum computers that can chain a finite and constrained number of quantum gates[1913]. In December 2020, they published a theorical model that could prove some quantum advantage, solving binary function problems, and tested on a low scale on a 27 qubits superconducting system[1914]. These various, sometimes convoluted, performances are very hard to compare and evaluate.

We cannot avoid mentioning the debates around the term supremacy with its bad social and political meaning. So far, I've seen only one replacement proposal, that hasn't been adopted yet, which consists in using the simpler term **primacy** with the same meaning[1915]. Another interesting fringe phenomenon is the usage of some quantum supremacy for things that are not at all related to quantum computing. It's borderline click baiting[1916]!

[1906] See A density-matrix renormalization group algorithm for simulating quantum circuits with a finite fidelity by Thomas Ayral, Thibaud Louvet, Yiqing Zhou, Cyprien Lambert, E. Miles Stoudenmire and Xavier Waintal, August 2022 (25 pages).

[1907] See Simulating the Sycamore quantum supremacy circuits by Feng Pan and Pan Zhang, March 2021 (9 pages). The authors improved their work in Solving the sampling problem of the Sycamore quantum supremacy circuits by Feng Pan et al, November 2021 (9 pages).

[1908] See Efficient parallelization of tensor network contraction for simulating quantum computation by Cupjin Huang et al, Alibaba, September 2021 (10 pages).

[1909] See Closing the "Quantum Supremacy" Gap: Achieving Real-Time Simulation of a Random Quantum Circuit Using a New Sunway Supercomputer by Yong (Alexander) Liu et al, October 2021 (18 pages). The China team behind this was awarded the 2021 ACM Gordon Bell Prize. Their work was later contradicted by ORNL researchers who had developed Google's supremacy classical simulation in 2019. See China's exascale quantum simulation not all it appears by Nicole Hemsoth, NextPlatform, November 2021.

[1910] See Google's 2019 "Quantum Supremacy" Claims: Data, Documentation, and Discussion by Gil Kalai, Yosef Rinott and Tomer Shoham, October 2022 (32 pages).

[1911] See Efficient approximation of experimental Gaussian boson sampling by Benjamin Villalonga, Hartmut Neven et al, September 2021 (15 pages).

[1912] See The boundary for quantum advantage in Gaussian boson sampling by Jacob F.F. Bulmer et al, 2022 (8 pages).

[1913] See Scientists Prove a Quantum Computing Advantage over Classical by Bob Sutor, October 2018, Quantum advantage with shallow circuits, Sergey Bravyi, David Gosset and Robert Koenig, 2017 (23 pages) and the video Quantum advantage with shallow circuits, IBM Research, December 2017 (44 minutes).

[1914] See Quantum advantage for computations with limited space by Dmitri Maslov, Sarah Sheldon et al, IBM Research, December 2020 (12 pages). Also published in Nature Physics in June 2021.

[1915] See Quantum Computing 2022 by James D. Whitfield et al, January 2022 (13 pages)

[1916] See Quantum supremacy in mechanical tasks: projectiles, rockets and quantum backflow by David Trillo et al, IQOQI Vienna, September 2022 (18 pages). It deals with some relativistic physics phenomenon.

Quantum advantage is a different concept. It corresponds to a situation where a quantum computer executes a useful algorithm faster than on the most powerful supercomputers. It seems at first glance not as strong an argument as with quantum supremacy, but it happens that it's more difficult to reach a quantum advantage than a quantum supremacy.

But some are pushing various definitions for quantum advantage. Sometimes, it even has the same meaning than quantum supremacy but with a more politically correct terminology and for others, it's a stronger statement than quantum supremacy, meaning the same but for a useful algorithm.

One key aspect of all supremacy claims is that they implement some random benchmark that is difficult to simulate digitally. Like with boson samplings, these are physical processes that are difficult to simulate. Supremacies are obtained with algorithms using no input data. Thus, they don't solve any useful problem. An advantage is supposed to solve a useful problem with some input and output data.

There are much fewer advantage claims than supremacy claims. And sometimes, they are misnomers or applied to very specific cases, even beyond quantum computing[1917]. And they have no more input data than with quantum supremacy claims.

One first example comes from an interesting work from a team of researchers from France and Edinburgh announced in February 2021, including Eleni Diamanti and Iordanis Kerenidis[1918]. It involved a complicated photonics-based experiment that didn't do any real calculation. It was about putting in place a QMA (Quantum Merlin Arthur) verification protocol. The implemented protocol is an interactive test that requires, through a network, the verification of the solution of a complex NP-complete optimization problem without having to communicate the whole solution. The breakthrough that made this possible was the creation of a system encoding the solution result with partial information about the solution to be verified from one network node to another. The protocol compresses a large vector state describing the partial information on the solution, involving some entanglement and multi-mode photons quantum communications. This compression protocol would make it possible to verify the results in a much smaller time. No actual verification was done on the other end of the system.

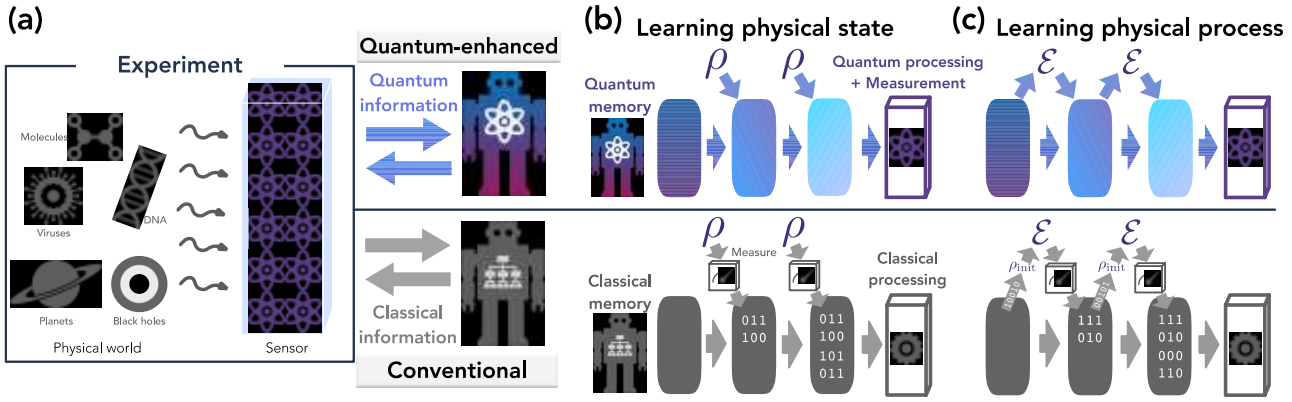


Figure 656: a quantum advantage can come from connecting quantum sensors and quantum computers, avoid the tedious steps of quantum-to-classical and classical-to-quantum data conversions. Source: Quantum advantage in learning from experiments by Hsin-Yuan Huang, Hartmut Neven, John Preskill et al, December 2021 (52 pages) with 40 Sycamore qubits.

[1917] See Quantum Advantage of Threshold Changeable Secret Sharing Scheme by Xiaogang Cheng et al, September 2022 (11 pages) which deals with secret key exchanges using quantum computing but not about solving an NPish problem.

[1918] See Experimental demonstration of quantum advantage for NP verification with limited information by Federico Centrone, Niraj Kumar, Eleni Diamanti, and Iordanis Kerenidis, published in Nature Communications, February 2021 (13 pages). This was a follow-up of Quantum superiority for verifying NP-complete problems with linear optics by Juan Miguel Arrazola, Eleni Diamanti & Iordanis Kerenidis, Nature, 2018 (8 pages).

We have here a quantum advantage coming from the way to connect a quantum computer solving an NP-complete SAT problem and another quantum computer verifying the solution with partial information. Both computers do not exist yet. Another view on this would be that it proposes an architecture to verify a solution to an NP-problem on an end-to-end solution.

Another example of quantum computing advantage could be reached with feeding a quantum computer with data coming from quantum sensors data and transmitted "quantumly" instead of classically. That's what demonstrated a team of Google and other researchers in 2021 and shown in Figure 656[1919]. This requires some form of quantum memory that is still to be created.

Many experts estimate that the threshold of 50-ish quality qubits, with a low error rate and a long coherence time, will be needed to achieve any real quantum advantage. These will probably be logical qubits, assembling physical qubits and some quantum error correction codes.

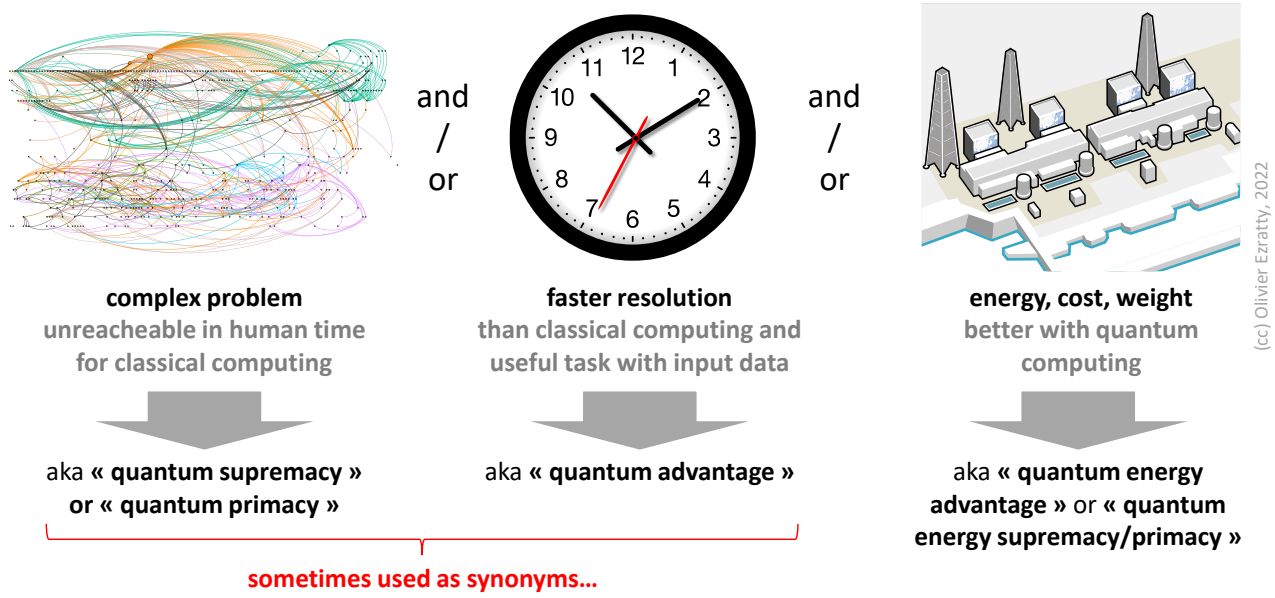


Figure 657: trying to define quantum supremacy (or primacy) and quantum advantage. (cc) Olivier Ezratty, 2022.

Quantum energy advantage is another threshold that may arise someday when on top of some computing time benefits, we could highlight the fact that quantum computers consume much less energy than supercomputers for solving similar problems. This is still a subject of research and dealt with as part of the QEI that is described page 251[1920].

Here's a tabulated consolidation of the various quantum supremacies and advantages announced since 2019[1921]. It shows that between 2019 and 2021, none of these achieved real useful computing with some application input data. And in 2022, we start to see appearing some real or potential interesting and narrow quantum advantages with input data.

The IBM et al example below was touting a quantum advantage, but it would require a NISQ QPU with 96-qubits and 99,99% 2-qubit gates and measurement fidelities which is extrapolated from a 12-qubit Quantinuum QPU having such fidelities. Problem is these trapped ion QPUs are quite hard to scale.

[1919] See Quantum advantage in learning from experiments by Hsin-Yuan Huang, Hartmut Neven, John Preskill et al, December 2021 (52 pages) with 40 Sycamore qubits.

[1920] See the Quantum Energy Initiative already discussed elsewhere in this book starting page 259.

[1921] The Arizona performance is documented in Researchers demonstrate a quantum advantage by University of Arizona, June 2021, referring to Quantum-Enhanced Data Classification with a Variational Entangled Sensor Network by Yi Xia et al, June 2021 (17 pages). Their setting used variational quantum circuits for a classification of multidimensional radio-frequency signals using entangled sensors.

who and when	architecture	algorithm	input data	comment
Google, Oct 2019	Sycamore, 53 superconducting qubits	cross entropy benchmarking	**none**	running a random gates algorithm
China, December 2020	70 photons modes GBS (Gaussian Boson Sampling)	interferometer photons mixing	**none**	running a random physical process
IBM Research, December 2020	IBM 27 superconducting qubits	symmetric Boolean functions	SLSB3 function parameters	**theoretical demonstration of quantum advantage**
Kerenidis, Diamanti et al, March 2021	multi-mode photon dense encoding of verified solution	Quentin Merlin Arthur based verification	output from some quantum computation (not implemented)	**no actual computing done in the experiment**
China, April 2021	Quantum walk on 62 superconducting qubits	simple quantum walk	simulating a 2-photons Mach-Zehnder interferometer	**no quantum advantage at all**
University of Arizona, May 2021	supervised learning assisted by an entangled sensor network	variational algorithm, classical computing	data extracted from three entangled squeezed light photonic sensors	**not a quantum « computing » advantage per se**
China, June 2021	66 superconducting qubits and 110 couplers, Zuchongzhi 1, then 2.1	cross entropy benchmarking	**none**	56 used qubits
China, September 2021				60 used qubits
China, June 2021	144 photons modes GBS and up to 113 detected events	interferometer photons mixing	**none**	**parametrizable photon phases could lead to a programmable system**
Google, AWS, Harvard et al, December 2021	quantum sensors feeding a quantum computer	learning about the principal component of a noisy state	**quantum output from quantum sensors**	**requires some quantum memory**
Xanadu June 2022	216 squeezed photons modes GBS (Gaussian Boson Sampling)	time domain multiplexingand interferometer photons mixing	**programmable GBS with 1,296 parameters**	**first programmable GBS**
IBM et al, September 2022	hybrid algorithm that could run on NISQ QPUs	QML-TDA unsupervised machine learning technique for extracting valuable shape-related data features	**small data sets related to cosmic microwave background**	**exponential speedup, resilient to noise, requires 96-qubit QPU with 2Q gate and measurement fidelity of 99.99%...**

Figure 658: an inventory of past quantum advantages/supremacies announcements and their underlying characteristics. (cc) Olivier Ezratty, 2022. Sources: Google 2019: Quantum supremacy using a programmable superconducting processor by Frank Arute, John Martinis et al, October 2019 (12 pages). China 2020: Quantum computational advantage using photons by Han-Sen Zhong et al, December 2020 (23 pages). IBM 2020 : Quantum advantage for computations with limited space by Dmitri Maslov et al, December 2020 (12 pages). Kerenidis / Diamanti 2021: Experimental demonstration of quantum advantage for NP verification with limited information by Federico Centrone, Niraj Kumar, Eleni Diamanti, and Iordanis Kerenidis, published in Nature Communications, February 2021 (13 pages). China April 2021: See Quantum walks on a programmable two-dimensional 62-qubit superconducting processor by Ming Gong, Science, May 2021 (34 pages). Arizona 2021: Quantum-Enhanced Data Classification with a Variational Entangled Sensor Network by Yi Xia et al, June 2021 (19 pages). China June 2021: Strong quantum computational advantage using a superconducting quantum processor by Yulin Wu, Jian-Wei Pan et al, June 2021 (22 pages). China September 2021: Quantum Computational Advantage via 60-Qubit 24-Cycle Random Circuit Sampling by Qingling Zhu, Jian-Wei Pan et al, September 2021 (15 pages). China June 2021: Phase-Programmable Gaussian Boson Sampling Using Stimulated Squeezed Light by Han-Sen Zhong, Chao-Yang Lu, Jian-Wei Pan et al, June 2021 (9 pages). Google, AWS, Harvard: Quantum advantage in learning from experiments by Hsin-Yuan Huang, Hartmut Neven, John Preskill et al, December 2021 (52 pages) with 40 Sycamore qubits. Xanadu: Quantum computational advantage with a programmable photonic processor by Lars S. Madsen et al, Xanadu, June 2022 (11 pages). IBM: Towards Quantum Advantage on Noisy Quantum Computers by Ismail Yunus Akhalwaya et al, September 2022 (32 pages) also discussed in Quantifying Quantum Advantage in Topological Data Analysis by Dominic W. Berry, Ryan Bab bush et al, September 2022 (41 pages) and contested in Complexity-Theoretic Limitations on Quantum Algorithms for Topological Data Analysis by Alexander Schmidhuber and Seth Lloyd, September 2022 (24 pages).

Quantum software development tools key takeaways

- Gate-based programming involves either graphical circuit design (mostly for training purpose) and (usually) Python based programming when qubit gates structures must be designed in an automated way.
- Python based programming is relying on libraries like IBM's Qiskit or Google's Cirq. There are however many development tools coming from universities and research labs like Quipper. Some tools like ZX Calculus are highly specialized and used to create quantum error correction codes or low-level systems.
- Quantum computing is based on running code multiple (thousands...) times and averaging the results. A single individual run yields a probabilistic outcome while many run averages will converge into deterministic ones.
- Most quantum computers are used in the cloud, through offerings coming from the computer vendors themselves like IBM or D-Wave or from cloud service providers like Amazon, Microsoft, Google and OVHcloud.
- Quantum emulators are very useful to learn programming, test it until the limits of classical emulation (about 40-50 qubits) and also help debug small-scale quantum algorithms. When these emulators include physical simulators of the underlying qubit physics like with Bosonic Qiskit and Quandela Perceval, they help create algorithms that are error-resilient and create quantum error correction codes. Quantum emulation is an indispensable part of any quantum cloud offering.
- Gate-based programs debugging is a significant challenge as it is difficult to implement equivalents of classical code breaking points. As a result, quantum code certification and verification is a new key discipline, particularly for distributed computing architectures such as the ones relying on the concept of blind quantum computing.
- Benchmarking quantum computers is an unsettled technique with many competing approaches. It includes the various techniques used to qualify so-called quantum supremacies and quantum advantages. Not a single of them, as of 2021, did show a real computing advantage compared to classical computing. The reasons were multiple, the main ones being that these experiments didn't implement any algorithm using some input data. But starting in 2022, we see appearing some relevant quantum advantage with actual data and useful algorithms running on NISQ hardware.

Quantum computing business applications

Most algorithms mentioned before are generally very low-level. How about assembling them into business solutions, market by market? We are still far from having things settled for that respect. The quantum software industry is still very immature and for good reasons, since quantum computers are very limited at this stage. We are still in a stage equivalent where the computer industry was in the mid-1950s, when the software industry was in its infancy.

Still, you can discover here and there a lot of so-called case studies, mostly pushed by D-Wave and IBM and their customers or partners. These relate to proof-of-concepts and software prototypes. Most of these are not yet production grade nor bring any practical benefit compared to classical computing due to the limitations of existing hardware. Still, all this is very useful. This is an indispensable learning phase for research, startups and the industry. It's part of a readiness process that will speed things up when hardware will ramp-up. And this ramp-up will happen progressively.

Market forecasts

Any new technology wave brings its market forecasts data born out of analysts and market survey companies. They have a very traditional closed-loop system in place: vendors want to get some ideas of customer demand or positive confirmation of their own biases, analysts poll large customers to get some understanding about their plans, and *voila*, you get your nice market predictions. It often looks like linear or simple nonlinear regressions. These predictions can become either self-fulfilling prophecies or total failures. The Gartner Group has turned its simplistic hype curve into a kind of Schrödinger's time and topic-independent wave equation of technology trends. But nobody really checked it, particularly when this curve was highly dependent on complicated scientific and technology challenges. It's more about probabilities than simplistic curves. Today, avoiding any cautious, the current analyst mantra is to claim that the uncertainty on the advent of quantum computing is not "if" but "when", based more on market assessments than on quantum physics and technologies roadmaps understanding.

So, how could you predict the size and shape of the quantum software market, vertical per vertical, when you have no idea of when actual useful quantum accelerators will show up? Will it follow an exponential market growth rate worthy of those of the microcomputer and smartphones industries? Let's look at what we have in store.

BCG's quantum computing growth forecasts illustrate this strong uncertainty. They showcase predictions with an optimistic scenario, which starts seeing growth around 2030, and a very conservative one, which only takes off after 2040[1922]. In both cases, the quantum computing market grows linearly. They don't integrate a scenario of the emergence of the NISQ, or "Noisy Intermediate-Scale Quantum", or any advent of quantum simulators before NISQ become usable[1923].

BCG has however created in 2018 a good inventory of the current potential qualitative use cases of quantum computing per vertical market. This covers both case studies coming from D-Wave and prospective applications devises by research labs and with large industry companies including the usual suspects from the aerospace, chemistry, energy, pharmaceuticals and financial sectors.

Most of these big names worked with either D-Wave or IBM, and sometimes with some independent software vendors or large IT services firms like Accenture.

[1922] See The coming quantum leap in computing, BCG, May 2018 (19 pages).

[1923] See Quantum Computing in the NISQ era and beyond, John Preskill, 2018 (20 pages).

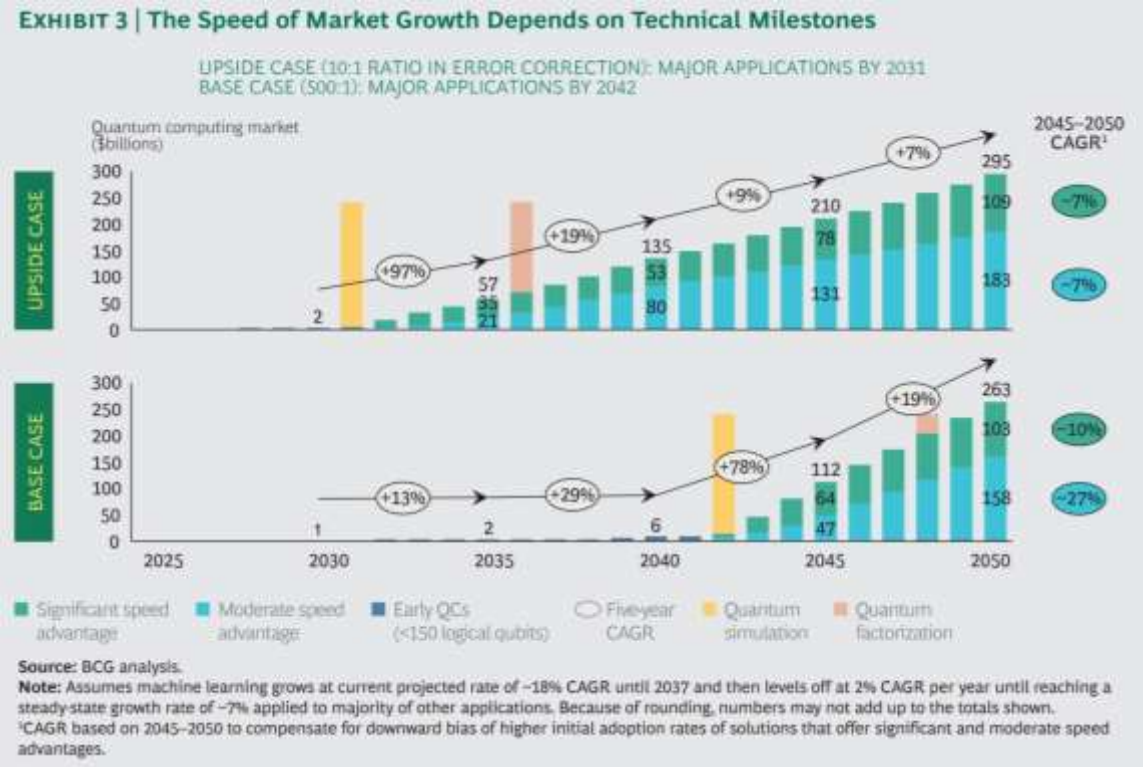


Figure 659: BCG market forecast from 2018 with optimistic and pessimistic scenarios. Source: [The coming quantum leap in computing](), BCG, May 2018 (19 pages).

Figure 660: quantum computing use-case scenarios per vertical. Source: [The Next Decade in Quantum Computing and How to Play]() by Philippe Gerbert and Frank Ruess, BCG, 2018 (30 pages).

In another chart, BCG positions these vertical markets along two dimensions: business value and expected time of quantum advantage. This is more gut feeling than any real rationale thinking since there are too many variables to have any idea of where each of these industries sit in this fancy chart. We are at a too early stage of the quantum computing innovation cycle to make such predictions.

Figure 661: correlation between use cases business value and expected timing for a quantum advantage. Four years later, this raw classification remains valid. Source: The Next Decade in Quantum Computing and How to Play by Philippe Gerbert and Frank Ruess, BCG, 2018 (30 pages).

Predicting the size of the quantum computing market is indeed highly probabilistic. It's supposed to reach $553M in 2023 according to **Markets and Markets** (in 2017), $830M in 2024 for **Hyperion Research** (in 2021[1924]), $1,9B in 2023 for CIR and $2,64B in 2022 for **Market Research Future** (2018). Then we reached $8,45B in 2024 for **Homeland Security** (in 2018), $10B in 2028 for **Morgan Stanley** (as of 2017), $15B by 2028 for **ABI Research** (2018) and $64B by 2030 for **P&S Intelligence** (in 2020). **ResearchAndMarkets** predicted in May 2021 that the global quantum technology market would even reach $31.57B by 2026, including $14.25B for quantum computing[1925]. **IDC** planned for a 6-year compound annual growth rate (CAGR) of 50.9% over the 2021-2027 period with a market reaching $8.6 billion in 2027[1926]. At last, **The Quantum Insider** has its own predictions with a total quantum computing market between $300M and $1.3B in 2021 that could grow to between $3.5B and $10B by 2025 and between $18B and $65B by 2030 with a CAGR of between 70% and 80% from 2021 to 2025, to slow down between 39% to 45% between 2025 to 2030[1927].

[1924] See Quantum Computer Market Headed to $830M in 2024 by John Russell, HPC Wire, September 2021. Hyperion's forecasts have ups and downs. See New Study Estimates More Than 20 Percent Annual Growth of Global Quantum Computing Marketplace Through 2024, Hyperion Research, February 2022. The forecast is based on polling 112 quantum computing vendors from around the world and was funded by QED-C and QC Ware. A previous 2020 forecast did plan for a 27% annual increase and now, we are at 21,9%!

[1925] See The Worldwide Quantum Technology Industry will Reach $31.57 Billion by 2026 - North America to be the Biggest Region, May 2021.

[1926] See Quantum computing market landscape by TBR Research which is reviewing only 26 vendors, including two who have either nothing to sell (Intel) or doing nothing (Nokia) in quantum computing.

[1927] See Quantum Computing Market Size Expects Double-Digit Growth by Matt Swayne, December 2021.

Some forecasts can reach other crazy heights. For **Bank of America**, quantum technologies will be as important as smartphones. The main reason? Its potential applications in healthcare. To make sure, the point is made, Haim Israel from this bank also touted that quantum computing will be more important that the invention of fire which is a bit stretch[1928].

The only problem: many analyses behind these predictions gets confused between big data and quantum computing[1929]. Some are based on vendors expectations, other on customers fuzzy plans to adopt quantum computing, given nobody has a real clue of when and how it will work.

As of early 2020, **McKinsey** even predicted that quantum computing would be worth $1 trillion by 2035[1930]. It is easy to identify the forecast bias used here. It's based on a trick that was used a few years ago to evaluate the size of Internet of things and artificial intelligence markets. In 2022, they reused the same methodology to forecast the Metaverse would create $5T of value by 2030[1931]. It is not the market estimation for quantum technologies as such, but the incremental revenue it could generate for businesses, such as in pharmaceuticals, financial services or transportation. It is a bit like evaluating the software market (which was around $593B in 2021, including $237B in enterprise software, source Statista) by summing up the total revenue of the companies who use some software! This would be quite a large number and a significant share of worldwide GDP[1932]. Market predictions should focus on IT products, software and services and should be compared with existing reference markets. For example, the 2020 worldwide servers market size was $85.7B according to IDC[1933].

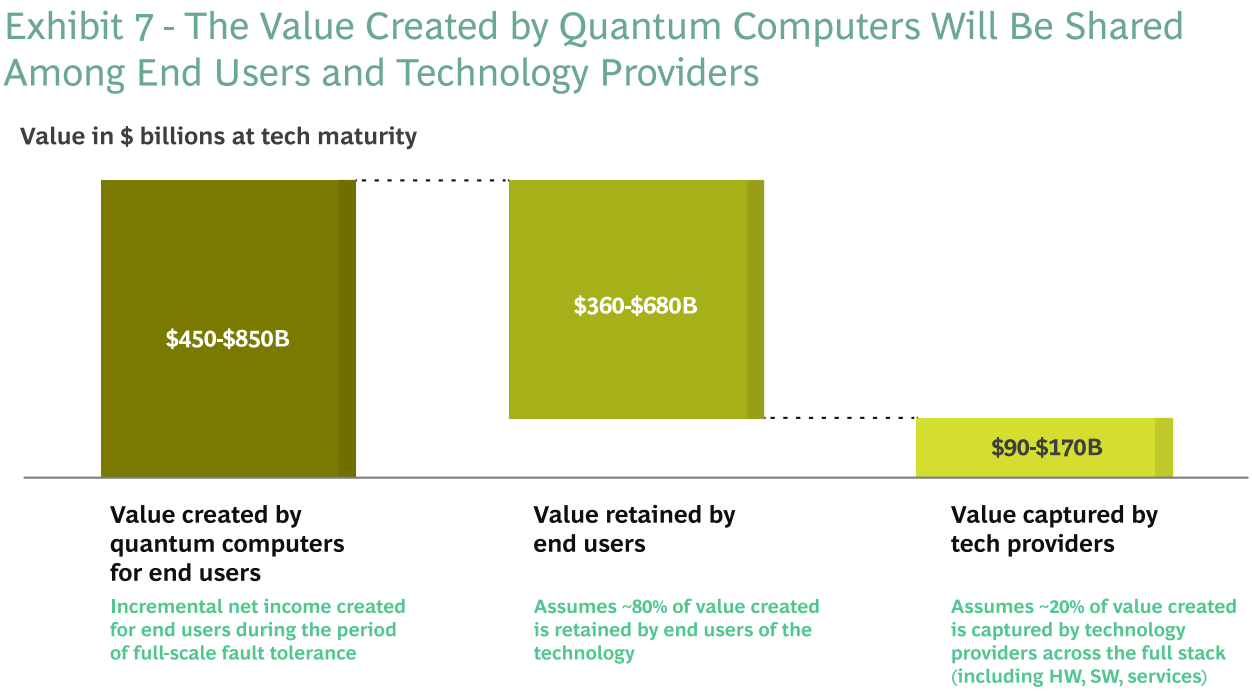


Figure 662: BCG's 2021 estimation of the market value created by quantum computers and the share of this value that could be captured by the quantum industry, broadly estimated at 20%. By 2040! Source: What Happens When 'If' Turns to 'When' in Quantum Computing, BCG, July 2021 (20 pages).

[1928] See Quantum Computing Will Be Bigger Than the Discovery of Fire! By Luke Lango, August 2022.

[1929] See Quantum computing will be the smartphone of the 2020s, says Bank of America strategist by Chris Matthews, December 2019.

[1930] See Quantum computing will be worth $1 trillion by 2035, according to McKinsey, March 2020.

[1931] See On the road to change Value creation in the metaverse, McKinsey, June 2022 (77 slides). Il mentions "$120B invested in 2022" but this includes M&As like the $69B acquisition of Activision by Microsoft and only $6B to $8B real investments in startups through venture capital.

[1932] Analysis shared in McKinsey Forecasts Quantum Computing Market Could Reach $1 trillion by 2035, April 2020.

[1933] IDC quarterly 2020 server market estimates: Q1, Q2, Q3 and Q4 with respectively $18,6B, $18,7B, $22,6B and $25,8B.

In a 2021 publication[1934], **BCG** estimated the size of the quantum computing market as 20% of its estimated generated value with customers of $850B, ending with a $90B to $170B market captured by technology providers, including software and services... some day after 2040, and a more reasonable $1B to $2B before 2030 and $15B to $30 after 2030.

So, we have here an uncertainty based on an unknown estimated with some fuzzy technology capability predictions. The problem is some vendors take these data for a market size in their investor pitch presentations, not as a generated value size[1935]. It is highly misleading.

On its end, The Quantum Daily forecasted in 2021 that the "Quantum Cloud as a Service" (QCaaS) market would reach $26B by 2030, and tried to document its methodology with reminding us that it was based on vendors questionable roadmaps[1936].

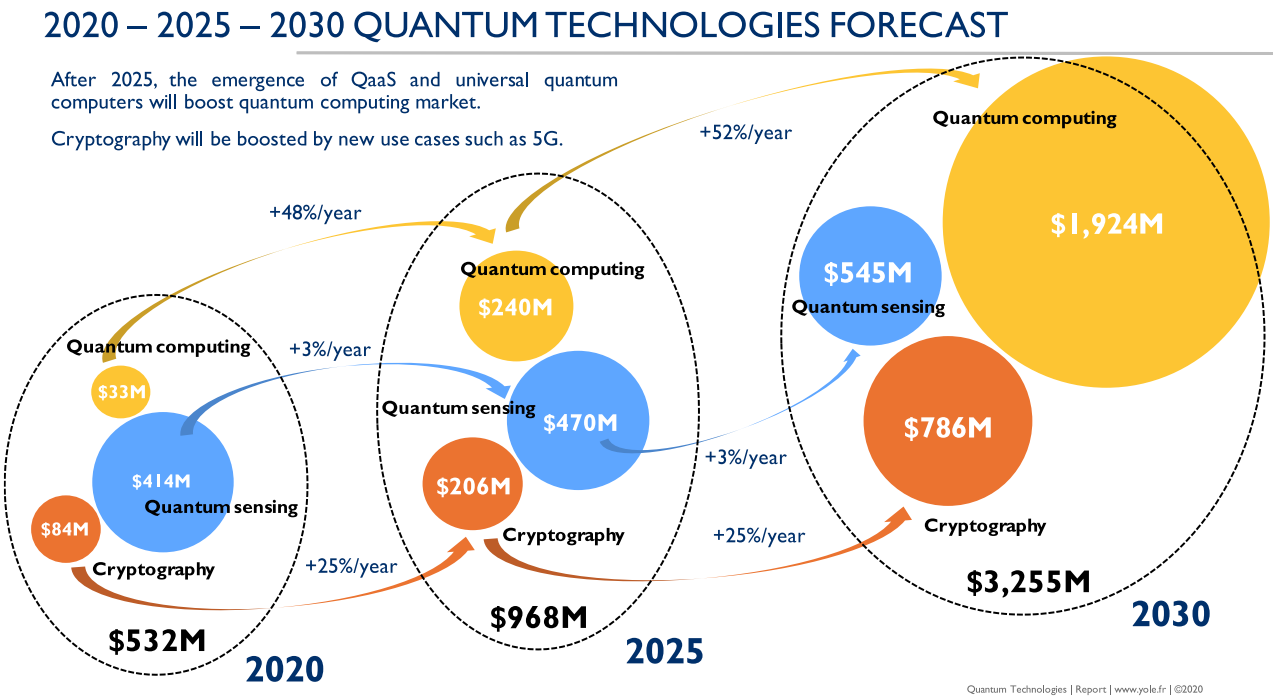


Figure 663: Yole Development's sizing of the quantum technology market by 2030. Source: Quantum Technologies Market and Technology Report 2020 -Sample, Yole Development, 2020 (22 slides).

A more detailed market size assessment was made in 2020 by **Yole Development** with seemingly more reasonable predictions for quantum technologies, with an increase to $3.2B per year by 2030, with 17% average annual growth, including $650M for hardware, $1.37B for cloud-based software and $785M for quantum cryptography (QKD)[1937].

The sensor market would grow from $400M in 2019 to $545M in 2030. This moderate growth seems a bit bearish since quantum sensors are the quantum objects with the lowest technological uncertainties and it is a market in its infancy.

[1934] See What Happens When 'If' Turns to 'When' in Quantum Computing, BCG, July 2021 (20 pages).

[1935] Two examples here with the Q2 Rigetti Quarterly report in August 2022 which describes these $850B as a highly ambiguous "*forecasted quantum computing generated operating income*" and Atlantic Quantum Emerges from MIT's Engineering Quantum Systems Lab, Raises $9M Seed Funding to Make Large-Scale Quantum Computing a Reality by James Dargan, from The Quantum Insider that is reusing a press release from Atlantic Quantum, July 2022, saying "*The enterprise quantum computing market could grow to a $450—$850 billion market in the next 15-to-30 years, according to Boston Consulting Group (BCG)*". It says it all about the confusion generated by these market value market data.

[1936] See Quantum Computing as a Service Market Sizing - How we dit it, The Quantum Daily, August 2021.

[1937] See Quantum technologies: a jump to a commercial state, Yole Development, 2020 and their sample Quantum Technologies Market and Technology Report 2020 -Sample, 2020 (22 slides).

The quantum team at **Total** constructed this interesting roadmap to provide an idea of the order in which practical quantum applications could emerge according to the number of available qubits.

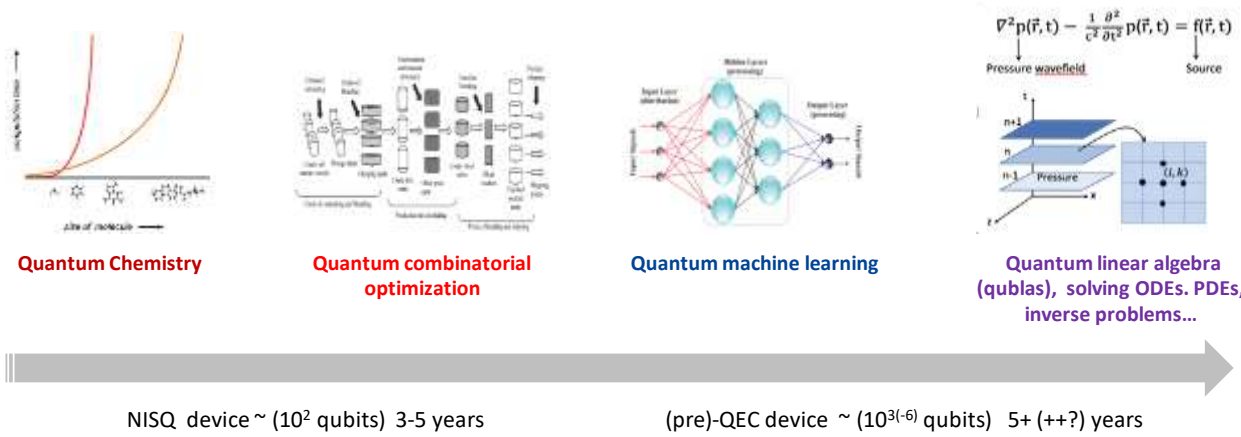


Figure 664: practical quantum computing use cases emergence by domain. Source: Total QCB Conference, Paris, June 2019.

Since we have no real idea of when scalable quantum computing will really work, let's try another exercise to determine the critical factors enabling some sort of technology commoditization for quantum computing:

Technology. The first factor is a mix of where and when we'll have first, useful quantum simulators, then useful NISQ, and then scalable **universal quantum computers** with more than a hundred logical qubits. Meanwhile, optimization solutions adapted to D-Wave's annealer will continue to be developed and may reach a point where they make a real difference with classical computing.

Software Tools. The second factor may be the consolidation of software development tools. These tools will continue to mature, raising their level of abstraction, and adapt to hardware evolutions. Libraries adapted to the needs of specific markets will undoubtedly consolidate, as in molecular simulation or finance. As the market matures, there will be some consolidation in this market.

Skills. One critical path to market growth as it's been the case for most previous major technology wave will be the availability of skilled workforce, particularly with developers. They will have, at least at the beginning, to handle abstractions levels that have nothing to do with the different forms of programming techniques that dominate today's computing, even in its event-driven programming variants that are common in the creation of websites and graphic applications. It's more an extension of the existing scientific computing community. A new generation of algorithm designers and developers will emerge. These will probably be young professionals who will have been able to digest new quantum computing concepts with a clean state mind.

Startups. The market will rely mostly on the fabric of startups, probably slightly ahead of traditional software publishers and IT services companies that may not necessarily venture first into this new world of quantum.

Experience. The first feedback from pilot projects, already underway, particularly with D-Wave, will be important. Most recent projects bring interesting learnings on the actual accelerations that quantum computing can provide. We will have to learn to make objective comparison between quantum algorithms, quantum hardware architectures and their equivalents running (or not) on supercomputers. It will also be necessary to sort out into "proof of concepts" and projects actually deployed.

Mass impact. At last, quantum computing commoditization will depend on the potential emergence of solutions that will have an impact on our daily lives. So, mostly consumer applications. It could come from healthcare and transportation. Who knows. Uses cases will move gradually from the research community, to the corporate world, and then to consumer applications.

Healthcare

The healthcare market, and particularly pharmaceutical industries, is one of the most sought after by quantum computing players. It is the vertical markets with the largest number of dedicated startups. Most major pharmaceutical companies have been exploring and evaluating the potential of quantum computing for a few years, starting by conducting a few pilot projects with D-Wave[1938]. The dream is to extend the capabilities of today's supercomputers to simulate living organisms' molecules "in silico", mainly in order to create or discover new treatments. This is the field of "*in-silico drug discovery*".

This quest is linked to the pharmaceuticals industry worrisome situation, that is discovering fewer new treatments and seeing diminished portfolio of commercial patented drugs. The drugs development cycle from discovery to market is becoming increasingly expensive, particularly during clinical trials. It costs up to a $1B, if not more, and failure rates are numerous. 45% of cancer therapies clinical trials fail in phase III in the USA, and 97% of the new therapies tested are not approved by the FDA in the USA! If we could better digitally simulate the effects of new treatments before clinical trials, we might be able to increase these success rates. Also, quantum computing could be a critical tool to create digital twins of molecular complexes, used to find the right combinations and optimize their efficiency.

On top of news drugs discovery, pharmaceutical companies are also trying to leverage their existing portfolio with drugs re-targeting. It can speed up clinical trials since their adverse effects are already known. Even though this has not prevented the long controversy surrounding hydroxychloroquine in 2020! In any case, pharmaceutical players need simulation tools and in particular molecular simulation tools: to create molecules, from the simplest (peptides) to the most complicated (proteins, antibodies, vaccines), to model them in 3D, to analyze their interactions between their active sites and targets like cell surface proteins (transmembrane glycoproteins)[1939], and also to identify contraindications. Such treatments can be created ex-nihilo, but most often, they are derived from existing ones (known protein, enzyme, bio-inspiration, ...).

The pharmaceutical industry is organized in a couple consortia which help it share best practices, including in quantum computing adoption. The **Pistoia Alliance** was created in Pistoia, Italy, in 2007 by AstraZeneca, GSK, Novartis and Pfizer in 2007. It entertains a quantum computing community. **QuPharm** is a consortium of 17 pharmaceutical companies, including AbbVie, Bayer, GSK, Takeda, and Pfizer that is dedicated to quantum computing.

Molecular simulations

Molecular simulations are based on the broad field of computational chemistry. It originated with the description of the nature of chemical bonds by **Linus Pauling** in 1928, which launched the vast field of quantum chemistry. Chemical bonds describe the way electrons of covalent liaisons are shared between atoms and the shape of their related orbitals.

Pauling's work came just after the creation of the **Born-Oppenheimer** approximation in 1927[1940] which simplified Schrödinger's equation for a molecule by separating the nuclei of the atoms from their electrons. The same year, **Llewellyn Thomas** (1903-1992, English) and **Enrico Fermi** (1901-1954, Italian American) created the later-called Thomas-Fermi model which describes the electronic structure of multi-atoms systems.

[1938] Like Abbvie, Amgen, AstraZeneca, Bayer, Biogen, Bristol-Myers Squibb, Johnson&Johnson, Merck, Roche, Sanofi and Taleda.

[1939] We could try to digitally simulate an entire cell with all its organelles. This would become quite complicated since a living cell comprises about 100 trillion atoms!

[1940] The Max Born from the probabilistic explanation of Schrödinger's equation and the Robert Oppenheimer from the atomic bomb.

The field of computational chemistry began much later, in 1964, with the creation of the two Hohenberg-Kohn theorems by **Walter Kohn** (1923-2016, Austrian then American) and **Pierre Hohenberg** (1934-2017, French American).

This was closely followed by **Kohn-Sham**'s equations from **Lu Jeu Sham** (1938, Chinese) in 1965. They are the basis of **DFT** (Density Functional Theory), a mathematical model that describes the structure of molecules at rest as a function of inter-atomic interactions and the structure of their electron clouds, and in a simpler way than with Schrödinger's equation which manipulates too many variables. Walter Kohn was awarded the Nobel Prize in Chemistry in 1998 for this work, along with **John Pople** (1925-2004, English) who had contributed to the modeling of electronic orbitals in molecules.

DFT was followed by the work of **Martin Karplus** (1930, American), **Michael Levitt (**1947, Israeli-American) and **Arieh Warshel** (1940, Israeli-American) who contributed to the digital modeling of chemical reactions in the 1970s. They were awarded the Nobel Prize in Chemistry in 2013 for their work. The DFT model was also simplified by **Axel Becke** (1953, Canadian) in 1993 with the hybrid DFT. Some quantum versions of DFT are developed for quantum computing and with some progress, even for NISQ QPUs[1941].

Molecular simulation faces quasi-quantum effects related to the continuous vibrations of molecules in their aqueous medium. Chemical bonds oscillate at a femto-second rate, atoms vibrate collectively at a one picosecond rate. On the other hand, more complex chemical processes such as the production and folding of proteins occur on scales ranging from micro-seconds to seconds.

The Holy Grail would be to understand how the assembly and then operations of ribosomes work. These molecular complexes are made of 73 proteins and 4 large RNA molecules. Ribosomes produce all proteins in our cells using messenger RNA code, which is itself synthesized from DNA through an also amazing biochemical process involving many complex molecules. Thousands of ribosomes operate in every living cell and each ribosome is made of about 250,000 atoms[1942].

One of the most recent protein folding algorithm was able to simulate the folding of the 10 amino acid Angiotensin on 22 qubits. The same method was also applied to folding a 7 amino acid neuropeptide using 9 qubits, all on an IBM quantum computer[1943]. Many other projects have been launched to improve quantum-based protein folding and there are still theoretical since no existing quantum computer is powerful enough to execute them[1944]. One common algorithm used here is QAOA but its applicability is questioned[1945].

Today, most molecular simulation calculations are carried out using algorithms running on classical supercomputers, increasingly using GPGPUs such as those from Nvidia or Google's TPUs.

[1941] See Toward Density Functional Theory on Quantum Computers? by Bruno Senjean, Saad Yalouz and Matthieu Saubanère, University of Montpellier and University of Strasbourg, April-October 2022 (19 pages).

[1942] The number of 2.5 or 3.5 million atoms is often mentioned, but this is not true. These are "Daltons" which are equivalent to one twelfth of the mass of carbon 12, or about the mass of a hydrogen atom. However, these organic molecules contain, in addition to hydrogen, a lot of carbon, nitrogen, phosphorus and oxygen. The latter contribute to a large part of the mass of the molecule, hence the fact that the number of daltons must be divided by 10 to obtain the number of atoms of an organic molecule.

[1943] See Resource-efficient quantum algorithm for protein folding by Anton Robert et al, 2021 (5 pages).

[1944] See QFold: Quantum Walks and Deep Learning to Solve Protein Folding by P A M Casares, Roberto Campos and M A Martin-Delgado, March 2022 (22 pages), Folding lattice proteins with quantum annealing by Anders Irbäck et al, Lund University and Forschungszentrum Jülich, May 2022 (21 pages) which runs on a D-Wave Advantage and Protein Folding Neural Networks Are Not Robust by Sumit Kumar Jha et al, September 2021 (8 pages).

[1945] See Peptide conformational sampling using the Quantum Approximate Optimization Algorithm by Sami Boulebnane et al, April 2022 (30 pages). Conclusion: "*these results cast serious doubt on the ability of QAOA to address the protein folding problem in the near term, even in an extremely simplified setting*".

Another test was published in 2021 by GSK[1946]. It was about solving a mRNA codon optimization problem. Each amino acid in a protein sequence can be encoded by as many as six different codons, these series of three DNA/RNA bases encoding one amino acid. The goal was to find the right combination of these codons. The codon selection in mRNA impacts protein folding and functions. The main task is to balance G and C bases in mRNA to optimize gene expression. This was one of the first published case studies using D-Wave Advantage annealer and its 5000 qubits and their Leap Hybrid Solver. It worked well with 30 amino acids and could scale up to 1000 amino acids.

The codon optimization problem is formulated as a Binary Quadratic Model that is itself close to an Ising model adapted to D-Wave annealers. It did fare well when compared to genetic and machine learning algorithms running on classical computers.

The first small-scale tests of simulation using quantum algorithms were done on D-Wave and superconducting qubits accelerators. However, the most common approach is based on hybrid algorithms associating HPCs and quantum accelerators.

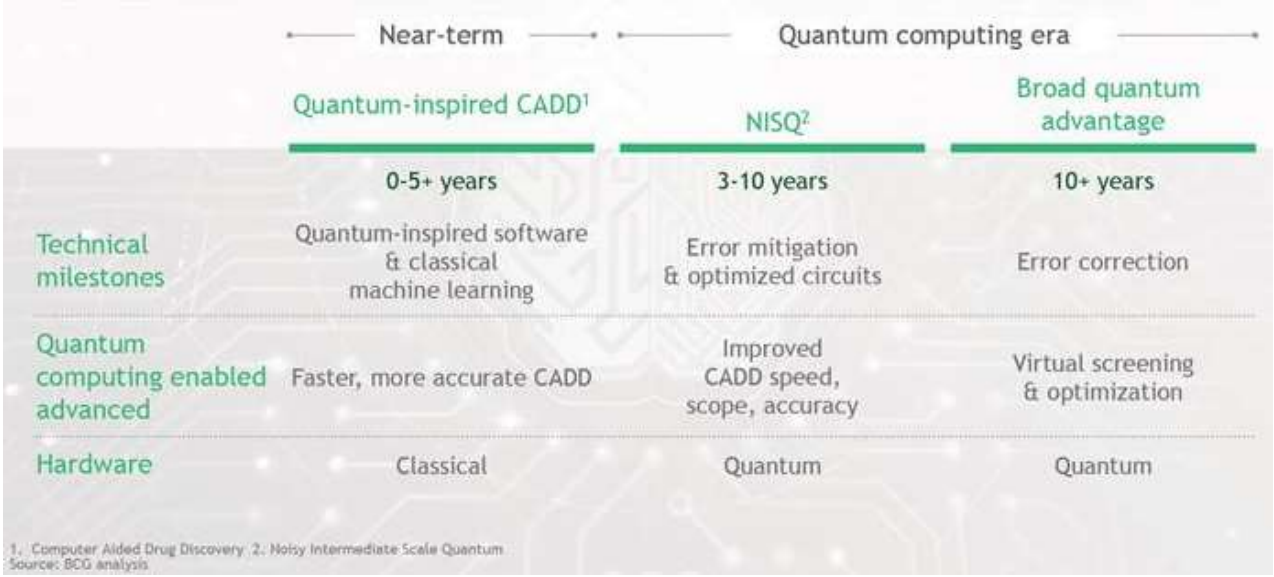


Figure 665: Source: Will quantum Computing Transform Biopharma R&D? by Jean-Francois Bobier et al, December 2019.

Quantum simulators are also machines suitable for simulating the interaction of atoms within molecules. BCG is thus presenting molecular simulation roadmaps spread out over time and following the rate of evolution of quantum computers between today's NISQ (intermediate-size noise computing) and LSQ (large scale quantum computing[1947].

One approach consists in relying on generic frameworks that can be distributed over classical computing in massively parallel architecture, and then progressively over quantum computing. This is the case of the **Tinker-HP** framework co-created by Jean-Philip Piquemal, co-founder of **Qubit Pharmaceuticals** and that the company plans to extend with hybrid quantum algorithms[1948].

[1946] See GlaxoSmithKline Marks Quantum Progress with D-Wave by Nicole Hemsoth, February 2021 pointing to mRNA codon optimization on quantum computers by Dillion M. Fox et al, February 2021 (35 pages).

[1947] See Will Quantum Computing Transform Pharma R&D by Jean-Francois Bobier, April 2020 (14 slides) and the written version Will quantum Computing Transform Biopharma R&D? by Jean-Francois Bobier et al, December 2019.

[1948] See Computational Drug Design & Molecular Dynamics by Jean-Philip Piquemal, April 2020 (28 slides) and Tinker-HP: a massively parallel molecular dynamics package for multiscale simulations of large complex systems with advanced point dipole polarizable force fields by Louis Lagardère, Jean-Philip Piquemal et al, 2018 (17 pages). The company plans to rely first on cold atoms simulators like those from Pasqal.

At this point in time, however, the priority is with quantum inspired algorithms[1949].

Most other quantum startups like **ApexQubit**, **HQS Quantum Simulations**, **MentenAI**, **ProteinQure** and **Qulab** are indeed adopting hybrid computing models, if only to have something practical to market[1950]. The most common hybrid method is the VQE (Variational Quantum Eigensolver)[1951].

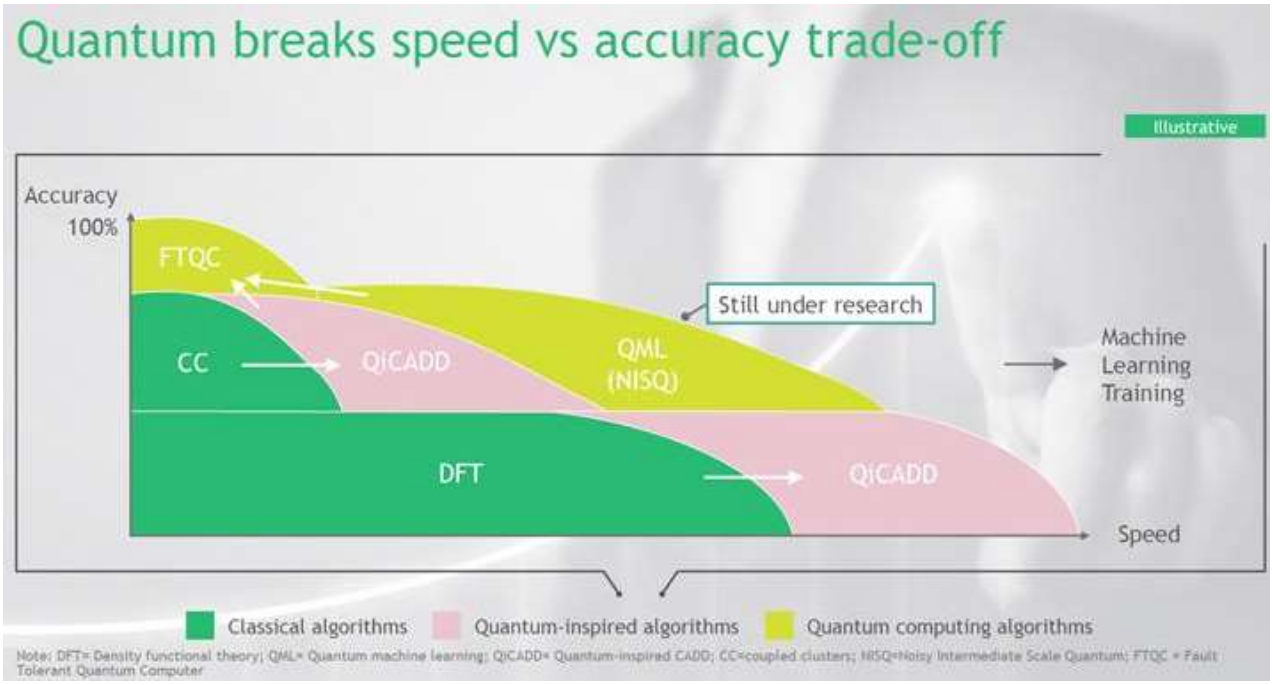


Figure 666: Source: Will quantum Computing Transform Biopharma R&D? by Jean-Francois Bobier et al, December 2019.

Another method is being developed to create quantum inspired algorithms, *aka* classical algorithms based on quantum algorithms[1952]. Quantum and quantum inspired computation complete the vast field of machine learning which is already very common in the discovery of therapeutic molecules[1953].

Molecules simulation can start with simple organic molecules like cholesterol up to protein folding which is many orders of magnitude more complex[1954]. This last feat is therefore bound to be a very long-term one.

Today, we can simulate peptides with about ten amino acids. The best algorithms require a number of qubits that evolves according to the power 4 of the number of amino acids[1955]. This simulation is also at the limit of feasibility in terms of complexity because it is in the class of NP-Complete problems as seen in the section dedicated to complexity theories, starting on page 629.

[1949] See Development of the Quantum Inspired SIBFA Many-Body Polarizable Force Field: I. Enabling Condensed Phase Molecular Dynamics Simulations by Sehr Naseem-Khan, Jean-Philip Piquemal et al, January 2022 (50 pages).

[1950] See Can Quantum Computing Play a Role in Drug Discovery? At least one Startup Thinks so by James Dargan, 2020, which mentions Menten AI.

[1951] See Quantum Chemistry and the Variational Quantum Eigensolver by S Kokkelmans et al, December 2019 (56 pages).

[1952] See Quantum and Quantum-inspired Methods for de novo Discovery of Altered Cancer Pathways by Hedayat Alghassi et al, 2019 (27 pages).

[1953] See Concepts of Artificial Intelligence for Computer-Assisted Drug Discovery by Xin Yang et al, 2019 (75 pages). A good review paper with 879 bibliographical references!

[1954] See Designing Peptides on a Quantum Computer by Vikram Khipple Mulligan, September 2019 (20 pages) which presents Rosetta, a protein quantum design tool running on D-Wave.

[1955] See Resource-Efficient Quantum Algorithm for Protein Folding by Anton Robert et al, August 2019.

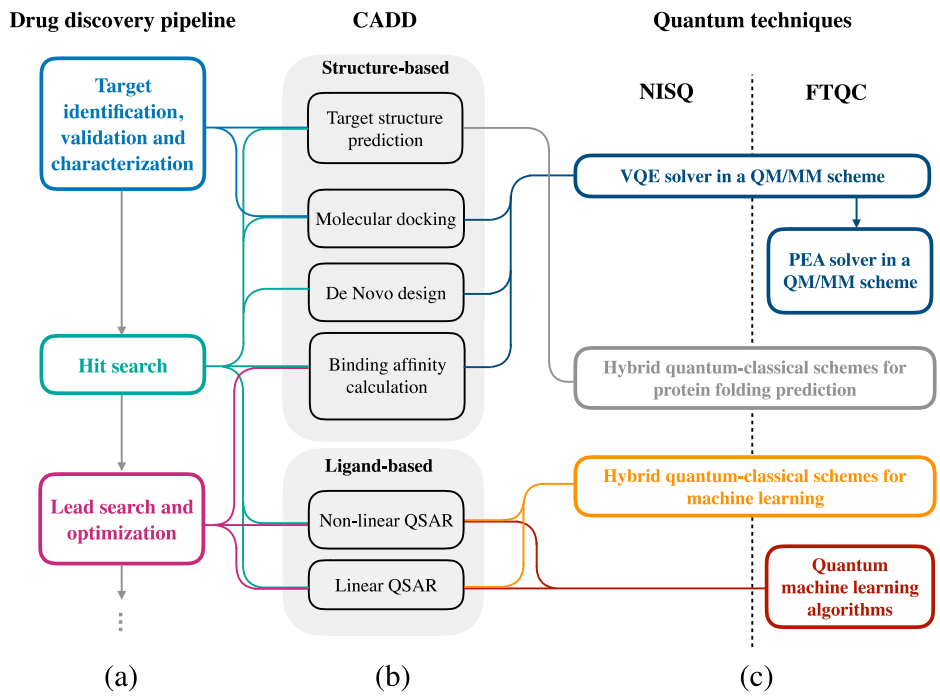


Fig. 1. (a) General workflow of drug discovery process. Here we focus on the early phase where computationally intensive quantum chemical analyses are involved. (b) Components of each stage of drug discovery that heavily involve quantum chemistry or machine learning techniques. (c) Quantum techniques that can be applied to the components listed in (b) and potentially yield an advantage over known classical methods. Here we make the separation between techniques for noisy intermediate scale quantum (NISQ) devices [21] and fault-tolerant quantum computing devices.

Figure 667: a process flow for drug discovery. CADD = Computer Aided Drug Design. Source: Potential of quantum computing for drug discovery by Alán Aspuru-Guzik et al, 2018 (18 pages).

78% of the search for therapies is focused on light molecules of less than 900 Daltons, i.e. about a hundred atoms. Its function is to associate itself with a target in the cells, often a specific protein that controls a metabolism that we want to attenuate or amplify[1956]. The discovery of small molecules of a few dozen atoms could be within the scope of the NISQ quantum computers within a few years. The first molecular simulation experiments were carried out on D-Wave. They work with the search for energy minima, which can be suitable in theory for the simulation of the organization of molecules.

A collaboration was launched in June 2017 between **Biogen,** the Canadian quantum software company **1QBit,** and **Accenture** for the creation of new molecules. **Biogen** (1978, USA) is a mid-size biotech company with 7300 employees specialized in the treatment of neurodegenerative diseases and leukemia.

Their use of quantum computing was aimed at retargeting therapeutic molecules, looking for matching between existing treatments and therapeutic targets in neurodegenerative or inflammatory diseases. **Amgen** is also active in the search for new therapies and is working since 2020 with **QSimulate** (2018, USA).

A similar project was launched in Spain with the consortium "QHealth: Quantum Pharmacogenomics applied to aging" launched in August 2020 with **aQuantum** (alhambraIT, Prologue Group) with **Gloin**, **Madrija** and various Spanish Universities. Its goals are to find correlations between physiological and genetic variables, drug usage history, side effects and/or potential lack of response of new drugs to fight aging. They plan to do simulations using quantum algorithms. The project totals 5.1M€ including a grant of 3.7M€ from CDTI awarded in November 2022 by the **Center for the Development of Industrial Technology** (CDTI) of the Ministry of Science and Innovation of Spain.

[1956] See Potential of quantum computing for drug discovery by Alán Aspuru-Guzik et al, 2018 (18 pages).

A hybrid quantum/classical machine learning algorithm was used for drug retargeting using Ligand Based Virtual Screening (LB-VS). It was developed in 2022 by **IBM** and **The Hartree Center** in the UK[1957].

In June 2019, **Merck** announced a three-year partnership with the Karlsruhe, Germany-based startup **HQS Quantum Simulations** for the development of quantum algorithms for chemical simulation. As already mentioned in the part related to SeeQC, **Merck** and SeeQC created together a consortium in 2021 to build a "*commercially scalable application-specific quantum computer designed to tackle prohibitively high costs within pharmaceutical drug development*". The project aw due for completion "*in 18 months*"! We are here in the pure overselling realm.

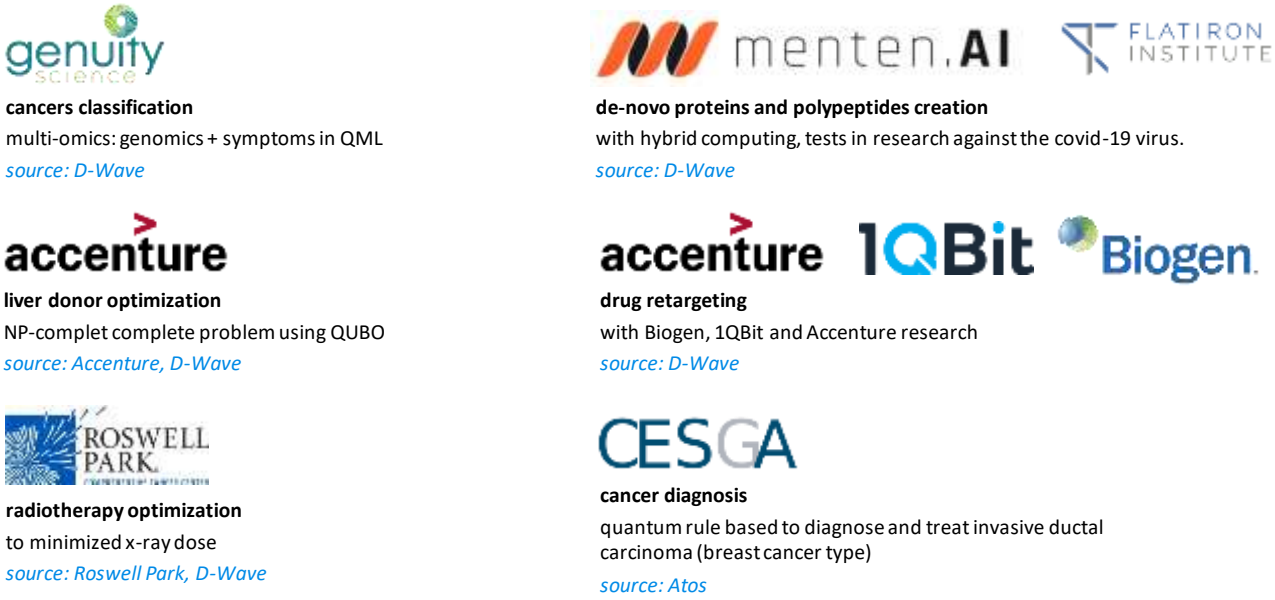


Figure 668: a couple quantum computing use cases in the healthcare industry. (cc) Olivier Ezratty, 2022.

In September 2022, **Novo Nordisk** (Denmark) made an announcement that was unique in shape and form. It is launching the Novo Nordisk Foundation Quantum Computing Programme with the goal to build Denmark's generic quantum computer in 2034 with a funding of $200M, and obviously to become a platform for chemical simulations. It will fund the Niels Bohr Institute but also embed partners from the USA, the Netherlands and Canada. They will invest first in three different qubit platforms and select the best one after a first 7-year period.

Genomics

The **DNA-Seq Alliance** combines the startup DNA-Seq and D-Wave, which also does molecular retargeting by combining genomics, protein kinase crystallography, quantum computing and the search for effective cancer treatments.

Let's also mention that quantum computing, both annealing and gate-based, could be used to accelerate **DNA sequencing**, particularly in de-novo mode, when no existing DNA mapping exists. It's about reconstructing a giant puzzle with small parts of DNA sequences which come out of sequencing[1958].

[1957] See Quantum Machine Learning Framework for Virtual Screening in Drug Discovery: a Prospective Quantum Advantage by Stefano Mensa et al, The Hartree Centre, STFC and IBM Research, April 2022 (16 pages).

[1958] See QuASeR - Quantum Accelerated De Novo DNA Sequence Reconstruction by Aritra Sarkar et al, TU Delft, April 2020 (24 pages).

As with any new technology, quantum computing specialists must learn to interact with bioinformatics specialists. Fortunately, bioinformaticians are already bridging the gap between molecular biology and computer science and are well positioned to learn quantum methods[1959].

Radiotherapy optimizations

Also on D-Wave quantum annealing computers, an application of radiotherapy optimization was experimented as shown in Figure 669.

The principle consists in minimizing patients' exposure to X-rays while optimizing their efficiency. It is a complex problem of simulating the diffusion of electromagnetic waves in the human body.

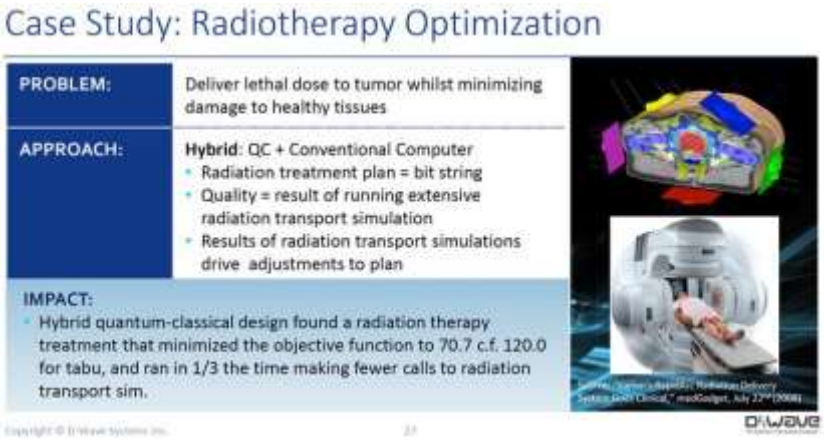


Figure 669: quantum computing can be used to optimize cancer radiotherapy. Source: D-Wave.

Medical imaging

Using quantum machine learning algorithms to do image recognition is also investigated. It may help train these systems with fewer data. At this point in time, however, existing algorithms are just on par with their classical peers[1960].

Precision medicine

David Sahner, who created his own consulting firm **Eigenmed**, is one of the promoters of precision medicine based on predictive machine learning techniques using D-Wave annealers[1961].

Omnicom Healthcare did not hesitate to promote in 2017 the use of quantum computing in healthcare in a white paper containing strictly no relevant information on the subject, especially since they seem to confuse machine learning applications analyzing data from connected objects with the ability of quantum computers to manage problems that are intractable by traditional computers[1962].

Network medicine analyzes disease pathogenesis, coupling information coming from Omics databases (protein-protein interaction, genomics data) and environmental factors with Bayesian networks and machine learning tools. The idea it to identify novel disease genes and pathways, their diagnostics and therapeutics. A 2022 paper from Algorithmiq and a Finland research team outlined how quantum computing could help there. Unfortunately, it didn't contain sizing recommendations for hardware and the problems it could solve[1963].

[1959] See Thirteen tips for engaging with physicists, as told by a biologist by Ken Kosik, January 2020 which describes how to bring physicists and biologists together.

[1960] See Quantum-classical convolutional neural networks in radiological image classification by Andrea Matic et al, April 2022 (12 pages).

[1961] See Predictive Health Analytics by David Sahner, 2018 (54 slides).

[1962] See Exponential Biometrics: How Quantum Computing Will Revolutionize Health Tracking, 2017 (7 pages).

[1963] See Quantum network medicine: rethinking medicine with network science and quantum algorithms by Sabrina Maniscalco et al, June 2022 (15 pages).

Covid-19

Finally, the covid-19 pandemic has led to a renewed interest in quantum computing. Several market players have put the cart before the horse in this respect. D-Wave has thus offered some of its machine time in the cloud for researchers in the field.

A couple tests were run in 2020 using D-Wave and IBM systems. In one case performed by Turkish scientists to classify CT scans images[1964]. Their quantum software generated 94% to 100% successful classifications while its classical counterpart did achieve 90% successful results. It was using only 4 qubits from 5-qubits systems (IBM Q-Rome and Q-London). It was a hybrid computing using the quantum transfer learning method. Quantum computing was used only for the classification part at the end of a convolutional network, not for the convolutions that remain classical, using 224x224 pixels versions of the CT scans, using a training set made of 2658 lung CT images with 1296 COVID-19 and 1,362 Normal CT images. They also tried emulators running with PennyLane, Qiskit and Cirq. The classification layer compressed 512 vectors into 4 vectors with a linear transformation.

Another test related to covid-19 research used a quantum assisted SVM classification using 16 qubits running on the IBM Q-Melbourne system and implementing feature mapping and hyperplane calculation with a variational quantum classifier[1965]. Classification was using time series of number of cases per counties in the USA. The classical part was done using the scikit-learn framework from Inria, France. Well, in the end, the research team observed that classical methods outperformed QML in accuracy, particularly with a high number of data points (>300).

Developed in China in 2022, **DeepQuantum** is a hybrid quantum deep learning algorithm was used to make predictions on mutant covid-19 variants[1966]. It was trained using a database of available mutated SARS-CoV-2 RNA sequences.

In practice, conventional HPCs helped molecules screening for therapies and to create 3D models of the covid virus and, in particular, of its glycoproteins that cling to the membranes of human cells in order to attack them and enable virus reproducing within cells[1967]. In 2022, a new SARS-CoV-2 main protease (Mpro) inhibitors was discovered using a classical GPU-based HPC using Atlas's platform from Qubit Pharmaceuticals[1968]. In the more or less distant future, quantum computing may have its say in similar pandemics[1969].

Energy and chemistry

Energy and chemistry are gathered here for their tight relationship. Quantum computing could help save energy in chemical engineering like with ammonia production. It could help improve the chemistry of batteries or carbon capture processes. At last, it could also help energy utilities optimize power grids. Most of these applications have been prototyped at a low scale but are not yet production-grade. The associated research can help determine the characteristics of the quantum computers needed to solve these various problems. The associated research works are relying mostly on quantum annealing with D-Wave machines and/or hybrid quantum computing.

[1964] See COVID-19 detection on IBM quantum computer with classical-quantum transfer learning by Erdi Acar and Ihsan Yilma, November 2020 (16 pages).

[1965] Another one: Quantum-Enhanced Machine Learning for Covid-19 and Anderson Insulator Predictions by Paul-Aymeric McRae and Michael Hilke, December 2020 (25 pages).

[1966] See Quantum Deep Learning for Mutant COVID-19 Strain Prediction by Yu-Xin Jin et al, TuringQ, CAS and USTC, March 2022 (34 pages).

[1967] See an example in TACC Supercomputers Run Simulations Illuminating COVID-19, DNA Replication, March 2020.

[1968] See Computationally driven discovery of SARS-CoV-2 Mpro inhibitors: from design to experimental validation by Léa El Khoury, Jean-Philip Piquemal et al, Chemical Science, 2022 (14 pages).

[1969] See Covid-19: Quantum computing could someday find cures for coronaviruses and other diseases by Todd R. Weiss, April 2020.

When we move away from organic molecules and living organisms, everything suddenly becomes almost realistic in quantum computing even if we're still far away from having the appropriate quantum hardware to run it! The molecular structures to study and simulate here are generally simpler than with organic chemistry of living organisms, particularly proteins[1970].

The first plausible quantum computing applications deal with the creation of innovative materials. The energy and chemistry sectors are interested in solving complex analysis and optimization problems, in the in-silico simulation of crystalline molecules and structures, and in creating new materials[1971].

The first case studies were, not surprisingly, first carried out with D-Wave's annealers. These seem to be well suited for simulations of atomic interactions in materials even though the provided accelerations are not stellar[1972]. Simulations can also be done with air, water and other liquid flows, and in particular their turbulence. In particular, they can exploit the famous Navier-Stokes equations[1973]. Beyond aerospace applications, it could have some applications in energy production turbines optimizations.

Chemistry

Most quantum chemical use case applications start with simulating molecules, and then, potentially, chemical reactions. Current quantum computers are able to simulate only molecules with a couple atoms[1974]. In September 2017, **IBM** simulated on a 16-qubit superconducting quantum computer a set of beryllium hydride molecules and their minimum energy balance[1975]. But this was done without reaching a quantum advantage, meaning, these simulations can well also be done on classical computers. It went up to 12 atoms from the benzene molecule, which was simulated with a quantum emulator supporting 35 qubits, by Total and Jean-Philip Piquemal (CNRS)[1976].

Many quantum computing hardware and software startups now propose development framework for quantum simulation of matter and chemical processes. They are mentioned in a later section with software vendors. We have for example **HQS** (Germany), **Quantinuum** who launched their InQuanto computational chemistry platform coming from CQC[1977], **Pasqal** (France, thanks to their 2021 M&A with Qu&Co), **Good Chemistry** (Canada), **Menten AI** (USA), **Q1t** (The Netherlands), **Qsimulate** (USA), **Qunasys** (Japan), **Riverlane** (UK) and **Zapata Computing** (USA).

[1970] See Enabling the quantum leap Quantum algorithms for chemistry and materials Report, January 2019 (115 pages) which provides a good overview of chemical simulation methods. It is a report of a workshop organized by the NSF.

[1971] See Quantum hardware calculations of periodic systems: hydrogen chain and iron crystals by Kentaro Yamamoto et al, September 2021 (13 pages) with some potential applications in steel manufacturing.

[1972] See Quantum Computing: Fundamentals, Trends and Perspectives for Chemical and Biochemical Engineers by Amirhossein Nourbakhsh et al, January 2022 (28 pages).

[1973] See Quantum Navier-Stokes equations by Pina Milišić from the University of Zagreb, 2012 (12 pages) and Navier-Stokes equations using Quantum Computing, July 2020.

[1974] See Is there evidence for exponential quantum advantage in quantum chemistry? by Seunghoon Lee, Ryan Babbush, John Preskill et al, August 2022 (81 pages). The study says that exponential speedups are not generically available.

[1975] See Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets, October 2017 (22 pages).

[1976] See Calculating the ground state energy of benzene under spatial deformations with noisy quantum computing by Wassil Sennane, Jean-Philip Piquemal and Marko J. Rancic, March 2022 (11 pages). See also Open Source Variational Quantum Eigensolver Extension of the Quantum Learning Machine (QLM) for Quantum Chemistry by Mohammad Haidar, Jean-Philip Piquemal et al, June 2022 (39 pages).

[1977] See Quantinuum launches InQuanto, a state-of-the-art quantum computational chemistry software platform using quantum computers, 2022.

Some chemical industry corps are investigating quantum computing use cases. **Dow Chemical** has been a **1Qbit** partner since June 2017 for pilot projects in quantum chemical simulation. **Mitsubishi Chemical** and the **Materials Magic** subsidiary of **Hitachi Metals** are also testing quantum computing with IBM.

Covestro (Germany), a polymer chemical production company and QC Ware started a 5-year collaboration in 2022 to use quantum algorithms for the discovery of new materials and catalysts on NISQ hardware. They started to work in 2021 and already published some results on the way to reduce the quantum computing resources required for simulating and designing new materials and chemical processes and to compute energy gradients[1978].

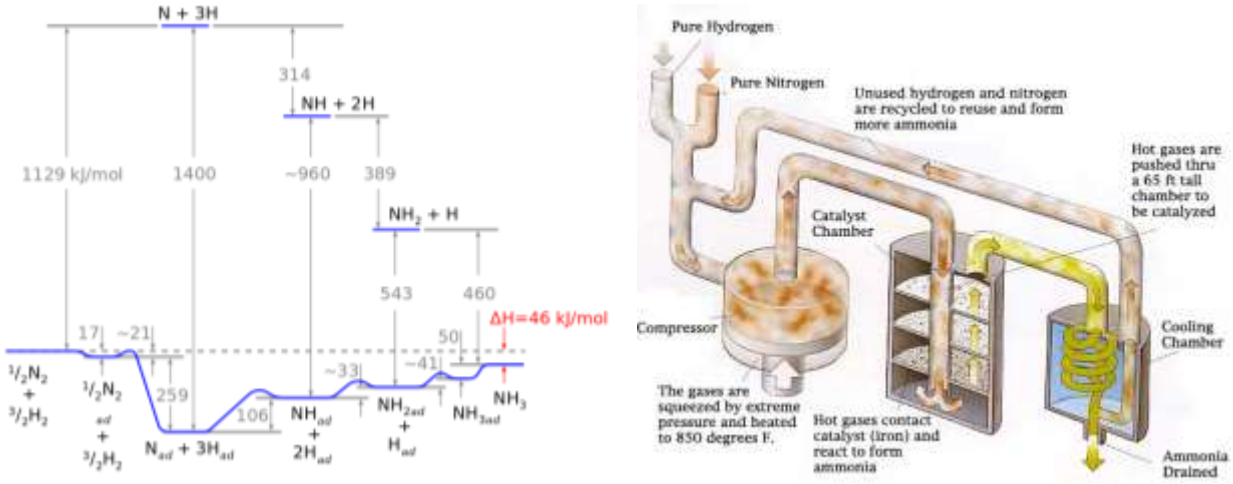


Figure 670: the usual Haber-Bosch process. Source: Catalysis How Dirt and Sand Catalyze Some of the Most Important Transformations, by Justin J. Teesdale, Harvard Energy Journal Club, September 2017.

However, one of the most famous chemical process that could benefit from quantum simulation would be to find a way to produce ammonia more efficiently. It's used in the production of fertilizers (88% of total) and also explosives. Right now, ammonia (NH_3) is produced using the famous Haber-Bosch chemical process that uses N_2 coming from the atmosphere and hydrogen usually coming from methane (CH_4). The Haber-Bosch process is currently responsible for 1% to 2% of global energy consumption and of 1.4% of CO_2 emissions.

The result of quantum software optimization

- Estimates for an example molecule: Fe_2S_2 with 118 spin-orbitals

Gate count	10^{18}	Reduced gate count	10^{11}
Parallel circuit depth	10^{17}	Parallel circuit depth	10^{10}
Run time @ 10ns gate time	30 years	Run time @ 10ns gate time	2 minutes

- Attempting to reduce the horrendous runtime estimates we achieved
  Wecker *et al.*, PRA (2014), Hastings *et al.*, QIC (2015), Poulin *et al.*, QIC (2015)
  - Reuse of computations: $O(N)$ reduction in gates
  - Parallelization of terms: $O(N)$ reduction in circuit depth
  - Optimizing circuits: 4x reduction in gates
  - Smart interleaving of terms: 10x reduction in time steps
  - Multi-resolution time evolution: 10x reduction in gates
  - Better phase estimation algorithms: 4x reduction in rotation gates

From materials to models on quantum computers

	Material	Model
Orbitals per unit cell	≈ 50	1
Unit cells needed	20x20	20x20
Number of orbitals	$N \approx 20'000$	$N \approx 800$
Number of terms	N^4	$O(N)$
Scaling of algorithm	$O(N^{5.5})$	$O(N^{0.5})$
Estimated runtime	age of the universe	seconds

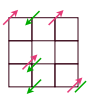


Figure 671: resource estimates for simulating the spin-orbitals of Fe_2S_2 molecule. Source: TBD.

The nitrogenase process uses a catalyst that is usually some iron doped with potassium and fixed on silica or alumina. Its natural equivalent is FeMoCo, a natural cofactor of nitrogenase. The Haber-Bosch process is highly energy-consuming particularly in the part producing pure H_2 and due to the heat and pressure needed in the main reactor (500°C and 100 bars).

[1978] See Local, Expressive, Quantum-Number-Preserving VQE Ansatze for Fermionic Systems by Gian-Luca R. Anselmetti et al, May 2021 (26 pages) and Analytical Ground- and Excited-State Gradients for Molecular Electronic Structure Theory from Hybrid Quantum/Classical Methods by Robert M. Parrish et al, October 2021 (23 pages).

Two processes could be developed thanks to quantum simulation for improving the energy efficiency of ammonia production. The first would be to simulate the nitrogenase enzyme, FeMoCo, that converts nitrogen into ammonia in cyanobacteria at ambient temperature and pressure. The second would be to invent new catalysts serving to operate the Haber-Bosch process at lower temperature and pressure. One example is the design of Fe/K mixtures supported on carbon nanotubes. But the number of qubits and gates to implement for solving these problems seems quite mind boggling, even with corrected qubits[1979].

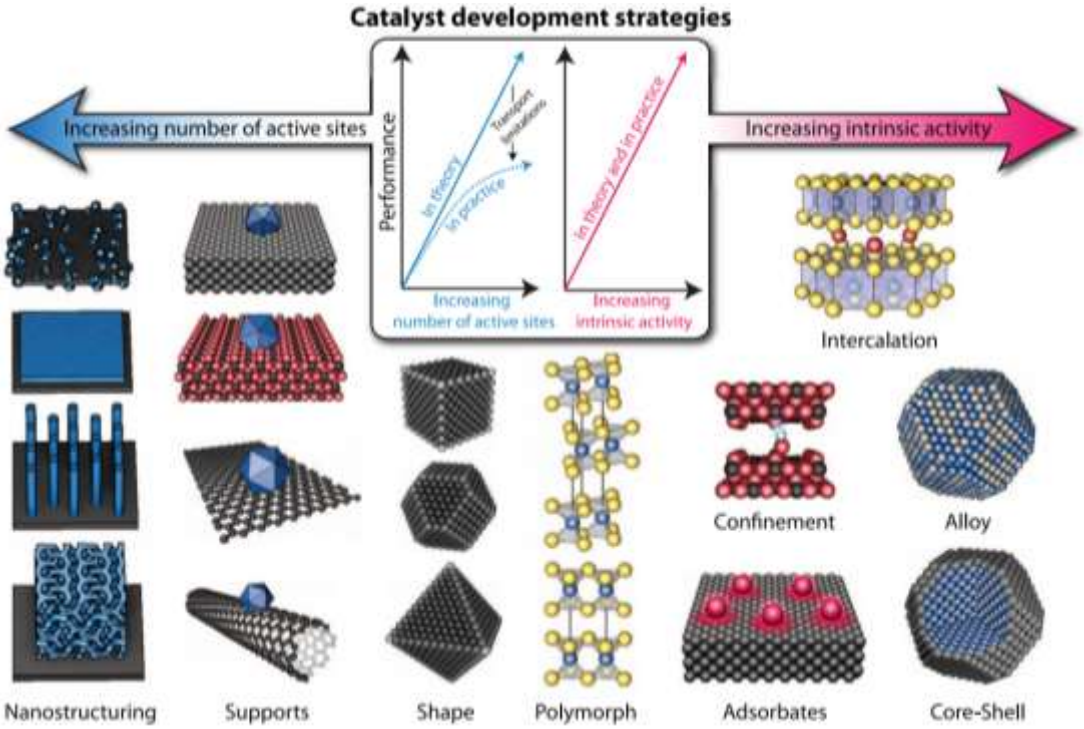


Figure 672: Source: Combining theory and experiment in electrocatalysis: Insights into materials design by Jens Jaramillo et al, Science, 2017 (33 pages).

You may wonder why cement production that is also responsible for significant CO^2 emissions is less talked about as a quantum case. Maybe is it because nature is not producing it and biomimetics harder to implement. Still, creating innovative cement production techniques is about testing many variants of clinkers who reduce CO^2 emissions during production. Quantum computing could help simulate these various material combinations to identify a more durable solution.

Batteries

Research is well underway to create batteries that are more efficient in terms of energy density, charging speed and supported charging/discharging cycles[1980]. Simulation is most often used to understand the operations of the chemical reactions taking place on cathodes and anodes and in the crystalline intercalation structures and to find ways to improve energy density and avoid battery wear phenomena.

[1979] See Even More Efficient Quantum Computations of Chemistry Through Tensor Hypercontraction by Joonho Lee et al, PRX Quantum, July 2021 (62 pages). With this recent method, 4 million physical qubits with an error rate of 0,1% would still be necessary.

[1980] See The Promise and Challenges of Quantum Computing for Energy Storage (4 pages) and Can quantum computing fuel a leap in battery research? Not any time soon, but automakers and quantum companies are exploring it right now by Grace Donnelly, Emerging Tech Brew, April 2022.

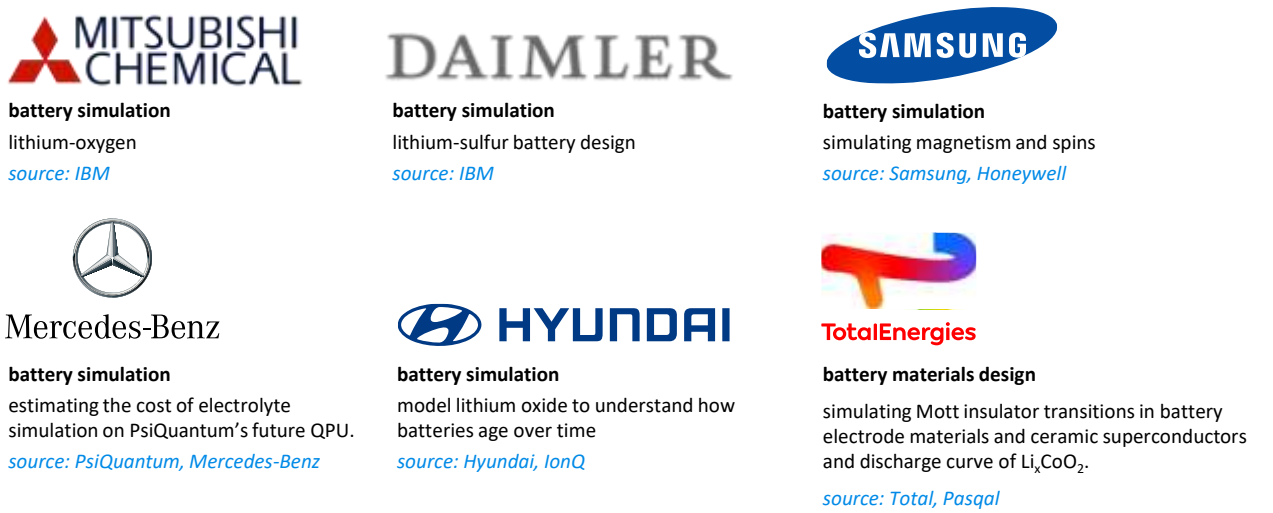


Figure 673: quantum computing use cases in the battery development domain. (cc) Olivier Ezratty, 2022.

Several companies are pursuing this goal. IBM and **Mitsubishi Chemical** have simulated on a super-conducting qubit computer the initial steps of the reaction between lithium and oxygen in lithium-air batteries[1981].

Mercedes-Benz worked with IBM to simulate lithium-sulfur batteries[1982] and later, with PsiQuantum to estimate the computing requirements for electrolyte simulation on PsiQuantum's system. For one of the simulation needs, they would need to have about 16K logical qubits. Given, PsiQuantum plans for requiring 10,000 physical qubits to create a single logical qubit. We end up with 160M physical qubits. PsiQuantum's plan is to reach 1M physical qubits by 2030[1983].

Hyundai and IonQ are developing a quantum application to model lithium oxide using IonQ's existing hardware. Lithium oxide is not used in EV batteries but its modeling could potentially help mitigate how batteries break down over time. But no IonQ computer has a computing advantage vs a classical computer! They use the Aria with 32 physical qubits and 20 "algorithmic qubits". The current project is focused on a relatively small molecules containing up to two lithium and one oxygen atom. In the end, it would require 2000 logical qubits that are far away beyond 2030 in IonQ's roadmap.

Volkswagen is also working on simulating lithium-ion batteries, teaming up with 1Qbit and Xanadu. They concluded that we are far off from being able to implement it[1984].

At last, quantum sensing could also help develop new batteries. That's what **AMTE Power** (UK) is doing with leading the 3 years Project Quantum to use quantum sensing to develop lithium-based battery manufacturing solutions, which got a funding of £5.4M from Innovate UK. This project is about using NV center-based magnetic quantum sensing to evaluate the battery aging process[1985].

[1981] See Computational Investigations of the Lithium Superoxide Dimer Rearrangement on Noisy Quantum Devices by Qi Gao et al, 2018 (6 pages).

[1982] See Quantum computation of dominant products in lithium–sulfur batteries by Julia E. Rice et al, Journal of Chemical Physics, 2021 (7 pages)

[1983] See PsiQuantum, Mercedes-Benz Study How Quantum Computers Can Accelerate EV Battery Design by Matt Swayne, The Quantum Insider, April 2022. Mentioning Fault-tolerant resource estimate for quantum chemical simulations: Case study on Li-ion battery electrolyte molecules by Isaac H. Kim et al, Physical Review Research, April 2022 (27 pages).

[1984] See How to simulate key properties of lithium-ion batteries with a fault-tolerant quantum computer by Alain Delgado et al, April-September 2022 (31 pages). The paper concludes that there is a need of 2,375 to 6,652 logical qubits to simulate Li_2FeSiO_4 with their 156 electrons.

[1985] See AMTE Power's Project Quantum Signals New Era of British Battery Manufacturing, September 2020.

Carbon capture

Carbon capture is another issue and researchers are simulating its molecular modus-operandi by bio-mimetics.

BASF is trying to simulate synthetic polymers, first on HPCs, then eventually on quantum computers. They invested in both **HQS** (Germany) and **Zapata Computing** (USA).

Since 2017, **Dow Chemicals** has been collaborating with the Canadian software publisher **1Qbit** to create new molecules, using D-Wave annealers.

TotalEnergies is working with CQC from Quantinuum to capture carbon on Metal-Organic Frameworks using a VQE based algorithm. They did simulate the use of up to 16 qubits which is way below any quantum computing advantage threshold[1986].

Oil exploration

Well, that stinks but oil companies are still trying to optimize oil exploration and extraction.

BP is working on the design of algorithms for optimizing oil exploration. This involves using data from various sensors, particularly seismic sensors, to consolidate models for simulating geological layers under the ground. They joined in 2020 the **IBM Quantum Network** as an industry partner to get access to IBM's 65-qubit quantum computer, software and experts.

It follows **ExxonMobil** who entered the program in 2019 as one of the major companies associated with IBM.

TotalEnergies also want to optimize oil prospection and reserves evaluation using seismic probes. They plan to address complex optimization problems such as **MINLP (**Mixed Integer NonLinear Programming[1987]) to optimize refining, planning, production and transportation[1988].

Power grid

In 2019, the **Dubai Electricity and Water Authority** (DEWA) was working with Microsoft to solve complex power and water distribution problems. It was just a matter of testing a few algorithms on Intel simulators running on Azure. And for good reason, Microsoft did not yet have its own quantum computer[1989]. In 2020, DEWA announced that it would train their algorithms in D-Wave annealers[1990]**!**

EDF is another major French company that is studying the use cases of quantum computing very closely: quantum new materials simulations, material aging simulations particularly under radiations, safety statistics, combinatorial optimization for smart grids and battery management (teaming up with Pasqal and ParityQC[1991]) and also customer segmentation using Quantum Machine Learning.

[1986] See Modelling Carbon Capture on Metal-Organic Frameworks with Quantum Computing by Gabriel Greene-Diniz et al, March 2022 (18 pages), CQC and Total Announce Multi-Year Collaboration to Develop Quantum Algorithms for Carbon Capture, Utilization and Storage (CCUS), April 2020 and Total Exploring Quantum Algorithms to Improve CO2 Capture, May 2020.

[1987] A version of the MINLP problem solving algorithm exists for D-Wave via their QUBO framework. See Quantum Computing and Non-Linear Integer Optimization by Sridhar Tayur February 2019 (42 slides).

[1988] Total has partnered with private players (IBM, Atos, Rigetti QC Ware, Google) and various research laboratories around the world: PCQC (Paris), LIRMM Montpellier, CERFACS, Université ParisSud, Jülich Forschungszentrum (Germany) and the University of Leiden.

[1989] See Microsoft and DEWA bringing quantum computing to Dubai, June 2018.

[1990] See DEWA organises training sessions on quantum computing in partnership with D-Wave, February 2020.

[1991] See Qualifying quantum approaches for hard industrial optimization problems. A case study in the field of smart-charging of electric vehicles by Constantin Dalyac et al, June 2021 (29 pages).

DTU experimented in Denmark a grid optimization using an HHL algorithm with up to 7 IBM qubits QPUs. They found that they have scalability issues. Surprise[1992]!

Transportation and logistics

Beyond energy matters mentioned above, transportation industries are mainly interested in algorithms for optimizing complex systems[1993]. Let's look at what can be done with road, rail, air and maritime transportation.

Road

Quantum computing could be implemented in many domains to improve both vehicle production and their operations. In the product design phase, quantum computing could help optimize vehicle fluid dynamics thanks to solving complex partial differential problems (aka Navier Stokes equations), minimizing drag and improving battery/fuel efficiency. It could also simulate the physics of various materials to improve weight/strengths vehicle ratios and design new batteries (but in the very long term).

In the operations stage, QC could handle complex optimization problems like supply-chain optimizations, warehouse robots routing, improving the accuracy of demand forecasting both with end-users and for their suppliers and inventory optimization. You have also traffic flow optimization or multimodal fleet operations[1994]. Machine learning based solutions could under some circumstances benefit from QC, for improving pattern recognition in images and various classification tasks used in manufacturing, predictive maintenance as well as in marketing[1995].

One less credible use case is autonomous vehicle control whether or not it's based on some machine learning technique. It doesn't make much sense for quantum computing due, at least, to the data-loading problem. Vehicles sensors are generating a huge stream of high-volume data that can't be ingested in a quantum computer, and particularly with one such computer sitting in the vehicle. So, let's forget this for a while.

Let's first look at the manufacturing of vehicles. And, surprise, they are mostly if not all… Germans! In 2022, **Volkswagen** Data:Lab published two papers coauthored with Terra Quantum AG related to hybrid computing associated with D-Wave quantum annealers in two areas: the optimization of assembly line work-flow scheduling[1996] and hybrid machine learning to enhance image recognition systems used for car classification[1997]. It is still not clear whether these applications really went into production.

[1992] See Quantum Computing for Power Flow Algorithms: Testing on real Quantum Computers by Brynjar Sævarsson et al, July 2022 (8 pages) and DTU first to use quantum computer for the power grid, 2022.

[1993] See this inventory of needs, but no solutions in Quantum Applications Transportation and Manufacturing by Yianni Gamvros, IBM, 2017 (20 slides).

[1994] See Quantum computing for transport optimization by Christopher D. B. Bentley et al, Q-CTRL, June 2022 (12 pages).

[1995] See Will quantum computing drive the automotive future? by McKinsey, September 2020. The listed use cases are interesting but the list contains some misleading case studies that are not relevant with quantum computing like "*processing vast amounts of data to accelerate learning in autonomous-vehicle-navigation algorithms*" (QC is not good at handling big data) and "*ensure car-to-car communications in almost real time*" (no quantum technology is bound to ensure real-time whatever communication). Most use cases related to autonomous vehicles operations are also quite unrealistic.

[1996] See Solving workflow scheduling problems with QUBO modeling by A. I. Pakhomchik et al, May 2022 (10 pages). The experiment is using QUBO on a D-Wave Advantage annealer. They found that the hybrid and classical algorithms were the most successful in solving the instances, although no solver was able to solve all QUBOs at all sizes. One caveat is that the paper doesn't mention computing time but only results quality.

[1997] See Hyperparameter optimization of hybrid quantum neural networks for car classification by Asel Sagingalieva et al, May 2022 (10 pages). It's about improving the accuracy of image recognition that is used for fault detection in manufacturing. They created an hybrid QML algorithm and deployed it on the QMware cloud from Terra Quantum running on D-Wave's annealers. The benchmark compared this new method over classical machine learning and quantified performance improvements in reduced expected run times and model fitness as the problem size scales. But it's very uncertain as of a real potential quantum advantage.

Daimler AG is one of the leading companies working on quantum technology with IBM, with applications for logistics and planning optimization and everything to do with autonomous vehicle routing at the forefront. In 2018, they also launched an initiative with IBM to develop lithium-sulfur batteries, which improve energy density and make it possible to do without metals such as cobalt and nickel. All of this will be achieved through quantum simulation.

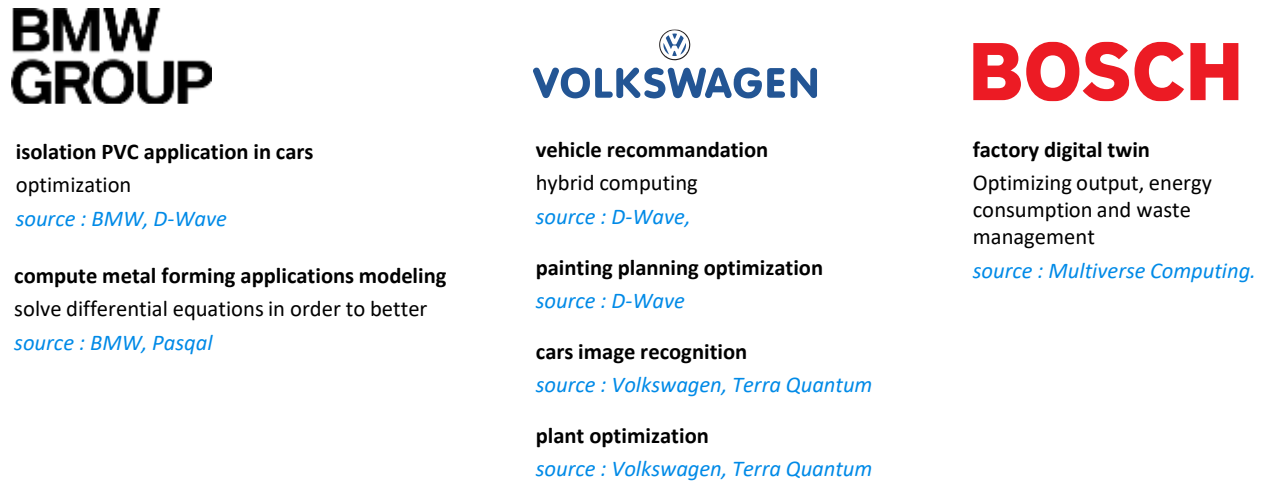


Figure 674: a sampler of quantum computing use cases in the automotive industry. (cc) Olivier Ezratty, 2022.

BMW is also willing to learn how to use quantum computing in various tasks, one being the optimization of its spare parts supply chain[1998]. They are partnering with Honeywell to do this as well as with Cambridge Quantum Computing, Zapata Computing and Entropica Labs. They started using the Honeywell trapped ions-based H0 and H1 with 10 qubits. They used a Recursive Quantum Approximate Optimization Algorithm (R-QAOA) to manage their combinatorial problem. The quality of these trapped ions qubits made the trial promising although of course not usable at all given the small number of available qubits[1999]. In May 2022, BMW started a partnership with Pasqal to solve differential equations in order to better compute metal forming applications modeling.

Multiverse Computing and a **Bosch** Automotive Electronics plant in Madrid announced in 2022 that they are exploring the creation of a digital twin of a factory with quantum computing. They plan to capture data to assess the performance of individual equipment and optimize quality control and overall efficiencies, including energy consumption and waste management. What they call digital twins are actually optimization systems.

In 2021, the German auto industry (BMW, Mercedes-Benz, Volkswagen, and Bosch) and research organizations (DFKI who runs contract research on AI and Forschungszentrum Jülich) even launched the **Q(AI)2** project to test AI applications for quantum computers[2000]. It particularly wants to study the usage of AI to solve various manufacturing optimization problems.

The deployment of autonomous vehicles fleets is a nice target application for quantum computers. The more autonomous the vehicles are, the greater the need for automation and route coordination. The problems to be solved will be to determine step-by-step the vehicle fleet routes in order to optimize each of these vehicles and passengers the travel time.

[1998] See this excellent use cases inventory: Quantum Computing: Towards Industry Reference Problems by Von Andre Luckow, BMW, April 2021.

[1999] See How BMW Can Maximize Its Supply Chain Efficiency with Quantum, Honeywell, January 2021.

[2000] See Quantum AI For The Auto Industry by DFKI, June 2021.

This was an experiment done in 2017 by **Volkswagen** on D-Wave annealers[2001]. Its goal was to optimize the routes of a (virtual) cab fleet in Beijing[2002]. The experiment was using the T-Drive data set published by Microsoft in 2008 which describes the routes of 10,357 cabs. The algorithm used was QUBO (Quadratic Unconstraint Binary Optimization). The diagram below shows the result of the optimization of the route of 418 cabs making the journey from the city center to the airport taking into account the route of 10,357 vehicles[2003].

There is a lack of hindsight in estimating the size of quantum computers needed to practically handle such large-scale problems. How many qubits would be needed to optimize a fleet of hundreds or even millions of autonomous vehicles? Volkswagen also experimented small-scale algorithms with D-Wave for optimizing vehicle recommendations and also optimizing cars painting planning. A fairly less ambitious version of this algorithm was used to optimize the individual travel routes of nine public-transit buses during the November 2019 Web Summit event in Lisbon.

So, we're off wondering what they really achieved or could achieve. Similar trucks routing algorithms were already explored by **Accenture** and **Denso** using D-Wave annealers. Annealers are so far in a better position to solve these problems than existing superconducting gate-based qubits systems from IBM. In an adjacent domain, **Toyota** worked with D-Wave to optimize traffic lights on a 50x50 road grid, using a D-Wave 2000Q[2004].

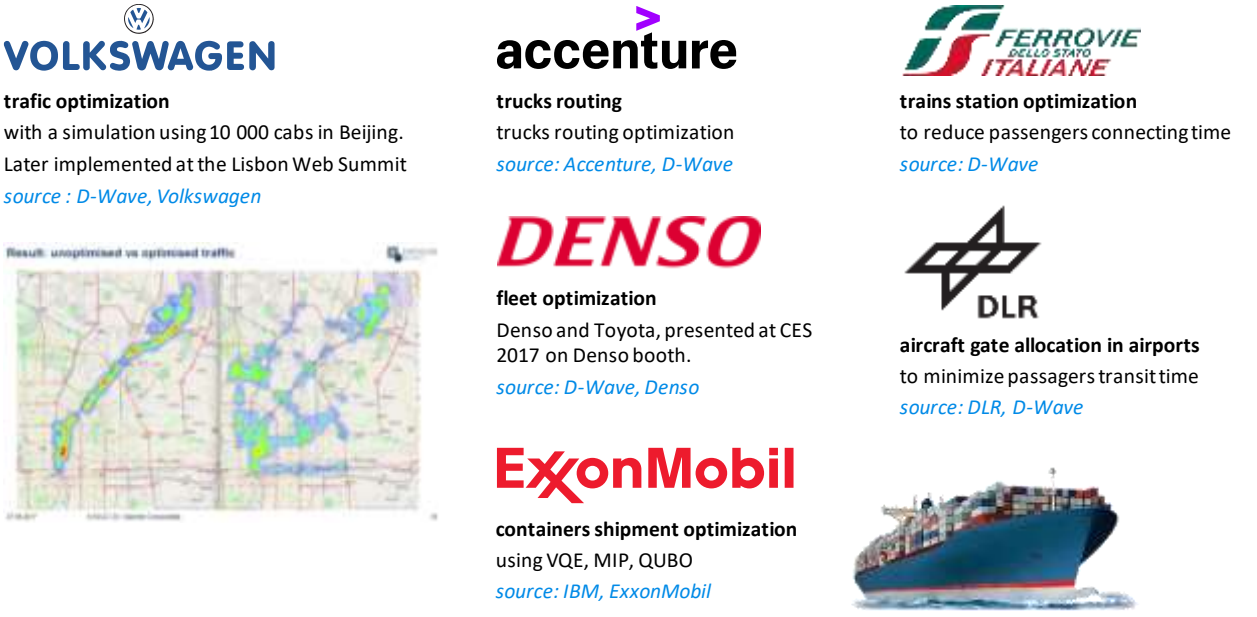


Figure 675: a sampler of quantum computing use cases in the transportation industry. (cc) Olivier Ezratty, 2022.

At last, another work conducted by **Hyundai** with IonQ is to improve 3D object detection with quantum computing. IonQ did demonstrate a "101" image recognition with 43 road signs (this is the basic test for a classical convolutional network running on a simple PC) and plans to expand it to recognize pedestrians and cyclists.

[2001] See Volkswagen takes quantum computing from the lab to the factory by Volkswagen, August 2021.

[2002] It is documented in Quantum Computing at Volkswagen Traffic Flow Optimization using the D-Wave Quantum Annealer, 2017 (23 slides).

[2003] The results are published in Traffic flow optimization using a quantum annealer, August 2017 (12 pages). As with many case studies from D-Wave, this one is also contested by HPC specialists.

[2004] See Toyota Central R&D Labs: A Quantum Approach to Transportation by D-Wave (2 pages) and Traffic Signal Optimization on a Square Lattice with Quantum Annealing by Daisuke Inoue et al, February 2021 (14 pages).

They believe they can do better with quantum computers than with classical NPUs (the neural processing units now embedded in most CPUs and mobile chipsets). They may forget the constraints of embedded systems in cars. An IonQ wouldn't fit in the trunk!

Rail

An experiment was done by **Ferrovie dello stato Italia** to optimize train arrivals in railways stations, also to minimize passengers' connection times, again with D-Wave.

AlphaRail (2000, USA) is a railways software company using machine learning and quantum computing to improve railways operations.

They are relying on quantum and quantum-inspired approaches to solve routing and scheduling optimization problems.

Air

With airlines, the current focus about optimizing aircraft fleets planning, to maximize the capacity to meet demand while optimizing the aircraft fill rate.

Also, quantum computing can enable optimizing airport and aircraft gates management, in order to minimize passenger waiting time, as tested by **DLR** in Germany[2005]. This is an NP-difficult problem that is difficult to deal with using conventional algorithms.

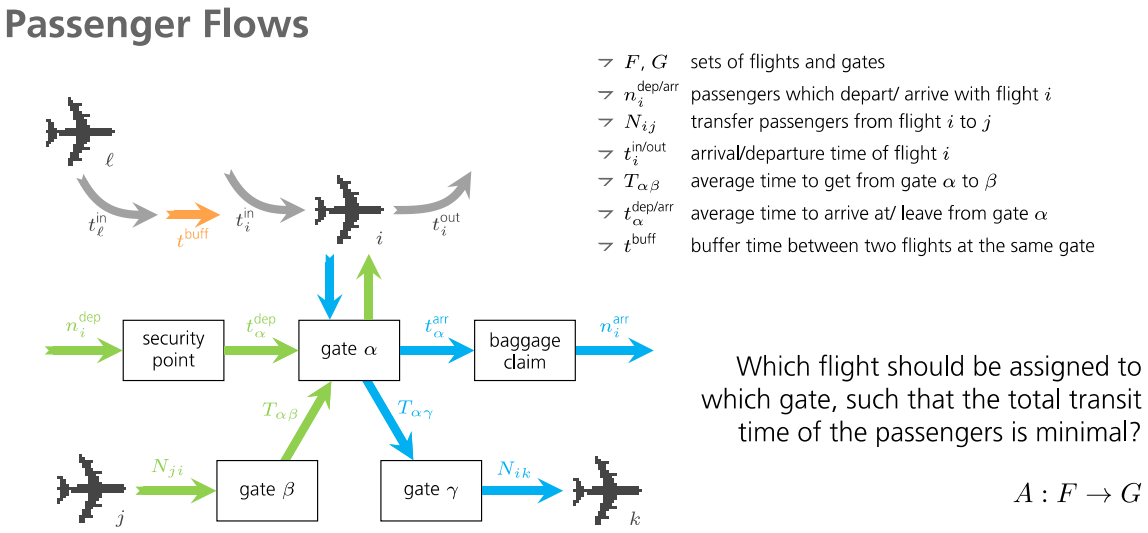


Figure 676: Flight Gate Assignment with a Quantum Annealer by Elisabeth Lobe and Tobias Stollenwerk, March 2019 (15 slides).

In Japan, **Sumitomo** launched in June 2021 a pilot experiment for optimizing flight routes for urban air mobile vehicles (air taxis and unmanned drones). They will rely on resources from Tohoku University. No precision on the problem sizing and on which quantum system they plan to pilot their solution even if D-Wave is a logic contender.

Researchers from **Chalmers University** in Sweden prototyped a promising QAOA hybrid algorithm solving the "tail Assignment problem", which is the task of assigning individual aircraft to a given set of flights, minimizing the overall cost for the airline. They said it worked with only 2 qubits, to optimize 2 flights and would scale well as flights are added[2006].

[2005] See Flight Gate Assignment with a Quantum Annealer by Elisabeth Lobe and Tobias Stollenwerk of the German Aerospace Center (or DLR for Deutsches Zentrum für Luft- und Raumfahrt e.V.), March 2019 (15 slides). The case study uses a D-Wave. It shows that the solution is not obvious to develop.

[2006] See Two-Bit Quantum Computer Solves Real Optimization Problem by Matt Swayne, December 2020 pointing to Applying the Quantum Approximate Optimization Algorithm to the Tail-Assignment Problem by Pontus Vikstål et al, September 2020 (11 pages).

These are needs that can be addressed both by machine learning algorithms to take into account the past or with quantum optimization algorithms based on a description of the parameters of the problem. The former does prediction and the latter simulation. Simulations avoids the back-mirror bias that can be induced by prediction methods based on past data. A combination of the two methods is possible.

Airbus is also involved in quantum. In 2015, one of their teams based in Newport in the United Kingdom began working on the subject. In 2016, Airbus Ventures invested in the American startup QC Ware. They experimented with the use of a D-Wave for fault tree analysis (FTA), which is used to determine the origin of complex failures with a gain of a factor of 4 compared with traditional methods. This is a difficult NP-difficult combinatorial problem that is easier to solve in quantum programming. In January 2019, Airbus launched its "Quantum Computing Challenge", a way to outsource the development of quantum solutions to help them solve their business problems, in fluid mechanics, differential equations, flight optimization, wing design, cargo bay filling, etc.[2007]. As of May 2019, 475 teams from 57 countries had competed in this challenge. They came mainly from the USA and India, followed by Europe. They announced the challenge results in October 2020 with five finalists selected out of 36 contestants.

One team from **Capgemini** devised a new hybrid matrix inversion algorithm mixing the famous HHL algorithm and a QSVM (Quantum-enhanced Support Vector Machine (QSVM). Other teams worked on plane loading optimization problems, on quantum machine learning models and on fluids dynamics applied to aircraft design.

How about designing autonomous **quantum flying drones** using a quantum computer, a project from Indian researchers[2008]? It makes no sense from a practical standpoint, at least due to real-time constraints. Since the quantum computer can't sit in the drone, a fortiori, one from IBM, there's an inevitable lag in the communication between the drone and the quantum computer which, by the way, should be entirely dedicated to a single drone to work real-time. You already have autonomous drones and robots, thanks to their embedded computing systems, and they don't yet need a quantum computer to run their symbolic and connectionist artificial to fly.

Maritime

ExxonMobil and **IBM** are working on finding algorithms to optimize maritime traffic routing. Existing solutions rely on heuristics and simplifications. They were willing to see whether quantum computing could transform these complex optimization problems and solve them more efficiently with quantum computing. Their vision is about container shipments volumes. They formatted their problem as a "vehicle routing problem with time windows" (VRPTW) which is a NP-hard problem. They compared various methods, using a QUBO algorithm that can be transformed on a lower-level VQE or QAOA hybrid algorithm and experimented it with Qiskit on the QasmSimulator IBM quantum emulator backend[2009]. As in many similar cases, the published paper does not provide any clear answers on the gain and on the quantum computer specification that would make it possible to solve a real-life problem. On top of that, it was not at all formulated as a container shipment optimization problem per se but as a simpler truck routing problem.

Maritime containers shipment is also a center of interest. **DP World**, the Dubai Port operator, is partnering with **D-Wave** to find ways to use quantum computing to optimize their port operations. At this stage, it's just exploratory work with no details at all about envisioned applications.

[2007] See Airbus gets aerodynamic with quantum computing by Michael Feldman, January 2019.

[2008] See Design and Simulation of an Autonomous Quantum Flying Robot Vehicle: An IBM Quantum Experience by Sudev Pradhan et al, June 2022 (7 pages).

[2009] See ExxonMobil & IBM Explore Quantum Algorithms to Solve Routing Formulations by Stuart Harwood et al, February 2021 which refers to Formulating and Solving Routing Problems on Quantum Computers by Stuart Harwood, January 2021 (17 pages).

The ones that are easy to guess are containers loading/offloading optimizations[2010]. Another such project was also undertaken with the **Port of Los Angeles** by SavantX, also using D-Wave annealers and quantum machine learning[2011].

Retail

The retail sector could benefit from quantum computing generic use cases in transportation and logistics improvements as well as in some marketing optimization techniques. Robotized warehouse operations could also benefit from some quantum-driven optimizations like what **Ocado Group** (UK) is piloting with D-Wave[2012]. Beyond that, consultants and analysts have not much to say about it or they sometimes err in mention big data applications, which are out of scope of quantum computers[2013].

PayPal is also testing a D-Wave quantum annealer to solve some optimization problems and detect fraud using quantum machine learning[2014].

Telecommunications

At this stage, the main quantum involvement of telecom companies is mainly related to quantum telecommunications and cryptography.

In the USA, **Verizon** launched a QKD trial on three sites in the Washington, D.C., area[2015]. In 2021, they also tested a VPN using a PQC (post-quantum cryptography) solution based on the Saber NIST competition finalist, for connection between two sites in the US and UK. **AT&T** is also investing resources in QKD networks, teaming up with Caltech.

In France, **Orange** participated to a QKD trial in the Nice region with partners including the InPhyNi research lab.

In the UK, **British Telecom** has also experimented a QKD setup to demonstrate some secured backup of datacenter resources. In October 2020, they deployed a pilot 6 km long QKD infrastructure in Bristol to connect several industry sites, in partnership with **Toshiba** as part of the **AQuaSec** (Agile Quantum Safe Communications) program, cofunded by UKRI[2016]. In October 2021, BT and Toshiba announced the deployment of a commercial QKD network in London, mixed with PQC for non photonic endpoints.

Quantum computing can still play a role to solve various optimization problems in the telecom industry. The most commonly presented are the placement, power and frequency assignment of overlapping cells in 4G/5G mobile networks, the configurations of paths and wavelengths on land line fiber optics networks and similar optimization problems for satellite communications[2017] and MIMO

[2010] See DP World explores quantum computing technology, April 2021.

[2011] See SavantX, D-Wave Collaborate on Quantum Algorithms to Tackle Supply Chain Problems at U.S.'s Busiest Port by Matt Swayne, The Quantum Insider, January 2022.

[2012] See Towards Real Time Multi-robot Routing using Quantum Computing Technologies by James Clark et al, SFTC Hartree and Ocado, 2019 (10 pages).

[2013] See Quantum computing in the consumer and retail sectors by Linda Ellett and Ian West, KPMG, July 2021. Extract: "*quantum computing could process data sets envisioned but not feasible at the current time to provide real-time consumer insights*".

[2014] See PayPal: Harnessing Quantum Computing in FinTech | D-Wave Qubits 2021, December 2021 (30 mn video).

[2015] See This Executive Director Is Leading Verizon Into the Future Through Quantum Computing by Joanna Goodrich, IEEE Spectrum, November 2020.

[2016] See BT and Toshiba install UK's first quantum-secure industrial network between key UK smart production facilities, October 2020.

[2017] See Heterogeneous Quantum Computing for Satellite Constellation Optimization: Solving the Weighted K-Clique Problem by Gideon Bass et al, Booz Allen Hamilton, 2017 (17 pages).

antennas optimization[2018]. It could also be used to enhance wireless networks energy efficiency with index modulation, a task that is a NP-hard problem[2019]. It uses a Grover Adaptive Search (GAS) providing a quadratic speedup (not an exponential one) and still requires a fault-tolerant large-scale quantum computers that doesn't exist yet.

In Italy, the telecom operator **TIM** used a D-Wave QUBO based algorithm to optimize the setup of 4G/5G radio cells frequencies.

In another realm, more in the home automation space, researchers from **Mitsubishi** developed a quantum human activity monitoring algorithm using Wi-Fi in the ultra-wideband range of 60 GHz and a variational quantum circuit (VQC) building a QNN (quantum neural network)[2020].

Finance

Finance is another great playground for experimenting quantum technologies and particularly quantum computing[2021]. Both because this vertical is quite hungry with forecasting and optimization needs and also because it is a rather solvent market with many economic players having the critical mass to invest in new technologies.

Banks have a pressing need to transform themselves to adapt to constant technological and societal changes. They manipulate valuable data dumps. They need to optimize many facets of their business, starting with investment portfolios. It's all about optimizing portfolio returns, minimizing risks, manage regulations, mainly the Basel III framework rules with their liquid coverage radio constraints, and at last detect fraud risks as efficiently as possible. Also, assets are interdependent and transaction costs are variable depending on the type of assets. Their evolution responds to varying levels of uncertainty and risk.

Question	Broad approach solution
Which assets should be included in an optimum portfolio? How should the composition of the portfolio change according to what happens in the market?	Optimization models
How to detect opportunities in the different assets in the market, and take profit by trading with them?	Machine learning methods, including neural networks and deep learning
How to estimate the risk and return of a portfolio, or even a company?	Monte Carlo-based methods

Figure 677: examples of financial problems and approaches with quantum computing. Source: to Quantum computing for finance: overview and prospects by Roman Orus et al, 2018 (13 pages)

There are also some interesting mathematical relationships between some key equations in finance and in quantum physics.

This is the case of the Black-Scholes differential equation, which makes it possible to calculate the price of financial derivatives that are indexed on the price of underlying different financial instruments. It can indeed be considered as a variant of Schrödinger's wave function!

[2018] See Evaluation of quantum annealer performance via the massive mimo problem by Zsolt I. Tabi et al, August 2021 (14 pages). An Hungarian team assessed the use of D-Wave annealers to optimize MIMO antennas configurations. They found that some interesting results were obtained with the latest D-Wave Advantage annealer but that it will require at least another generation of better-connected qubits annealers to bring some form of quantum annealing advantage for this problem's solving.

[2019] See Quantum Speedup for Index Modulation by Naoki Ishikawa , IEEE Access, July 2021 (11 pages).

[2020] See Quantum Transfer Learning for Wi-Fi Sensing by Toshiaki Koike-Akino and Pu Wang, Ye Wang Toshiaki Koike-Akino, Mitsubishi, May 2022 (6 pages).

[2021] See overview in Quantum Computing and Finance from the Quantum World Association, August 2018, which refers to Quantum computing for finance: overview and prospects by Roman Orus et al, 2018 (13 pages) and the review paper A Survey of Quantum Computing for Finance by Dylan Herman et al, JP Morgan, Universities of Chicago, Delaware, DoE Argonne National Lab and Menten AI, January 2022 (56 pages).

A recent review paper from Isaiah Hull, Or Sattath, Eleni Diamanti and Goran Wendin from Sweden, Israel and France, describes the wealth of quantum algorithms that could be used in the economic and financial spheres[2022]:

- **Numerical differentiation** algorithms used in financial econometrics, structural microeconometrics, maximum likelihood estimation, dynamic stochastic general equilibrium (DSGE) modelling, and large-scale macroeconomic modelling conducted by central banks and government agencies.
- Solving **dynamic economic models** using interpolation algorithms.
- **Pricing of derivatives** using linear systems algorithms including matrices inversions, linear regressions, and matrix powers [2023].
- **Macro-economic models** using finite elements methods.
- **Portfolio optimization** using most of the time quantum annealers but that could run on a gates-based quantum computer [2024].
- **Macroeconomics**, **forecasting**, **modeling credit spread,** and **pricing financial derivatives** based on quantum machine learning algorithms including principal component analysis, including some work done by Goldman Sachs in partnership with IBM[2025].
- **Simulation of agent choices** over time using Monte Carlo simulations.
- **Investment portfolio optimization** including a model published in 2015 and running on a D-Wave quantum annealer and based on a QUBO model and graph modeling [2026].
- **Model market instability**, also on a quantum annealer [2027].
- **Random number generation** used beyond cryptography, for simulations and estimation, particularly with Monte Carlo simulations.

Most of the existing pilot algorithms have been tested with a small number of assets, in the 1-500 range, particularly on D-Wave quantum annealers, while real-world scenarios are based on thousands if not hundred thousand of them.

When you look at some of the referenced papers, you discover that gate-based solution hardware constraints are most of the time gigantic[2028].

[2022] See One Bit, Qubits, A Dollar: Researchers Say Economists Should Prepare for Quantum Money by Matt Swayne, January 2021, making reference to Quantum Technology for Economists by Isaiah Hull, Eleni Diamanti et al, December 2020 (120 pages). The report was published by Sveriges Riksbank, the employer of one of the contributors. They didn't fund any research related to this paper.

[2023] See Quantum computational finance: martingale asset pricing for incomplete markets by Patrick Rebentrost, Alessandro Luongo, Samuel Bosch and Seth Lloyd, September 2022 (31 pages).

[2024] See Quantum computational finance: quantum algorithm for portfolio optimization by Patrick Rebentrost and Seth Lloyd, 2018 (18 pages), Benchmarking the performance of portfolio optimization with QAOA by Sebastian Brandhofer et al, July 2022 (28 pages) and NEASQC financial application library v1.0 available, 2022, a quantum quantitative finance library released by the NEASQC European consortium.

[2025] See for example Study: Quantum Computers Can't Match Classical Computers in Derivative Pricing... Yet by Matt Swayne, December 2020 making a reference to A Threshold for Quantum Advantage in Derivative Pricing by Shouvanik Chakrabarti et al, , Goldman Sachs, IBM and University of Maryland, May 2021 (41 pages). This work was improved in Towards Quantum Advantage in Financial Market Risk using Quantum Gradient Algorithms by Nikitas Stamatopoulos, William Zeng et al, Goldman Sachs and IBM, November 2021 (20 pages) which reduced the QPU clock rate requirement to 30kHz, not far from the 2.5kHz record from existing IBM QPUs and their plans to reach 10kHz in the near future.

[2026] In Solving the Optimal Trading Trajectory Problem Using a Quantum Annealer, 2015 (13 pages).

[2027] See these slides in this D-Wave presentation. See also Applications of Quantum Annealing in Computational Finance, 2016 (29 slides) and the Quantum For Quants website they created.

[2028] See Credit Risk Analysis using Quantum Computers by Daniel J. Egger et al, 2019 (8 pages).

For example, some credit risks analysis and derivative pricing use cases mention a need for 7500 logical qubits (in Figure 678), which is a level above the 4098 minimum threshold for breaking a 2048 bits RSA key with Shor's algorithm[2029]. And it requires millions of physical qubits!

	(d, T)		Error		T-count		T-depth		# Logical Qubits	
Method	**Auto**	**TARF**	**Auto**	**TARF**	**Auto**	**TARF**	**Auto**	**TARF**	**Auto**	**TARF**
Riemann Sum	$(3, 20)$	$(1, 26)$	2×10^{-3}		$\geq 10^{43}$	$\geq 10^{18}$	$\geq 10^{43}$	$\geq 10^{18}$	-	-
Riemann Sum (no-norm)					1.4×10^{11}	5.5×10^{10}	1.9×10^{8}	1.7×10^{8}	24k	15k
Re-parameterization					4.2×10^{9}	3×10^{9}	4.6×10^{7}	6.2×10^{7}	7.5k	9.5k

TABLE I: Resources estimated in this work for pricing derivatives using different methods for a target error of 2×10^{-3}. We consider a basket autocallable (Auto) with 5 payment dates and a knock-in put option, and a TARF with one underlying and 26 payment dates. We find that Grover-Rudolph methods [10] are not applicable in practice (details in Appendix B) and that Riemann summation methods require normalization assumptions to avoid errors that grow exponentially in T. Even if those normalization issues were avoided, as detailed in the Riemann Sum (no-norm) row, the re-parameterization method still performs best. See Section IV A for a discussion of the Riemann summation normalization. The detailed resource estimation is discussed in Sections IV A 2 and IV B 3.

Figure 678: Source: A threshold for quantum advantage in derivative pricing by Shouvanik Chakrabarti et al, Goldman Sachs, IBM and University of Maryland, May 2021 (41 pages).

The Hull/Diamanti et al paper also reviews the broad topic of quantum money, and idea born circa 1969 and published in 1983 by **Stephen Wiesner**. The idea is to use quantum objects properties and the no-cloning theorem to avoid any counterfeiting and forging. Any bill has two unique identifying numbers: one classical serial number that is public and one secret random quantum number called a "random classical bill state". The central bank is the only one keeping the classical bill state. It's encoded using for example polarized photons on a 0° or 45° basis. Only the bank knows this sequence of encoding.

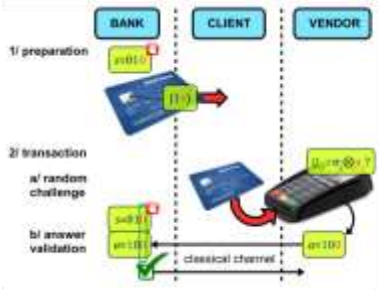


Figure 1. **Practical quantum money protocol.** The sequence of interactions between the credit card holder (client), the bank and the vendor involved in the transaction. In the preparation phase, the bank uses a secret key to prepare the quantum state loaded on the credit card, which is then given to the client. In the transaction phase, the vendor randomly selects one out of two challenge questions, measures the qubits and sends the outcome to the bank, who can then verify the validity of the credit card or detect a forgery attempt.

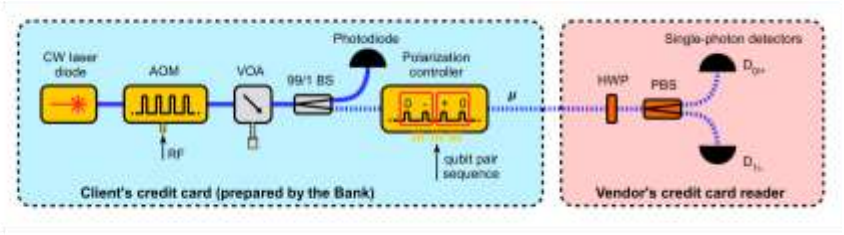


Figure 2. **Experimental setup of the quantum money system.** The credit card state preparation is performed using pulses carved from light emitted by a telecommunication wavelength laser diode using an acousto-optic modulator (AOM). A multi-stage polarization controller (EOSPACE) is then used to select the polarization states according to the protocol by applying suitable voltages. The average photon number of pulse μ is set by a variable optical attenuator (VOA) and is calibrated with a 99/1 beam splitter (BS) and a photodiode. The credit card reader is materialized by a standard polarization analysis setup including a half-wave plate (HWP), a polarization beam splitter (PBS) and two InGaAs single-photon avalanche photodiodes (ID201). The entire setup is synchronized using a multi-channel delay generator and is controlled by software incorporating the random state generation and data acquisition and processing.

Figure 679: Source: Experimental investigation of practical unforgeable quantum money by Mathieu Bozzio, Iordanis Kerenidis, Eleni Diamanti et al, 2017 (10 pages).

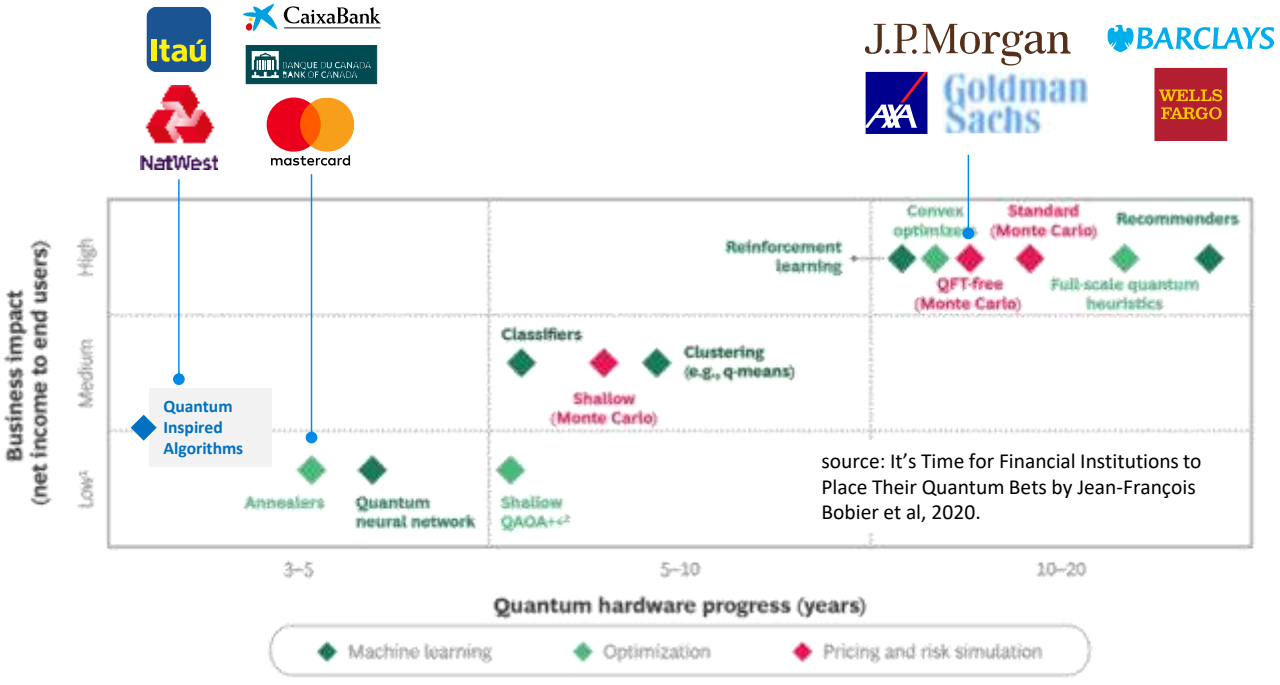
There are many variations of this concept of quantum money, with different degrees of anonymity and private and public schemes. Quantum money could be physical segmented into bills, coins and lightning schemes[2030]. An untraceable quantum coin proposal was made around 2010. But there are many shortcomings with these schemes which are just non implemented ideas at this stage.

[2029] See again A threshold for quantum advantage in derivative pricing by Shouvanik Chakrabarti et al, May 2021 (41 pages). 7.5K logical qubits and T-depth of 54 million are needed for pricing derivatives.

[2030] Quantum Lightning is a public key quantum money type.

One of these being that it requires quantum memory that doesn't exist yet, and which, by the way, is therefore not miniaturizable to be embedded in devices like a credit card[2031]. The Quantum Lightning variation prevents the bank to create multiple bills with the same serial number. You also have semi quantum money that requires no quantum communication infrastructure. All in all, it's quite difficult to assess the practicality of such quantum money ideas.

BCG published another review on quantum computing financial use cases including a roadmap against the estimated progress of quantum hardware in the next 5 to 20 years (in Figure 680)[2032]. For its part, McKinsey is more upbeat and is pushing banks to evaluate as fast as possible the potential use cases of quantum computing[2033]. D-Wave and IBM have been very active to push financial organizations to evaluate quantum computing benefits. So far, we have mainly proof of concepts and trials. Indeed, as the authors of another review paper published in 2020 point out: "*to date, quantum hardware is not advanced enough for solving any problem of practical relevance faster than classical computers*"[2034]. As a result, most banks are either using quantum inspired algorithms and small scale quantum annealing algorithms, or investigating highly demanding gate-based solutions that are positioned in the far-fetched future, in the 10-20 year timeframe at best.



Sources: Adapted from QC Ware; BCG.
Note: Quantum advantage over classical computing is uncertain in many areas listed. Business impact assumes that quantum advantage is realized in each area and is not risk-adjusted. QFT = quantum Fourier transform.
[1]Best estimates as of November 2020.
[2]QAOA = quantum approximate optimization algorithm; ++ refers to updates to QAOA that include using different mixing operators, initial states, and alternating operators.

Figure 680: Source: It's Time for Financial Institutions to Place Their Quantum Bets by Jean-François Bobier et al, 2020, and logos placed by Olivier Ezratty, 2022.

[2031] See Experimental investigation of practical unforgeable quantum money by Mathieu Bozzio, Iordanis Kerenidis, Eleni Diamanti et al, 2017 (10 pages).

[2032] See It's Time for Financial Institutions to Place Their Quantum Bets by Jean-François Bobier et al, 2020.

[2033] See How quantum computing could change financial services by Miklos Dietz et al, McKinsey, December 2020.

[2034] See Quantum algorithms are coming to finance, slowly by Sarah Butcher, November 2020, mentioning the review paper Prospects and challenges of quantum finance by Adam Bouland, Iordanis Kerenidis et al, 2020 (49 pages). This paper documents the quantum speedups theoretically achievable with Monte Carlo simulation and portfolio quantum algorithms.

Since 2017, IBM has been highlighting partnerships with **JPMorgan Chase**[2035], **Barclays**[2036] and more recently with **HSBC**[2037] and **Wells Fargo**[2038] to study the uses of quantum in trading strategy optimization, investment portfolio optimization, pricing and risk analysis. Even if quantum algorithms that meet their business needs are conceivable, the capabilities of today's IBM quantum computers are insufficient to put anything into production.

In a recent review paper, IBM researchers describe some case studies of quantum computing in finance such as simulations (new customer identification, create new financial products, incorporate market volatility, improve customer retention), optimization and machine learning, options pricing, and quantum amplitude estimation with a quadratic speedup that can be used to estimate value at risk in an investment portfolio or in a credit[2039].

TABLE 5: Algorithms can improve computational efficiency, accuracy, and addressability for defined use case.

	Quantum Algorithm	Description	Impact	Needs	Simulation	Optimization	ML
VQE	Variational Quantum Eigensolver	Use energy states to calculate the function of the variables to optimize	Procedure to assign compute-intensive functions to quantum and those of controls to classical	Qubit number increases significantly with problem size		x	
QAOA	Quantum Approximate Optimization	Optimize combinatorial style problems to find solutions with complex constraints	Simplify analysis clauses for constraints and provide robust optimization in complex scenarios	Uncertain ability to expand to more optimization classes		x	
AE	Quantum Amplitude Estimator	Create simulation scenarios by estimating an unknown property, Monte Carlo style	Handle random distributions directly, instead of only sampling, to solve dynamic problems quadratically speeding up simulations	High Quantum Volume required for good efficiency	x	x	x
QSVM	Quantum Support Vector Machines	Supervised machine learning for high dimensional problem sets	Map data to quantum-enhanced feature space to enable separation and better separate data points to achieve more accuracy	Runtime can be slowed by kernel computation and data structure			x
HHL	Harrow, Hassidim, and Lloyd	Estimate the resulting measurement of large linear systems	Solve high dimensional problems speeding up exponentially calculations	Hard to satisfy prerequisites and high measurement costs to recover solutions		x	x
QSDP	Quantum Semidefinite Programming	Optimize a linear objective over a set of positive semidefinite matrices	Estimate quantum system states with less measurements to exponentially speedup in terms of dimension and constraints	High Quantum Volume required for good efficiency		x	

TABLE 6: Financial services focus areas and algorithms.

Financial Services	Example Problems	Solution Approach	Quantum Algorithm
Asset Management	Option Pricing Portfolio risk	Simulation	AE
Investment	Portfolio Optimization	Optimization	Combinatorial: VQE, QAOA
Banking	Portfolio Diversification Issuance: Auctions		Continuous: QSDP AE
Retail & Corporate Banking	Financial Forecasting Credit Scoring (e.g. SME Banking) Financial Crimes: Fraud + AML	Machine Learning	QSVM HHL AE

Figure 681: Source: Quantum Computing for Finance: State of the Art and Future Prospects by Daniel Egger et al, IBM Quantum, January 2021 (24 pages).

D-Wave is at the origin with some of its customers such as **Deutsche Bank** of the creation of the Quantumforquants website, dedicated to the uses of quantum in finance. **Atos** also published a white paper on quantum applications in finance[2040] .

[2035] J.P. Morgan recruited an IBM veteran in quantum computing, Marco Pistoia, who had contributed to the development of Qiskit Aqua. See JP Morgan Chase poaches an IBM 'Master Inventor' with 26 patents for quantum computing by Hugh Son, January 2020. This quantum activity is integrated in their "Quantitative Research Group". See also Option Pricing using Quantum Computers by Nikitas Stamatopoulos, Daniel J. Egger, Yue Sun, Christa Zoufal, Raban Iten, Ning Shen and Stefan Woerner, JPMorgan Chase, ETH Zurich and IBM, May 2019-July 2020 (20 pages).

[2036] See Why banks like Barclays are testing quantum computing, de Penny Crossman, July 2018, Barclays demonstrates proof-of-concept quantum clearing algorithm by Cliff Saran, October 2019, Quantum Algorithms for Mixed Binary Optimization applied to Transaction Settlement by Lee Braine et al, October 2019 (8 pages) and Quantum Machine Learning in Finance: Time Series Forecasting by Dimitrios Emmanoulopoulos and Sofija Dimoska, Barclays, February 2022 (20 pages).

[2037] See HSBC Working with IBM to Accelerate Quantum Computing Readiness, IBM, March 2022 and Unsupervised quantum machine learning for fraud detection by Oleksandr Kyriienko and Einar B. Magnusson, University of Exeter, HSBC and Canada Square, August 2022 (7 pages).

[2038] See Wells Fargo prepares to take a quantum leap by Poornima Apte, CIO Magazine, June 2022.

[2039] See Quantum Computing for Finance: State of the Art and Future Prospects by Daniel Egger et al, IBM Quantum, January 2021 (24 pages).

[2040] See Quantum finance opportunities: security and computation, 2016 (20 pages). This is also the case of Everest Group with Quantum Computing in the Financial Services Industry-Infinite Possibilities or Extreme Chaos, 2018 (15 pages, $990... not really worth it).

In 2022, they announced an R&D partnership with **Mastercard** to create quantum-hybrid applications for optimizing consumer loyalty and rewards programs, cross-border settlement, and fraud management.

NatWest is experimenting quantum inspired algorithms running on traditional computers to optimize its investment portfolios (HQLA for High Quality Liquid Assets).

Goldman Sachs recruited Will Zeng, from Rigetti Computing, who had developed the Quil language. Will also works for the Unitary Fund which promotes open sourced quantum solutions, tools and benchmarks. With IBM, they work on different algorithms designs like the one on pricing derivatives already mentioned above. They are not yet operational but help define the hardware requirements to be able to run them. It's still at least in the mid-term.

JP Morgan Chase researchers created the NISQ-HHL approach, a hybrid version of the HHL algorithm that works on NISQ devices small-scale portfolio-optimization problems, using 6 and 14 assets from the S&P 500. It uses various techniques like mid-circuit measurement, Quantum Conditional Logic and qubit reset and reuse in the Quantum Phase Estimation routine used for eigenvalue estimation. The technique can reduce the number of ancillary qubits to just one and qubit connectivity requirements and (usually costly) SWAP gates. The test was implemented on a Quantinuum System Model H1 with 11 qubits. In other words, we are obviously far from getting any sort of quantum advantage in such a situation[2041].

Microsoft devised a way to make stock value predictions using topological computing, a farfetched idea given the state of the art of their Majorana fermion based qubits[2042].

GE Research with IonQ developed a risk management hybrid algorithm with 20 qubits from the IonQ Aria QPU[2043].

Also, noteworthy is the investment by the **Royal Bank of Scotland** (RBS) in 1Qbit along with Fujitsu and Allianz.

The **Bank of Canada** and **Multiverse Computing** created a prototype quantum simulation of the cryptocurrency market using a D-Wave quantum annealer. It simulated a financial network with 8-10 players[2044].

Itaú Unibanco (South America) and **QC Ware** (USA) undertook a four-month joint project in the customer retention domain with QML algorithms improving customer churn prediction models. The main outcome of the project is a new method to do this on classical computers and improved predictions by 2% and the model precision by 6,4% (from 71%). They used 180,000 data points[2045].

Of course, you must add to this quick review all the quantum software startups that are entering this market. They are either using quantum inspired algorithms or pilot projects using gate-based or annealing-based quantum computing. Among these are **1Qbit**, **Multiverse Computing**, **ApexQubit**, **JosQuantum** and **QuantFi**.

[2041] See NISQ-HHL: Portfolio Optimization for Near-Term Quantum Hardware by Romina Yalovetzky et al, January 2022 (14 pages). Presents a version of the HHL algorithms suitable for NISQ quantum computers.

[2042] As documented in Decoding Stock Market Behavior with the Topological Quantum Computer, 2014 (24 pages).

[2043] See IonQ and GE Research Demonstrate High Potential of Quantum Computing for Risk Aggregations, June 2022 and Copula-based Risk Aggregation with Trapped Ion Quantum Computers by Daiwei Zhu et al, June 2022 (10 pages). They say the results are better than full classical algorithms which always puzzles me given 20 qubits are very easily emulated on a classical computer.

[2044] See Bank of Canada and Multiverse Computing Complete Preliminary Quantum Simulation of Cryptocurrency Market by Multiverse, April 2022.

[2045] See QC Ware Applies Quantum Computing Principles to Increase Customer Retention at Itaú Unibanco by James Dargan, May 2022.

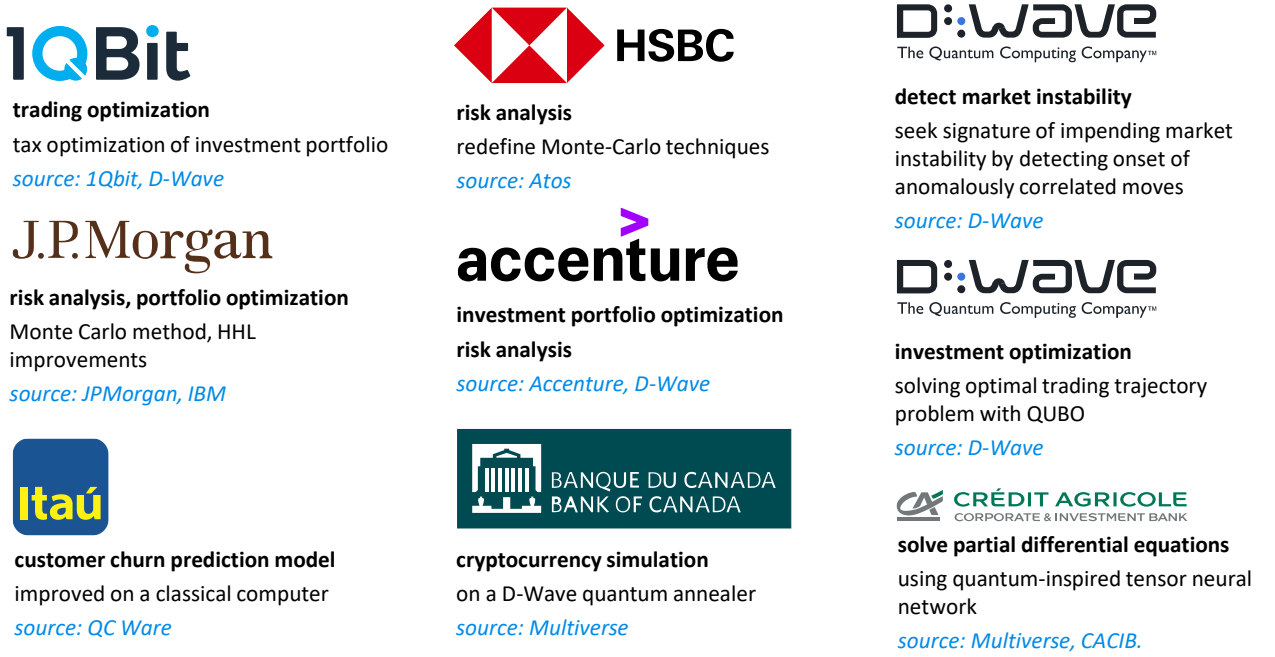


Figure 682: a quantum computing use case sampler for financial services. (cc) Olivier Ezratty, 2022.

Insurance

The insurance market is a vertical that also must fix complex optimization problems, particularly related to risk modelling. The various related surveys and review papers I have found are not as rich as in the financial services vertical[2046].

Some analysts are using the usual Shor based codebreaking attacks cybersecurity red flag and explaining all the risks businesses may face in the future[2047]. The related reports are clearly misleading, stating for example that quantum-based communications could be "*quicker over long distances*" on top of being better secured[2048].

A 11 pages report was published late 2019 by **Novarica**, an US insurance consulting services company[2049]. Besides the usual generic description of the whereabouts of quantum computing, it contains only one and a half pages of insurance related use cases ideas. They are related to risk modelling and portfolio optimization. It also mentions quantum machine learning used to better detect and mitigate fraud, risks assessment with actuarial models for enhanced pricing and risk pooling precision, investments portfolio optimization and model life expectancy algorithms for large populations.

Another paper was published in 2022 by Michael Adam from **AXA Konzern AG** dealt with the potential applications of quantum computing in insurance. It is focused on the use case of valuation of insurance contracts based on quantum amplitude estimation, which would provide a quadratic speedup compared with classical Monte-Carlo based algorithms[2050]. However, it doesn't (yet) make an assessment of the quantum hardware resources needed to run this type of algorithm in production.

[2046] See The impacts of quantum computing on insurance - From theory to reality from Lloyds's, February 2021 (34 pages).

[2047] See Quantum computing a potential cyber risk for re/insurers by Charlie Wood, November 2019.

[2048] See Top 5 insurance quantum computing use cases by Danni Santana, January 2018. One speaker in Quantum Computing in Insurance - Interactive discussion, February 2021 (59 mn) estimates that the Shor threat can materialize in between 7 and 10 years, this being "conservative". Well that's kind optimistic.

[2049] See Quantum Computing to Affect Insurer Tech Strategies, December 2019.

[2050] See Potential Applications of Quantum Computing for the Insurance Industry by Michael Adam, AXA Konzern AG, October 2022 (43 pages).

One risk modelling algorithm created by **JoS QUANTUM** is indeed documented[2051]. Another use case was publicized by **Caixabank** with D-wave in 2022. They developed an investment portfolio hedging and portfolio optimization solution that generated a 90% decrease in time-to-solution when compared to their classical legacy system[2052].

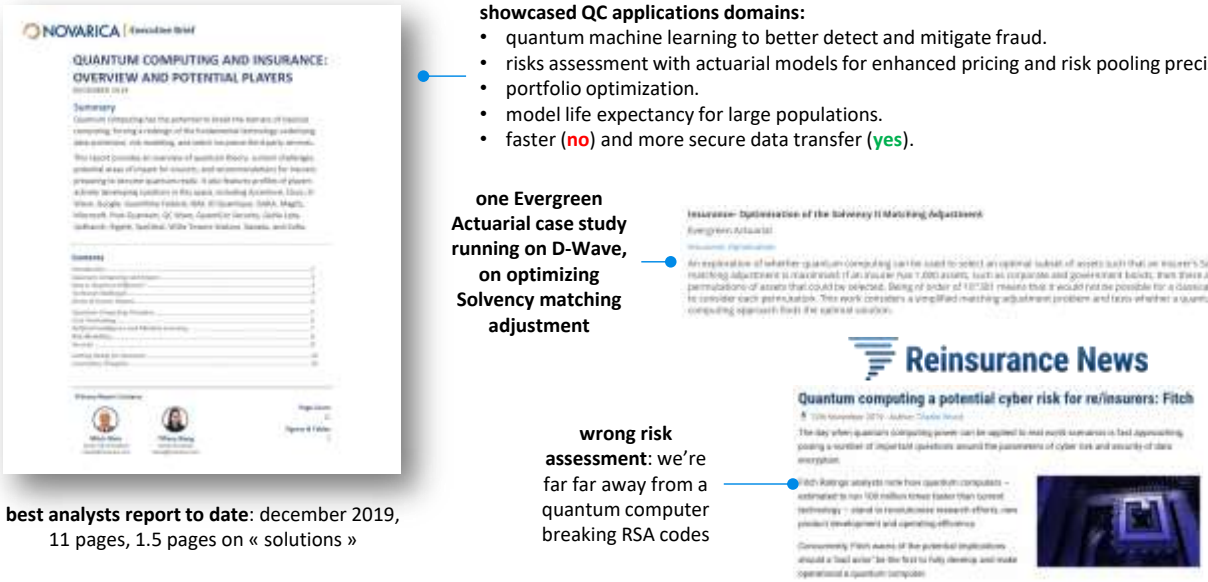


Figure 683: some use cases and constraints for quantum computing in the insurance business. (cc) Olivier Ezratty, 2021.

Marketing

Marketing is also an area where optimization algorithms for complex systems based on quantum computers could be of interest. This concerns the optimization of the marketing mix, that of media plans, or the maximization of advertising revenues, various areas that are also invested by the AI field.

Volkswagen experimented a vehicle recommendation system in online sales sites, with a D-Wave.

Once again, predictive systems based on the exploitation of past data and simulation based on the knowledge of market operating rules are once again opposed to each other. However, these rules do not fall under the notion of AI expert systems, which manage logical predicates, but more complex causality models[2053].

Content and media

Wondering how we could use quantum computing to create some content and art? That's the weird idea some have, at least with regards to music creation.

Computer have played a role in music creation for a while so why not quantum computers? Quantum mechanics is about waves, like music[2054]!

[2051] In A Quantum Algorithm for the Sensitivity Analysis of Business Risks by M. C. Braun et al, March 2021 (21 pages).

[2052] See CaixaBank Group, D-Wave Collaborate on Innovative New Quantum Applications for Finance Industry, March 2022.

[2053] See for example Display Advertising optimization by quantum annealing processor by Shinichi Takayanagi, Kotaro Tanahashi and Shu Tanaka of Waseda University and A quantum-inspired classical algorithm for recommendation systems by Ewin Tang, July 2018 (36 pages). The latter classical algorithm exceeds the performance of a quantum algorithm realized for D-Wave quantum computers.

[2054] See Quantum music Physics has long looked to harmony to explain the beauty of the Universe. But what if dissonance yields better insights? by Katie McCormick, May 2021.

The **Quantum Music** project[2055], was run by Volkmar Putz and Karl Svozil in Austria from 2015 to 2018. It led to the **QuTune** project[2056]. **Eduardo Miranda** from the Interdisciplinary Centre for Computer Music Research (ICCMR) at the University of Plymouth (UK) also works on using quantum computers to create music[2057]. He is currently preparing the release of the book "Quantum Computer Music", several of its chapters having already been published on arXiv[2058].

At this point, quantum music is about finding another source of randomness to create melodies (using quantum walks-based algorithms) and to generate credible synthetic voice. It led to the organization in November 2021 of a quantum music online event, organized, unsurprisingly, by the University of Plymouth (UK) with the sponsoring from IBM and Cambridge Quantum Computing[2059].

In 2019 **Quantum Sound** was the first music created and performed from measurements of superconducting qubits. It was not far from some form of random music generator. The project was run with the financial support of the Yale University Quantum Institute as well as from their top quantum scientists Michel Devoret and Robert Schoelkopf[2060].

At last, quantum music was generated in a more sophisticated way with a quantum annealer from D-Wave in 2021 by a very international team (India, Poland, Mexico, Estonia)[2061]. More recently, voice synthesis was studied using quantum algorithms[2062].

In 2022, a first “visual art” was created with the help of a quantum computer. The Quantum Prophet was created with the quantum artists trio Insight and **Kipu Quantum**. With the support of some AI, the author interfaced himself in real time with a quantum computer. Via motion capture, he manipulated qubits to modify aesthetically his animated 3D artwork which is sold with an NFT. All-in-all, the creative process was still largely in the hands of some humans!

Figure 684: The Quantum Prophet.

A last content field explored are games. Proof of concepts of quantum computing based games were recently proposed for Mastermind[2063] and Go[2064] and of games using quantum principles[2065].

This is all early stuff. Don’t count yet to see quantum computers having an impact on classical video games and the Metaverse, its most recent incarnation.

[2055] See Quantum music by Volkmar Putz and Karl Svozil, 2015 (5 pages).

[2056] It was linked to QuTune Project Quantum Computer Music Resources, about making music with quantum computing, and making quantum computing with music. This project started in Spring 2021.

[2057] See Quantum Computer: Hello, Music! by Eduardo R. Miranda, June 2020 (32 pages), Creative Quantum Computing: Inverse FFT Sound Synthesis, Adaptive Sequencing and Musical Composition by Eduardo R. Miranda, 2021 (32 pages) and The Arrival of Quantum Computer Music by Eduardo R. Miranda, May 2020.

[2058] See Making Music Using Two Quantum Algorithms by Euan J. Allen, Jacob F. F. Bulmer and Simon D. Small, January 2022 (13 pages), New Directions in Quantum Music: concepts for a quantum keyboard and the sound of the Ising model by Giuseppe Clemente et al, April 2022 (14 pages), QuiKo: A Quantum Beat Generation Application by Scott Oshiro, April 2022 (23 pages) and A Quantum Natural Language Processing Approach to Musical Intelligence by Eduardo Reck Miranda et al, December 2021 (41 pages).

[2059] See 1st International Symposium on Quantum Computing and Musical Creativity.

[2060] See Superconducting qubits as musical synthesizers for live performance by Spencer Topel, Kyle Serniak, Luke Burkhart and Florian Carle, March 2022 (17 pages).

[2061] See Music Composition Using Quantum Annealing by Ashish Arya et al, January 2022 (29 pages).

[2062] See Teaching Qubits to Sing: Mission Impossible? by Eduardo Reck Miranda and Brian N. Siegelwax, July 2022 (31 pages).

[2063] See Winning Mastermind Overwhelmingly on Quantum Computers by Lvzhou Li et al, July 2022 (27 pages).

[2064] See Quantum Go: Designing a Proof-of-Concept on Quantum Computer by Shibashankar Sahu et al, June 2022 (7 pages).

[2065] See Defining Quantum Games by Laura Piispanen et al, May 2022 (19 pages) which deals with the games using some principles of quantum physics but not games handled by quantum computers.

Another form of quantum art without pretentions is to exbibit art to explain what quantum physics and technologies are about, like was done in Switzerland in 2020[2066].

Defense and aerospace

The military-industrial complex has always been a big consumer of advanced IT. It is therefore not surprising that it is interested by quantum technologies. This is obviously the case in the USA but also in Europe, with Airbus being one of the first to take an interest in quantum applications, and also China and Russia to name a few others[2067].

The **US Air Force** has also identified various needs that can be covered by the four categories of quantum technologies with a special mention for quantum sensing in time measurement and navigation[2068]. They are also interested in quantum radars and, finally, in quantum computing applied to optimization problems.

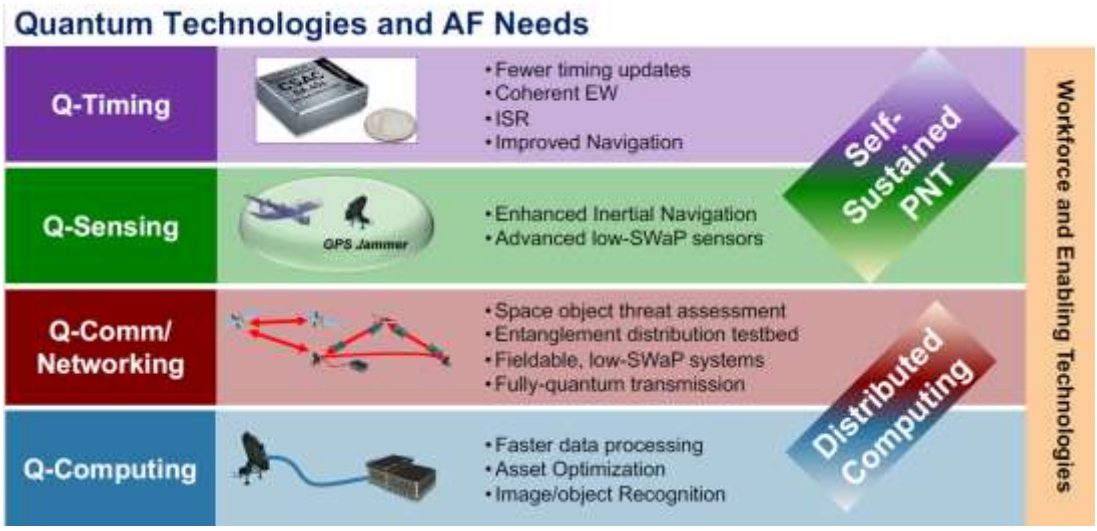


Figure 685: quantum technology and US Air Force needs. Source: Quantum Information Science at AFRL by Michael Hayduk, December 2019 (21 slides).

In France, the **DGA** has funded or co-funded since 2011 about twenty thesis on quantum and eight projects for €6.6M. The **Defense Innovation Agency** (reporting to the DGA) planned to launch a call for projects for quantum sensors in 2020 and in 2021 to fund a research project to support PQC in dedicated hardware. In July 2020, it became an ASTRID RFP on sensors, cryptography and quantum communications and on the creation of quantum computing algorithms[2069].

Quantum communications is also studies by the military around the world to secure communications[2070], particularly on the battlefield. **NATO** is experimenting it[2071]. Of course, **China** is working on it although with the visible part being only the civil use cases.

[2066] See "Do you speak quantum?" A quantum physics and art exhibition by Chiara Decaroli and Maciej Malinowski, June 2022.

[2067] See the review paper Quantum Technology for Military Applications by Michal Krelina, EPJ Technology, November 2021 (52 pages) that makes a pretty extensive inventory of defense use case for quantum sensing, communications and computing. On quantum radars, it showcase some adequate prudence. It still contains some misunderstanding like on page 27 on "*processing Big Data from surveillance and reconnaissance and identifying targets using quantum ML/AI*". Quantum computing is probably not bound to manage big data per se.

[2068] See Quantum Information Science at AFRL by Michael Hayduk, December 2019 (21 slides).

[2069] See Defense Research and Innovation: launch of a new ASTRID call for projects on quantum technologies, July 2020.

[2070] See Quantum Communication for Military Applications by Niels M. P. Neumann et al, TNO, November 2020 (11 pages).

[2071] See NATO cybersecurity center finishes tests of quantum-proof network by Jonathan Greig, March 2022.

Here are some various published case studies of quantum use in this vast sector.

It starts with **Lockheed Martin** partnering with **Google** and **NASA** to test D-Wave annealers staring in 2014. They developed with it a solution for formal proof of software operation. NASA co-founded the Quantum Artificial Intelligence Laboratory (QuAIL) with Google, operating a D-Wave Two. They test quantum optimization algorithms in different directions to optimize spacecraft filling, a variant of the bin-packing problem, on quantum versions of machine learning and deep learning algorithms, on problem decomposition and embedded computing[2072] .

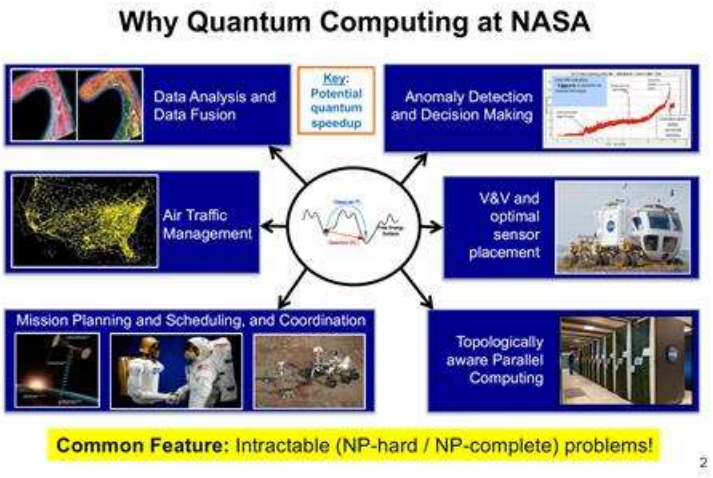


Figure 686: Source: Quantum Computing at NASA: Current Status by Rupak Biswas, September 2017 (21 slides).

In 2015, **Raytheon** and **IBM** demonstrated the efficiency of a quantum algorithm using a "black box" or "oracle" to reconstruct an unknown bit string, all running on an IBM 5 qubit general purpose quantum computer[2073]. This is obviously far from a real-world use case.

The **Airbus** group has created a team based at their Newport site in Wales, which is tackling the uses of quantum, particularly in the analysis of aerial imagery (not obvious...) or for the design of new materials (more obvious). They also want to optimize the air flow on the wings, a problem that is nowadays dealt with by finite element simulation. They could try to optimize the air conditioning in airplanes, the biggest source of cabin noise, above the plane's engines!

In a different field, navies are interested in quantum sensing and particularly in micro-gravimetry measurement tools used to detect submarines.

Thales prototyped in 2021 a quantum annealing solution running on D-Wave Advantage (5000 qubits) to optimize radar configuration (the "Integrated Side Lobe Ratio" or ISLR NP-hard problem, which solution is "*the finding optimal sequences of phase shifts to minimize the mean squared cross-correlation sidelobes of a transmitted radar signal and a mismatched replica*")[2074]. Yet, it didn't reach any quantum computing advantage but the authors think future evolutions of D-Wave annealers may be promising for this respect.

In collaboration with **Fraunhofer IAIS**, Thales also prototyped a quantum image alignment solution for satellite images with quantum-based keypoints extraction and feature matching. It was tested with D-Wave quantum annealers and gate-based quantum computers.

The outcome is always the same: classical systems still deliver superior results but the proposed methods have the potential to outperform classical systems with future quantum computers[2075].

Thales Alenia Space is investing with CNES and DGA in quantum satellite telecommunications.

[2072] This is well described in Quantum Computing at NASA: Current Status by Rupak Biswas, September 2017 (21 slides).

[2073] This is documented in Demonstration of quantum advantage in machine learning (12 pages).

[2074] See Phase-coded radar waveform AI-based augmented engineering and optimal design by Quantum Annealing by Timothé Presles, Cyrille Enderli, Rémi Bricout, Florence Aligne and Frédéric Barbaresco, Thales, 2021 (9 pages).

[2075] See Towards Bundle Adjustment for Satellite Imaging via Quantum Machine Learning by Nico Piatkowski et al, April 2022 (8 pages).

The use of quantum technologies in the military field also gives rise to elucubrations that hybridize the plausible and the offbeat, such as those of the American political scientist **James Der Derian**, director of Project Q at the University of Sydney[2076].

Defense and quantum are also the playground of disinformation. For example, the battle is amplified between the USA and China, with many news reports touting an enormous China's quantum investment of $13B to $15B, which happens to be a misleading and exaggerated number[2077]. Very few sources, like a February 2022 report from **Rand Corporation** are pinpointing this and detailing China's real quantum investments which are probably either on par or slightly below similar investments in the USA and Europe, in the broad range of $2B to $4B across 10 years[2078]. The report estimated that only 1,700 students earned a PhD in quantum technology in China.

You also have weird plans like the UK military who seems interested to put quantum computers in tanks, which doesn't make much sense, at least for the next 20 years. The reason is they've been lured in this path by Orca which touts ambient temperature quantum computing[2079].

Intelligence services

The world of intelligence and targeted eavesdropping is obviously on the lookout for the quantum. Shor's algorithm is the main application targeted by organizations managing electronic eavesdropping such as the **NSA** and all its colleagues. They are firefighters who are eager to decode information intercepted from various targets (embassy communications, economic intelligence, etc.) and to protect the sensitive communications of their own states against this type of decryption. They are therefore investing simultaneously in quantum computing (the "arsonist" dimension) and in quantum keys and post-quantum cryptography (the "firefighter" dimension).

On the other hand, these investments are not very public. The NSA has communicated well for almost ten years on the firefighter dimension but very little on the arson dimension.

They have surely acquired the various generations of D-Wave computers to get their hands on, in conjunction with **Lockheed Martin** which is one of their major suppliers. NSA also maintains a joint laboratory with NIST and the University of Maryland, **QuICS**, which will be launched in 2014.

One way to lift a veil on these activities is to detect laboratory and startup grants awarded by **IARPA**, the intelligence innovation agency led by the DNI (Director of National Intelligence), who oversees all American intelligence. It consolidates collaborative research funding for all intelligence agencies.

[2076] See Drones, radars, nuclear: how the quantum will change the war by Vic Castro, February 2020. Some remarks on this article: Rydberg atom-based qubits are only one of the types of qubits currently being studied. They are said to be "cold atom-based" and are moreover the specialty of Pasqal (France). There are many other types of qubits. The text also makes a big confusion in qubits and logical gates between qubits. These gates connect qubits together. They are often systems based on the diffusion of microwaves, photons emitted by lasers or magnetic couplers. Rydberg atoms are qubits and not qubit couplers.

[2077] See this example among others: The quantum tech arms race is on by Stuart Rollo, Asia Times, March 2022.

[2078] See An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology by Edward Parker, Rand Corporation, February 2022 (140 pages). Extracts on China: « *Even higher levels of announced investment are associated with the main Chinese quantum research facility, the Hefei National Laboratory for Physical Sciences at the Microscale (HFNL), which is led by Pan and a part of the University of Science and Technology of China in Hefei, Anhui Province. Chinese-language news media reported $1.06 billion in laboratory funding in 2017,6 and the Anhui Business Daily newspaper reported plans (though not confirmed funding) for $2.95 billion per year over the 2017–2022 period.* ***These announced spending goals are in stark conflict with the government-wide spending estimates*** *given in Table 4.11. The $1.06 billion start-up funding that Chinese news media announced in 2017 for Pan's quantum laboratory alone hugely exceeded Pan's own 2019 estimate for the PRC's total government spending over the same time period.* ***Our team's China experts assess that these conflicting reports of funding levels are not unusual in China; the PRC government often announces ambitious (and often highly politicized) spending goals, and it is not uncommon for these goals to go unmet****… […] In summary, official reports of the PRC's government investment in quantum R&D in recent years have varied widely, from a low of $84 million per year (Pan's estimate) to a high of at least $3 billion per year (the Anhui Business Daily's reported funding for Pan's laboratory). We are unable to assess from public information which figure is more accurate. By comparison, the U.S. government has spent $450–$710 million per year in recent years;* ***we cannot determine whether the PRC total is higher or lower than this amount***.".

[2079] See UK Military Wants to Install Quantum Computers in Tanks for Some Reason by Lonnie Lee Hood, Future Society, June 2022.

It has already launched five programs around quantum technologies: in superconducting qubits (CSQ), logical qubits (LogiQ, with IBM), error correction (MQCO, also with IBM), the creation of development tools (QCS, with Raytheon and GeorgiaTech) and quantum annealing computation (QEO). But it is not clear that this has significantly advanced the state of the art.

Other Western intelligence services may also have acquired D-Wave, notably the British CGHQ. The NSA is also in contact with IBM and Google to explore the path of superconducting quantum general-purpose computers.

Industry

Industry in the broadest sense of the term is another outlet for quantum computing. As soon as there is a complex optimization problem for scheduling, logistics or complex system design support, quantum will have its say.

The Japanese **JSR Corporation** is one of the companies working with IBM in the quantum field, mainly for the creation of new materials. **LG Electronics** announced a similar partnership with IBM in January 2022 to "*support big data, artificial intelligence, connected cars, digital transformation, IoT, and robotics applications*", you name it all.

It seems that quantum computing could be used within computer-aided design tools[2080]. But the document cited in the note comes back to the basics of quantum computing without being very elaborated on quantum computing uses in CAD, a very common phenomenon when quantum computing is pushed in various industries.

The routing of electronic circuits is also a NP-complete problem that could be partly handled by quantum algorithms, provided they have a sufficient number of qubits. This could be useful for designers of ASIC-type circuits and especially FPGAs, these circuits whose operating logic is dynamically programmable via two key parameters: the decision tables of the processing units and the links between these units.

Science

Fundamental research is starting to test and use quantum computing, particularly in materials development and particle physics research[2081].

After having investigated quantum computing for a good number of years with a first workshop organized in November 2018, **CERN** launched a formal **Quantum Technology Initiative** (QTI) in September 2020[2082]. They want to use quantum computing to analyze the noisy data coming from their ultrasensitive particles detectors and to simulate the behavior of many-body quantum phenomena.

[2080] According to Computer-Aided Design for Quantum Computation by Robert Wille, Austin Fowler and Yehuda Naveh (Google and IBM), 2018 (6 pages).

[2081] See Applying quantum computing to a particle process by Glenn Roberts Jr., Lawrence Berkeley National Laboratory, February 2021, referring to Quantum Algorithm for High Energy Physics Simulations by Benjamin Nachman et al, February 2021 (6 pages). The algorithm used to detect particles using the 20 qubits IBM Q Johannesburg quantum system in the cloud is not providing any quantum advantage but would be promising with a larger number of qubits. See also the review paper Quantum Simulation for High Energy Physics by Christian W. Bauer et al, April 2022 (103 pages) and Simulating Collider Physics on Quantum Computers Using Effective Field Theories by Christian W. Baue et al, November 2021 (7 pages), Quantum computing hardware for HEP algorithms and sensing by M. Sohaib Alam et al, April 2022 (23 pages), Quantum Computing for Data Analysis in High-Energy Physics by Andrea Delgado et al, March 2022 (22 pages) and Snowmass White Paper: Quantum Computing Systems and Software for High-energy Physics Research by Travis S. Humble, March 2022 (17 pages).

[2082] It was later formalized in their CERN Quantum Technology Initiative Strategy and Roadmap by Di Meglio et al, October 2021 (46 pages).

CERN also participates to international quantum computing education and training with its online training resources. IBM worked with CERN to select/classify LHC events using QSVM[2083].

Back in 2017, **Caltech** used a D-Wave Two X quantum annealer with 1098 qubits to "rediscover" the Higgs boson using CERN LHC data and a QAML algorithm (quantum annealing machine learning)[2084]. Later in 2020, they improved it with their QAML-Z algorithm, quantum annealing machine learning model zooming in on a region of the analyzed energy surface[2085].

In astrophysics, superconducting qubits are also used to detect dark matter, in the form of axions, a dark matter candidate and hidden photons, that would interact with the photons[2086]. Other researchers are also using squeezed states to detect axions[2087]. Quantum computing is also tested to simulate exotic magnetic materials[2088].

Two scientific areas drive the attention with quantum computing, **weather forecast** and how to mitigate **climate change**. It's so politically trendy that many researchers and vendors are focusing their messaging on these application domains. They obviously tend to make significant overpromises since most of the related applications will require large-scale fault-tolerant quantum computers to be viable, like for the quantum simulations related to the improvements of the Haber-Bosch process or for designing new more efficient batteries. Overpromises on fixing climate change come for example from **McKinsey**[2089] or **PsiQuantum** who has no functional quantum computer yet[2090] and on weather modelling from **Pasqal** and **BASF**[2091]. **Quantinuum** is a little more credible with working on low-emission refrigerant production which deals with more simple problems although their existing 20 functional qubits are of no real use today[2092].

[2083] See Application of quantum machine learning using the quantum kernel algorithm on high energy physics analysis at the LHC by Sau Lan Wu et al, Physical Review Research, 2021 (9 pages).

[2084] See Solving a Higgs optimization problem with quantum annealing for machine learning by Alex Mott et al, 2017 (5 pages).

[2085] See Quantum adiabatic machine learning with zooming by Alexander Zlokapa et al, Caltech, October 2020 (9 pages).

[2086] See Searching for Dark Matter with a Superconducting Qubit by Akash V. Dixit et al, April 2021 (7 pages).

[2087] See A quantum enhanced search for dark matter axions by K. M. Backes et al, 2021 (8 pages).

[2088] See Quantum computing enables simulations to unravel mysteries of magnetic materials by Elizabeth Rosenthal, Oak Ridge National Laboratory, February 2021, using a 2000Q D-Wave annealer.

[2089] See Quantum computing just might save the planet, McKinsey, May 2022.

[2090] See PsiQuantum Announces Qlimate Initiative Developing Breakthrough Climate Technologies Enabled by Quantum Computing, May 2022.

[2091] See Pasqal, BASF to collaborate on quantum compute-powered weather modeling, July 2022. This works seems serious from the pure mathematic standpoint, with modelizing weather models using differential equations and quantum neural network models labelled PINNs (physics-informed neural networks). What these stories don't tell is the size of the models that would be required in real use cases. Most of the time, these sizes are way beyond the capacities of the related quantum computers, even when taking into account their 5-year roadmap. On top of that, one unaddressed issue is how these quantum simulators are fed with training data. The larger the data set, the slower it is, and it requires a lot of classical pre-processing.

[2092] See How Quantum Computing Can Help Keep Things Cool, 2022.

Software and tools vendors

There are already many quantum software and development tools startups, particularly with regards to what suitable hardware is available. Initially, many of them were developing software running on D-Wave annealers. Then, as gate-based vendors like IBM started to put their hardware in the cloud, most software vendors adopted it. Many software vendors adopt hybrid approaches that combine business knowledge, associated algorithms and their execution on classical machines and quantum computers, hybrid classical-quantum algorithms, or so-called "quantum inspired" algorithms that run on classical computers. Only a few software vendors have adopted the quantum simulation paradigm which is a pity given these systems may be the most viable in the mid-term.

Even though quantum software won't solve all business and technical problems, it's time for legacy software vendors to give a look at the value it could provide[2093].

(cc) Olivier Ezratty, 2022

Figure 687: a nice logo map of the quantum software industry. (cc) Olivier Ezratty, 2022.

These approaches are essential for survival. Indeed, a startup cannot be exclusively dedicated to quantum computing at the risk of only being able to sell proofs of concepts on a very small scale that cannot generally be deployed industrially[2094].

There are real opportunities to position yourself in this emerging market! You will notice that this inventory does not include any Chinese startup. This is probably not by chance. This ecosystem is therefore still very young. It will evolve in parallel with the development of commercial quantum computers. You see already the startup scene maturing with many vendors adopting platforms approaches and developing partnerships models all over the place[2095]. China is not very well versed in software compared to hardware and seems to have put the quantum priority on cybersecurity more than on quantum computing.

[2093] See Why quantum software will be eating the world by Yuval Boger, June 2022.

[2094] This principle of reality is well described in The hard sell of quantum software by Jon Cartwright, 2019.

[2095] See a couple examples in Collaboration is Dominating Quantum Computing by Russ Fein, The quantum Leap, April 2022.

1QBit (2012, Canada, $35M) is a multi-sector quantum software company. It was funded among others by Fujitsu, as well as by Accenture and Allianz.

They have developed various low-level quantum algorithmic components that are hardware neutral. This includes, for example, the graphs processing that they apply in several markets, via their consulting activity. They cover financial markets, for the dynamic optimization of investment portfolios or to simplify the allocation of asset classes in a portfolio[2096].

They also developed QEMIST, a library for accelerating innovation in materials science and drug discovery. In addition to being a long-standing partner of D-Wave, they also work with IBM. The startup already has above 100 employees. Their customers include Dow Chemical (chemicals), Biogen (biotechs) and Allianz. In April 2020, they launched the "Quantum Insights Network", a network of around 100 experts and content in quantum computing.

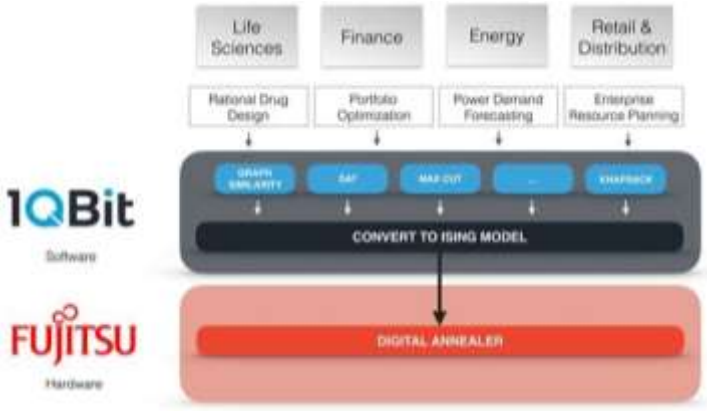


Figure 688: 1QBit Software running on Fujitsu Hardware. Source: Fujitsu.

Adaptive Finance Technologies (2020, Canada) came out of the Creative Destruction Lab. It was created by Roman Lutsiv, Vlad Anisimov and Edward Tang and develops investment and credit risk management software for the finance industry.

They used classical machine learning methods and are prototyping quantum machine learning solution running on D-Wave annealers.

Algorithmiq (2020, Finland) is a spin-off from the University of Turku which develop quantum software for life science and data science. They also created an online quantum science and technologies learning. Their CEO is Sabrina Maniscalco.

AIQTECH Inc (2018, Canada**)** is a machine learning specialist that explores the uses of QML. They are partners of the IBM Quantum Network. It is a two-person shop.

Aliro Quantum (2018, USA, $2.7M) is a startup that came out of the blue in September 2019. It started with developing software tools telling developers whether cloud quantum computing resources are available to perform calculations faster than on traditional processors, especially on GPUs.

They are partnering with HQAN (Hybrid Quantum Architectures and Networks, funded by the NSF, and belonging to the University of Illinois) to develop the seeds of a distributed quantum computing network in the USA. The startup founded by Prineha Narang (CTO, coming from Harvard) and Jim Ricotta (CEO) is positioned as a quantum Internet service company providing EaaS services, or entanglement as a service. In October 2022, they released AliroNet, a software solution providing emulation services of entanglement-based quantum networks, which can help design small scale pilots and universal entanglement-based quantum networks, including quantum networks connecting quantum sensors.

[2096] See Solving the Optimal Trading Trajectory Problem Using a Quantum Annealer, 2015 (13 pages).

Apply Science (2019, Italy) is an applied mathematics services company who is experimenting quantum computing in the IBM Quantum Network. They are testing QML algorithms for virtual drug development.

ApexQubit (2018, Belarus and USA) is a drugs discovery company that develops quantum software solutions for the pharmaceutical sector targeting rare diseases. They operate in project mode and publish some research papers on their web site.

Aqemia (2019, France, 31.6M€) is a software company developing drug discovery and retargeting algorithms using statistical physics, AI and quantum inspired algorithms. The startup is a spin-off from Ecole Normale Supérieure run by Maximilien Levesque and Emmanuelle Martiano. In December 2020, they announced a partnership with Sanofi to discover new treatments for covid-19. They raised 30M€ in October 2022 to fund their AI-enabled drug discovery pipeline, but not part of their future quantum-based algorithms efforts.

aQuantum (2018, Spain) is quantum software engineering service company doing contract research, development and consulting. They develop hybrid classical-quantum computing software and provide quantum software project management expertise, particularly in quantum machine learning.

They also developed |QuantumPath⟩ (*aka* Q|Path⟩), a quantum software development and lifecycle application platform. It contains all the tools to handle the whole software design and execution lifecycle covering both gate-based, quantum simulators and quantum annealing based computing, supporting Qiskit (IBM), Forest (Rigetti), Ocean (D Wave), ProjectQ and Quantinuum's |tKet⟩. They embed the open sourced Quirk graphical tool in their development environment. Since April 2022, QuantumPath is integrated with AWS and Amazon Braket making it possible for developers to access the quantum emulation and quantum hardware platforms supported by Amazon Braket.

A*Quantum (2018, Japan, $3M) specializes in the development of quantum software solutions for both annealers (including digital annealers from Fujitsu) and gate-based quantum computers (from IBM). Their ambition is to create high-level software libraries for users.

Ankh.1 (2018, USA) has developed Anubis Cloud, a virtual machine in the cloud for data scientists that integrates with the open source solution Jupyter as well as with the TensorFlow and Keras learning machine frameworks.

AppliedQubit (2019, UK) presented itself as a publisher of quantum software for businesses.

In particular, they targeted the two main markets: finance and chemical simulation, in addition to generic optimization problems and predictive analysis.

They were developing both classical/quantum hybrid computing and quantum machine learning solutions. The company stopped operating in March 2021.

Arclight Quantum (2020, China, $3M) is a quantum software company spun out of the Institute of Software Research of the Chinese Academy of Sciences. With CAS, they developed isQ-Core, a quantum cloud software development platform that can execute gate-based quantum code on both classical emulators and quantum processors. They also created an EDA (electronic design automation) tool for the creation of quantum processors.

Arline (2020, Germany) is developing a compiler optimizing QML algorithms execution, reducing the number of quantum gates used and taking into account all qubits characteristics such as their connectivity.

They also propose Arline Benchmarks, an automated benchmarking platform for quantum compilers. It compares gate count, circuit depth and compiler runtime.

It can also be used to combine compiled circuits and optimization routines coming from different compilers in a custom pipeline to optimize algorithms performance.

Artificial Brain (2022, India/USA) is developing hybrid quantum-classical algorithms targeting energy, aviation, finance and climate change use cases.

Its first achievement was an algorithm identifying optimal locations for electric vehicle charging. It is running on D-Wave quantum annealers (probably from the Pegasus generation) using a mix of quantum annealing and genetic algorithm developed on QBSolv[2097]. It produces some result in 3 seconds for $8.5*10^{15}$ combinations. Its scalability depends on how D-Wave will expand the capacity of its annealers in the future. The company was founded by Jitesh Lalwani, who worked beforehand in the software industry.

Artiste-qb.net (2018, Canada) has a business model similar to that of 1Qbit: they develop algorithmic bricks of intermediate levels that they then assemble according to the needs of their customers.

They have even filed patents for certain methods. The startup was created by an international team including German researchers. They develop a Python based set of libraries in open source, available on Github.

Automatski (2014, USA) is a software company established in London, India in Bangalore and in California. They do applied contract research to develop quantum algorithms on any form of computer and quantum simulator. They have developed a software solution for emulating a large, unspecified number of qubits on conventional computers. They focus on creating biochemistry algorithms and claim to have solved protein folding and to cure diabetes, cancers and 4000 other diseases. Seems like some sort of overselling.

Avanetix (2019, Germany) develops hybrid algorithms dedicated to solving supply chain problems. They combine classical optimization methods, machine learning and quantum computing. They target the automotive and logistics markets. The startup is founded and managed by serial entrepreneur Naimah Schütter.

Beit.tech (2016, Poland, $1.4M) is specialized in quantum machine learning. It is mainly a research project funded by the European Union, covering the period 2017-2010. The founder Wojtek Burkot is a former Google employee who even tries to make D-Wave useless by creating algorithms for optimizing complex graphs that can run on traditional computers.

[2097] See Towards an Optimal Hybrid Algorithm for EV Charging Stations Placement using Quantum Annealing and Genetic Algorithms by Aman Chandra, Jitesh Lalwani Babita Jajodia, November 2021 (6 pages).

Blueqat (2008, Japan, $2.3M), formerly MDR for Machine learning and Dynamics Research, is creating algorithms integrating AI and chemistry, working among other with customers from the cosmetics industry like KOSÉ[2098].

They are working with D-Wave annealers. The startup was founded by Yuichiro Minato and various other alumni of the University of Tokyo.

Boltz.ai (2020, Canada) is specialized in the development of AI and quantum software for the agriculture business. They create crop field allocation optimization tools.

BosonQ Psi (2020, India) created the cloud-based BQPhy software suite, a computer-aided engineering (CAE) solution performing complex simulations with using hybrid quantum-classical algorithms. It covers structural mechanics, thermal analysis and design optimization. The startup was created by Abhishek Chopra, Rut Lineswala and Jash Minocha.

Boxcat (2017, Canada) is a startup created by Ystallonne Alves that develops image and video processing solutions based on hybrid quantum algorithms. They target the media and medical imaging markets. Their algorithms are based on currently available hardware architectures (D-Wave, IBM, Rigetti, Xanadu). The process they present on their site is an image realized on a D-Wave, which could have been realized with Nvidia's latest GPUs.

Figure 689: an artificial image generated on a D-Wave 2000Q by Boxcat. Source: Boxcat.

Cambridge Quantum Computing Limited (2015, UK, $72.8M) develops the $t|ket\rangle$ quantum operating system and various quantum algorithms including Arrow for machine learning[2099]. They are partnering with Oxford Quantum Circuits and with IBM which is one of their investors. CQC is also active in post-quantum cryptography.

$t|ket\rangle$ is available broadly and for free to everyone since February 2021 and also open sourced. It covers many quantum computing platforms (IonQ, Honeywell, AQT, IBM Qiskit, Rigetti, Amazon Braket and Azure Quantum) and incorporates circuit optimization and routing. It's interfaced with Python with Pytket. $t|ket\rangle$ is also used by EUMEN, CQC's quantum computational chemistry platform, and the company's QML framework. QQC is also partnering with Roche to use quantum algorithms for drug discovery targeting Alzheimer's Disease, as announced in January 2021.

In 2021, CQC launched a cloud software random quantum number generator. It is using a classical random generator, a quantum random number generator amplifying the randomness of the first and a Bell test used to check the resulting randomness, all running on an IBM quantum system[2100].

[2098] Blueqat developed an algorithm that analyzes the distribution of cosmetics product features in a multidimensional space. It visualizes existing areas and reveals unknown product areas they were able to open up, to create possibilities for new cosmetic designs that humans never thought of. The solution was patented and thus, is not yet publicly documented.

[2099] See t|ket> : A Retargetable Compiler for NISQ Devices, April 2020 (43 pages).

[2100] See Quantum-Proof Cryptography with IronBridge, TKET and Amazon Braket by Duncan Jones, March 2021 and Practical randomness and privacy amplification by Cameron Foreman et al, 2020 (26 pages). It was branded as (origin)^{cQ} in December 2021.

CQC has also been demonstrating how NLP (Natural Language Processing) could be implemented on current NISQ IBM quantum computers. Their researchers explain that the structure of natural language is natively quantum, which could lead to efficient translating, and better understanding of complete sentences and texts. The paper however doesn't provide much indication on the way data was actually encoded in the qubits. It lacks supporting data on actual system performance[2101]. In October 2021, this was packaged in an open source Quantum Natural Language Processing (QNLP) toolkit and library, lambeq.

The company announced a merger with Honeywell Quantum Systems in 2021. In December 2021, it became Quantinuum with a staff of over 350 employees.

ChemAlive (2014, Switzerland) is a quantum computational chemistry startup and contract research company. It provides simulation tools for getting molecular properties and synthetic reactions using basic 2D chemical syntax.

They deal with reaction mechanism elucidation and optimization, kinetic observed rate modeling, molecular design, virtual screening and drug discovery, molecular and spectroscopic property prediction, materials modeling and design, data and computation driven synthetic planning, experimental execution of chemical synthesis and experimental research on spectroscopic and electronic molecular properties. They developed ConstruQt, a software tool transforming molecular drawings into 3D structures and energies.

All of this is quantum... but seems to be computed classically. Quantum chemistry doesn't necessarily mean quantum-computed quantum chemistry. Once quantum computing hardware will scale, they'll naturally switch to it.

ClassiQ Technologies (2020, Israel, $51.8M) develops a quantum programming tool providing a higher level of abstraction than classical quantum gate programming[2102]. Their platform is on Amazon Bracket as announced in June 2022.

The company was created by Nir Minerbi (CEO), Amir Naveh (VP-R&D) and Yehuda Naveh (CTO, who spent 20 years at IBM Research in Haifa, including quantum, condensed matter specialist). Their CMO, Yuval Boger, also runs the Qubit Guy's podcast series

CogniFrame (2016, Canada) is a software publisher of data analysis platform software exploiting machine learning. They also develop hybrid algorithms for the financial sector based on D-Wave annealers.

One of their first customers is the Canadian investment bank Alterna Savings. The proposed applications are classic in the financial field: credit risk assessment and investment portfolio optimization. Late 2021, they launched **FirstQ Store**, an aggregation platform of quantum computing applications, provided as an application running on Windows, Mac and Linux desktops. It supports QUBO applications for Toshiba's Simulated Bifurcation Machine (a sort of digital annealer) and gate-based algorithms[2103].

ColibrITD (2019, France) is a quantum software R&D company created by Hacène Goudjil and Laurent Guiraud that develops vertical use case software components with a team of a dozen skilled PhDs/post-docs, focused on gate-based computing models.

[2101] See Foundations for Near-Term Quantum Natural Language Processing by Bob Coecke et al, December 2020 (43 pages). By the way, they are using ZX calculus in this work.

[2102] See A revolutionary approach to building quantum circuits by Amir Naveh and Yuval Boger, Classiq, November 2021 (32 minutes).

[2103] See Benchmark of quantum-inspired heuristic solvers for quadratic unconstrained binary optimization by Hiroki Oshiyama and Masayuki Ohzeki, December 2021 (11 pages).

They created a set of framework tools branded “QUICK” for “Quantum Innovative Computing Kit” for solving problems in the financial, pharmaceutical, material design and logistic fields. They also contribute to the advancement of quantum software engineering tools like in functional testing[2104].

CreativeQuantum (2010, Germany) is specialized in quantum physics-based R&D in the chemical and pharmaceutical industries.

They seem however to run these many algorithms with classical computers. Which makes sense given quantum computers are not yet powerful enough to run these physics simulation tasks efficiently.

Culgi (2004, Netherlands) is yet another computational chemistry company that will someday adopt quantum computing or simulation for its software. It was founded in 1999, changed its name in 2004 and was acquired by Siemens in 2020.

Dirac (2021, USA) is developing quantum software and algorithms for robotic applications. That New York City startup was created by Filip Aronshtein. I’d advise them to revisit their branding since the search engine optimization of Dirac is not obvious. On top of these nasty white logos on dark backgrounds!

dividiti (2014, UK) develops quantum algorithms, particularly in machine learning and using hybrid methods. Their solutions are open source. It is a service model, which is rather the standard in this market at the moment.

D Slit Technologies (2018, Japan) develops custom quantum software solutions for creating proofs of concept. Their website is not very talkative about their achievements.

Elyah (2018, Japan/Dubai) is developing quantum software to "*improve people's lives*". The company is made up of two people, a certain Salman Al Jimeely based in Dubai and an American, Sydney Andrew, based in Tokyo. I’m still looking for those developing software worsening people’s lives, besides pirates.

Entanglement (2017, USA) is a quantum software development service company. One of their achievements was to create a quantum inspired software for vaccine distribution optimization in the USA in 2021.

Entropica Labs (2018, Singapore, $1.8M[2105]) is a startup dedicated to the creation of quantum (and non-quantum) algorithms for life sciences and in particular for genomics, based on quantum machine learning.

The result is faster development of therapies, in partnership with pharmaceutical companies. The company was founded by Tommaso Demarie (CEO), Ewan Munro (CTO), joined in 2018 by Joaquin Keller, a former Orange researcher based in France, who left them to later create **exaQ.ai**. It offers its Entropy Development Framework that manages the workflow of quantum software. They are working with Honeywell/Quantinuum and BMW to create proof of concepts for supply chain optimization.

exaQ.ai (2020, Singapore) is a quantum machine learning created by Joaquín Keller, who formerly co-founded Entropica Labs and was a teacher in France and a R&D lead at Orange.

[2104] See Principles of quantum functional testing by Nadia Milazzo, Olivier Giraud, Giovanni Gramegna and Daniel Braun, ColibrITD, Université Tübingen and Université Paris Saclay CNRS LPTMS, September 2022 (13 pages).

[2105] See Singapore quantum computing startup Entropica Labs bags $1.8m in seed funding by Miguel Cordon, May 2020.

Their offering is based on the "polyadic QML Library[2106]" that does supervised quantum machine learning for multi-class classification on NISQ architectures.

It was tested on IBM Quantum hardware with accuracy levels similar to classical machine learning, doing a ternary classification of the Iris flower dataset that contains only 150 objects to classify in three classes. They also provide their ManyQ quantum computer emulator that is optimized for quantum machine learning and supports CPUs and GPUs.

FAccTs (2016, Germany) is a spin-off from Max Planck Institute for Chemical Energy Conversion that develops ORCA, a quantum-chemical software package.

FAR Biotech (2016, USA) does drug discovery based on quantum representation of molecular structures done, so far, on classical computing.

Foqus (2021, Canada) The company is a spin-out from University of Waterloo, led by Michele Mosca and Sadegh Raeisi which creates a software solution to improve the performance of MRI and NMR systems with machine learning and quantum computing. Quantonation is one of its investors.

GenMat (USA-Canada, $15M) aka Quantum Generative Materials is a stealth quantum computing software startup. They got a funding of $15M (plus $35M following development milestones) from **Comstock Mining** (USA), a gold and silver mining Company also invested in lithium-ion battery manufacturing.

Good Chemistry Company (2022, Canada) is a spin-off from 1Qbit which developed QEMIST Cloud, a cloud developers platform associating classical machine learning and quantum computing to undertake computational chemistry simulations. Accenture is an investor in the company.

Grid (2009, Japan) is a specialist in deep learning and learning by reinforcement with their ReNom platform.

They have adapted this library in a quantum version called ReNomQ. And they have been IBM Quantum partners since September 2019. On the other hand, their AI was probably not very efficient to help them find a company name easy to be found via search engines.

Groovenauts (2012, Japan, $4.5M) developed in 2016 a D-Wave based cloud service called Magellan Blocks to solve complex optimization problems.

They exploit hybrid algorithms combining machine learning and quantum algorithms. Their first customers include a Japanese retailer who optimizes its planning and Mitsubishi Estate who optimizes household waste collection[2107].

Hafnium Labs (2016, Denmark) develops software that provides physical property data for molecules and mixtures by combining quantum chemistry and AI. So, not yet a quantum software vendor.

[2106] See Polyadic Quantum Classifier by William Cappelletti, Rebecca Erbanni and Joaquın Keller, Entropica Labs, July 2020 (8 pages) and https://dev.exaq.ai/.

[2107] See Groovenauts and D-Wave collaborate on hybrid Quantum Computing, December 2019.

Horizon Quantum Computing (2018, Singapore, $15.23M[2108]) creates quantum development tools. Their ambition is to compile code from classical development tools such as Matlab and then run it on quantum computers, in order to make quantum computing accessible to traditional developers. In short, they want to democratize quantum software development.

They also work on quantum Internet software. As such, they announced in 2022 that they will establish a quantum communication on Singapore's National Quantum-Safe Network. The startup was launched by Joe Fitzsimons and Si-Hui Tan, both coming from Singapore's CQT research center. Their last funding of $12M in April 2022 came from Tencent Holdings.

HQS Quantum Simulations (2017, Germany, €14.3M) is a Karlsruhe Institute of Technology spin-out startup led by Michael Marthaler. They are developing quantum algorithms in the field of organic and inorganic molecular simulation of simple molecules (methane, light emission in OLEDs, diffusion of molecules in liquids). It mostly targets the chemistry industry.

They announced in July 2018 an open source porting tool for ProjectQ code (IBM platform) to Cirq (Google platform). They released their Quantum Assisted Design toolbox in 2020 and qoqo, a quantum circuit representation library in 2021. They already have BASF and Bosch as customers. In practice, they also develop classical versions of their algorithms, running on datacenters or supercomputers[2109] . Their latest 12M€ funding round in February 2022 was led by Quantonation.

Ingenii (2021, USA) is a startup created by Christine Johnson (CEO) and Marko Djukic (CTO, coming from Purdue University) that wants to simplify the work of scientists using quantum computers.

They started with creating a Python package to submit data science jobs like quantum chemical simulations to quantum hardware like IonQ through Microsoft Azure for a starter. These algorithms are of course limited by the current capacities of existing quantum computers.

Innovatus Q (2018, Singapore) is a spin-off from the Centre for Quantum Technologies in Singapore. They work on hybrid quantum algorithms based on trapped ions and superconductors.

Jaynes Computing (2019, Canada) is creating a cloud-based solution based on some quantum machine learning (QML) in the supply chain market. They are supposed to use some NISQ hardware, without any details. The startup was created by German Alfaro and was spun out of the Creative Destruction Labs.

Jij (2018, Japan, $1.9M) was created by researchers from the Tokyo Tech Institute of Technology. It develops software for quantum annealing, including OpenJij, an open source framework for implementing Ising models to model particle interactions, built on D-Wave's QUBO APIs. They are also partners of Microsoft Azure.

JoS Quantum (2018, Germany) develops quantum software solutions for the financial services industry, particularly in risk management and fraud detection. They also do contract research.

[2108] See the QSI Seminar presentation: Dr. Joe Fitzsimons, Horizon Quantum Computing, Abstracting Quantum Computation, April 2020 (1h26). Joe Fitzsimons create the blind quantum computing protocol with Anne Broadbent and Elham Kashefi in 2008.

[2109] See HQS Quantum Simulations: How to survive a Quantum winter by Richard Wordsworth, 2020.

Ketita Labs (2018, Estonia) develops unspecified quantum software for NISQ computers, and for good reason. It is a university spin-off.

KiPu Quantum (2021, Germany, 3M€) was created by Enrique Solano, a prolific and outspoken researcher working in Spain (Bilbao) and Germany. The startup's goals are to "*design and manufacture of modular and co-designed Quantum computers*" tailored to solve specific tasks with NISQ, without waiting for LSQ generations.

In 2021, they announced their NISQA paradigm merging digitized-counterdiabatic quantum computing (DCQC) and digital-analog QC (DAQC) for NISQ computers without error correction overhead. It uses digital and analog compression techniques to reduce the physical qubits required to solve specific industry problems (combinatorial and optimization problems, chemistry, QML, ...).

Kuano (2020, UK, $3.6M) creates quantum software solutions for the design of molecules and in particular for the inhibition of enzymes, which is used both in pharmaceuticals and to create protective agents in agriculture.

They use quantum emulation and quantum algorithms as well as machine learning. The company was founded by defectors of GTN, including their CEO Vid Stojevic who was the CTO of GTN.

Menten.ai (2018, USA, $4M) develops hybrid algorithms combining machine learning and quantum programming to simulate organic chemistry and design enzymes, peptides and proteins, working with D-Waves annealers.

Molecular Quantum Solutions (2019, Denmark) or MQS, provides computational tools for pharma, biotech and chemical industries. It's using HPC and quantum computers.

Multiverse Computing (2019, Spain, 24M€) develops quantum and quantum-inspired software for various markets, starting with financial services, with portfolio optimization, risk analysis, market simulation and fraud detection.

They announced in August 2021 their Singularity Spreadsheet app solution which gives access to some portfolio optimization algorithm running on D-Wave annealers in the cloud, directly from within Microsoft Excel (video). It is now part of their Singularity SDK for Portfolio Optimization. They have then expanded their reach to the mobility, energy, and manufacturing verticals. They also use more traditional techniques based on machine learning, digital annealing (with Fujitsu) and quantum inspired solutions using tensor networks.

They published several papers in 2022 on combinatorial problem solving using quantum annealing with ZF in Germany[2110], on artificial vision using both gate-based and quantum annealers with the research institute Ikerlan Technology Center in Basque country, Spain, showing qualitative improvements vs classical machine learning method[2111], on a quantum-inspired tensor neural network to solve partial differential equations, in partnership with CACIB (French investment bank)[2112], and on portfolio optimization with Ally and Protiviti on D-Wave annealers[2113]., as well as with Bankia[2114]. This is a good practice and track record for a quantum software vendor.

[2110] See Multi-disk clutch optimization using quantum annealing by John D. Malcolm et al, August 2022 (11 pages).

[2111] See Quantum artificial vision for defect detection in manufacturing by Daniel Guijo et al, August 2022 (11 pages). They make a comparison with classical machine learning methods instead of deep learning convolutional neural networks, which may be misleading.

[2112] See Quantum-Inspired Tensor Neural Networks for Partial Differential Equations by Raj Patel et al, August 2022 (14 pages).

[2113] See Financial Index Tracking via Quantum Computing with Cardinality Constraints by Samuel Palmer et al, August 2022 (8 pages).

[2114] See Hybrid Quantum Investment Optimization with Minimal Holding Period by Samuel Mugel et al, December 2021 (6 pages).

Their Fair Price quantum solution computes accurate fair prices for financial institutions and seems to run on IonQ quantum processors[2115]. The solution is leased as a cloud service for 100K€ to 200K€ a year.

The company is partnering with Xanadu, Microsoft, Fujitsu, IBM, Rigetti, DWave, NTT, Strangeworks, Pasqal (France), IQM (Finland), Objectivity IT (UK, an IT services company), among others. They have several offices outside Spain in Toronto (Canada, with one of their cofounders), Munich (Germany) and Paris (France) with about 55 people as of August 2022. The EIC (European Innovation Council) provided them with 12,5M€ comprising a mix of grant and venture funding. They have 22 patents pending in quantum computing algorithms.

NetraMark (2016, Canada) develops quantum software solutions for the pharmaceutical industry to define therapeutic targets. They are part of the Quantum Machine Learning program at the Creative Destruction Lab in Toronto. It was acquired by the brain biotech **Nurosene Health** (2019, Canada) in October 2021.

Novarion (2016, Austria) is a server storage and GPU server vendor who wants to create the first hybrid quantum computer by 2025, without mentioning what sort of quantum processor it will integrate.

In October 2020, they started a partnership with **Terra Quantum AG** (Switzerland) to create a Joint Venture to create '<Qa|aS> by QMware'. It supports machine learning and big data analytics. QMware's customers will be able to develop and effectively run completely Hybrid Quantum Applications. Applications built on QMware's Hybrid Quantum Cloud are supposed to run on upcoming native quantum processors when they show up. Meanwhile, it runs on some classical emulators, seemingly a QLM from Atos. And it's Gaia-X and GDPR compatible.

Nordic Quantum Computing Group (NQCG) (2000, Norway) does R&D in areas at the crossroads between AI and quantum computing. They are creating a platform agnostic quantum software using superconducting and photonic qubits.

ODE L3C (2018, USA) is an American NGO involved in the creation of chemical simulation algorithms. Its ambition is to solve "difficult NP" problems with quantum computation, which is far from obvious.

This sounds more like a service provider than a software publisher. The company was created by a certain Keeper Layne Sharkey.

Opacity (2020, Australia) offers Quiver, a quantum code optimization software compatible with IBM's Qiskit.

Their hardware-agnostic solution maps processor errors at the global and individual qubit level, including parasitic interactions between qubits. It then allows the code to be optimized to take into account this duly mapped noise. The tool seems to be dedicated to developers as well as to quantum computers designers.

OTI Lumionics (2011, Canada, $5.7M) is specialized in the design of new materials and in particular LEDs and OLEDs. They have developed quantum and quantum-inspired molecular simulation algorithms for this purpose.

[2115] See Quantum portfolio value forecasting by Cristina Sanz-Fernandez et al, November 2021 (9 pages).

In particular, this allows them to predict the properties of the created materials like their color when being excited[2116], model chemical relationships and determine geometric structures. They are partners of Microsoft Azure (video).

ParityQC (2020, Austria) is a spin-off of the University of Innsbruck created by Wolfgang Lechner and Magdalena Hauser, the first being the scientist and the second, handling business aspects of the venture[2117].

By September 2022, the company had about 25 employees plus 15 researchers working at the University of Innsbruck. As architects, they connect the dots between hardware and software.

They develop software solutions to solve optimization problems (CADD, N-body problems, constraint problems) adapted to digital and analog quantum computers (qubits with universal gates or quantum simulators[2118]). Their ParityOS software suite optimizes the software parameters of the solution as well as those of the hardware control.

They support an architecture called LHZ, created by Wolfgang Lechner and Austrian colleagues Philipp Hauke and Peter Zoller, which is compatible with different hardware quantum platforms with 2D qubit connectivity architectures[2119].

Its principle consists in encoding a problem requiring n-to-n relations between qubits (all to all) to run it on a physical architecture where qubits are only connected to their closest neighbors as is the case in most quantum computers, except for some that rely on trapped ions. Their solution also includes an in-house error correction system[2120]. They are partnering with **Pasqal** whose cold atom-based architecture seems adapted to their model.

They announced in 2021 a partnership with **NEC** to help them with their superconducting qubits.

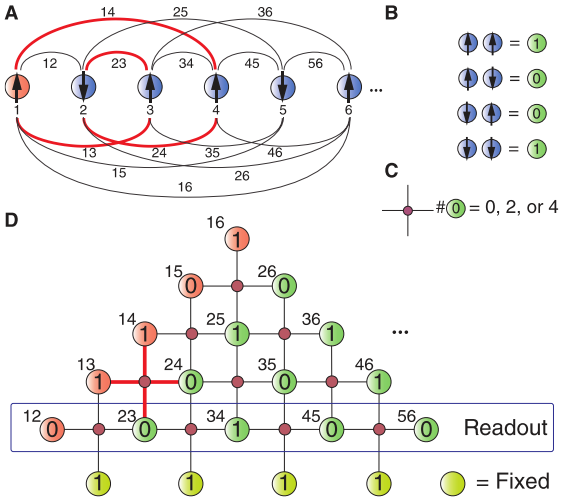


Figure 690: LHZ architecture. Source: A quantum annealing architecture with all-to-all connectivity from local interactions by Wolfgang Lechner, Philipp Hauke and Peter Zoller, October 2015 (5 pages).

Phase Space Computing (2017, Sweden) is a spin-off from the University of Linköping that develops training solutions on quantum computing for secondary and higher education.

[2116] See Estimating Phosphorescent Emission Energies in Ir(III) Complexes using Large-Scale Quantum Computing Simulations by Scott N. Genin et al, October 2021 (32 pages). It is based on using a 72 logical qubits classical emulator.

[2117] She is a family relative of Hermann Hauser, the co-founder of Arm, now a serial entrepreneur and investor in deep techs, including Graphcore (UK). He is also a member of the EIC Council.

[2118] Like in Rydberg blockade based parity quantum optimization by Martin Lanthaler, Clemens Dlaska, Kilian Ender, Wolfgang Lechner, October 2022 (10 pages) which describes a solution to quantum optimization problems using MWIS and UDG on quantum simulators using neutral atoms.

[2119] This LHZ architecture is documented in A quantum annealing architecture with all-to-all connectivity from local interactions by Wolfgang Lechner, Philipp Hauke and Peter Zoller, October 2015 (5 pages) for universal gated qubit platforms which they perfected in Universal Parity Quantum Computing by Michael Fellner, Anette Messinger, Kilian Ender and Wolfgang Lechner, May 2022 (6 pages). See also Rapid counter-diabatic sweeps in lattice gauge adiabatic quantum computing by Andreas Hartmann and Wolfgang Lechner, September 2019 (11 pages) for quantum annealing computing. See also Quantum Approximate Optimization with Parallelizable Gates by Wolfgang Lechner, 2018 (5 pages) which describes the implementation of a QAOA optimization algorithm with CNOT and unit gates.

[2120] See Error correction for encoded quantum annealing by Fernando Pastawski and John Preskill, 2015 (4 pages).

PhaseCraft (2018, UK, $1M) is a quantum software company spun out of University College London and the University of Bristol by Toby Cubitt, Ashley Montanaro and John Morton (also a cofounder of Quantum Motion). They plan to exploit quantum computing to create better energy collection and storage systems (batteries, solar PV, ...).

They launched in 2022 a partnership with Oxford PV, a perovskite photovoltaic panel company, to improve PV efficiencies thanks to quantum computer-based simulations.

Their researchers developed an optimized version of an algorithm solving the Fermi-Hubbard model with fewer resources which could be helpful to create high-temperature superconducting materials[2121]. In 2021, they also published a proposal for how to simulate a "kagome magnet". While it did not show any quantum advantage on existing quantum hardware and worked only with 20 qubits, it extrapolated that with 50 qubits, the problem could be solved by 200 two-qubit gates, something high-fidelities NISQ qubit system could achieve in the near future[2122].

PiDust (2019, Greece) is a startup launched by Vasilis Armaos, Paraskevas Deligiannis and Dimitris Badounas, who are alumni of University of Cambridge, Stanford and the University of Patras. They develop quantum algorithms in chemistry.

Pine.ly (2019, Canada) is positioned on software to assist in the creation of innovative materials with quantum computing. They aim in particular at the recycling of CO^2 emissions. The startup was created by three women, Nayer Hatefi, Shabnam Safaei and Rachelle Choueiri, all three scientists.

POLARISqb (2020, USA, $2M) is a startup that wants to use quantum computing to create new therapies. One more! It built the Tachyon platform.

But what kind of quantum computer and tools are used in Tachyon is a mystery. The startup was founded by Shahar Keinan (CEO) and Bill Shipman (CTO). They are partnering with Fujitsu, probably to use their conventional supercomputers and their digital annealing computer. Their idea is to use personalized medicine techniques to create ad-hoc therapies. Shahar Keinan received a PhD in chemistry from the Hebrew University of Jerusalem. She specializes in computational chemistry. In August 2022, they worked with **Auransa** to identify interesting target proteins for curing specific breast cancers using Tachyon and Auransa's SMarTR Engine based on classical AI.

Allosteric Bioscience (2021, USA, $920K) is a company integrating quantum computing and AI with biomedical sciences to create improved treatments for aging and longevity. In February 2022, the company announced it was teaming up with and investing in Polaris Quantum Biotech (Polarisdb). They first work on creating an inhibitor of a key protein involved in aging.

ProteinQure (2017, Canada) is a Toronto-based startup that uses various technologies including quantum computing to create and simulate new "*in silico*" therapies. They use quantum algorithms to simulate protein folding.

They are also developing hybrid algorithms also using GPUs. They support different hardware architectures including D-Wave computers.

[2121] See Strategies for solving the Fermi-Hubbard model on near-term quantum computers by Chris Cade, November 2020 (27 pages) which turned into Observing ground-state properties of the Fermi-Hubbard model using a scalable algorithm on a quantum computer by Stasja Stanisic, Jan Lukas Bosse, Filippo Maria Gambetta, Raul A. Santos, Wojciech Mruczkiewicz, Thomas E. O'Brien, Eric Ostby and Ashley Montanaro, Nature Communications, October 2022 (11 pages).

[2122] See Probing ground state properties of the kagome antiferromagnetic Heisenberg model using the Variational Quantum Eigensolver by Jan Lukas Bosse and Ashley Montanaro, October 2021 (12 pages).

In their experiments, they manage to simulate molecules with 6 atoms in universal quantum computers and reach 11 atoms with D-Wave. In practice, however, it would seem that they have put quantum computing on the backburner and are now focused on classical learning machines in the meantime.

Q1t (2018, Netherlands) creates mathematical models and software for classical and quantum computers in the field of quantum chemistry, quantum optics and financial analysis. They have tried these algorithms on quantum simulators and quantum optics.

They developed the q1tsim quantum simulation library published on Github which implements new quantum gates types for creating simpler circuits, the ability to simulate measurements without affecting qubit quantum states and the option to re-run a circuit starting with the previous quantum state for debugging purpose.

QbitLogic (2014, USA, $1.5M) is another startup that develops quantum machine learning applications, without more precision in their communication. They also develop an AI based system, CodeAI, to debug software.

Qbraid (2020, USA) provides a quantum online coding platform. Based in Chicago, the company was created by Kanav Setia who has a PhD from Dartmouth College in quantum simulation and worked with IBM research.

The platform supports the most popular programming frameworks (Qiskit, TensorFlow Quantum, Q#, Xanadu PennyLane, Braket, IonQ, Rigetti pyQuil, D-Wave...) and contains a transpiler that optimized the quantum code for the target hardware platforms. Access to IBM quantum computers seems embedded in the software solution which targets students. The company also developed quantum programming courseware.

Quantum Computing Inc aka QCi (2018, USA, $7,5M) is a quantum software, hardware consulting company that started with the creation of Qatalyst, a high-level software development and cloud provisioning tool.

It's mainly enabling developers to solve constrained optimization problems (QAOA, QUBO, graph optimization) with either gate-based accelerators, quantum annealers or classical computers. It's based on using six simple high-level APIs. It is commercially available. They support their home QikStart Program, a marketing initiative to accelerate real-world use cases with their customers. Qatalyst supports D-Wave, IonQ and Rigetti accelerators through Amazon's Braket cloud services. In March 2021, the company hired a "Chief Revenue Officer" (Dave Morris) and a Marketing VP (Rebel Brown) after having announced in December 2020 that they were filing for a Nasdaq IPO.

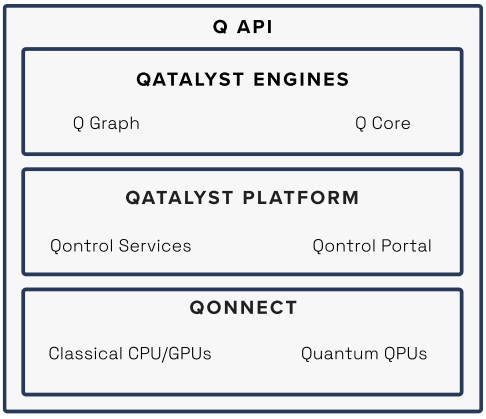


Figure 691: QCi software platform.

In July 2021, it became the first publicly traded pure player quantum computing company. QCi also created QUBT University in August 2021, an online initiative to train students on their Qatalyst tool. It's also a tactic to partner with academic institutions, like Notre Dame University in Indiana. They also have QCi Qonsulting practice, implementing their Path2Quantum (P2Q) methodology, a four-phase framework to planning quantum computing deployments.

In March 2022, QCi announced a partnership looking like an acquisition of a stealth company, QPhoton (2020, USA) from New Jersey and created by Yuping Huang (also assistant professor at the Center for Quantum Science and Engineering at Stevens Institute of Technology), and which develops some sort of photonic quantum computer of unspecified nature.

QCI with hook this system with its Qatalyst software. QPhoton was funded by various US federal agencies (DARPA, NSF, NASA, DoD). QCI launched in September 2022 its Dirac 1 Entropy Quantum Computer (EQC) cloud-based subscription based on Qphoton's technology.

In June 2022, QCi announced QAMplify, a solution supposedly increasing the processing power of quantum computers by x20. Of course, it deserves some scrutiny. Their patented process is supposed to increase the number of variables that can be handled in quantum hardware by a factor x5 for gate-based and x20 for quantum annealing. How they are doing this is not yet documented.

Q-CTRL (2017, Australia, $70.8M) is a startup created by Michael Biercuk of the University of Sydney. They develop a set of enabling software tools to improve the operations and programming of quantum computers.

Their Boulder Opal is quantum control infrastructure software working at the firmware level. It leverages machine learning to improve qubits control pulses and optimize quantum error correction codes. It is a Python toolkit used by quantum computers designers that works with IBM Qiskit, Rigetti and with Quantum Machines pulse generators. They implement error-correction techniques that increases the likelihood of quantum computing algorithm success between 1000x and 9000x on quantum hardware, as measured using the QED-C algorithmic benchmarks, but probably with a very low number of logical qubits. These impressive numbers relate to the impact of optimized quantum error correction.

They are relying on Google Cloud and TensorFlow to run the classical machine learning algorithms of their solution[2123]. Fire Opal is a set developer tools for quantum algorithm designers while Black Opal is an educational tool for students new to quantum programming.

In May 2022, Q-CTLR combined a 5-qubit QEC code (using 9 qubits, due to the additional helper qubits) with Fire Opal and could improve the code's ability to correctly identify errors by 70% on IBM QPUs (meaning: one qubit error detection rate was improved by 70%)[2124].

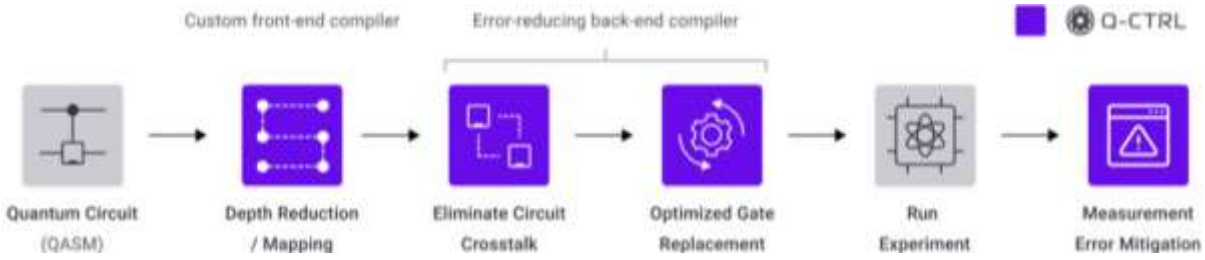


Figure 692: Q-CTRL error reduction techniques. Source: Q-CTRL.

They also work on optimizing quantum sensing solutions and are creating quantum sensors of their own for acceleration, gravity and magnetic fields measurement in space applications. They are partnering with the Australian company **Advanced Navigation**, which specializes in geopositioning. At last, they are also creating prototype algorithms for buses dynamic scheduling of buses in Sidney, Australia (*disclaimer: it can't be operational given the power of existing quantum computers*).

QC Ware (2014, USA, $39.7M) develops a platform for cloud-based quantum software development. They create quantum algorithms and software for large companies with two layers: their proprietary Forge platform and open source libraries for optimization, chemical simulation and machine learning.

[2123] See Boosting quantum computer hardware performance with TensorFlow by Michael J. Biercuk, Harry Slatyer, and Michael Hush, October 2020.

[2124] Fire Opal's process is documented in Experimental benchmarking of an automated deterministic error suppression workflow for quantum algorithms by Pranav S. Mundada, Michael J. Biercuk, Yuval Baum et al, September 2022 (16 pages).

They provide tools to load training data from learning machine models into memory more quickly. They have also developed an algorithm for calculating the distance between objects, which can be used to train both supervised (classification) and unsupervised (clustering) machine learning models. Their first customers include **Equinor** for oil exploration optimization, Japan's **AISIN** for certification testing of automatic gearbox software, **Airbus** for aircraft flight envelope optimization and **BMW** for autonomous vehicle route optimization. They are also targeting financial markets as well. It supports universal gate quantum computers (IBM, Rigetti), D-Wave quantum annealing computers and software emulators (IBM, Google, Microsoft, Rigetti).

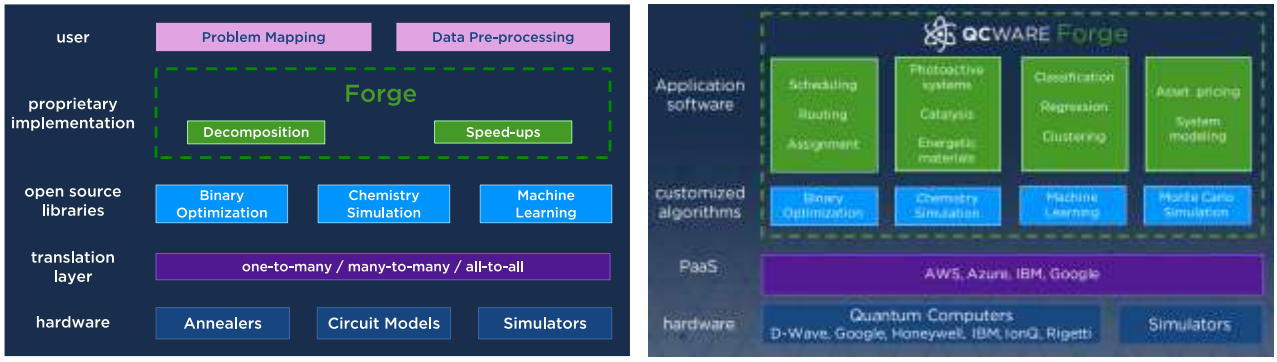


Figure 693: QC-ware software platform. Source: Enterprise Solutions for Quantum Computing by Yianni Gamvros, December 2019 (25 slides).

Airbus Ventures is one of their investors on top of the Koch group. They have received a $1M US public funding via the NSF in 2017. The startup, which already includes over 20 people, was created by Matt Johnson, who has a financial background, and Kin-Joe Sham and Randy Correll, who seem to have gotten late into quantum computing. The team also includes Iordanis Kerenidis, who is based in France and is a leading specialist in quantum machine learning. He oversees international algorithms development. Scott Aaronson is their Chief Scientific Advisor. Finally, the startup organizes an annual conference on quantum computing, the **Q2B**, the last edition of which was held in December 2020 online[2125].

QEDma Quantum Computing (2020, Israel) is a quantum software company created by Dorit Aharonov of the Hebrew University, Nathaniel Lindner of the Technion and Asif Sinai. It creates quantum algorithms and software tools.

Qindom Inc. (2018, Canada, $2M) is a startup developing quantum machine learning (QML) software running on D-Wave quantum annealers.

Qoherent (2019, Canada, $173K) is developing machine-learning based RF signals analysis tools that helps create adaptive RF communications and sensing systems in the Software-Defined Radio (SDR) realm. They analyze signals in the telecom ranges (4G, 5G, V2X, Satellite communications...). The company is investigating the usage of quantum machine learning techniques to improve its solutions.

Qrithm (2018, USA) develops quantum algorithms in diverse and rather disparate fields: machine learning, materials science, cryptography and finance.

Qu&co (2017, The Netherlands) was created by Benno Broer and Vincent Elfving, both quantum physicists who worked at TU Delft.

[2125] View presentation materials and videos from the 2019 Q2B conference, in December 2019.

They develop tailor-made quantum software solutions for large companies, accompanied by benchmark tools, particularly for chemical simulation applications based on DFT. They develop solutions for simulating fluid mechanics with nonlinear differential equations solved with VQE algorithms (hybrid variational quantum eigensolvers). They even solve Navier-Stokes 1D equations. They partner with IBM, Microsoft and Schrodinger (USA).

In March 2021, they launched a beta release of QUBEC, a chemistry and materials science toolkit. It comprises Q-time, a tool estimating when quantum advantage can be expected for solving chemistry or materials problems. QUBEC workflow manager supports quantum systems from IBM, IonQ and Rigetti. It is available through the IBM Quantum Experience and Amazon Braket platforms. LG Electronics is one of their customers.

In August 2021, they announced a new funding round with Quantonation, Runa Capital and SPInvest, with an undisclosed amount and in January 2022, the company merged with Pasqal (France). Benno Broer is now the CCO of Pasqal (Chief Customer Officer).

QUANSCIENT

Quanscient (2021, Finland) was created by Alexandre Halbach, Asser Lähdemäki, Valtteri Lahtinen and Juha Riippi.

It provides Quantum Simulation-as-a-Service (QSaaS) software. Its multiphysics simulation algorithms use finite element method and partial differential equations solvers.

They say hint about using hybrid classical/quantum computing but given the state of the art of quantum computers, it's probably wholly made of classical computing. They help simulate physics in the electromagnetism, mechanics and fluid dynamics fields.

QuantFi

QuantFi (2019, France/USA) is a young startup specializing in the creation of quantum software solutions for finance.

It was created by Paul Hiriart (French, ex of Lehman Securities, who left the startup early in 2021), Kevin Callaghan (coming from the New York financial sector) and Gabrielle Celani (on sales and marketing). They are creating goals-based investment optimization algorithms, and also handle trends detection, derivatives pricing and risk management. In 2020, they joined the IBM Quantum network.

Quanterro Labs (2019, Abu Dhabi) is an association of researchers and entrepreneurs created by Kaisar Parvez and Ram Soorat and AiFi Technologies, an AI software startup, working in quantum information and security. They work on middleware and software development for D-Wave, Google, IBM and others. It's mostly a consulting services company.

QUANTICA COMPUTACAO

Quantica Computacao (2019, India) is the first Indian quantum startup and a software company working on creating a cloud development environment an QML algorithms. It's incubated in the Indian Institute of Technology Madras from Chennai.

QUANTOPTICON

Quantopticon (2017, UK) develops the Quantillion modeling and simulation software for the design of photonic components for quantum communication and computing applications. It is a tool for the design of new materials.

The company was created by a mother-daughter duo: Mirella Koleva (CEO) and Gaby Slavcheva (CSO). Their first customers are Quandela, QuiX and Toshiba.

quantum benchmark

Quantum Benchmark Inc (2017, Canada) provides an error-correcting code software solution for general-purpose quantum computers and error evaluation. It was thus apparently a competitor to Q-Ctrl.

They also offer a quantum computer performance validation system. The package is integrated into the True-Q suite, launched in 2018, with True-Q Design, which is used to evaluate the error rate of a quantum computer and to optimize its architecture, and True-Q OS, which helps optimize the accuracy of software solutions.

The target market is initially the manufacturers of quantum computers and those who evaluate them. Eventually, it will be that of user customers. Note that they have already tested Google's Cirq framework, having been part of Google's beta test program for this language, and that Google is using their solution, as it did in its 2019 supremacy experiment. They are also partnering with IBM (since 2018, on error characterization, mitigation, correction, and performance validation) as well as with Fujitsu Labs (since 2020, to develop quantum algorithms). The company was acquired by **Keysight Technologies** in May 2021, on top of Labber Quantum in 2020. Among its key people are Joseph Emerson (CEO), Joel Wallman (CTO) and Daniel Gottesman (Senior Scientist, specialized in error correction, MIT), Stefanie Beale and Kristine Boone (both researchers).

Quantum Flytrap (2020, Poland) is a quantum computing and cryptography software company. They created a real time browser-based emulator using photonic elements instead of quantum gates[2126]. They are behind the "Quantum Lab" that is being used at Stanford University and the University of Oxford.

Quantum-South (2019, Uruguay) is a spin-off from the University of Montevideo who is specialized in developing quantum optimization software, first targeting the cargo shipments in ships and airlines. The software was released in 2022.

They also target the financial sector which may be more dynamic although more crowded with many existing quantum software startups. In cargo shipments, they are partnering with Quantum Brilliance (Australia) with their prototype (5) NV centers qubits.

QBaltic (2019, Estonia) develops algorithms for quantum computing, quantum cryptography and artificial intelligence. QBaltic is a contract research spin-off from the University of Latvia, University of Tartu in Estonia and QuBalt, Germany and Latvia.

Qsimulate (2018, USA, $1.5M) develops quantum solutions for molecular simulation for healthcare and chemistry. They are partners of Amazon Braket and Google and are already working with Amgen. The company was co-founded by Toru Shiozaki and Garnet Chan, both specialized in chemistry.

Quacoon (2020, USA) is a small startup created by Tina Sebastian and Barbara Dunn that develops software solutions for the food supply chains combining AI and quantum annealing.

Quantum Thought (2019, USA) develops quantum or quantum inspired algorithms for chemical, AI and security markets. According to their website, it seems to be mainly a service company operating in project mode and doing consulting services. Their CEO is Rebecca Krauthamer.

Quantumz.io (2019, Poland) develops the Quantum Simulator Platform (QSP), a quantum program emulation solution running with GPUs. They are also developing a PQC (post-quantum cryptography) solution called banax, including some dedicated hardware to implement it.

Quantagonia (2021, Germany) is a quantum software company. Their Quantum Virtual Platform is a hybrid classical/quantum computing platform (gate-based and quantum-annealing based). It was created by Dirk Zechiel (CEO), Sabina Jeschke, Sebastian Pokutta and Philipp Hannemann.

[2126] See Visualizing quantum mechanics in an interactive simulation -- Virtual Lab by Quantum Flytrap by Piotr Migdał et al, May 2022 (29 pages).

Quantastica (2019, headquarter in Finland with offices in Estonia and Serbia) develops hybrid quantum algorithm software tools including Quantum Programming Studio, a graphical web development environment for creating quantum algorithms executable on quantum computers or simulators, including a classical simulator they have developed themselves.

Quantistry (2018, Germany) created a cloud-based simulation platform for material research and development, using quantum simulations, molecular dynamics and machine learning.

Quantum Mads (2020, Spain) was created in Bilbao by Eriz Zárate and Alain Mateo Armas and is positioned in the financial market. It offers four software tools with a mix of quantitative/classical/hybrid/quantum-inspired software.

With Q-MADS, an investment strategy analysis framework for traders, Q-RETAIL, a framework for retail banks, Q-ALLOCATE, for asset allocation optimization and Q-CRYPTO, a framework for optimal path finding in graphs. The whole is based on the HHL linear algebra algorithm.

Quantopo LLC (2017, USA) is a company specialized in machine learning algorithms. They focus on biotechs, supply chain and logistics. They are part of the Creative Destruction Lab in Canada. But as they don't have an active website, it is not certain that they still exist.

Quantum Open Source Foundation got a $4K grant from Unitary Fund. It publishes a list of quantum open source projects on Github, with various software development tools and libraries for gate-based quantum as well as and quantum annealing computing.

It's a repository of existing open source projects including IBM Qiskit and PennyLane from Xanadu. NISQ. Provides financial funding for quantum open source software projects. Organize events. More a community than a foundation like the Apache or Mozilla foundations.

QuantyCat (2020, USA) creates cloud-based APIs for quantum software development, supporting D-Wave, IonQ and Rigetti through Amazon Braket.

Qubit Engineering (2018, USA) was founded by University of Tennessee alumni. They develop classical and quantum optimization algorithms suitable for wind turbine design and location optimization. Another very niche market. They are partners of Microsoft Azure.

Qubitera (2018, USA) develops solutions combining AI and quantum.

Qubitl Quantum Technologies (2018, India) is a contract research laboratory developing quantum machine learning software. They were initially specialized in cybersecurity, having created a QRNG solution (Q-RandCon), a PQC protected healthcare solution (HealthCetra) and a Quantum Differential Phase Shift technology for QKD (Q-Shift).

Qubit Pharmaceuticals (2020, France/USA, $16.1M) is a startup co-founded by Jean-Philip Piquemal, a CNRS professor-researcher at Sorbonne University, a long-time specialist in molecular dynamics simulation that mathematically models the quantum mechanics of organic molecules.

The co-founders of the startup are based in Austin and at Washington University in Saint Louis. Its algorithms have been in use for a long time. Jean-Philip Piquemal is the co-author of the Tinker molecular simulation library and its Tinker-HP version adapted to supercomputers. It exploits massively parallel CPU-based systems and Nvidia GPU tensors, all with high-precision computation. In particular, it uses the Jean Zay computer from GENCI in Orsay, France, as well as those from the DoE in the USA. In this context, they have been involved in molecule screening for the search for covid-19 treatments by therapeutic retargeting. Re-targeting is easier to simulate than the 3D structure of the whole covid-19 which is more than 200,000 atoms or the simulation of protein folding.

What about quantum computing in all this? It could be used to define optimized parameters for classical simulation, in short, within the framework of hybrid algorithms. They will also be able to exploit quantum simulators in the future, such as those being developed with cold atoms at Pasqal[2127].

Jean-Philip Piquemal's laboratory at Sorbonne University has received a €9M ERC for the development of simulation solutions for organic systems of several million atoms[2128]. They finally welcomed the investment fund Quantonation in their capital in June 2020[2129].

QbitSoft (2022, France) is a new software and service vendor targeting in priority the retail and logistics market. It was created by Olivier Pegeon, a former business executive from IBM France.

QuDot (2018, USA) develops software for the simulation of quantum circuits on traditional computers, the QuDot Net. They use techniques based on Bayesian networks to optimize the in-memory representation of qubits.

QunaSys (2018, Japan, $12.8M) also develops quantum algorithms in chemistry and healthcare. From the universities of Tokyo, Osaka and Kyoto, they also maintain the Qulacs simulator developed at Kyoto University.

It was followed in 2021 by Qamuy, a quantum cloud platform. They also created in 2020 the Japanese consortium QPARC with 50 participating companies investigating various use cases of quantum computing. The company is also participating to the **Pistoia Alliance**.

QuSoft (2014, The Netherlands) is a spin-off from TU Delft University specializing in quantum algorithms and software. Like its sister company QuTech, it is more a private applied research laboratory than a startup.

QxBranch (2014, USA, $8.5M) was created by former Lockheed Martin employees. It offers solutions, probably tailor-made, for the financial, insurance, aerospace and cyber security markets.

Based in Washington DC, they already have offices in Hong Kong, London and Adelaide, Australia. They are partners of D-Wave and IBM. The startup was acquired by Rigetti (USA) in July 2019.

Rahko (2018, UK, £1.3M) is a quantum machine learning and chemical simulation software development company based in London. It was founded by Leonard Wossnig. They are among the first Amazon AWS partners for the use of quantum resources in the cloud, and the first in Europe.

In May 2020, they announced that they would work with Merck on "quantum inspired" algorithms, i.e. on conventional computers.

[2127] See the presentation Computational Drug Design & Molecular Dynamics: an HPC perspective by Jean-Philip Piquemal, April 2020 (28 slides).

[2128] See Extreme-scale Mathematically-based Computational Chemistry (EMC2), 2020.

[2129] See Qubit Pharmaceuticals closes a pre-seed round with Quantonation, Quantonation, June 2020.

In 2021, they announced that they were collaborating with Honeywell and achieved excellent accuracy executing a Discriminative Variational Quantum Eigensolver algorithm on Honeywell's H0 6-qubit trapped ion system. The company was acquired by **Odyssey Therapeutics** in January 2022, a company specialized in drug discovery in the fields of inflammatory diseases and cancers.

ReactiveQ (2018, Canada) develops quantum simulation algorithms for the design of innovative materials such as high-temperature superconductors, all on a NISQ quantum computer.

Riverlane (2016, UK, $24.1M) is a spin-off from the University of Cambridge that provides services in quantum computing and develops new algorithms combining machine learning and quantum in chemistry.

They develop with dividiti Ltd, a one man shop created by a certain Grigori Fursin, the Quantum Collective Knowledge, a benchmark SDK for quantum hardware and software.

They have also developed what they call a quantum operating system, Deltaflow.OS dedicated to NISQ systems and which optimizes access to hardware resources for qubit control. It was deployed in mid-2020 at several sites in the UK and in partnership with SeeQC and, later, CQC.

In July 2021, Riverlane created a consortium with **Astex Pharmaceuticals** and **Rigetti UK** to develop quantum drug discovery algorithms running on Rigetti platforms in the cloud. This is part of a 18-month feasibility study funded by a grant from UKRI as part of the UK quantum plan[2130]. Of course, you may wonder what they will do with the 31 qubits from Rigetti.

RQuanTech (2018, Switzerland) develops RTranscender, a quantum machine learning tool for finance, healthcare, automotive, seismology and cyber security. It supports Fourier transforms, qubit-based arithmetic operations which can help craft oracles (additions, multiplications, divisions, exponentials), factorization, discrete logs, etc.

Sanctuary (2021, Canada) is a startup created by Geordie Rose, the cofounder and first CTO of D-Wave.

It wants to implement reinforcement learning algorithms with quantum computing. At this point, the company is hiring a bunch of scientists and developers, with no offering yet looming.

SavantX (2015, USA) was created by Ed Heinbockel and David Ostby who in the past worked for the FBI, the Department of Defense and the US Intelligence Community including the DIA where they developed OSINT collection tools (open source intelligence, using unstructured data).

They core skills are data search, discovery, analysis and visualization. They plan to leverage quantum computing to identify hidden patterns in data and help optimize complex systems. One of their first realization in that domain was implemented for the Port of Los Angeles in 2020, to optimize cargo flow and container handling using D-Wave quantum annealers and classical machine learning. Their target markets are the nuclear, healthcare, utilities and defense industries.

Schrodinger (1990, USA, $193) is a digital drug design company, mainly using molecules screening and doing drugs retargeting.

It is an established competitor of Qubit Pharma (France). They work with Sanofi. The company is listed on the NASDAQ. They inevitably became interested in quantum computing and have started a partnership with Qu&Co to ramp-up their skills in quantum computing.

[2130] See Riverlane and Astex Pharmaceuticals join forces with Rigetti Computing to drive drug discovery forward by Amy Flower, July 2021.

Semicyber (2018, USA) develops algorithms in various fields: data analysis (non-quantum), quantum and others for critical applications for the USA defense sector, particularly the US Air Force.

So they are probably closer to the service company than to the product-oriented startup. The startup is co-founded and managed by Kayla Farrow, an engineer specializing in algorithm creation and signal processing.

Sigma-i Labs (2019, Japan, $3.7M) is a consulting company and private laboratory that grew out of the Tohoku University Quantum Annealing Computing Research Laboratory, based in Sendai and led by their CEO Masayuki Ozeki. They started by doing consulting around the creation of software for D-Wave's annealers, using their cloud Leap platform since 2019[2131].

SolidState.AI (2017, Canada) develops machine learning solutions for the industry covering yield improvement, production calibration and predictive maintenance.

All of this is based on hybrid classical/quantum algorithms. They work with Bosch, Applied Materials, Mercedes-Benz as well as with D-Wave, Rigetti, Microsoft and IBM Q, among others.

Spin Quantum Tech (2018, Colombia) develops quantum algorithms in the field of cybersecurity that combine AI and quantum. They seem to create PQC (post-quantum cryptography) that exploits new encryption algorithms. They are also working on chemical simulation, which has nothing to do with it.

SHYN (2016, Bulgaria) develops solutions for the visualization of data coming from quantum calculations. So, some quantum dataviz! With a use case consisting in detecting quantitative fake news. It was co-funded by Google's Digital News Information Fund dedicated to the press. This €150M fund distributed funding of a few 100K€ to more than 400 projects in Europe.

SoftwareQ (2017, Canada) offers development software for quantum computing including a compiler, simulator and optimizer. The company was co-founded by Michele Mosca (on top of evolution) and Vlad Gheorghiu of the Canadian Institute of Quantum Computing.

It is a startup from the Quantum Machine Learning program at Creative Destruction Lab in Toronto.

Strangeworks (2018, USA, $4M) develops quantum software. Like many colleagues, they target the aerospace, energy, finance and healthcare markets. They are at the origin of the creation of a Q&A site on quantum computing, Quantum Computing Stack Exchange. The company was founded by William Hurley aka whurley, and is based in Austin, Texas, with a staff of about 15.

In 2019, they launched a beta of their multi-platform development environment for quantum applications supporting quantum computers or emulators from Rigetti Computing (Forest), DWave (Leap), Microsoft (Q#), Google (Cirq), IBM (Qiskit) and ColdQuanta Hilbert gate-based cold atom QPU (as of late 2021).

This environment seems to facilitate collaborative work and sharing of results. In February 2021, it turned into an initiative to “humanize quantum computing”.

[2131] See Sigma-i and D-Wave Announce Largest-Ever Quantum Cloud-Access Contract | D-Wave Systems, July 2019.

It's based on Strangeworks QS (Quantum Syndicate) which consolidates quantum hardware vendors solutions and software tools, Strangeworks QC (Quantum Computing), a free quantum computing ecosystem to learn quantum code using common quantum programming languages and Strangeworks EQ (Enterprise Quantum), an enterprise infrastructure solution consolidating QC and QS with better security, IP protection, quantum machine access, resource aggregation, custom integrations, private deployments, project management and the likes. In January 2022, Strangeworks announced a partnership with **Entangled Networks** (Canada) to support their future Multi-QPU Computers Entangled Networks and the associated MultiQopt code compiler. This scale-out approach to quantum computers is of course to be first validated at the hardware level and with physical (optical) connections between several QPUs before becoming operational.

Stratum.ai (2018, Canada) develops a quantum software dedicated to a very specialized market, the optimization of mineral prospecting, particularly in gold.

Super.tech (2020, USA, $150K) is a startup launched by Pranav Gokhale, Fred Chong and Teague Tomesh that develops a software stack dedicated to the control of quantum computing systems ranging from a hundred to a thousand qubits.

The solution is the result of the NSF-funded Practical-Scale Quantum Computation (EPiQC) research project involving five Chicago-area and MIT universities and stars such as Peter Shor and Aram Harrow. It is creating a software infrastructure targeting the development of NISQ solutions. The company was acquired by ColdQuanta in May 2022.

Terra Quantum (2019, Switzerland, $85.8M) was cofounded by Markus Pflitsch (CEO) with, as recent hires, Valerii Vinokur (co-CTO) and Dr Florian Neukart (CPO). Their recent $75M funding helps them expand their R&D effort and also, their international expansion, with the opening of new offices in Munich and in the Silicon Valley.

It develops quantum software solutions in all possible quantum fields: quantum computing, quantum cryptography and quantum sensing. They modestly position themselves as being in a position to build the "*European quantum ecosystem*"[2132] and working on the "*development of revolutionary quantum computing applications*", with supporting the development of more efficient fertilizers, batteries and power grids. Their "Quantum Algorithms as a Service" is an algorithms library with the usual optimizations and QML pieces. The company then customizes it according to the needs of their customers making them a mixed product/services company. Then, their "Quantum Computing as a Service" provides access to its "*high performing logical qubits to equip them with real quantum advantages already today*".

In January 2022, Terra Quantum launched an alpha release of its QMware hybrid quantum cloud data center (QMware), in partnership with Novarion Systems (Austria, covered earlier in this section). Their HPC and quantum emulation workloads are powered by Intel Xeon Platinum CPUs and Nvidia A100 GPGPUs. Their CPU-GPU-QPU interconnect is based on CXL (Compute Express Link), a unified in memory communication open standard protocol created in 2019 by Intel for high-speed CPU-to-device and CPU-to-memory connections, designed for HPCs and built on the PCI Express (PCIe) interface. Their hybrid quantum computing approach is described in a white paper where they claim it outperforms classical approaches[2133].

[2132] See Terra Quantum secures EUR10m to build the European Quantum Ecosystem by James Dargan, April 2020. On 1st April, their CTO declared: "*We plan to implement a useful quantum algorithm on the IBM machine with 20 qubits in order to test quantum supremacy*". Well, 20 qubits for a quantum supremacy? It's fine if it's an April's fool.

[2133] See Practical Application-Specific Advantage through Hybrid Quantum Computing by Michael Perelshtein et al, 2021 (14 pages).

Their architecture is based on a memory-centric compute architecture that supports processing with QPUs, CPUs and GPUs as well as hybrid quantum computing with 12 TB of NVRAM shared by all systems. They also developed a unified information theoretical model for classical and quantum information that allows for efficient QPU emulation via a hardware agnostic intermediate representation of the quantum circuits. In 2022, they launched QUANTON-HGX2, a new generation of servers with Nvidia GPGPU and AMD EPYC CPUs.

Their last offering is a "Quantum Security as a Service" using a QKD solution, given the physical architecture and related hardware are not specified.

Tinubu Software (France) is a credit insurance software company that is investigating the usage of quantum computing to extend its offering to improve prediction on time series. They had participated to the ClassiQ 2022 quantum computing coding challenge and were the bronze winners with Thomas Frossard, Ayoub El Qadi, Quoc Viet Nguyen and Marcelin Gallezot.

Tokyo Quantum Computing (2017, Tokyo) wants to develop quantum annealing computer simulation software like many of the software startups from Japan.

Tradeteq (2016, UK, $6.3M) is a financial trading platform that uses AI for risk assessment and portfolio optimization. Their ambition is to use quantum computing to develop their own quantum tools.

In April 2020, they announced that they would work in this direction with the Singapore Management University (SMU) and with quantum neural network algorithms.

Turing (2016, USA) is a company created by Seth Llyod and Michele Reilly that wants to solve key societal problems with hybrid classical-NISQ software solutions using AI and quantum machine learning techniques. Seth Lloyd is a famous prolific quantum scientist in quantum computing and Michele Reilly has been working on qRAM.

Unitary Fund (international) is a kind of equivalent of the Mozilla Foundation for quantum technologies. It's a non-profit organization creating open source quantum libraries, tools, hardware and content[2134].

They fund through a microgrant program ($4K) developers. They sponsored about 20 projects including the error mitigation framework mitiq[2135], Qrack (emulator accelerator on GPUs), OLSQ (Optimal Layout Synthesizer for Quantum Computing, a pre-compiler optimizer reducing the SWAP gates count), a quantum machine training textbook and Pulser, developed by Pasqal. They partner with Rigetti and IBM.

Xofia (2019, USA) develops software solutions based on quantum machine learning for classification. They want to distribute their software in open source. They exploit Atos' 40 qubit quantum emulator, a QLM server, sitting in the cloud.

Zapata Computing (2017, USA, $67.4M) is a quantum software and services company founded by Harvard researchers including Christopher Savoie and Alán Aspuru-Guzik from the University of Toronto who has developed many founding algorithms in chemistry quantum applications.

[2134] See their 2021 Annual Report, Unitary Fund (23 pages).

[2135] See Mitiq: A software package for error mitigation on noisy quantum computers by Ryan LaRose, William J. Zeng et al, September 2020-August 2022 (33 pages).

Their partners include Google, Rigetti and IBM. Also, Bosch (Germany) is one of their corporate investors. Honeywell invested in the company in March 2020. The company established an office in the UK in June 2021.

They initially developed a complete quantum operating system serving as a hub between application algorithms and quantum accelerators of all types. In April 2020, this took the form of Orquestra, a platform for managing quantum application workflows with:

Building code using their Orquestra Studio. It offers a set of code libraries supporting Cirq (Google), Qiskit (IBM), PennyLane (Xanadu), PyQuil (Rigetti), Q# (Microsoft) as well as pyAQASM (Atos).

Orchestrate its deployment across multiple QPU and classical emulation platforms using Zapata Computing Quantum Workflow Language (ZQWL), which is YAML-compatible and supports various quantum hardware architectures (NISQ, quantum annealing) and classical computing (quantum emulators such as those from Atos, supercomputers, cloud servers) [2136]. Orquestra includes tools for managing batch computing. The Orquestra Data Correlation Service (ODCS) collects treatment data in a MongoDB database which is then exported as Excel tables, a Jupyter notebook or for the Table software.

Deploying the Orquestra runtime locally or on the cloud.

Orquestra was in beta in April 2020 as part of an Early Access Program and is released since 2021.

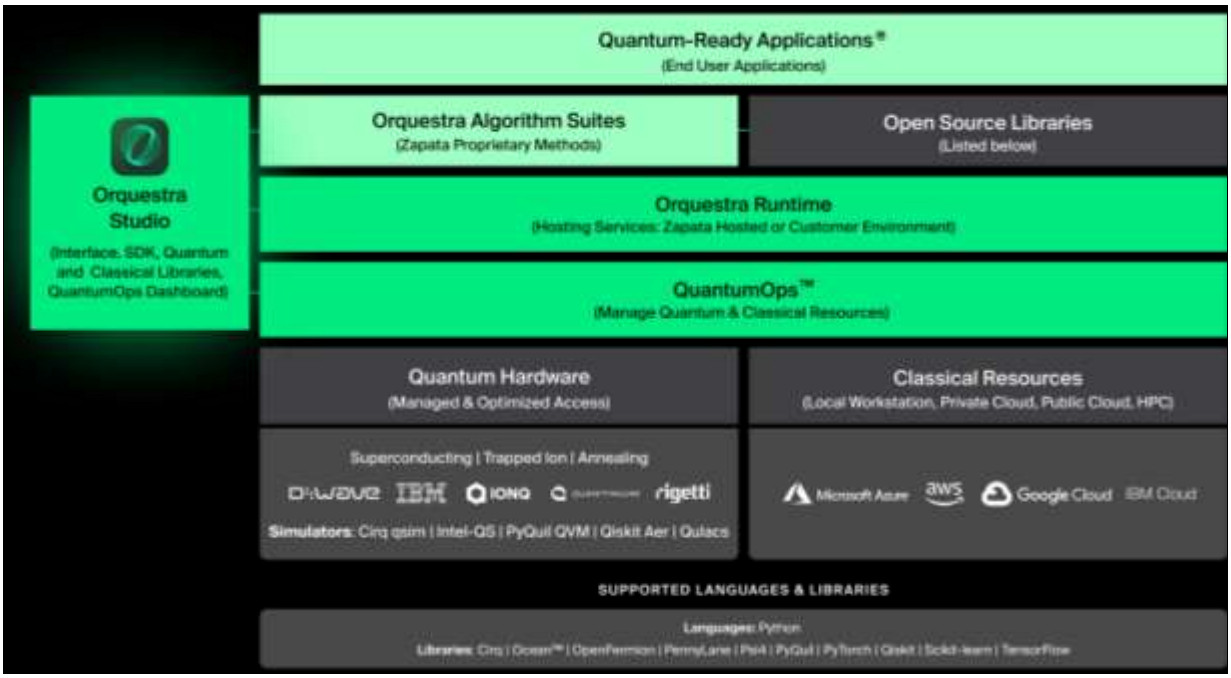


Figure 694: Zapata Computing Orquestra platform. Source : Zapata Computing.

Service vendors

On top of software vendors, the service vendors industry is getting structure to work with end-user customers and help them adopt quantum technologies, mostly focused on quantum computing.

Large IT service vendors like **Accenture**, **Capgemini** and **KPMG** have launched quantum technology practices, often partnering with hardware and software vendors. Accenture teams up with IonQ, Quantinuum, D-Wave and 1Qbit. KMPG is with Microsoft, selling “quantum inspired” projects. Capgemini created its Quantum Lab (Q-Lab) early in 2022, partnering with IBM and positioned in

[2136] YAML is a language that dates back to 2001. It is used to create configuration files. It is used in conjunction with Python.

Germany, Portugal and India. It covers all branches of quantum technologies (computing, telecommunications and cryptography, sensing) and focuses on life sciences, financial services, automotive and aerospace verticals[2137].

Here are a bunch of more specialized quantum services and consulting companies throughout the world: **Safe Quantum Inc** (2020, USA) sells PQC services, **D-fine** (2002, Germany), **Q&I** (UK) also called Qandi, **QuantGates** (UK), **Kvantify** (2022, Denmark), **Quantum Phi** (2018, Czech Republic). **RayCal** (UK) which is an analyst firm in quantum technologies, **Inside Quantum Technology** (2018, UK) created by Lawrence Gasman with the help of 3DR Holdings, **Qureca (**Spain) whose name means Quantum Resources & Careers and which does training, recruitment, business development and events, **Max Kelsen (**Australia), **Quantum Quants** (Netherlands). **SoftServe** (1993, Ukraine), **StrategicQC** (USA) is also specialized in recruiting talent in quantum technologies. **Quantum Computing Engineering** (USA) or QCE, provides generic consulting services on quantum computing. **Aspen Quantum Consulting** (USA) does due diligence investigation of startups for investors. **AmberFlux** (2013, India) provides quantum computing consulting services on top of existing machine learning and data science services. **QRDLab** does about the same, also in India. **Quemix** (2019, Japan) is an IT company specialized in providing quantum computing solutions. **QuRISK** (2021, France) does consulting on quantum computing originated risks on cybersecurity and also develops quantum algorithms and **Q. BPO Consulting** (2020, France) seems to be a generalist quantum computing consulting shop. At last, **Reply Data IT** (Italy) is a quantum computing service company that deployed its custom MegaQUBO solver in the cloud, first on classical computers, and supposedly on quantum computers.

Plantagenet Systems (2014, UK) is a consulting service shop run by Roberto Desimone who runs projects for various UK organizations including their Ministry of Defense, InnovateUK, the UK National QT program, the National Quantum Computing Centre (NQCC) and the UK Quantum Hubs.

Protiviti (USA) is a large 7000 people consulting company with a quantum practice focused like many other on the potential applications from quantum computing and on securing IT infrastructures against the potential related threats (so, PQC et al). They are partnering with Multiverse Computing.

Psi-Ontic (USA) is a quantum consulting created in Florida by Alan Martin, a management consultant coming from the automotive industry and with a physicist PhD. background. He works with large end-user customers as well as with investment funds and startups. He also creates market studies and quantum strategy assessments for various government organizations.

Quantum Computing Engineering Inc. (QCE) (2019, USA) is a company created by Gonzalo Florez Giraldo that does consulting for putting in place quantum computing solutions in most addressable markets (optimization, chemistry, healthcare, finance, machine learning). It also addresses cybersecurity and cryptography. The company is based in Houston, Texas. The company has no visible web site.

Q-iSIM (2016, Germany) aka "Quantum Interdisciplinary Simulations" develops quantum annealing software in physics simulation and fluids dynamics.

DN-Quantum Computing (2019, India) aka DishaNitish Technologies | Quantum Computing is a service company helping corporations develop quantum computing solutions, noticeably in chemistry and with transmon qubits.

QKrishi (2021, India) develops quantum models, algorithms and kernels for applications in automotive, finance, agriculture, seismology, signal processing and other areas.

[2137] See Capgemini, IBM Launch Quantum Lab to Promote Quantum Use Cases by Matt Swayne, The Quantum Insider, January 2022.

Silicofeller (2021, India) develops quantum solutions and advertises doing it in simulation, optimization and quantum machine learning which is fine, and then, crosses the line with mentioning the metaverse and Blockchain as application domains which are a bit farfetched.

Quanta-ly (2020, Libya) is preparing Libyan industries for the adoption of quantum products and services with training, consulting and advanced secure communications. No country, even in war, can escape quantum technologies!

Quanvia (2022, Spain) is a quantum consulting, service, research and training company targeting the usual suspect industries (retail, finance, logistics, energy, transport, automotive, pharmaceuticals, chemistry).

The company spun out of the University of the Basque Country, Bilbao, Spain. It is run by Enrique Solano (President, also cofounder of Kipu Quantum), Javier Mancilla Montero (Managing Partners), Dawoon Choi (Quantum Machine Learning Director) and Ariela Strimling (Quantum Computing Tech Lead). The team is spread in Spain, Chile and the USA. The Latin America expansion came from the acquisition of Nimoy Cognitive Computing, a data-science service shop.

Qubitech (2021, Greece) is a quantum consulting company cofounded by Alexis Askitopoulos (CSO). Not to be confused with QubitTech, a scam crypto trading company that "*uses quantum technology to generate a monthly ROI of 25% for its investors and a total of 250% in 10 months*".

QuGeeks (2022, Switzerland) is a jobs board and search company specialized in quantum technologies. Their outreach includes "The Quantum Hubs" newsletter and its related social network activity.

Quant-X Security & Coding (2019, Germany) is a quantum service company created by Xenia Bogomolec (CEO) and Peter Nonnenmann (Scientific Advisor and Analyst). They develop quantum algorithms for quantum annealing and gate based systems. They also integrate PQC for dynamic partner authentication in QKD networks.

Unitary Zero Space (2020, Finland) quantum consulting and training services company. Their services portfolio includes helping organization commercialize their own quantum technologies, educating customers on quantum technologies and cybersecurity expertise.

They packaged their training offering in a half-day quantum computing workshop format (that's quite short...). The company was created by Topias Uotila (quantum programming), Risto Hakala (cybersecurity) and Juha Muhonen (quantum physics).

Quantum computing business applications key takeaways

- Most quantum computing market forecasts are highly optimistic and plan for an early advent of scalable quantum computers. They also sometimes tweak forecasts with pushing business value numbers instead of an actual market for quantum technologies.
- There are interesting potential use cases of quantum computing in nearly every vertical market, particularly in energy, chemistry, healthcare, transportation and then finance.
- Most of them are theoretical or have been evaluated at a very low scale given the capacity of existing quantum computers. Some may be useful with advanced noisy computers (NISQ) while most of them will require highly scalable fault-tolerant quantum computing systems (LSQ/FTQC). Others may find their way on quantum simulators.
- In some cases, the potential use cases are in the overpromising twilight zone like simulating very complex molecules, fixing global warming, curing cancers or optimizing large fleets of autonomous vehicles. All these are dubious long-term promises.
- The main purveyor of case studies is D-Wave with its quantum annealer although it has not demonstrated yet a real quantum advantage. IBM is second there, having evangelized a broad number of customers and developers since 2016.
- Beyond computing time, a quantum advantage can also come from the system energetic footprint and/or the precision of the outcome.
- There are already many software vendors in the quantum computing space. How do they strive as there are no real functional quantum computers around yet? They sell pilot projects, develop software frameworks, build quantum hybrid algorithms and create quantum inspired algorithms running on classical hardware. On top of being funded by venture capital! We also cover in this book the burgeoning IT and consulting services in quantum technologies.

Unconventional computing

This part consolidates a set of technologies and companies that propose to significantly increase the computing power of computing machines while not relying on quantum technologies.

We will discuss supercomputing in general, and then cover a wealth of so-called **unconventional computing** paradigms like digital annealing, reversible and adiabatic classical computing, superconducting computing, probabilistic computing, photonics computing and chemical computing[2138].

Many of these avenues have been explored by major players such as IBM for superconducting components or by startups and with ups and downs. Some, such as MemComputing and InfinityQ, go so far as to tout exponential computing accelerations on more or less traditional architectures based on classic CMOS components. To the point of proving implicitly that P=NP in complexity theory, i.e. that the class of problems that can be solved in polynomial time with respect to their size is equal to the class of problems that can be verified in polynomial time. The consensus being that P<>NP, this is obviously questionable!

Unconventional computing paradigms differ in one way or another from Turing's machine-based technologies and Von Neumann's architecture based on control units, computing, registers and memory that are the basis of today's classic computers.

These do not all necessarily bring significant computing acceleration competing with quantum computing. This is particularly the case for the different domains that are part of **natural computing** that use physical elements from nature or are inspired by nature. This includes computers based on biological components like DNA, p-systems, chemical computers or membrane computers, spintronics and neuromorphic processors that are adapted to artificial intelligence processing[2139].

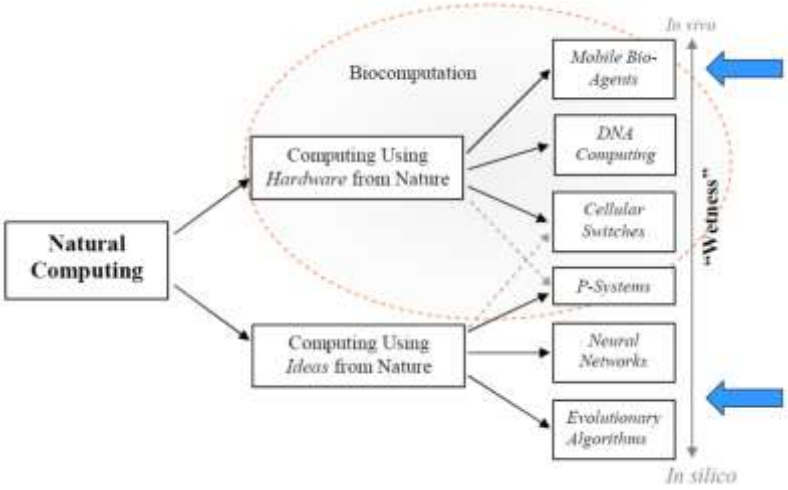


Figure 695: how biomimetics is used in computing. Source: Unconventional Computing: computation with networks biosimulation, and biological algorithms by Dan Nicolau, McGill University, 2019 (52 slides).

I won't cover here the special old case of analog computing made of analog electronics has been abandoned in favor of digital electronic systems due to their high flexibility and absence of noise. But for some respect, quantum computing is a return of the analog computing paradigms as we've seen.

Others, such as superconducting classical computing, could be useful to allow quantum computers to "scale". We can therefore also evaluate these different technologies from the point of view of their complementarity, rather than competition, with quantum computing. It explains why this broad topic is incorporated in the enabling technologies part.

[2138] I don't cover analog computing which seems entirely out of fashion. See Analog Computers by Francis Massen (80 slides).

[2139] See Unconventional Computation by Bruce MacLennan, University of Tennessee, who is a reference in the field, October 2019 (306 pages) and Unconventional Computing by Andrew Adamatzky et al, Springer, 2018 (698 pages).

Supercomputing

The so-called "quantum supremacy" announced by Google in October 2019 systematically referred to power comparisons with supercomputers, in particular with the **IBM Summit** installed at the Oak Ridge laboratory of the US Department of Energy since 2018[2140].

This kind of supercomputer falls within the field of "High Performance Computing", which we will study briefly here to put it into perspective in relation to quantum computing.

The notion of HPC has not always been well defined, particularly since it is a moving target. The power of a supercomputer from the 1980s is now available in a simple recent server if not in your smartphone. However, it is possible to describe the category with its application requirements. HPC and supercomputers are essentially used for digital simulation and the analysis of complex data. These tools are provided to both researchers, public services and industry for their most advanced computational needs[2141].

HPC are used for weather forecasting[2142], organic and inorganic chemistry simulations, aerospace and automotive simulation, nuclear weapon simulation[2143], in finance, more recently in machine and deep learning and, we tend to forget, also to create computer graphics in movie and TV series productions. The mathematical models used in supercomputers are used in particular to solve partial differential equations and to carry out N-body simulations.

These systems are demanding in several ways: in computing capacity, often evaluated in floating-point operations per second, if possible, in double precision (FLOPS), in data storage capacity, and above all, in the ability to transfer data rapidly between storage, memory and processing units. It is in these areas that supercomputers are most distinct from commodity servers used in data centers.

Function	Energy in Picojoules	
8-bit add	0.03	computing
32-bit add	0.1	
FP Multiply 16-bit	1.1	
FP Multiply 32-bit	3.7	
Register file access*	6	cache and memory access
Control (per instruction, superscalar)	20-40	
L1 cache access	10	
L2 cache access	20	
L3 cache access	100	
Off-chip DRAM access	1,300-2,600	

Figure 696: in classical computing, the biggest energy cost comes with moving the data and not computing. It may be the same with quantum computing. Source: The End of Moore's Law & Fater General Purpose Computing and a Road Forward, by John Hennessy 2019 (49 slides).

[2140] We'll see in a later part that this comparison was non-sense and was mixing apples and oranges in an unfair way towards the IBM Summit and HPC overall. With factoring-in the noise generated by Sycamore, emulating it requires only the power of a simple PC.

[2141] See this good review paper on HPCs: Reinventing High Performance Computing: Challenges and Opportunities by Daniel Reed et al, Universities of Tennessee, Utah and ORNL, March 2022 (22 pages).

[2142] As for IBM Weather Channel and its GRAPH (Global Hi-Resolution Forecasting System) forecasting model which is accurate to within 3 km. It is based on an HPC, the Dyeus with 76 nodes of 4 V100 GPUs and 2 Power 9 CPUs. See High Performance Computing for Numerical Weather Prediction at The Weather Company, an IBM Business by Todd Hutchinson and John Wong, 2019 (18 slides).

[2143] This is the role of the supercomputer at CEA-DAM in Bruyères-le-Châtel in the Ile-de-France region, which is fed with data from the Megajoule laser located in Aquitaine.

This table describes the power consumption gap between computing and memory access, which are becoming increasingly expensive the further away memory is from computing. The ratio goes up to more than 1 to 1000! It explains the attempts to bring memory closer to computing units.

Historically, supercomputers such as **Cray's** relied on home-grown vector processors and various proprietary massively parallel systems[2144].

These systems have been swept away over the last decade by cluster-based architectures using standard market processors of the CPU type, complemented in recent years by GPGPUs and A100 (in 2020).

A cluster contains several nodes, each containing several CPUs and/or GPGPUs, themselves multi-core, and fast interconnection between these nodes, between clusters, and fast access to data storage, increasingly based on SSDs, which are much faster than hard disks, and at last fast networking access.

Clusters based on standard microprocessors now account for 85% of the 500 largest supercomputers in the world[2145]. The CPUs most often come from Intel (Xeon), AMD (Opteron then EPYC), IBM (Power9) while Nvidia dominates the market with its GPGPUs (general purpose GPUs), including the famous V100 generation Volta launched in 2017 and its successor A100 Ampere announced in May 2020 and the H100 Hopper in March 2022 with 80 billion transistors and a data transfer speed of 3 TB/s with its associated HBM3 RAM. Two thirds of the top HPC now include such Nvidia GPGPUs. This trend accelerated as the OpenMP and OpenACC frameworks were ported to Nvidia GPUs, making these easier to use for a host of existing scientific applications.

This is a form of commoditization of supercomputing, even if these are heavyweight architectures to deploy in large clean rooms. The added value has shifted to the architecture of interconnection, memory and storage, and of course, software.

Interconnection in clusters uses technologies such as Nvidia's NVLink, which connects GPUs and CPUs at high speed. Clusters are interconnected by multiple 200 Gbits/s fiber optic links, often from **Mellanox,** Nvidia's subsidiary since 2019. On a larger scale, HPE is promoting the **Gen-Z** architecture optimized for data access in distributed "data-centric" systems.

Operations on supercomputers are programmed with different development tools. One example is **OpenFOAM**, an open source SDK used to simulate fluid mechanics, chemical reactions, heat transfer, solid mechanics, electromagnetism and also in finance. And besides **LS-DYNA** for structural simulation. Finally, the parallel application development library for Fortran, C and C++ **OpenMP** is very commonly used for scientific computing, as is **OpenACC**. Let's not forget also that there are many optimization algorithms based on practically acceptable approximations, such as for traveling salesman type problems.

Chinese and Japanese vendors are developing their own custom supercomputers microprocessors, in order to limit their dependence on USA companies. In Japan, the **Fujitsu** Fugaku supercomputer uses Fujitsu A64FX chipsets comprising 52 Arm cores and 32GB of HBM2 memory delivering a nominal power rating of 2.7 TFLOPS (processor layout *below*). The Fugaku, which is not a poisonous fish, has a total of 415 double precision PFLOPS with 396 racks and 152,064 processors. Its installation was completed in June 2020 and enabled Fujitsu to win first place on the podium of the world's most powerful supercomputers ahead of the USA with the IBM Summit[2146] .

[2144] Cray was acquired by HPE in 2019.

[2145] The Top 500 is based on a standardized benchmark, the HPL for High Performance Linpack. It is used to solve a set of linear equations using Gaussian elimination using dense matrices and floating number calculus. See the last published version as of the writing of this book: https://www.top500.org/lists/top500/2022/06/.

[2146] See Fujitsu and RIKEN Take First Place Worldwide in TOP500, HPCG, and HPL-AI with Supercomputer Fugaku, June 2020 and Japanese Supercomputer Development and Hybrid Accelerated Supercomputing by Taisuke Boku, 2019 (59 slides), Supercomputer Fugaku, 2019 (13 slides) and The first "exascale" supercomputer Fugaku & beyond by Satoshi Matsuoka, August 2019 (80 slides).

China's largest supercomputer is the **Sunway TaihuLight** at the National Supercomputing Center in Wuxi. With a capacity of 93 PFLOPS, it uses 40,960 SW26010 256-core 64-bit RISC architecture home-built processors (with simplified instruction set).

As of mid-2022, China had deployed 35% of the world's Top 500 supercomputers, ahead of the USA with 26%, but only 4% of the TOP50 for 38% in the USA and 8% for Japan, France, Germany and Russia.

In September 2021, the DoE started the installation of its Frontier new generation supercomputer in its Oak Ridge lab, the Aurora system built by HPE with 9400+ Cray EX nodes, each equipped with one AMD Epyc CPU and four Radeon Instinct MI250X GPUs. Operational since 2022, it currently provides 1.1 exaflops of HPC and AI computing power and consume only 21 MW, reaching a record of 52 GLOPS/W[2147].

The European Union launched the **EPI** (European Processor Initiative), a project aiming to bring technology independence with supercomputers multicore microprocessors as well as in car embedded systems. It mainly involves German and French players, notably **Atos**.

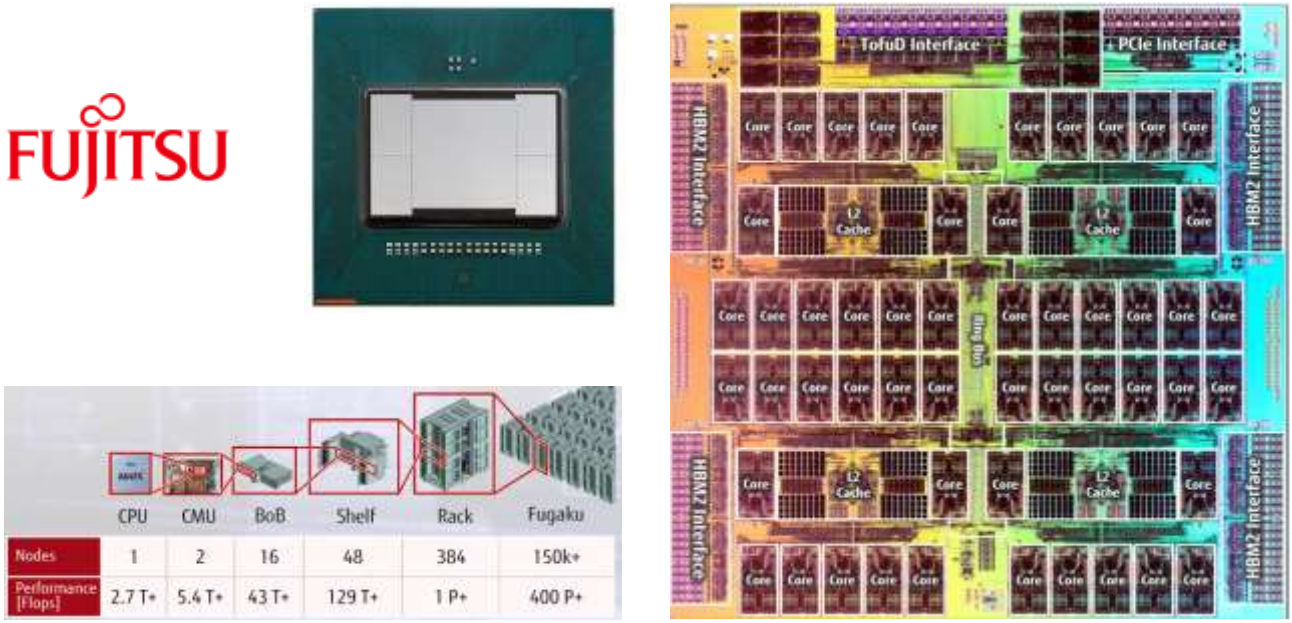


Figure 697: Fujitsu's Fugaku supercomputer is one of the largest in the world. It uses Fujitsu A64FX chipsets containing each 52 Arm cores and 32GB of HBM2 memory. Source: Fujitsu.

The effort is carried by the startup **SiPearl**, led by Philippe Notton. It is part of the **EuroHPC** project to create pre-exaflops and exaflops supercomputers, including one in Germany and one in France. The planned budget is 1B€, half of which will be allocated evenly between the European Union and its Member States.

[2147] See US Closes in on Exascale: Frontier Installation Is Underway by Tiffany Trader, HPCwire, September 2021.

In France, the **Jean Zay** supercomputer deployed at GENCI on behalf of the CEA, CNRS and Inria is equipped with 2696 Nvidia V100 GPUs and over 3462 Intel Xeon Cascade Lake CPUs. It is cooled by "hot water", from 30°C to 42°C. It was deployed as part of the French AI plan announced in 2018. Use cases are scientific simulation and machine learning.

Hewlett Packard Enterprise

GENCI

cea cnrs

Inria

HPE SGI machine
>3642 CPU **Intel Cascade Lake** with 12 and 20 cores
2696 GPU **Nvidia V100,** 1,3 PB SSD storage
28 PFLOPS in 2020
< 2 MW
hot water cooling (32°C-42°C)

Figure 698: the Jean Zay supercomputer in France is typical of the new generation of HPCs launched since 2018 with a mix of CPUs and GPGPUs from Nvidia. Source: GENCI.

The GENCI computing center is due to house a quantum accelerator, probably from **Pasqal**, within a few years. It will be integrated into a hybrid computing architecture. Many other European HPC centers have similar plans, in Germany, Italy and the Netherlands, among others.

Since the advent of the cloud, HPC and supercomputing resources are now available on demand. Cloud data center do not necessarily provide HPC resources. This depends on the servers and clusters deployed architectures and on the packaging of the cloud vendor's offering.

This notion can be associated with the notion of hyperscale, which covers the capacity of a cloud infrastructure to adapt to the increasing customer computing needs.

Machine learning and deep learning applications are the most recent applications implemented on supercomputers, particularly since they are using GPGPUs that run tensors enabling efficient matrix operations, which are very common in neural networks. In practice, however, most supercomputers continue to run scientific simulation applications.

The market for microprocessors dedicated to machine learning and deep learning acceleration has been booming for several years. A wide variety of approaches have been adopted by its vendors.

It can be represented as below on two axes: in the Y axis, the level of cores specialization, and on the X axis, the number of cores.

Google's TPUs (Tensor Processing Units) are highly specialized for training neural networks, especially convolutional image recognition networks. Nvidia's GPUs contain thousands of classical arithmetic calculation cores as well as hundreds of tensors for matrix computing, which optimizes their versatility.

The most extreme processor is the **Cerebras V2** launched in 2021 with its 850,000 cores. It's a 21 cm square chipset containing a hefty 2.6 trillion 7 nm transistors and 40 GB of integrated SRAM ultra-fast cache memory. Their first version launched in 2019 is already deployed in two test servers at the DoE in the USA with one and two of these chipsets. The first benchmarks published late 2019 did show excellent performance in neural networks training. In 2022, TotalEnergies found 100x speedups vs conventional GPGPU with various material simulations applications[2148]. The company raised a total of $720M, a similar amount to PsiQuantum.

[2148] See Cerebras shows off scale up AI performance for big pharma and big oil by Timothy Prickett Morgan, TheNextPlatform, March 2022.

Finally, **FPGA**s are dynamically programmable circuits that allow the creation of custom circuits at rather low cost and high flexibility[2149]. These are used by some cloud vendors such as Microsoft (with its Brainwave chipsets) and Chinese cloud companies like **Alibaba** and **Baidu**.

Some of these cloud players are developing their own supercomputers. **Google** has created its TPU pods over several generations for its data centers. A TPU v3 board contains four TPU chips, each with two cores, with 16 GB of HBM memory for each TPU core. A TPU v3 Pod has up to 2048 TPU cores and 32 TB of memory.

Graphcore (2016, UK, $692M) is another contender in this crowder market. It is now using 3D chips bonding using a TSMC technology, the main chip containing processing units and the secondary underneath chip containing connectivity between the computing chipsets cores. Its current processors have 1,472 cores and 900MB on-chip SDRAM memory, which helps them outperform Nvidia chipsets on some tasks[2150].

Nvidia integrates its A100 GPUs in SuperPods totaling 140 DGX A100 and 1120 A100 servers and 4 Po of storage, for 700 PFLOPS. These FLOPS are however not necessarily the same as those used to evaluate the TOP 500 supercomputers. Vendor communication is sometimes misleading.

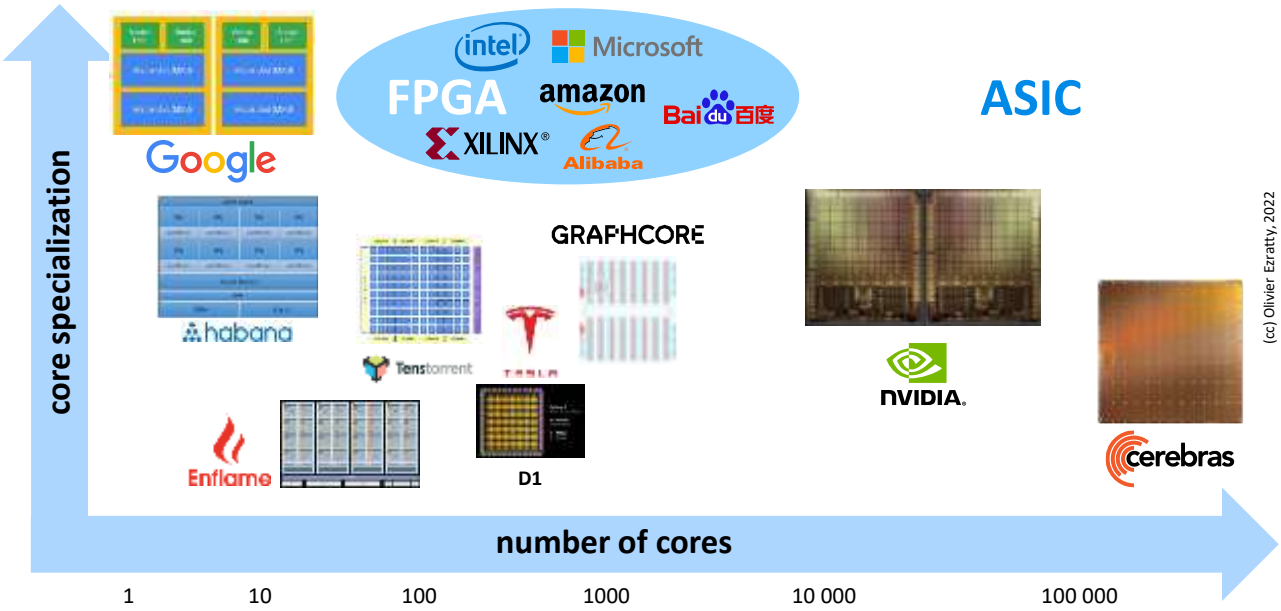


Figure 699: a map of the tensor-based processors with two dimensions: the number of cores and their specialization. The more specialized cores are in Google's TPU with large tensor operations capacity (128x128 values) while Cerebras's wafer scale chipset has 845 000 relatively simple cores. (cc) Olivier Ezratty, 2020.

Both to improve performance and to reduce energy consumption, there are a number of ways to make these calculations more efficient: **Approximate Computing**, which reduces precision in neural network training and/or inferences without affecting the results, **Quantization**, which switches from floating-point calculations to integer computing during or after training, **Binary Neuron Networks**, which is even simpler with 1 bit output neurons taking us back to the Perceptrons era of 1957 and **Sparse Computing**, which allows computations to occur on compressed representation of matrices, this being useful only for sparse matrices, without prior decompression.

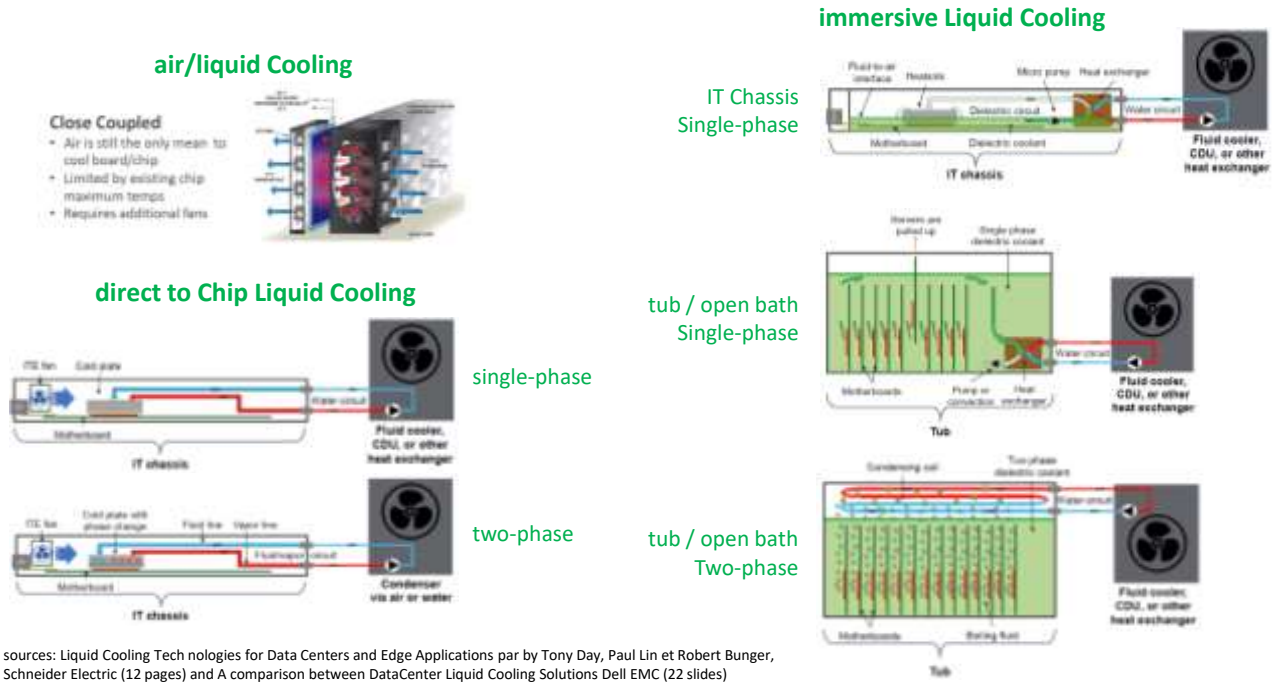
[2149] The FPGA market is currently dominated by two vendors: Intel, after its acquisition of Altera in 2015, and AMD, after its acquisition of Xilinx in 2020. In 2019, Xilinx had a 52% revenue market share and Intel about 35%.

[2150] See Graphcore Uses TSMC 3D Chip Tech to Speed AI by 40% Unveils plan for $120-million "brain-scale" supercomputers in 2024 by Samuel K. Moore, IEEE Spectrum, March 2022.

Last but not least, there is the close integration between memory and computing capabilities. For example, the French startup **UpMem** offers DRAM memory modules integrating dozens of RISC-V cores to perform in-memory computing and speed-up certain processes by a factor of 10, particularly for big data applications. It is also possible to tune the cores clock frequency when they are waiting for data from memory.

Supercomputers are quite energy hungry. Their increasingly powerful microprocessors consume several hundred of Watts. A third of the electrical energy consumed by a data center is spent on cooling. Specialized server racks now easily consume more up to 30kW. It has now reached the point where liquid cooling is preferred for removing heat from components, usually with water. This provides greater efficiency.

Whatever happens with quantum computers, supercomputers will always be relevant. Applications using large amounts of data are not suitable for quantum computing, even with zillions of qubits. Indeed, data loading time in qubits is a huge bottleneck because it relies on very long series of quantum gates that are not as fast as classical data processing. Applications adapted to quantum computing should not rely on high-volume data feeds. This is the case with weather forecast which requires heavy data sets. It will rely on classical supercomputing for a long time despite some exaggerated claims[2151].



sources: Liquid Cooling Tech nologies for Data Centers and Edge Applications par by Tony Day, Paul Lin et Robert Bunger, Schneider Electric (12 pages) and A comparison between DataCenter Liquid Cooling Solutions Dell EMC (22 slides)

Figure 700: the various ways to cool a server. Sources: Liquid Cooling Technologies for Data Centers and Edge Applications by Tony Day, Paul Lin and Robert Bunger, Schneider Electric (12 pages) and A comparison between DataCenter Liquid Cooling Solutions Dell EMC (22 slides).

It is used to solve complex problems of combinatorial or minimum energy research. It is likely that for a long time to come we will have hybrid architectures combining classical computers or supercomputers and quantum accelerators. This is the approach adopted by supercomputer suppliers like **Atos**.

[2151] See Forecasting the Weather Using Quantum Computers by 1Qbit, 2017. The paper references CES 2019: IBM unveils weather forecasting system, commercial quantum computer by Abrar Al-Heeti, January 2019, which covers two entirely unrelated announcements from IBM, one on weather forecasting using classical computing and another, related to their Q System One, both introduced at CES 2019. See also Rigetti Enhances Predictive Weather Modeling with Quantum Machine Learning, December 2021 who does this with a mere 32 qubits!

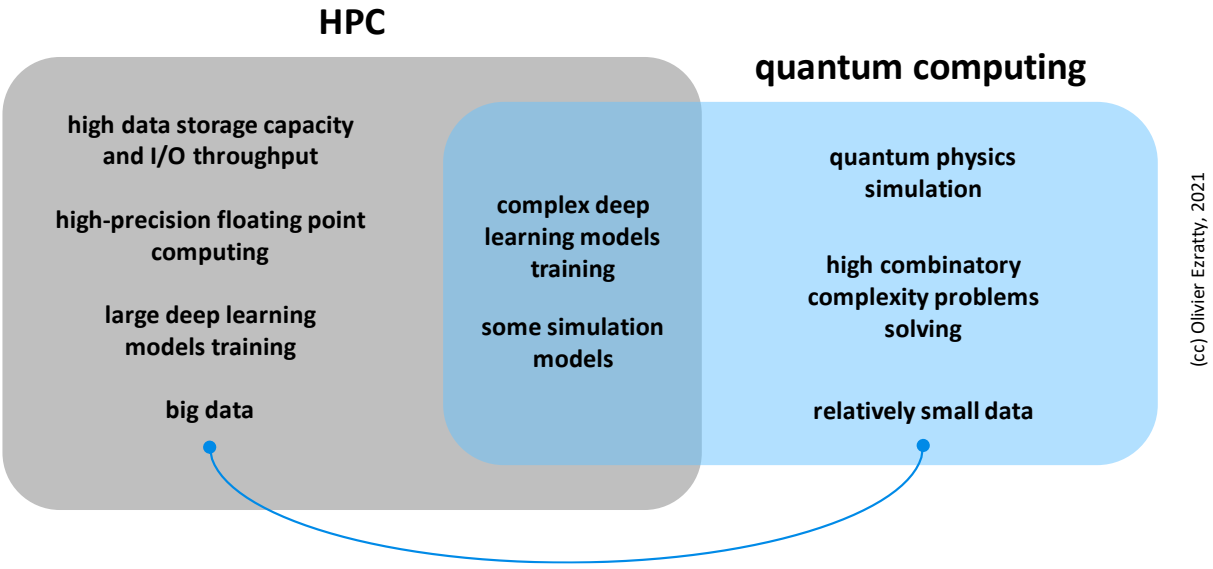


Figure 701: how to position HPCs vs (scalable) quantum computers. HPCs are for big data and high-precision computing. Quantum computing will be adapted to high complexity problems but with relatively reasonable amounts of data. There's some cross-over between both systems and they will work in sync in many cases. (cc) Olivier Ezratty, 2021.

Digital annealing computing

Digital annealing is a non-quantum variant of quantum annealing used in D-Wave computers. It has the advantage of exploiting standard component production technologies in CMOS. The level of acceleration provided at the calculation level is not a priori exponential.

Several industry vendors are in this market with **Fujitsu** and **Hitachi**. This part also includes some related solutions coming from **MemComputing** and **InfinityQ**. Let's also mention the support of annealing simulation by the **Atos** QLM with a capacity to handle 50,000 variables and an optimized implementation of the SQA algorithm (simulated quantum annealing).

Fujitsu announced in early June 2018 a digital annealing computer operating at room temperature. Fujitsu is one of the world leaders in the supercomputer market with IBM, HPE and Atos. It was therefore logical that they explored ways to upscale their HPC offering.

It is supposed to scale much better than D-Wave quantum annealers[2152].

The technology is developed on CMOS classical components in partnership with the University of Toronto. It is already proposed as a cloud offering. It is used to solve optimization problems and to carry out molecule screening in biotechs. The dedicated chipset contains 1,024 bit update blocks incorporating memory to store their weights with a precision of 16 bits, logic blocks to perform value inversions and the associated control circuits. This is reminiscent of memristor-based neural networks. As with D-Wave, problems are loaded into the system in the form of matrices with biases in the links between elements and the system looks for a minimum energy state to solve the problem. It has some familiarity with the Ising model used in D-Wave.

Figure 702: Fujitsu's DAU processor for implementing optimized digital annealing. Source: Fujitsu.

[2152] See Fujitsu's CMOS Digital Annealer Produces Quantum Computer Speeds, 2018.

Its designer, **Hidetoshi Nishimori** of the Tokyo Institute of Technology, believes that Fujitsu will be able to create solutions that outperform D-Wave. In 2019, Fujitsu announced its second generation of chips with 8,192 blocks. They expect to reach one million blocks thereafter.

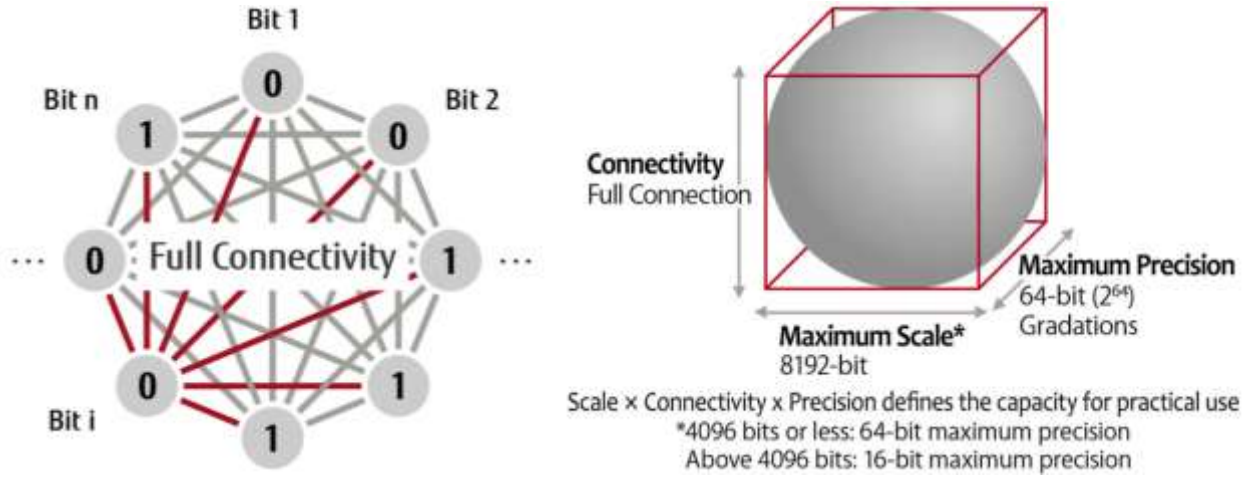


Figure 703: Fujitsu's DAU high-level architecture. Source: Fujitsu.

Development tools are provided by **1QBit,** in which Fujitsu has made an investment. Fujitsu has been collaborating since April 2020 with **Quantum Benchmarks (**Canada) on quantum algorithms and error suppression codes, based on an IA Fujitsu algorithm and their experience with their digital annealing[2153]. Fujitsu is also partnering with **Entanglement** (USA) which developed a Covid vaccine logistics optimization solution with its annealer.

HITACHI

Fujitsu is not the only Japanese company exploring digital annealing. Hitachi also launched a related initiative although, contrarily to Fujitsu, it seems it did stay in research lab and didn't reach commercialization.

Their system is implementing a hardware solution to solve Ising models. It's mixing probabilistic and deterministic approaches running in a CMOS component to find some energy minimum of a combinatorial problem expressed as an Ising model[2154]. It doesn't find the absolute minimum to the problem but an acceptable solution. The CMOS uses SRAM to store the virtual "spin states" of the Ising model problem. Hitachi stated that it could help solve combinatorial optimization problems such as the travelling salesman problem efficiently. The architecture was first relying on FPGAs which makes sense given it didn't reach volume production.

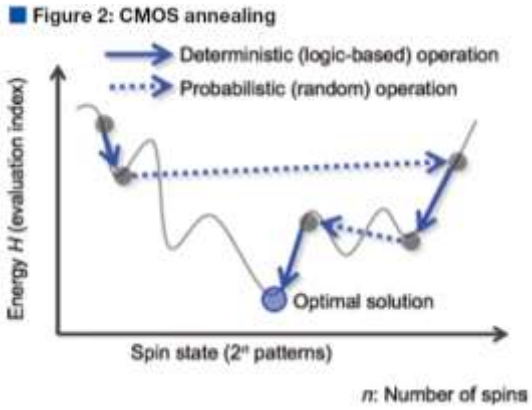


Figure 704: CMOS annealing principle.

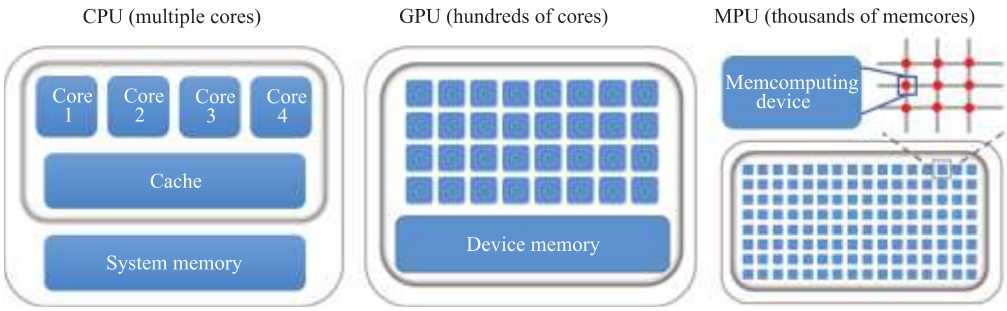
[2153] See Fujitsu Laboratories and Quantum Benchmark Begin Joint Research on Algorithms with Error Suppression for Quantum Computing, April 2020 and Fujitsu Laboratories and Quantum Benchmark Begin Joint Research on Algorithms with Error Suppression for Quantum Computing by Fujitsu, March 2020.

[2154] See CMOS Annealing Machine – developed through multi-disciplinary cooperation by Hitachi, Ltd., November 2018, Overview of CMOS Annealing Machines by Masanao Yamaoka, January 2019 (4 pages) and CMOS Annealing Machine: an In-memory Computing Accelerator to Process Combinatorial Optimization Problems, April 2019.

The mysterious startup **MemComputing** (2016, USA) can be positioned in a category close to Fujitsu's offer. It is a solution inspired by quantum annealing computation. They use the principle of invertible computing units, able to circulate data both ways, from input to output and output to input.

It also uses oscillating Boolean gates implementing a non-Von-Neumann computing model and some sort of tunnel effect[2155]. Their hardware solution MemCPU Coprocessor is to place memory next to computing units in processing unit[2156]. These memristor-like computing cells have symmetrical inputs and outputs interconnected to neighboring cells. It computes exclusively with integer numbers. There is no floating-point computing at all. They would automatically find a complex balance of a parameterized system. This is the principle of SOLGs (Self Organizing Logic Gates) in Figure 706[2157].

The company positions its technology as competing with quantum computing with a market ready solution although its real existence and packaging is in question[2158].



(Color online) Comparison of CPU, GPU, and MPU.

Figure 705: MemComputing architecture compared with classical computing. It's basically a mix of in-memory processing with bidirectional computing. Source: MemComputing.

The company was founded by **John Beane**, a serial entrepreneur, with two physics researchers, **Massimiliano Di Ventra** and **Fabio Traversa,** who have done extensive work on memory computing[2159].

Their architecture is supposed to solve various classes of NP-complete and NP-difficult problems in polynomial time such as 3-SAT problems[2160]. They tout significant performance gains such as four orders of magnitude for machine learning applications, i.e., performance multiplied by 10,000!

[2155] See Global minimization via classical tunneling assisted by collective force field formation by F. Caravelli, F. C. Sheldon and Fabio L. Traversa, February 2021 (15 pages).

[2156] It is described in Memcomputing: fusion of memory and computing by Yi Li et al, 2017 (3 pages) where this schema comes from.

[2157] SOLGs are described in the patent Self-Organizing Logic Gates and Circuits and Complex Problem Solving With Self-Organizing Circuits, March 2018 (37 pages). It is further detailed in Coupled oscillator networks for von Neumann and non von Neumann computing by Michele Bonnin, Fabio L. Traversa and Fabrizio Bonani, arXiv preprint, December 2020 (29 pages).

[2158] See MemComputing vs Quantum Computing by MemComputing, August 2022.

[2159] See Universal Memcomputing Machines by Fabio Traversa and Max Di Ventra, 2014 (14 pages) and Perspective: Memcomputing: Leveraging memory and physics to compute efficiently by Fabio Traversa and Massimilio Di Ventra, 2018 (16 pages).

[2160] See Memcomputing NP-complete problems in polynomial time using polynomial resources and collective states by Fabio Traversa, Massimilio Di Ventra et al, 2014 (10 pages) and Evidence of an exponential speed-up in the solution of hard optimization problems by Fabio Traversa et al, 2018. Then, See this Conference from Massimiliano Di Ventra at Berkeley in 2016 (26 minutes).

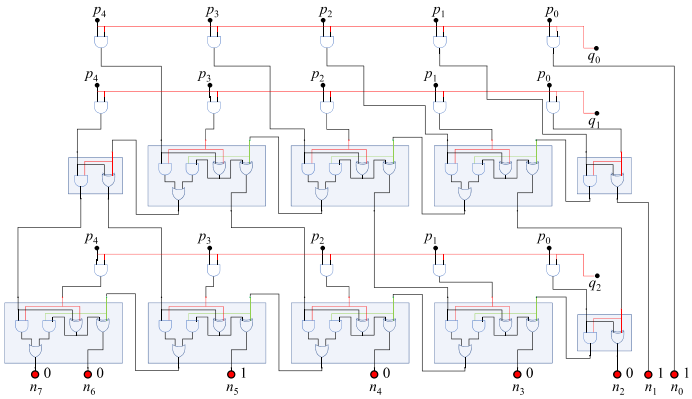


FIG. 2. A possible Boolean circuit that multiplies two integers p and q to give $n = 35 = (100011)_2$ (in the little-endian notation).

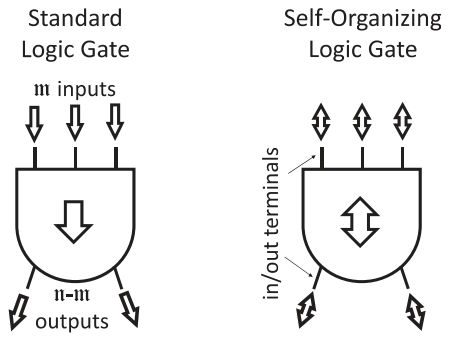


FIG. 3. Left panel: sketch and symbol of a standard $\mathcal{N}$-terminal logic gate with $\mathcal{M}$ inputs and $\mathcal{N} - \mathcal{M}$ outputs. Right panel: sketch and symbol of the corresponding self-organizing logic gate.

Figure 706: SOLGs (Self Organizing Logic Gates) from MemComputing. Source: MemComputing.

The application domains include the resolution of planning and optimization problems such as the traveling salesperson problem, combinatorial optimizations and searches[2161], bioinformatics, neural network training[2162] and even integer factoring[2163], each time with the promise of an exponential gain in computing time compared to traditional computing.

For the moment, their solution is only emulated in conventional computers like with the AMD EPYC microprocessor and provided as an SDK operated in the cloud they have designed in partnership with **Canvass Labs** (2017, USA). Their electronic component is not yet manufactured, even at the prototype stage, and it is not clear whether it is possible to manufacture it and would deliver the speedup promises. They announced that they would need to embed some memristor technology in their component, which can create significant delay in the manufacturing given this technology is not really mature.

They handle problems such as MIPLIB (Mixed Integer Programming Library), which are considered intractable with a 60-second response time on a server running Linux, and have even beaten a D-Wave. This is used to find a combination of given integers that can generate zero when added together (the "Subset Sum problem"). The startup manages to obtain a quantum scale advantage by emulating its process on traditional processors. This amounts to challenging all current theories of complexity. In short, it makes you dizzy.

In April 2020, MemComputing announced that it would make its XPC (Xtreme Performance Computing) software stack available in the cloud for researchers working on Covid-19[2164] .

So, is this technology simply revolutionary and could it nullify many efforts in quantum computing, or are there one or more shortcomings? There are plenty of them. How do you initialize the system so that it is close to a global minimum? What is their real capacity to create these SOLGs in current CMOS components? How is noise managed in their system[2165]?

[2161] See Stress-testing memcomputing on hard combinatorial optimization problems by Fabio Traversa, Massimiliano Di Ventra et al, 2018 (6 pages).

[2162] See Accelerating Deep Learning with Memcomputing by Haik Manukian, Fabio Traversa and Massimiliano Di Ventra, 2018 (8 pages).

[2163] See Polynomial-time solution of prime factorization and NP-hard problems with digital memcomputing machines by Fabio Traversa and Massimiliano Di Ventra, 2017 (22 pages).

[2164] See MemCPUXPC SaaS Platform available free for COVID-19 Research, 2020.

[2165] They provide an answer in Directed percolation and numerical stability of simulations of digital memcomputing machines by Yuan-Hang Zhang and Massimiliano Di Ventra, April 2021 preprint on arXiv (12 pages).

Is the system scaling well? Their approach would not be scalable according to several specialists including Scott Aaronson[2166].

In 2022, MemComputing published two papers in partnership with a scientist from the DoE Los Alamos lab on the potential effect of a tunneling effect with memristors to find global minimum, a task commonly used to solve various optimization and machine learning problems[2167]. All this remains very theoretical.

InfinityQ (2019, Canada, $6M) stated that they had built the "*first quantum computing CMOS microchip technology to work at room temperature*". It is supposed to be an analog quantum computer with between 1000 and 5000 qubits.

Their qubit architecture is "*based on an artificial atom in a lambda configuration*" which "*exploits superposition and entanglement to achieve quantum computing without the burden of maintaining very fragile quantum objects*". It is a cloud native platform and quantum analog-computing technology that can run any coding language, any problem up to 100,000x faster than an average laptop, with the same energy consumption as a lightbulb. Their first-generation machines is said to solve complex optimization problems, linear system and FFTs (fast Fourier transforms). That's quite a heavy stack of promises.

They created a proof of concept with 10 qubits late 2020 and announced a 100 qubits MVP in 2021 for and full commercialization after 2025. In April 2021, they mentioned that they had solved a traveling salesperson problem with 128 cities while other "*non-classical machines*" have solved such problems with a maximum of 22 cities (which is not really true). This system is currently programmed in C language.

The company was launched by Aurelie Hélouis (CEO) with Kristina Kapanova (CTO, who later left the company) and was supposedly backed by Philippe Dollfus, a CNRS Research Director in France who is specialized in computational nanoelectronics and John Mullen, former Assistant Director of the CIA. They also made business claims such as having projects starting with major unnamed UK and Canada banks, with a Swiss pharmaceutical and the Canadian government.

So, how can this feat be accomplished[2168]? How is it different than what MemComputing is doing? They share some similarities: use CMOS components and solve complex problems in a polynomial way. The difference seems that MemComputing is using an invertible digital logic while InfinityQ is based on some analog processing. It also looks like an analog annealing system. Their technology could be classified as some sort of reservoir computing running on CMOS doing rabi flops emulation[2169]. Their quantum, superposition and entanglement claims seem totally overexaggerated. In 2022, the company made a pivot, did reset its web site and claimed that its solution was "*A quantum-inspired technology to serve gaming & metaverse's intensive computation demands*". That smells quite fishy to move from the financial sector to the metaverse and gaming sectors.

[2166] See A Note on `Memcomputing NP-complete problems' and (Strong) Church's Thesis by Ken Steiglitz, 2015 (2 pages) which quickly demonstrates that this is not possible. The same goes for Memrefuting by Scott Aaronson in 2017 and for A review of Memcomputing NP-complete problems in polynomial time using polynomial resources' by Igor Markov, 2015 (3 pages).

[2167] See MemComputing Announces Collaboration with Los Alamos National Lab, January 2022, Global minimization via classical tunneling assisted by collective force field formation by Francesco Caravelli et al, Science Advances, December 2021 (9 pages) and Projective Embedding of Dynamical Systems: uniform mean field equations by Francesco Caravelli et al, MemComputing and DoE Los Alamos lab, January 2022 (45 pages). PEDS, projective embedding of dynamical systems (PEDS).

[2168] See a video of their presentation, December 2020 (17 mn).

[2169] See Quantum reservoir computing with a single nonlinear oscillator by L. C. G. Govia et al, Raytheon, January 2021 (9 pages).

Reversible and adiabatic calculation

Since the 1960s, researchers have been considering reducing computer power consumption by several orders of magnitude based on the principle of adiabatic reversible computing[2170].

The goal is primarily energy-based. It does not accelerate computing. In most cases, it is even contradictory with Moore's law, as the main techniques used result in a calculation speed decrease.

All this is due to our understanding, since the 1960s, of the link between computation and thermodynamic processes. **Rolf Landauer** created in 1961 the equation according to which the process of information processing that dissipates energy is related to memory erasure[2171]. The erased information is turned into heat sent outside the computer, increasing the environment entropy. Rolf Landauer estimated that the dissipated energy was always greater than **kTln(2)** per erased bit, k being Boltzmann's constant (1.38×10^{-23} J/K), T the temperature in Kelvin and ln(2) the logarithm of 2 (about 0.69315). At room temperature, this gives 0.017 eV. This is the famous Landauer limit[2172].

More generally, Landauer's limit illustrates the link between the notions of logical and physical reversibility of computation. The first is linked to the ability to determine the input values of a calculation according to the output values.

The second is that the unfolding of a physical process in reverse may not violate the laws of physics, including the inescapable second law of thermodynamics according to which the entropy of a thermodynamic system always increases unless the process is reversible.

Today, a CMOS component spends 5000 eV energy to erase one bit, almost 300,000 times more than the Landauer's limit. One could gain an order of magnitude and go down to 500 eV, but that would still be 30,000 times more than the Landauer limit. So, in order to reduce the computing energy consumption, why not avoid erasing information and, in the process, make all computing physically and logically reversible?

This would require a review of all current computational logic that relies at low-level on irreversible logic gates that destroy information, such as NAND or XOR gates that generate one bit from two bits.

In 1973, **Charles Bennett**, another IBM researcher and colleague of Rolf Landauer's, imagined a calculation method that would avoid this energy-dissipating erasure of information without requiring an infinite memory[2173].

[2170] To write this part, I used the many references from the excellent presentation Reversible Adiabatic Classical Computation - an Overview by David Frank, 2014, IBM (46 slides), as well as from The Future of Computing Depends on Making It Reversible by Michael P. Frank, 2017 and The Case for Reversible Computing by Michael P. Frank, 2018 (19 pages). See also Computers That Can Run Backwards by Peter Denning and Ted Lewis, 2017 and Theory of Reversible Computing by Kenichi Morita, 2017 (463 pages). See also the review paper Quantum Foundations of Classical Reversible Computing by Michael P. Frank and Karpur Shukla, April 2021 (70 pages).

[2171] See Irreversibility and heat generation in the computing process by Rolf Landauer, in IBM Journal of Research & Development, 1961 (9 pages).

[2172] Landauer's limit was experimentally verified fifty years later, in 2011, by a team from ENS Lyon in Sergio Ciliberto's group. See Experimental verification of Landauer's principle linking information and thermodynamics by Antoine Bérut et Al, 2011 (4 pages) and Information and thermodynamics: Experimental verification of Landauer's erasure principle by Antoine Bérut, Artyom Petrosyan and Sergio Ciliberto, ENS Lyon, 2015 (26 pages). Other experiments followed to validate this, with magnetic memories, such as Experimental test of Landauer's principle in single-bit operations on nanomagnetic memory bits by Jeongmin Hong et al, 2016 (6 pages). The principle consists in lowering the energy barrier of the bit state transition when an operation is required and then to raise it again to preserve the bit state. See also Delft's 2018 experiment in Quantum Landauer erasure with a molecular nanomagnet by R. Gaudenzi et al, 2018 (7 pages).

[2173] See Logical reversibility of computation by Charles Bennett, IBM Journal of Research and Development, 1973 (8 pages). Charles Bennett is also the creator of BB84 codes with Georges Brassard, which laid the foundations of quantum key distributions.

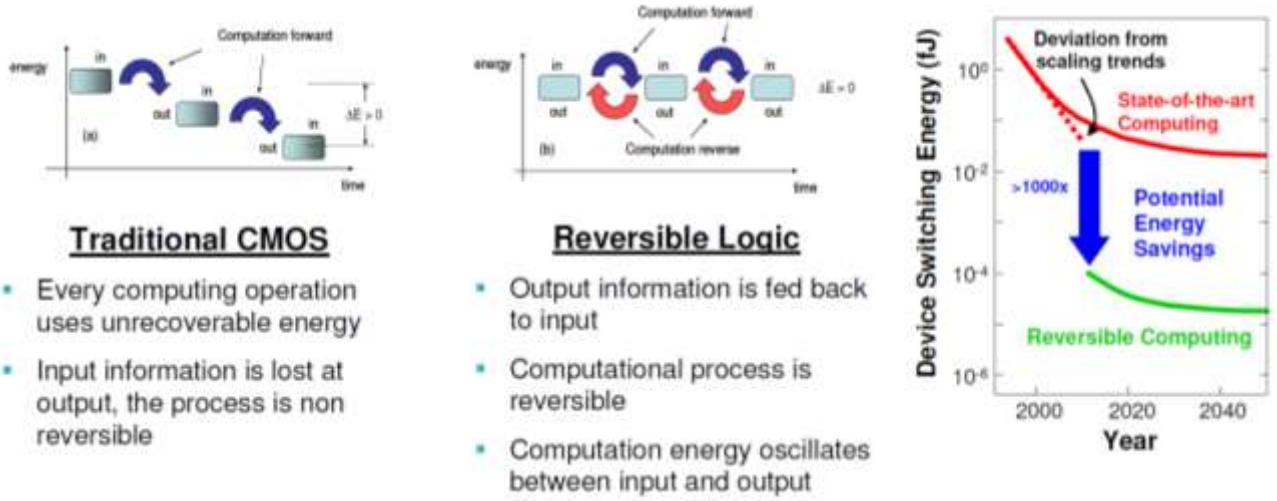


Figure 707: why reversible logic could help save energy. But it won't make it faster. Source: Reversible Adiabatic Classical Computation - an Overview by David Frank, 2014, IBM (46 slides).

He was followed by **Edward Fredkin** and **Tommaso Toffoli** who, in 1978 and 1982, imagined reversible logical gates inspired by a metaphorical physical model based on billiard balls, the BBM for billiard ball model[2174]. These logic gates have as many outputs as inputs and it is easy to understand why they become reversible. Although their model was not practically feasible with contemporary electronics, it was then applied to the quantum equivalent of these gates that we already covered.

Konstantin Likharev proposed in 1976, then in 1982, to implement this reversible computational logic by manipulating the energy levels of superconducting Josephson junctions, under the name of "parametric quantrons"[2175]. In 1991, this became the "quantron flux parametron" (QFP), capable of operating up to 10 GHz and developed by a Japanese team[2176].

This led then in 2003 to **Vasili Semenov**'s idea to use nSQUID circuits to realize these circuits, the n meaning "negative" because of a negative inductance that connects two SQUIDs of the device. As for any Josephson junction, it works under cryogenic temperature[2177].

Reversible computing is often associated with adiabatic computing but one could work without the other. The general principle of adiabatic computing is illustrated *below*: in a classical calculation, the energy barrier to switch the state of a system between a) and c) is high. In a quasi-adiabatic calculation, a physical system lowers the state energy transition barrier (in d) to trigger it (in e) and then in f, by raising the level of the barrier to its normal state.

The processing energy cost is thus lowered by approaching Landauer's limit. The high level of the non-calculation barrier guarantees the stability of the information managed outside of this operation. Lowering the barrier and raising it are often managed by trapezoidal voltage control of the transistors instead of looking like a square wave signal.

Between 1985 and 1993, reversible or partially reversible CMOS and CCD computing components were designed.

[2174] See Conservative Logic by Edward Fredkin et Tommaso Toffoli, International Journal of Theoretical Physics, 1982 (35 pages).

[2175] He tells this story in Josephson Digital Electronics in the Soviet Union by Konstantin Likharev, 2012 (18 slides).

[2176] See Quantum Flux Parametron: A Single Quantum Flux Device for Josephson Supercomputer by Mitsumi Hosoya et al, June 1991.

[2177] See an explanation of the process in Engineering and Measurement of nSQUID Circuits by Jie Ren, 2012 (26 slides). nSQUIDs are double SQUIDs connected by a negative inductance. SQUID = Superconducting Quantum Interference Device, a system used to accurately measure the magnetism of superconducting Josephson effect loops. These nSQUIDs were manufactured by Hypres.

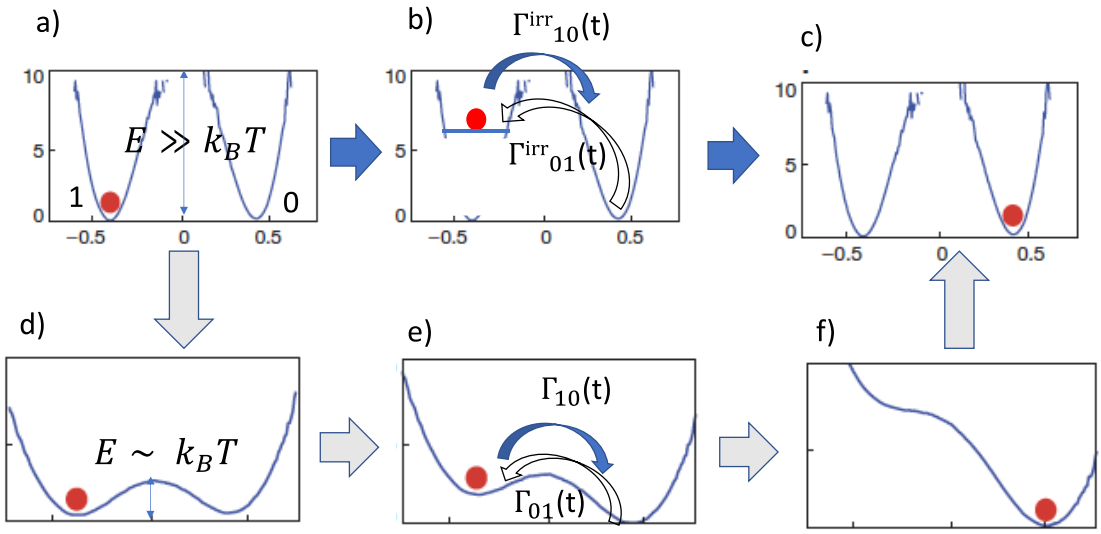


Figure 708: the thermodynamic principle of reversible computing. Source: "Thermodynamics of computing, from classical to quantum" by Alexia Auffèves, May 2020 (11 pages), adapted from Experimental verification of Landauer's principle linking information and thermodynamics by Antoine Bérut et Al, 2011 (4 pages).

Craig Lent then proposed in 1997 an adiabatic computation system based on quantum dots and cellular automata (QCA for Quantum dots Cellular Automata) to operate up to 100 GHz[2178] .

In the same manner, **Krishna Natarajan** suggested in 2004 to use MEMS (electro-micro-mechanical components) to drive the trapezoidal voltage control necessary to create adiabatic CMOS components with a very low energy dissipation of 1 eV[2179] .

The idea was pursued by a team from **CEA-Leti** and **Delft** in the Netherlands in 2017 and **Ralph Merkle** in 2019, with prototype circuits based on this kind of technology[2180].

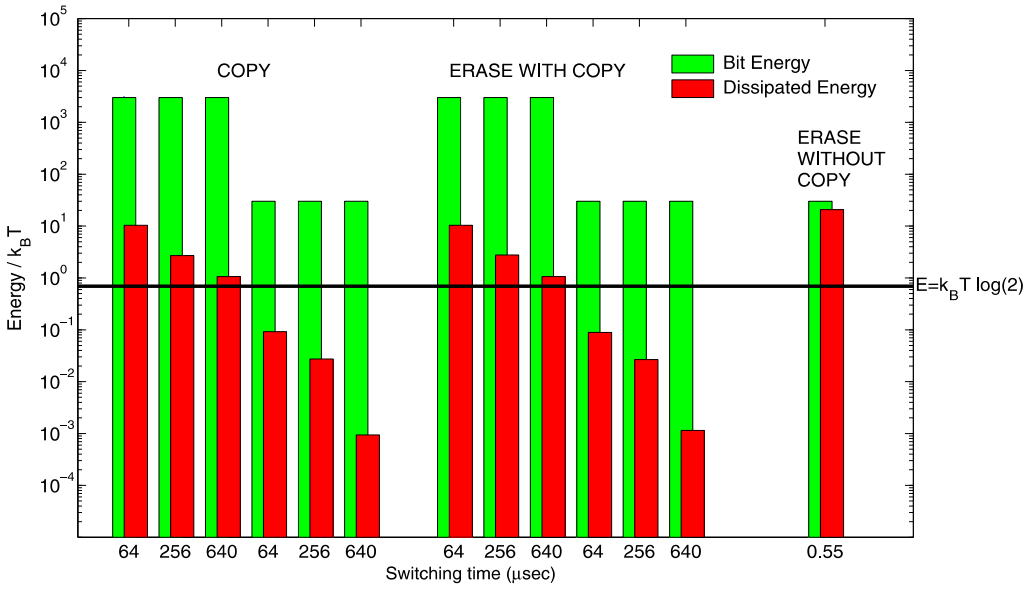


Figure 709: Source: Experimental Test of Landauer's Principle at the Sub-kBT Level by Alexei Orlov, Craig Lent et al, 2012 (5 pages).

[2178] See A Device Architecture for Computing with Quantum Dots by Craig Lent and Douglas Tougaw, 1997 (17 pages).

[2179] See Driving Fully-Adiabatic Logic Circuits Using Custom High-Q MEMS Resonators by Krishna Natarajan et al, 2004 (7 pages).

[2180] See Adiabatic capacitive logic: A paradigm for low-power logic by Gaël Pillonnet et al, CEA-Leti, 2017 (5 pages) and Mechanical Computing Systems Using Only Links and Rotary Joints by Ralph Merkle et al, 2019 (34 pages).

In 2012, **Alexei Orlov** et al. experimentally validated Landauer's limit and, above all, the possibility of overcoming it (from below) with reversible calculation, all with a few discrete classical electronic components, resistors and capacitors[2181]. Their experiment showed that a bit copy or erasing with copy could be done with an energy lower than Landauer's limit, at the price of slowing down the operation as shown in Figure 709.

Pure and simple erasing did consume more energy than Landauer's limit. The model was safe! And it all worked at room temperature. In 2019, Alexei Orlov's team from Notre Dame University in Indiana produced the equivalent of an 8-bit microcontroller using a subset of a RISC-type MIPS instruction set with 5766 transistors, 40% of which are adiabatic (Figure 710)[2182]. This seems to be, to date, the most successful realization of a reversible adiabatic processor. It remains however experimental and far from industry requirements. Its industrialization could be of interest to create microcontrollers for low power connected objects.

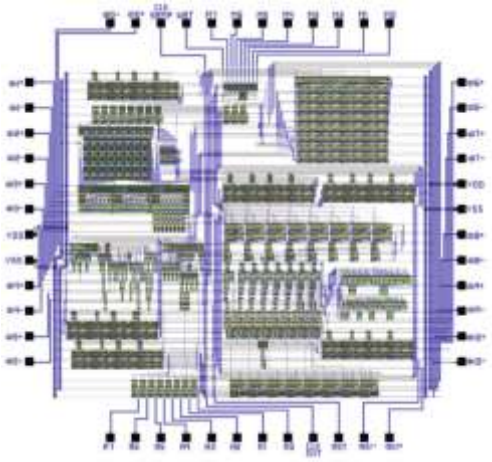


Figure 710: Source: Experimental Tests of the Landauer Principle in Electron Circuits, and Quasi-Adiabatic Computing Systems by Alexei O. Orlov et al, 2012 (5 pages).

However, this adiabatic CMOS technique requires a larger number of transistors. Therefore, emerges a new trade-off between a larger and more expensive to design and manufacture power saving component vs cheaper but more energy hungry conventional counterparts. Still, the environmental cause has recently revived interest in reversible and adiabatic computing. It is promoted by the Computer Community Consortium group of the American **Computing Research Association** with the lead from Michael P. Frank's team at **Sandia National Labs**[2183].

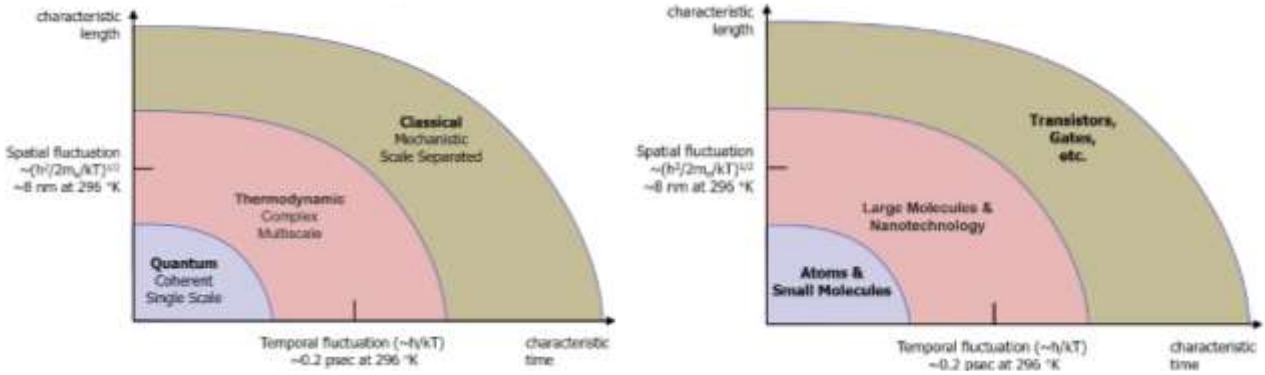


Figure 711: Source: Thermodynamic Computing, Computer Community Consortium of the Computing Research Association, 2019 (36 pages).

[2181] See Experimental Test of Landauer's Principle at the Sub-kBT Level by Alexei Orlov, Craig Lent et al, 2012 (5 pages).

[2182] See Experimental Tests of the Landauer Principle in Electron Circuits, and Quasi-Adiabatic Computing Systems by Alexei O. Orlov et al, 2012 (5 pages) which is integrated in Energy Limits in Computation by Craig Lent, Alexei Orlov et al, 2019 (245 pages).

[2183] See Thermodynamic Computing, Computer Community Consortium of the Computing Research Association, 2019 (36 pages). It is a manifesto to develop thermodynamically responsible computing inspired by biomimicry. The document is the result of a workshop with about 40 participants, almost all American except one researcher from London and another from Luxembourg, from universities and a few private actors such as Google, Rigetti, HPE, Knowm (which develops memristor-based circuits for AI applications, their kT-RAM technology) and Daptics (ex Protolife, created by Norman Harry Packard (1954) and which develops chemical simulation algorithms).

They position it in an intermediate architecture between classical and quantum computing, but on quantities that are not necessarily relevant (dimension of components and duration of state fluctuation, see Figure 711)[2184]. The purpose of the manifesto is to obtain US federal credits to finance this research. So, the story is not over!

Superconducting computing

The idea of creating superconducting computers capable of taking advantage of the lack of resistance of low temperature electronic components dates back to the early 1960s. Its history evolves in parallel with reversible and adiabatic computing. It started with the discovery of the Josephson effect in 1962. This effect was later used to create two-states superconducting qubits with research starting in the early 1980s.

The expected benefits of superconducting transistors are an increase in clock frequency and a decrease in power consumption[2185]! The gain is more significant with the clock frequency than with energy consumption. For example, in a Japanese SFQ component realized in 2019, the clock was 32 GHz while the power drain was 2.5 TOPS per Watt, in the average of most deep learning CMOS chipsets[2186].

Several generations of superconducting components have been developed over time[2187]:

- **SFQ** (Single Flux Quantum) was a first-generation circuit, limited to a 1 GHz and 300 Mhz clock frequency. Work started at IBM in the 1960s. They had invested the equivalent of $100M today in a program that was partly funded by the NSA and which was abandoned in 1983 which are also based on the Josephson effect[2188]. D-Wave's superconducting qubit use SFQ-type components for generating and reading qubit control signals[2189].

[2184] See Quantum Foundations of Classical Reversible Computing by Michael P. Frank and Karpur Shukla, April 2021 (70 pages) and The Reversible Computing Scaling Path: Challenges and Opportunities by Michael P. Frank, February 2022 (40 slides).

[2185] See this very interesting presentation on superconducting electronics: Superconducting Microelectronics for Next-Generation Computing by Leonard Johnson, MIT Lincoln Labs, November 2018 (27 slides). The gain in power consumption would be between 10 and 1000. The integration level is currently low, of the order of 200 nm compared to 7 nm for the densest CMOS processors. But it is steadily increasing. There are even investigations to combine superconducting transistors, optoelectronics and neural networks. See Superconducting Optoelectronic Loop Neurons by Amir Jafari-Salim, 2018 (48 pages).

[2186] See 29.3 A 48GHz 5.6mW Gate-Level-Pipelined Multiplier Using Single-Flux Quantum Logic by Ikki Nagaoka et al, 2019.

[2187] See Single Flux Quantum (SFQ) Circuit Fabrication and Design: Status and Outlook by V. Bolkhovsky et al, Lincoln Laboratory at MIT, 2016 (34 slides) which provides an interesting view on their manufacturing process and metal layers, and IRDS Cryogenic Electronic and Quantum Information Processing, IEEE, 2021 (93 pages) which provides a good overview of the various SFQ technologies around.

[2188] See The Long Arm of Moore's Law: Microelectronics and American Science by Cyrus Mody, 2017 (299 pages), page 58.

[2189] See Architectural considerations in the design of a superconducting quantum annealing processor by P. I. Bunyk et al from D-Wave, 2014 (9 pages).

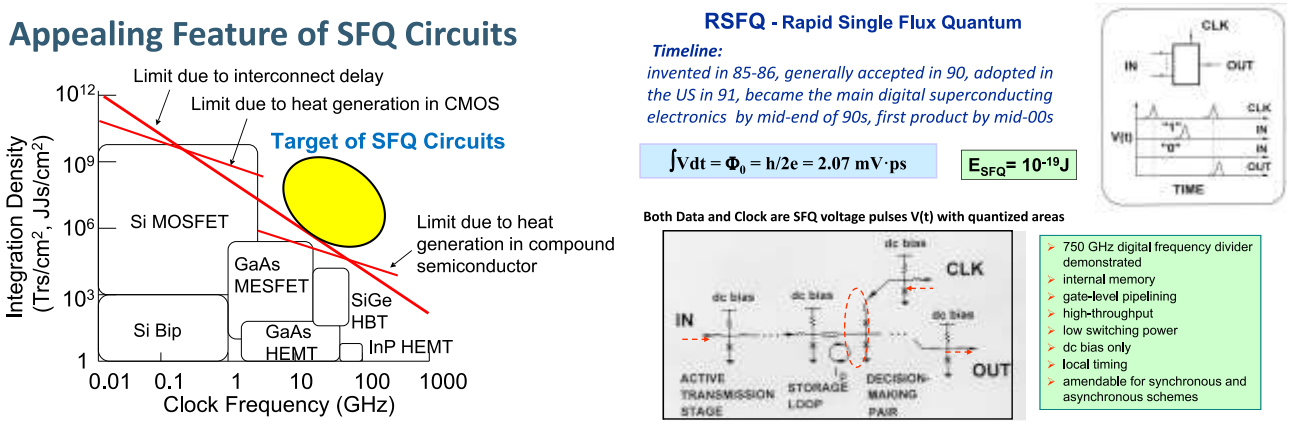


Figure 712: schematic positioning SFQs in terms of clock speed and integration compared to traditional electronic components. Source: Impact of Recent Advancement in Cryogenic Circuit Technology by Akira Fujimaki and Masamitsu Tanaka, 2017 (37 slides).

- **RSFQ** (Rapid Single Flux Quantum) was coinvented in Russia in the mid-1980s by Konstantin K. Likharev and his then-PhD student Oleg Mukhanov. Mukhanov then moved to the USA and joined Hypres in 1991 to launch the industry development of RSFQ. The first ones were produced in the mid-2000s[2190]. They have the advantage of being able to operate up to 750 GHz. They can be used to create ALUs (Arithmetic Logic Units[2191]) running at 20/30 GHz as well as ADCs (analog to digital converters) running up to 40 GHz[2192]. In RSFQ logic, binary information is managed in the form of quantum states of the Josephson junction flux, which is transferred as voltage pulses[2193]. However, the technology does not use state superposition and entanglement as in superconducting qubits. **Hypres** develops radio frequency reception systems using two superconducting components: **SQUID** (Superconducting Quantum Interference Device) based antennas that allow to capture magnetism with precision (invented in 1964) and an RSFQ chipset running at 30 GHz with 11K JJ (Josephson junctions)[2194]!
- **AQFP** (Adiabatic Quantum Flux Parametron) which comprises two superconducting Josephson loops connected together by an inductance, reminiscent of the nSQUID principle[2195]. The process is very energy efficient due to its ability to be reversible. A recent work from Japanese researchers prototypes a AQFP processor using 20,000 Josephson gates operating at 4.2K[2196].
- **RQL** (Reciprocal Quantum Logic)[2197], **eRSFQ** (Energy Efficient RSFQ) and **eSFQ** (Energy Efficient SFQ) are variants of the RSFQ that are more energy efficient due to the absence of bias resistance, replaced by an inductance. This is the variant chosen by Hypres and its subsidiary SeeQC. Their SFQs combine eRSFQs, of which they are the originators, and eSFQs. RQLs are studied to create superconducting memories.

[2190] Source: Single Flux Quantum Logic for Digital Applications by Oleg Mukhanov of SeeQC/Hypres, August 2019 (33 slides).

[2191] See for instance qBSA:Logic Design of a 32-bit Block-Skewed RSFQ Arithmetic Logic Unit, 2020 (3 pages).

[2192] This would be very useful to generate the microwaves to drive superconducting and silicon qubits.

[2193] Time management in logic programming must take this into account. On this topic, see A Computational Temporal Logic for Superconducting Accelerators by Georgios Tzimpragos et al, 2020 (14 pages).

[2194] See Superconducting Quantum Arrays for Wideband Antennas and Low Noise Amplifiers by Oleg Mukhanov et al, 2014 (36 slides).

[2195] See Adiabatic Quantum-Flux Parametron: Towards Building Extremely Energy-Efficient Circuits and Systems, by Olivia Chen et al, 2018 (10 pages) and Design and Implementation of a Bitonic Sorter-Based DNN Using Adiabatic Superconducting Logic also from Olivia Chen et al, 2019 (24 slides).

[2196] See MANA: A Monolithic Adiabatic iNtegration Architecture Microprocessor Using 1.4-zJ/op Unshunted Superconductor Josephson Junction Devices by Christopher L. Ayala et al, December 2020 (14 pages). They provide some impressive cryogenic needs for using this technology at a supercomputing scale.

[2197] See Ultra-Low-Power Superconductor Logic by Quentin P. Herr et al, 2011 (7 pages).

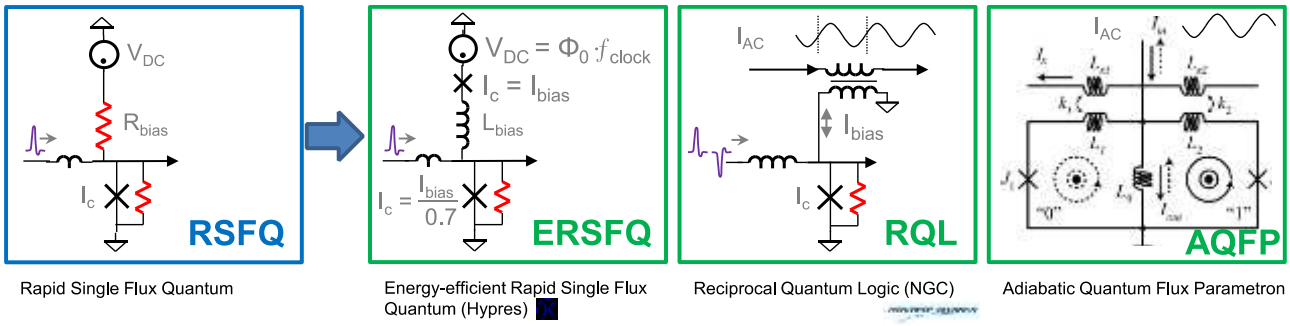


Figure 713: RSFQ and its evolutions, ERSFQ, RQL and AQFP. Source: Single Flux Quantum Logic for Digital Applications by Oleg Mukhanov of SeeQC/Hypres, August 2019 (33 slides).

- **SFETs** (Superconducting FETs, Field Effect Transistors) which implement a concept similar to adiabatic CMOS, but with a superconducting component. These components have been developed since the 1980s[2198].

There are a few other variants of superconducting components that I will just mention (SSV, SVJJ, STTJJ, S3JJ) because they do not seem to be common, on top of JMRAM that is investigated for implementing superconducting memory.

To date, the integration record for this type of component is only 144,000 Josephson junctions in a chipset, realized in a 248 nm integration[2199] if we don't account for D-Wave's Pegasus chipset with its million Josephson junctions including about 10,000 JJs used in their annealer qubits, the rest being used for qubits control logic and digital signals multiplexing/demultiplexing.

Another key component has been developed, superconducting diodes with zero resistance in one direction. They were experimented in 2022 with europium sulfide thin film separating a superconducting aluminum and a normal metal copper layer[2200] and, separately, with niobium bromide placed between layers of niobium diselenide[2201].

In the mid-2000s, the **NSA** invested $400M in the RSFQ over the 2005-2010 period. Its goal was to create a processor with one million logic gates running at 50 GHz. The NSA document describing the project is surprisingly detailed and highly informative. It reveals the scope of the related technological challenges[2202]. In particular, for creating cryogenic memories, superconducting or not: CMOS-Josephson junction hybrid, spintronic based[2203], SFQ or monolithic RSFQ-MRAM. Then the communication between the cryogenic electronics and room temperature components, with a 25 Gbits/s optical fiber that we would probably now reach 100 or 200 Gbits/s, leaving aside the question of the optical signal modulation and demodulation. Cryogenics must be sized to support a large number of components. For testing purpose, a simple pulsed tube would be sufficient but more imposing installations are planned as computing power would grow, as in the illustration in Figure 714: on the right.

[2198] See Josephson Junction Field-effect Transistors for Boolean Logic Cryogenic Applications by Feng Wen, 2019 (7 pages) and Superconducting silicon on insulator and silicide-based superconducting MOSFET for quantum technologies by Anaïs Francheteau, 2017 (153 pages).

[2199] See Advanced Fabrication Processes for Superconducting Very Large Scale Integrated Circuits by Sergey K. Tolpygo, 2015 (43 slides).

[2200] See Superconducting spintronic tunnel diode by E. Strambini et al, Nature Communications, May 2022 (7 pages).

[2201] And The field-free Josephson diode in a van der Waals heterostructure by Heng Wu et al, Nature, April 2022 (17 pages).

[2202] See NSA Superconducting Technology Assessment, 2005 (257 pages). The document is quite old but still very well crafted and interesting.

[2203] See Cryogenic Memory Architecture Integrating Spin Hall Effect based Magnetic Memory and Superconductive Cryotron Devices by Minh-Hai Nguyen et al, July 2019 (12 pages) and Modeling the computer memory based on the ferromagnet/superconductor multilayers by Serhii E. Shafraniuk, Ivan P. Nevirkovets and Oleg A. Mukhanov, July 2019 (27 pages).

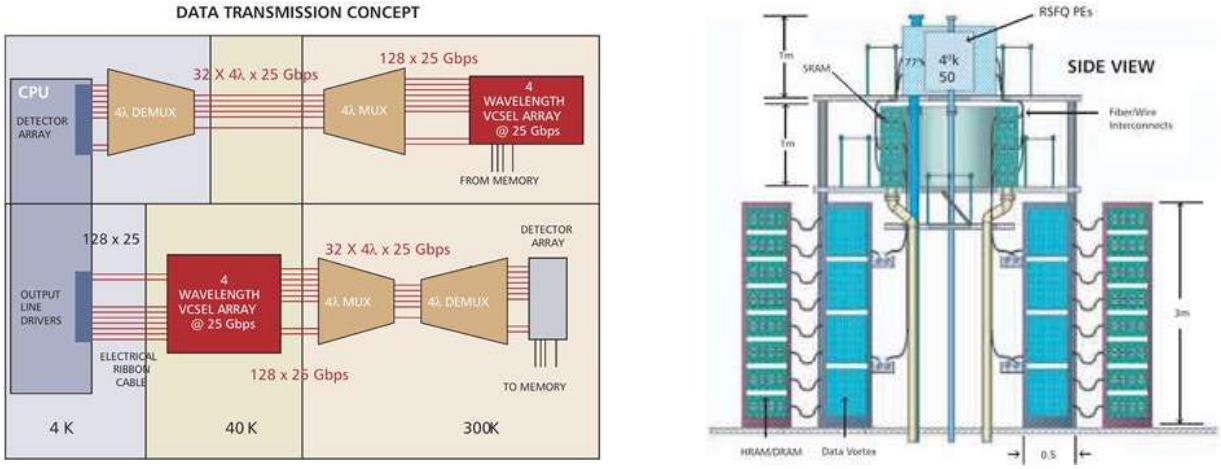


Figure 714: Left: A 64-fiber system for bi-directional transmission totaling 6.4 Tbps between a superconducting processor operating at 4K and high speed mass memory at ambient temperature. Optical connections are shown in red and electrical in black. This technology was to be available by 2010. Right: concept for a large-scale system including cryogenic cooling unit for supercomputers. Source: NSA Superconducting Technology Assessment, 2005 (257 pages), pages 100 and 125.

The project relied mainly on **Hypres,** the only American company entirely dedicated to the creation of superconducting components, who runs its own foundry since 1983, but then divested it to SeeQC and now seems to rely on SkyWater's foundry. They were supplying radio frequency components for military use cases. Out of this, they developed an 8-bit RSFQ processor and 28,000 Josephson junctions.

There is also **Northrop Grumman** with its foundry located in Linthicum, Maryland. Finally, **Chalmers University** in Sweden and various research laboratories in the USA (JPL, Berkeley, Stony Brook) as well as the **NIST** Boulder laboratory were also involved. **IMEC** has a lab in Florida that designs superconducting circuits with densities in the 10 nm to 20 nm range.

TABLE 2-2. SUPERCONDUCTOR RSFQ MICROPROCESSOR DESIGN PROJECTS

Time Frame	Project	Target Clock	Target CPU Performance (peak)	Architecture	Design Status
1997-1999	SPELL processor for the HTMT petaflops system (US)	50-60 GHz	~25G GFLOPS/CPU (est.)	64-bit RISC with dual-level multithreading (~120 instructions)	Feasibility study with no practical design
2000-2002	8-bit RLUX-1 microprocessor prototype (US)	20 GHz	40 billion 8-bit integer operations per second	Ultrapipelined, multi-ALU, multioperation synchronous long instruction word with bit-steering (~ 25 instructions)	Designed, fabricated; operation not demonstrated
2002-2005	8-bit serial CORE1 microprocessor prototypes (Japan)	14-21 GHz 64-bit, 1 GHz system	250 million 8-bit integer operations per second	Non-pipelined, one serial 1-bit ALU, two 8-bit registers, very small memory (7 instructions)	Designed, fabricated, and demonstrated
2005-2015 est.)	Vector processors for a petaflops system (Japan)	100 GHz	100 GFLOPS/CPU (target)	Traditional vector processor architecture	Proposal

TABLE 3.2-2. STATUS OF LOW-LATENCY CRYO-RAM CANDIDATES

Type/Lab	Access Time	Cycle Time	Power Dissipation	Density	Status
Hybrid Si-CMOS (UC Berkeley)	500 ps for 64 kb	0.1 - 0.5 ns depending on architecture	12.4 mW read 10.7 mW write (Single cell writing)	64 kb in < 3x3 mm²	All parts simulated and tested at low speed
RSFQ decoder w/ latching drivers (ISTEC/SRL)	?	0.1 ns design goal	107 mW for 16 kb (Estimate)	16 kb in 2.5 cm² (Estimate*)	256b project completed (Small margins)
RSFQ decoder w/ latching drivers (NG)	?	2 ns	?	16 kb/cm² *	Partial testing of 1 kb block
SFQ RAM (HYPRES)	400 ps for 16 kb (Estimate)	100 ps for 16 kb (Estimate)	2 mW for 16 kb (Estimate)	16 kb/cm² *	Components of 4 kb block tested at low speed
SFQ ballistic RAM (Stony Brook University)	?	?	?	Potentially dense Requires refresh	Memory cell and decoder for 1 kb RAM designed
SFQ ballistic RAM (NG)	?	?	?	Potentially dense Requires refresh	SFQ pulse readout simulated
MRAM (40K)	Comparable to hybrid CMOS	Comparable to hybrid CMOS	< 5mW at 20GHz (Estimate)	Comparable to DRAM (Estimate)	Room temperature MRAM in preproduction; Low temperature data sparse

*Densities of JJ memories are given for the technologies in use at the time of the cited work. Greater densities can be expected when a 20 kA/cm² process is used. The symbol ? signifies insufficient data.

Figure 715: various superconducting electronic projects launched about 20 years ago with processors on the left and cryo-RAM on the right, reminding us how long these projects can last or have their ups and downs. These projects became the C3 IARPA project that lasted until 2022. Source: NSA Superconducting Technology Assessment, 2005 (257 pages), pages 28 and 53.

The **IARPA** agency has taken over with the **Cryogenic Computing Complexity** (C3) project launched in 2014. It involved IBM, Northrop Grumman (Quentin Herr, who works at IMEC in Belgium since May 2021), Raytheon and Hypres and was due to end in 2018[2204].

It actually ended in 2022. A total of $700M were spent in R&D there given the project was considered to be strategic. Some of the showstoppers there were the lack of EDA tools (electronic design automation) adapted to superconducting circuits and of scalable cryogenic cabling (leading to the Supercables project). There are solutions with signals frequency upconvert to optical wavelengths with VCSEL chipsets but these are consuming a lot of energy.

This project was part of the **National Strategic Computing Initiative** (NSCI) launched in 2015 by the White House, which focused on the development of supercomputers. It's difficult to find out what this project has achieved as of 2021.

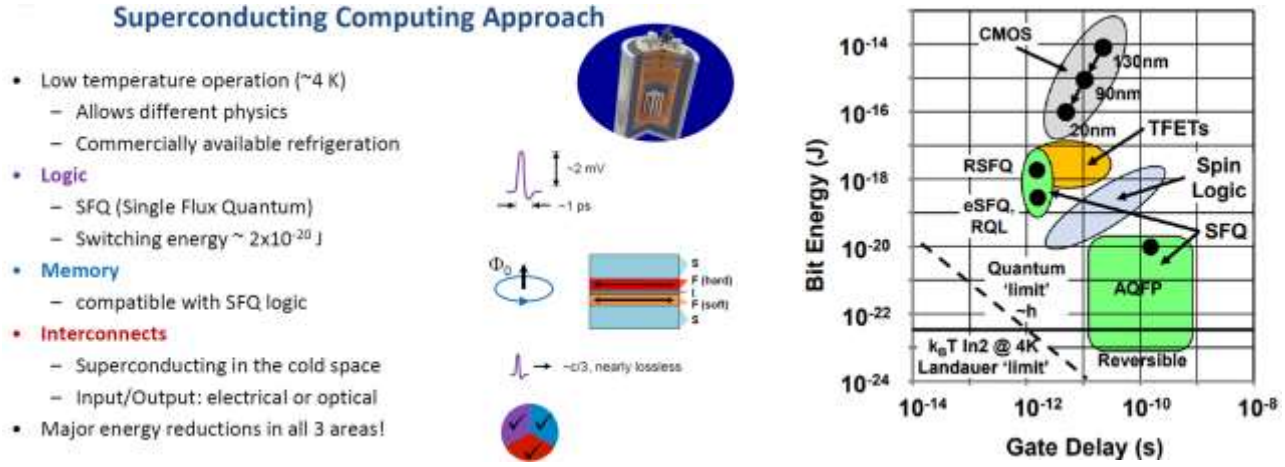


Figure 716: superconducting approach and gate delay. Source: TBD.

In the USA, the **DISCoVER** (Design & Integration of Superconductive Computation for Ventures beyond Exascale Realization) expedition is working on a "SuperSoCC" SFQ-based niobium chipset (superconductive system of cryogenic computing cores) operating at 4.2K. The project is led by Massoud Pedram, Timothy Pinkston and Murali Annavaram from USC. They are working on on-chip memory design and interface between room electronics and cryo-electronics. The team touts a potential energy gain of /100 vs classical computing or 10x speed improvement with the same energy consumption. With a relatively modest funding of $15M coming from the NSF, the project also involves Auburn University, Cornell University, Northeastern University, Northwestern University, University of Rochester and Yokohama National University in Japan.

Outside the USA, the **Japanese Superconducting Computing Program's** ambition in 2004 was to create a processor running at 100 GHz generating 100 GLOPS in SFQ, supplemented by 200 TB of DRAM running at 77K to generate a 1.6 PFLOPS system comprising 16,384 processors.

[2204] See Superconducting Computing and the IARPA C3 Program by Scott Holmes, 2016 (57 slides). All the presentations of the C3 conference are here.

PROCESS	Current density (kA/cm²)	Minimum area (µm²)	Maximum integration	Maximum frequency (GHz)
Hypres #03-10-45	0.03 1.0 4.5	~ 3.14	15,000	80 GHz RnIc=1.3mV @ 4.5 kA/cm²
Hypres #545/100/200	0.1 1 4.5 10 20 30	~ 0.4	10,000	200 GHz @ 30 kA/cm²
MIT Lincoln Lab SFQx	10 20 50	~ 0.06	~ 800,000	240 GHz RnIc=2.17 mV @50 kA/cm²
ADP2	10	1.0	1100 JJ/mm²	80 GHz
STP2	2.5 - 20	0.25 - 4.0	100 JJ/mm² - > 2,000 JJ/mm²	30 GHz - 150 GHz
NGTP	10	1.0	70,000	80 GHz
Fluxonics standard	1	12.5	100 JJ/mm²	40 GHz RnIc =0.256 mV
INRIM SNIS	up to 100	25	1,000 JJ/mm²	300 GHz RnIc >0.1mV - 0.7mV
NIST Nb/Nbx Si1-x/Nb	up to 110	?	70,000	300 GHz
INRIM SNIS 3D FIB	up to 100	0.1	10,000 JJ/mm²	300 GHz RnIc=0.1mV - 0.7mV

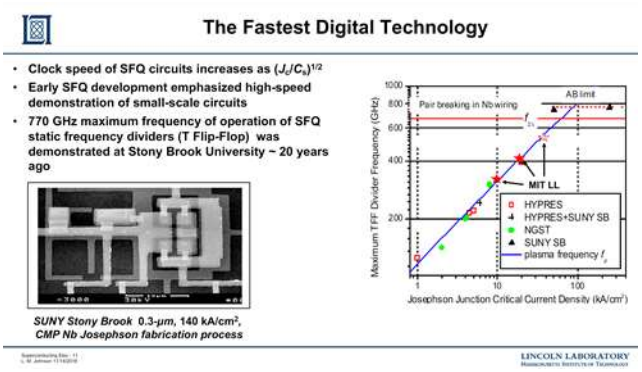


Figure 717: the left table comparing different types of superconducting components comes from Superconducting Computing by Pascal Febvre, CNRS, 2018 (56 slides). The right slide comes from Superconducting Computing and the IARPA C3 Program by Scott Holmes, 2016 (57 slides).

All this with a cryostat consuming 12 MW and generating a thermal power of 18 kW at 4.2K. It has not yet seen the light of day about 17 years later[2205]. Meanwhile, the IBM Summit supercomputer using traditional processors and GPUs generates 200 petaFLOPS consuming 13 MW, so why bother?

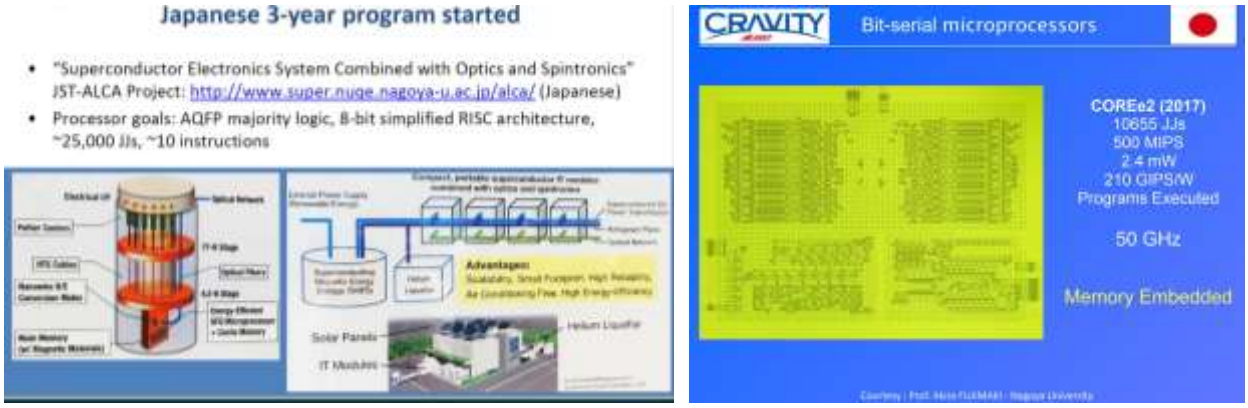


Figure 718: the left slide comes from Superconducting Computing and the IARPA C3 Program by Scott Holmes, 2016 (57 slides) and the right schema comes from Superconducting Computing by Pascal Febvre, CNRS, 2018 (56 slides).

China announced in 2018 a $145M plan to build a superconducting computer by 2022. They had then created a chip with 10,000 Josephson junctions. Not sure they are ready for this milestone. **Russia** also has ambitions in this field[2206].

In **France**, the laboratory CMNE (Micro Nano Electronic Components) of the IMEP-LaHC (Microelectronics, Electromagnetism, Photonics, Microwave) of the UGA (Grenoble) was working in this area, under the responsibility of Pascal Febvre who is based in Chambéry.

In Korea, researchers from **Seoul National University** have proposed another path, creating computers with CryoMOSFET chipsets operating at a relatively hot temperature of 77K, reducing cooling costs.

[2205] They managed to create the CORE1α in 2003 at 4999 JJ (Josephson junctions) running at 15 GHz, the CORE1β in 2006 at 10.955 JJ running at 25 GHz, the CORE1γ with 22,302 JJ also at 25 GHz, the CORE100 in 2015 at 3073 JJ and 100 GHz, the COREe2 in 2017 at 10,655 JJ and 50 GHz with an integrated memory. See Impact of Recent Advancement in Cryogenic Circuit Technology by Akira Fujimaki and Masamitsu Tanaka, 2017 (37 slides). This continued in 2019 with an 8-bit multiplier containing 20,251 JJ running at 48 GHz and consuming 5.6 mW. Source: 29.3 A 48GHz 5.6mW Gate-Level-Pipelined Multiplier Using Single-Flux Quantum Logic by Ikki Nagaoka et al, 2019.

[2206] See The Outlook for Superconducting Computers by R Colin Johnson, 2018.

Its benefits are less impressive than superconducting computing with an improvement of only 41% in single thread performance for the same power budget or a power reduction of 38% for the same performance, all of this including of course the cooling power budget[2207].

In the end, this branch of the superconducting computer industry is for the moment still immature. It has suffered from the uninterrupted advance of Moore's Law until the last few years and the difficulties of its practical implementation. It is not impossible that synergies will develop between quantum computing and this somewhat neglected branch. They can help each other, as can be seen with superconducting circuits for driving superconducting qubits or silicon. As we know, quantum computing will perhaps indirectly revive this sector[2208]!

Probabilistic computing

Probabilistic processors are another variation of exotic processors. They use probabilistic p-bits that can fluctuate rapidly between 0 and 1 with a low transition energy level. They are supposed to allow the resolution of so-called "quantum" problems without relying on quantum mechanisms. p-bits can be realized with nanomagnets and also with regular transistors[2209].

Various applications are promoted such as the creation of neural networks called BSN (Binary Stochastic Neuron) and the resolution of optimization problems similar to those treated by quantum annealing and gate-based quantum computing. The accelerations obtained are not qualified as exponential. It may be just polynomial, which is still interesting.

Work in this direction is quite recent and comes from **Purdue University** in Indiana[2210] and from **Tohoku University** in Japan[2211]. **HawAI.tech** (France), a Grenoble-based startup, is positioned on the same niche and targets applications in the field of AI in embedded systems using data from various sensors[2212]. Their roadmap should lead to the creation of a complete probabilistic computer by 2024.

Optical computing

Many research laboratories and startups are working on the creation of optical processors that are not based on photon qubits. Some are creating classical optical neural networks, others are adapted to convolutional neural networks or spiking neurons, the latter being closest to the way the human brain works. Others are even proposing to solve NP complete problems like Ising models, beyond the coherent Ising model machines I briefly discussed in the part dedicated to photon qubits.

[2207] See CryoCore: A Fast and Dense Processor Architecture for Cryogenic Computing by Ilkwon Byun et al, 2020 (14 pages).

[2208] At last, see this good review paper Beyond Moore's technologies: operation principles of a superconductor alternative by Igor I. Soloviev et al, Russia, 2017 (22 pages). It mentions the potential of a two orders of magnitude gain in energy efficiency with superconducting based supercomputers, cryogenics included. On top of the various variations of SFQ, RQL and SQUID superconducting circuits, the review also covers cryogenic memory. One of the limitations of superconducting circuits is their low potential miniaturization. Josephson junctions density seems limited to 2.5 million junctions per cm^2. To be compared with billions of CMOS transistors with 5nm/7nm nodes!

[2209] See an explanation of p-bits in Waiting for Quantum Computing? Try Probabilistic Computing by Kerem Camsari and Supriyo Datta, IEEE Spectrum, March 2021, then Integer factorization using stochastic magnetic tunnel junctions by William A. Borders et al, 2019, p-Bits for Probabilistic Spin Logic by Kerem Y. Camsari, 2019 (11 pages), Stochastic for Invertible Logic by Brian Sutton et al, 2017 (19 pages) and Probabilistic computing with p-bits by Jan Kaiser and Supriyo Datta, October 2021 (8 pages).

[2210] See From Charge to Spin and Spin to Charge: Stochastic Magnets for Probabilistic Switching by Kerem Y. Camsari et al, February 2020 and Hardware Design for Autonomous Bayesian Networks by Rafatul Faria et al, 2020 (10 pages).

[2211] See Demonstrating the world's fastest spintronics p-bit by Tohoku University, March 2021 and Waiting for Quantum Computing? Try Probabilistic Computing by Kerem Camsari and Supriyo Datta, 2021.

[2212] See Bayes from Cell to Chip by Pierre Bessière, 2018 (33 slides).

Let's mention **reservoir computing** which is a specific category of recurrent neural networks used to process time series (in language processing, finance, energy, robotics)[2213].

Their particularity is to use neuron weights and links between neurons randomly fixed in the reservoirs, all with nonlinear activation functions for these links. The hundreds of neurons in a reservoir are fed by input data stored in the reservoirs.

The activation functions nonlinearity makes this memory evanescent. The training parameters of these networks are located in the weights of the neurons that connect the reservoirs to the output data.

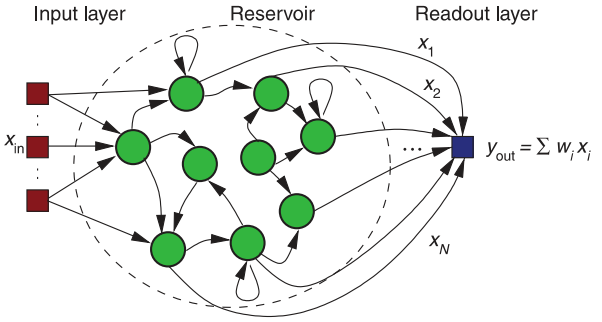


Figure 1: Standard layout of a reservoir computer, comprising an input layer (red), the reservoir (green) with randomized but fixed connections, and the linear readout layer (blue). Here, for simplicity a one-dimensional readout layer is drawn ($l = 1$).

Figure 719: the classical concept of reservoir computing in machine learning. Source: Advances in photonic reservoir computing by Guy Van der Sande et al, 2017 (16 pages) which provides an excellent focus on optronics based reservoir computing.

There are classic reservoir computing projects, rather based on memristors[2214], five types of optical reservoir computing and even quantum versions, for quantum reservoir computing[2215]! A mapping of the different types of optical neural networks is proposed in Figure 720.

We will now focus on solutions based on optical processes using image diffraction from DMD or DLP chips illuminated by a laser and sent on various structures such as random matrices or various metamaterials. They are often based on the principle of the Optical Fourier Transform which allows to decompose a 2D image into spatial frequencies, itself represented in 2D. This transform is an image that contains key points representing shapes and repetitions in the analyzed images.

This can be leveraged to build convolution layers in convolutional neural networks. These serve to detect the presence of shapes in an image, the shapes being represented by filters. The Fourier transform helps to automatically identify these key shapes in the image. These systems capture the result with a CMOS sensor, usually with a very high resolution, much higher than that of the DLP or DMD chip used upstream. The diffraction thus carries out a projection in a space of larger dimension than the original image. All this is supported by serious mathematics[2216] .

[2213] The concept of reservoir computing dates back to 2007. See Toward optical signal processing using Photonic Reservoir Computing by Kristof Vandoorne et al, 2008 (11 pages). It is also described in Novel frontier of photonics for data processing - Photonic accelerator by Ken-ichi Kitayama, 2019 (25 pages) as well as in this beautiful presentation Introduction to Reservoir Computing by Helmut Hauser (282 slides). The notion is different from the one of reservoir engineering.

[2214] See Memristors and Beyond: Recent Advances in Analog Computing by Nick Skuda, 2019 (12 slides).

[2215] See Universal quantum reservoir computing by Sanjib Ghosh et al, from Singapore, 2020 (23 pages) as well as Integrated Nanophotonic Structures for Optical Computing by Laurent Larger et al, 2019 (50 slides). See Experimental photonic quantum memristor by Michele Spagnolo et al, Nature Photonics, March 2022 (7 pages) which describes a way to implement quantum memristors and quantum reservoir computing. As explained in Quantum memristor: A memory-dependent computational unit Quantum memristor bridges conflicting quantum requirements in single device by Chris Lee, ArsTechnica, April 2022, a quantum memristor is a memristor that will change its properties based on the qubit traversing it, in the case of photons. And at last, see Quantum reservoir neural network implementation on a Josephson mixer by Julien Dudas, Erwan Plouet, Alice Mizrahi, Julie Grollier and Danijela Marković, September 2022 (7 pages) which proposes to use a large number of densely connected neurons by using parametrically coupled quantum oscillators instead of physically coupled qubits.

[2216] See An optical Fourier transform coprocessor with direct phase determination by Alexander Macfaden et al, 2017 (8 pages) and Performing optical logic operations by a diffractive neural network by Chao Qian et al, 2020 (7 pages).

These different solutions are in their infancy. They can accelerate certain calculations for training complex neural networks. These accelerations seem to be rather polynomial and not exponential as quantum computing is supposed to generate. Except that they do not seem to be handicapped by noise issues as qubits are.

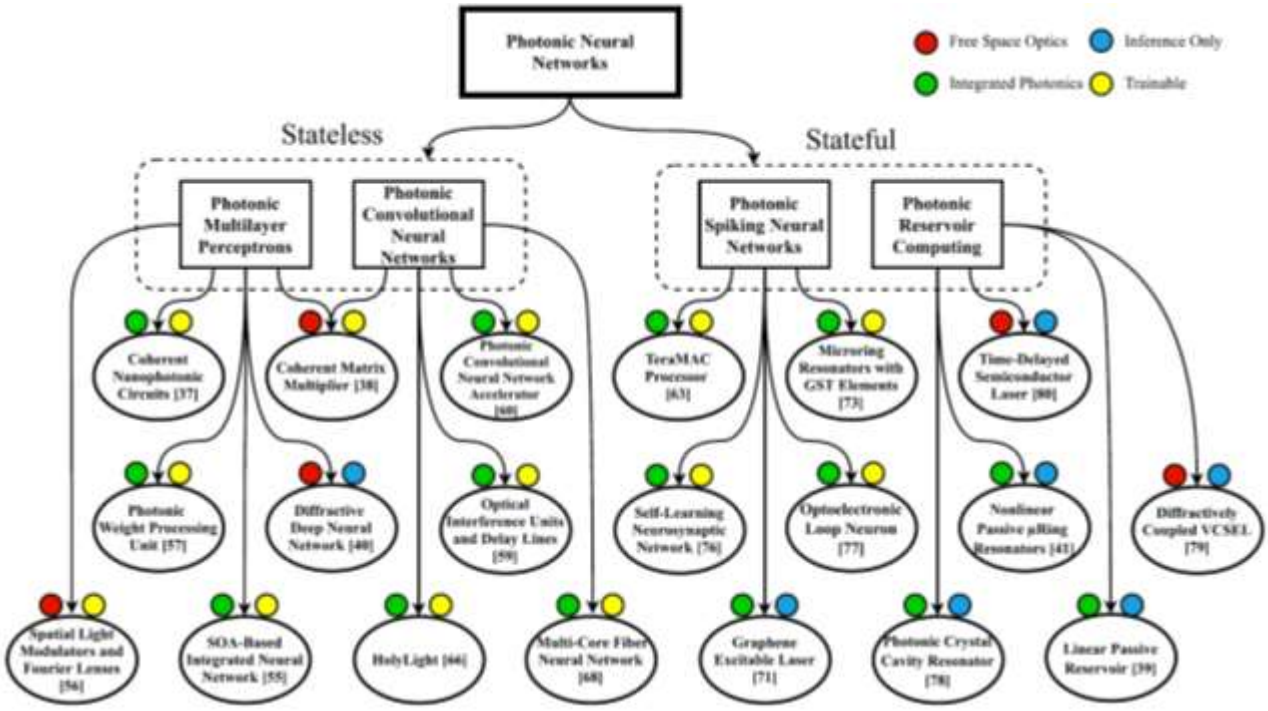


Figure 720: source: Photonic Neural Networks: A Survey by Lorenzo de Marinis et al, 2019 (16 pages).

Let's now have a look at various commercial vendors in this very specific market.

Lighton.io (2016, France, $3.7M) sells an optical coprocessor that accelerates neural networks training on large volumes of training data, such as with convolutional networks.

In their first system, a laser emits a beam that is magnified with some lenses to illuminate a parametrized DLP micromirror chip. The generated image then traverses a static random matrix playing the role of a scattering medium with focusing lenses L1 and L2 before and after the filter as illustrated in Figure 721. A monochrome CMOS imaging sensor then analyzes the resulting image[2217]. The sensor captures the interferences generated by the set and some mathematical computing interprets the result. This process enables a reduction of a complex data set dimensionality.

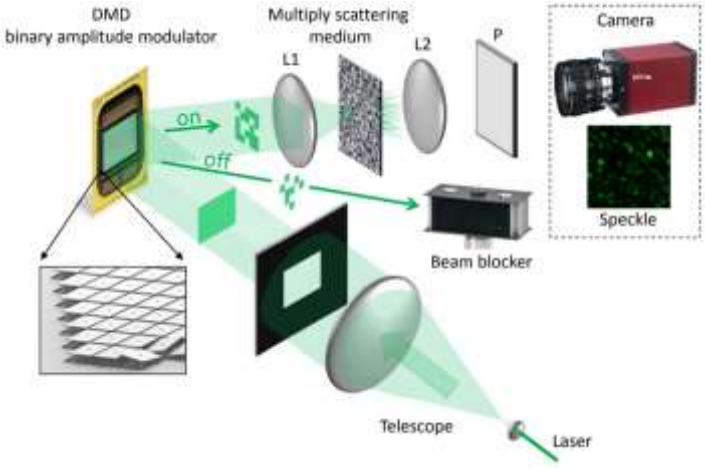


Figure 721: the LightOn optical accelerator architecture. Source: Random Projections through multiple optical scattering: Approximating kernels at the speed of light, 2015 (6 pages).

[2217] The process is described in Random Projections through multiple optical scattering: Approximating kernels at the speed of light, 2015 (6 pages).

The miniaturized device fits in a 2U server. The system computing power comes in particular from the DLP and the CMOS sensor resolutions, which is about several million pixels. Everything is driven by Python libraries developed with TensorFlow. The targeted applications are first and foremost genomics and Internet of Things solutions.

Since 2020, LightOn is also working on creating a photonic processor named QORE using reconfigurable linear optical networks to implement optical quantum information processing using multimode fiber with the programmable wavefront shaping of a SLM (spatial light modulator). It can have up to 8 laser inputs and 38 outputs, with fidelities >93% and losses <6.5dB. The device fits in a standard 19" server rack[2218]. The computing advantage brought by this platform is not obvious. However, its creators indicate that it could create high-dimensional entanglement from few single photon states, so these large photonic cluster states that are the Holy Grail of MBQC. The QORE project was funded as part of the H2020 OPTOlogic project.

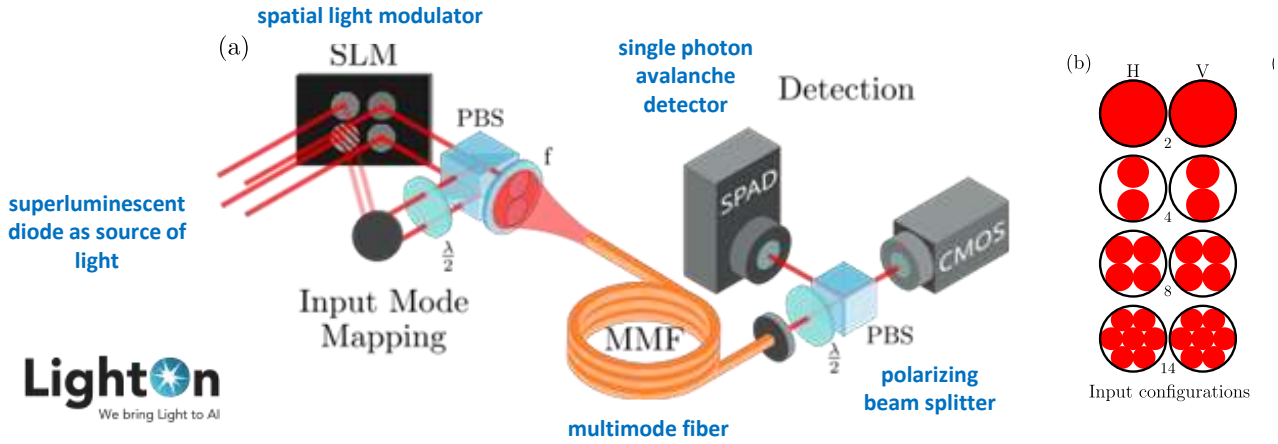


Figure 722: schematic of the Light QORE quantum processor. Source: A high-fidelity and large-scale reconfigurable photonic processor for NISQ applications by A. Cavaillès, Igor Caron, Sylvain Gigan et al, May 2022 (5 pages) with legends by Olivier Ezratty.

Optalysys (2013, UK, $5.2M) is a spin-out of the University of Cambridge created by Nick New, Robert Todd and Ananta Palani. Their FT:X 2000 system is structured around the realization of optical fast Fourier transforms based on diffraction[2219].

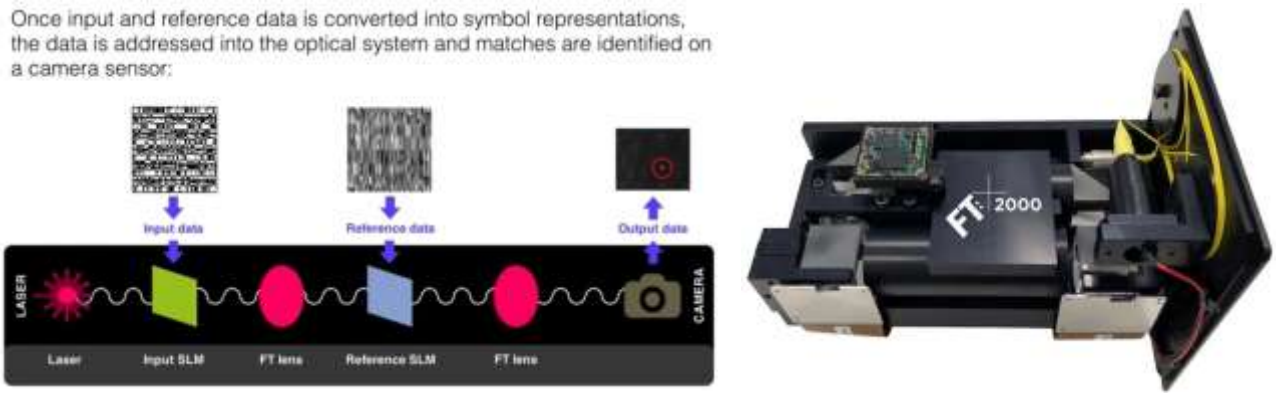


Figure 723: Optalysys process and apparatus. Source: Optalysys.

[2218] See A high-fidelity and large-scale reconfigurable photonic processor for NISQ applications by A. Cavaillès, Igor Caron, Sylvain Gigan et al, May 2022 (5 pages).

[2219] See Optalysys - Revolutionary Optical Processing for HPC, September 2017 (23 mn).

They were involved in various projects, one in genetics to do genome sequence alignment, GENESYS, carried out with the **Earlham Institute**. The other project dealt with weather forecasting for the European center ECMWF and a third one for plasma and fluid dynamics simulation, for DARPA. They also did run a convolutional network in 2018 on a MNIST base with 60,000 letters for training and 10,000 for testing. Its success rate was of only 70%.

Fathom Computing (2014, USA, $2.3M) uses an "electro-optical" architecture capable of training memory and convolutional neural networks (LSTM). Their Light Processing Unit (LPU) would be able to read 90% of the tests from the MNIST handwriting database, using the same test as the one performed by Optalysys.

The system is adapted to linear algebra and matrix multiplication. They still have to miniaturize their device, which according to them should take at least two years, as of 2018. In 2021, it doesn't seem they achieved any result. The startup was launched by two brothers, William and Michael Andregg.

Luminous Computing (2018, USA, $115M) aims to create a high-performance optical component that would replace 3000 Google TPUs! It would exploit multicolor lasers and light guides. According to the publications of their CTO, Mitchell Nahmias, it seems that they use optical spike neurons[2220]. They can perform calculations very quickly, including in classical CMOS.

So, in optical computation, it should be faster. Wait and see, given they are still in a rather stealth mode.

These various startup solutions have so far demonstrated interesting small-scale computing capabilities for ad-hoc needs. What remains to be done is to scale them up and integrate them into computing solutions that are generally hybrid. Efforts are therefore focused both on solutions packaging so that they can be integrated into standard server racks, on scaling the architectures and on development tools.

Let's add to this the **Copac** project funded as part of a H2020 project. Its goal is to create an exotic quantum computing solution that does not exploit qubits. Its ambition is to enable the resolution of data analysis problems such as the simulation of complex systems or machine learning.

The processor would have the capacity to evaluate all the variables of a logical function in parallel. It is based on a quantum dots-based architecture that can be excited simultaneously on several frequencies by wideband lasers. The results are read by 2D spectroscopy of quantum dots. The machine would operate at room temperature. The process mixes classical computation (for the evaluation of functions) and quantum methods (to do it simultaneously on several sets of variables).

The project is conducted with the Universities of Liège (Françoise Remacle), Hebrew University of Jerusalem (Raphael Levine), University of Padua, the CNR Institute for Physical and Chemical Processes of Bari, the company **KiloLambda (**2001, Israel) which manufactures the quantum dots and **ProBayes** (France), a subsidiary of La Poste which produces the compiler of the solution (Emmanuel Mazer and David Herrera-Marti, who now works at CEA-LIST)[2221]. The great uncertainty on this project, as is often the case, concerns its scalability. It depends on the superposition of optical frequencies. The project documentation does not describe well the application domains of the possible in terms of complexity classes of addressable problems.

[2220] See Progress in neuromorphic photonics by Thomas Ferreira de Lima, Mitchell Nahmias et al, 2017 (23 pages).

[2221] See Coherent Optical Parallel Computing, 2017. The European project is funded until 2021. See more details in Coherent Optical Parallel Computing Project Summary.

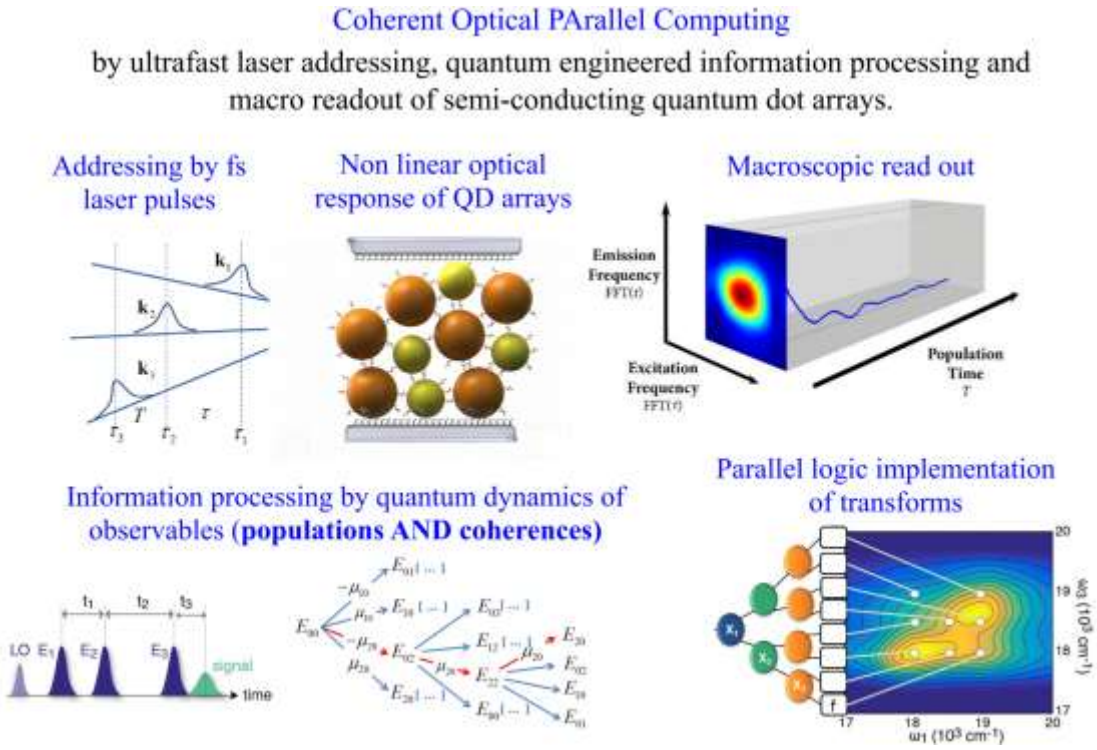


Figure 724: the optical technology behind the European Copac project.

Another collaborative effort in photonic chipsets development is with the **PhotonDelta Foundation** (The Netherlands, 1.1B€ including 470M€ from the Dutch government), a public and private European Integrated Photonics Ecosystem fund that supports photonic chip ventures, in collaboration with the MIT. They invested in 177 projects. The program launched in 2022 is supposed to last 6 years. IMEC, LioniX and Bright Photonics are among the industry partners of this fund which gathers 26 companies, 11 technology partners and 12 R&D partners.

Salience Labs (2021, UK, $11.5M) is a startup cofounded by Vaysh Kewada (CEO) and Johannes Feldmann (CTO) and spun out of Oxford and the University of Münster in Germany.

It develops a hybrid photonic-electronic silicon chip dedicated to AI applications. Other research participants are the Universities of Pittsburgh (USA) and Exeter (UK), EPFL and IBM Research Zurich. It implements fast tensor processing running at 100 GHz. It implements sort-of in-memory photonic computing implementing optical frequency combs coupled with a classical SRAM (Static Random Access Memory)[2222]. They could also use phase-change materials developed by Oxford University instead of SRAM[2223].

Lightelligence (2017, USA, $36M) develops PACE, another photonic processor that is supposed to be 100 times faster than a Nvidia RTX 3080 GPU. It is designed to solve Ising models problems like D-Wave quantum annealers and Fujitsu digital CMOS-based annealers.

[2222] It is documented in Parallel convolution processing using an integrated photonic tensor core by J. Feldmann et al, Nature, January 2021 (35 pages).

[2223] Oxford University researchers designed a light-based silicon photonic chip with hybridized-active-dielectric (HAD) nanowires enabling light polarization-selective tunability. They demonstrated the use of polarization as a parameter to selectively modulate the conductance of individual nanowires within a $Ge_2Sb_2Te_5$ (GST for germanium-antimony-tellurium, a phase changing material also used in RW optical discs and phase-change memories) and silicon multi-nanowire system. See Polarization-selective reconfigurability in hybridized-active-dielectric nanowires by June Sang Lee and al, Science Advances, June 2022 (8 pages).

Their chipset uses 12,000 thermal phase shifters and Mach-Zehnder interferometers (MZI) and runs at 1 GHz[2224]. It implements parallel photonic recurrent network[2225]. Now, how does it scale is yet to be shown.

So, imagine you didn't care about quantum computing because it's too complicated. Just with focusing on this optical classical and sometimes supposedly quantum photonic computing, you'd have to spend a significant amount of time to figure out which ones deserve some attention. It seems that you have many more projects run in parallel than specialists who could benchmark and compare them in a neutral fashion.

Chemical computing

Chemical computing is yet another form of unconventional computing. The underlying physical phenomenon was discovered in 1951 by a Russian chemist, Boris Belousov, with a self-reversible chemical reactions alternating the color of solution mixing salts and acids. It would enable the creation of chemical logic gates. It was thought initially that it broke the second law of thermodynamics (a bit like time crystals…). It was found later that it was not the case and that some form of logic gate could be implemented using this phenomenon and a chemical oscillator that is akin to chemical concentration waves blocking or amplifying each other depending on their setting. One benefit is a low energy consumption[2226].

Research in the domain started to generate some experimental results in 1989 and onwards, particularly in the UK, at EMPA in Switzerland, Stanford, Harvard and the University of Washington. But the benefits of this architecture are not obvious, noticeably due to its relatively slow speed. The most recent work came in 2020 from the University of Glasgow who used 3D-printed programmable chemical processor with a 5 by 5 array of cells filled with a switchable oscillating chemical and magnetic stirrers to control their oscillations and compute binary logic gates to perform pattern recognition[2227]. It can control 2.9×10^{17} chemical states.

The array is programmed with setting chemical relations between these chemical cells. It can implement a chemical autoencoder used for pattern recognition. Now, more comparisons have to be made with classical computing to see how it scales[2228]!

[2224] See Deep Learning with Coherent Nanophotonic Circuits by Yichen Shen et al, October 2016 (8 pages) and Accelerating recurrent Ising machines in photonic integrated circuits by Mihika Prabhu et al, Optica, April 2020 (8 pages). It seems the system can parametrize an Ising model only with coupling graph nodes with the equivalent of a longitudinal field, but not with setting longitudinal interactions at the graph node level like with D-Wave quantum annealers.

[2225] The system implements hybrid photonic/classical computing with the photonic part performing a unitary matrix product of a state-preparation rotation matrix R, the desired unitary (U or U†), and one of two homodyne detection matrices (h1 or h2). Phase-intensity reconstruction, a diagonal matrix multiplication, Gaussian noise addition, and a nonlinear threshold unit are performed classically.

[2226] See Chemical Computing, the Future of Artificial Intelligence by Javier Yanes, January 2019.

[2227] See A programmable chemical computer with memory and pattern recognition by Juan Manuel Parrilla-Gutierrez, Lee Cronin et al, Nature Communications, March 2022 (8 pages).

[2228] See the video The First Programmable Turing Complete Chemical Computer with Lee Cronin from the University of Glasgow (1h11mn).

Quantum unconventional computing key takeaways

- We study various non-conventional computing technologies that may compete with quantum computing or even be of some help, like reversible and superconducting technologies that may be useful to create cryogenic electronics enabling the creation of scalable quantum computers. But these technologies are so diverse and with different underlying science that they would deserve a lot of time and energy to be properly evaluated and benchmarked with both physicists and computer science specialists.
- Digital annealing computing is mostly proposed by Japanese companies like Fujitsu and Hitachi, using classical CMOS chipsets. These solutions are supposed to solve untractable problems faster than classical-classical computers but their scalability remains questionable.
- Reversible and adiabatic computation has been researched for a long time and has not yet turned into commercial products. It could probably be more interesting to create energy saving solutions more than faster solutions with some potential use case in quantum computing enabling technologies.
- Superconducting computing is an interesting area of research to create more energy efficient supercomputers, despite the cooling cost that, hopefully is not as expensive as with superconducting qubits quantum computers. There are synergies between this research area and superconducting logic electronics that could be used to control superconducting and quantum dots spin qubits at low temperatures.
- Probabilistic and optical computing are interesting research areas. These solutions may be competitive to solve particular problems.
- Optical processors are mainly used in the deep learning space, to accelerate the training and inferences in some layers of convolutional networks.
- Chemical computing is one of the many other areas in unconventional computing that may be interesting but have probably various scaling limitations.

Quantum telecommunications and cryptography

Quantum telecommunications cover a wide spectrum of use cases including quantum communications between quantum sensors, quantum computers and quantum key distribution used in cryptography. Some but not all of these technologies are based on using photon entanglement and quantum teleportation as resources. The field started to develop experimentally and industrially with quantum cryptography. It is already being deployed experimentally or at large scales like in China, while quantum telecommunications associated with quantum computers is still in its infancy.

Interest in quantum cryptography (using various quantum effects like measurement randomness and/or entanglement as resources to generate identical secured encryption keys between two communication endpoints) as well as in post-quantum cryptography (classical cryptography using techniques that are resilient to attacks by quantum computers) were triggered by the creation of Shor's algorithm in 1994. It theoretically enables integers factoring on a quantum computer in reasonable times, provided large scale quantum computers are available. This algorithm has been destabilizing computer security specialists since the advent of the first programmable quantum processors in the early 2000s and related scale-up promises and forecasts. It would make it possible to break the codes of many public key cryptography systems that are commonly used on the Internet. It is still highly hypothetical because quantum computers capable of executing Shor’s algorithms for RSA-2048 keys and requiring millions of high-fidelity qubits are really far in the distant future at best.

Once they are aware of the threat, however, governments, counterintelligence, intelligence and sensitive industries become seriously concerned or at least interested. The threat of quantum computing on cybersecurity even touches critical parts of the Bitcoin and Blockchain signatures and some proof of work protocols. Even though the threat is quite remote, the readiness inertia to counter this potential quantum threat means, for some, that it is necessary to launch it now.

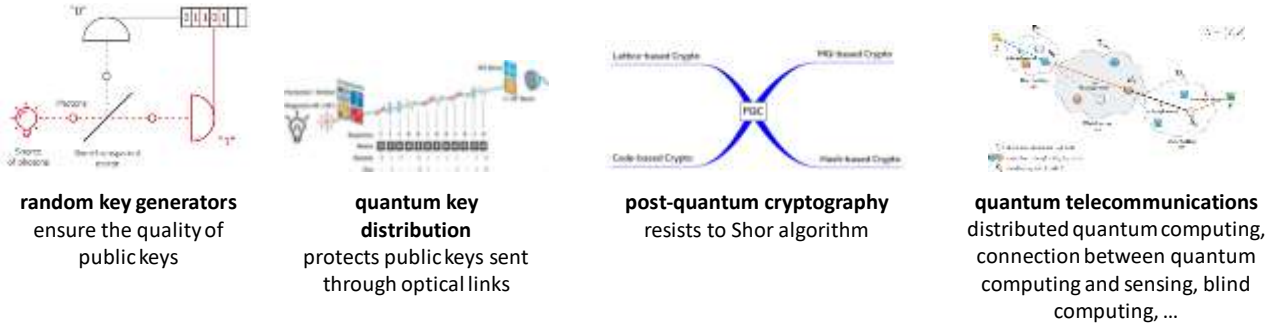
Even before Shor's phantom menace materializes, the cyber security industry started to prepare countermeasures. The markets affected first will be the IT and telecommunications industry in general, which will have to update many software and hardware offerings, financial institutions, the energy sector, healthcare, and government utilities and the military.

In this part, we will describe:

- The basic principles of classical cryptography, in particular **public key cryptography,** with the example of RSA public keys.
- The **nature of the threat** coming from integer factoring and other quantum algorithms and the cryptographic solutions involved.
- **Quantum random number generators** which have become an indispensable complement to classical cryptographic solutions and also quantum cryptography as well.
- **Quantum Key Distribution** based systems that secure the physical part of communications for the safe distribution of random symmetric keys.
- **Post-Quantum Cryptography** that is used to distribute public encryption keys using classical computation that are resilient to codebreaking done by quantum computers.
- **Quantum telecommunications** applications, outside of those related to cryptography, and in particular for the creation of distributed quantum computing systems.

- **Quantum Physical Unclonable Functions** which are sitting in between QRNG, embedded systems and cryptography.
- **Vendors** in these sectors around the world, in a market that already includes many players and in particular many startups.

Encryption and cryptography involve mathematical concepts that are not always obvious. I'll share with you here what I have been able to understand about it and make is as accessible as possible.



random key generators
ensure the quality of public keys

quantum key distribution
protects public keys sent through optical links

post-quantum cryptography
resists to Shor algorithm

quantum telecommunications
distributed quantum computing, connection between quantum computing and sensing, blind computing, …

Figure 725: the four classes of technologies covered in this part. (cc) Olivier Ezratty, 2020.

Public key cryptography

Cryptology is the science of secrets. It allows the transmission of sensitive information between a transmitter and a receiver in a secure manner. Cryptology includes cryptography, which secures transmitted and stored information, and cryptanalysis, which seeks to decrypt it by attack, or code breaking.

In the case of asymmetric public-key cryptography, encryption uses only public keys and decryption uses both public and private keys. Code-breaking exploits only the public keys, while trying to deduce the private keys through intensive computing.

Cryptography secures transmitted information in several ways:

- **Confidentiality**: only the recipient can retrieve the unencrypted version of the transmitted information.
- **Integrity**: the information has not been modified during its transmission.
- **Authentication**: the sender and receiver are who they claim to be.
- **Non-repudiation**: the issuer cannot deny having transmitted the encrypted information.
- **Access control**: only persons authorized by the issuer and the recipient can access unencrypted information.

Before computer telecommunications, confidentiality was ensured by the knowledge of a common secret between transmitters and receivers, the encryption and decryption codes, which could be the position of the wheels of a German Enigma machine during the World War II. This worked in closed environments such as for military communications or between embassies and their home countries.

With Internet communications, this modus operandi is inapplicable for consumer applications and for business relationships in general. Hence public key cryptography systems, such as RSA, which enabled most open Internet data exchanges. There are still highly protected systems using private and symmetrical keys, mainly used in government related applications (army, security, intelligence) as well as in various other cases (some file transfers, email encryption, server/client exchanges, in smart cards and associated payment terminals).

Asymmetric (public-key) cryptography is also exploited for pre-establishing common encryption keys between users of private-key systems, for managing the integrity of communications, and for authentication as in the TLS Internet protocol. Sensitive information is then encrypted with these keys and a symmetrical AES-type algorithm. AES is used to encrypt communications in WhatsApp, Messenger and Telegram. These applications often also use asymmetric cryptography for authentication, key exchange and communication integrity management. Asymmetric cryptography is very flexible while symmetric cryptography is more computationally efficient.In many cases, symmetric cryptography systems coexist with asymmetric (public key) cryptography systems. As a result, when you communicate securely over the Internet, different complimentary security protocols are activated.

With public key systems, different keys are used for encryption and decryption of the information transmitted, so that it is very difficult (if not sometimes impossible) to guess the private decryption key from the public encryption key. The message receiver sends its public key to the sender, who in turn uses it to encrypt the message. The receiver uses the private key that was kept to decrypt the received message. As explained in Figure 726, the private key is never transmitted. This is also called a PKI, for "Public Key Infrastructure".

The **RSA** cryptography system is the most widely used system for protecting public key information transmissions over the Internet. It was created in 1978 by **Ron Rivest** (1947, American), **Adi Shamir (**1952, Israeli) and **Leonard Adleman** (1945, American).

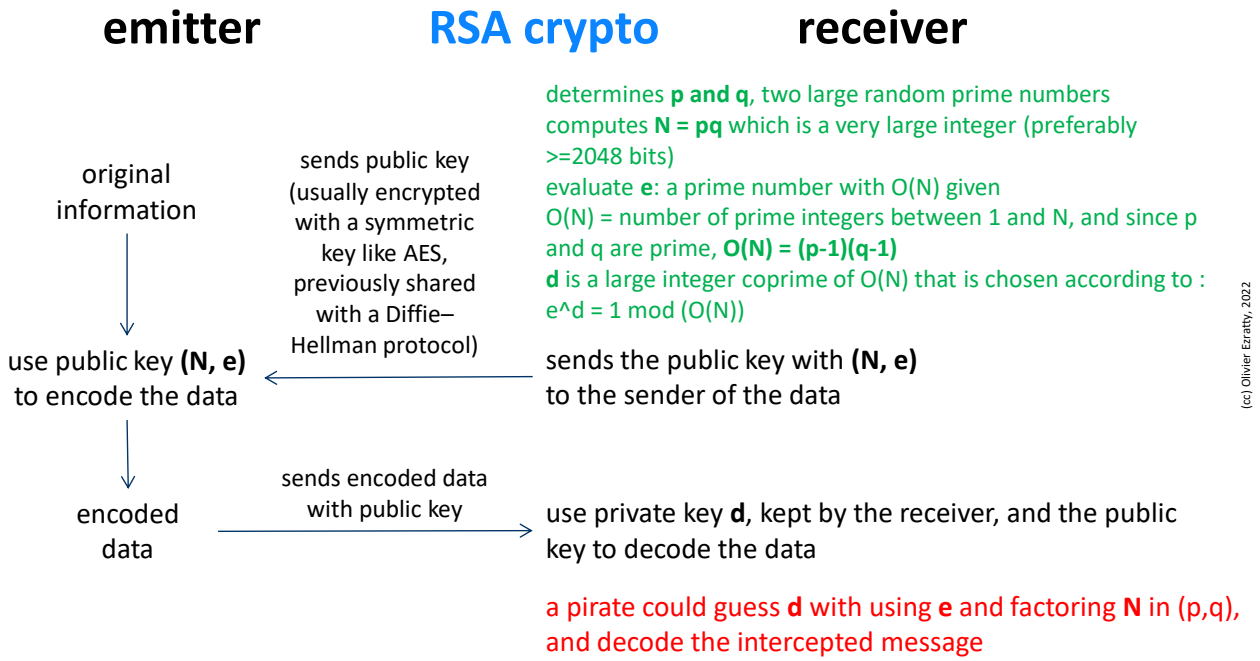


Figure 726: description of the RSA key generation process. (cc) Olivier Ezratty, 2022.

You don't necessarily need to understand the following that explains how keys are constructed. It starts by determining p and q, two large random prime numbers, with a "good" random number generator. We will see later that quantum physics can be used to create really random numbers. We calculate N = pq which is a very large integer. A good RSA key requires to have N stored on at least 2048 bits knowing that the NSA recommends 3072 bits keys for critical applications.

We then evaluate **e**, a prime number by exploiting O(N) which equals the number of prime integers between 1 and N relative to N, and which, as p and q are prime, equals (p-1)(q-1). d is a large integer which is co-prime of O(N) and is chosen according to: e^d = 1 mod (O(N)). At the end, we get a public key that includes the integers N and e, and a private key that includes d. All of this is based on the theory of numbers and uses in particular the Fermat's little theorem and Euler's theorem which make it possible to create two distinct keys that are the inverse of each other.

With that, anyone can encrypt a message using the public key and this message is being decipherable only by the person who has the private key that splits the public key into primitives.

A hacker could decrypt the information sent by intercepting e (the end of the public key) and factoring N, the other end of the public key, into the integers p and q, and then rebuilding the private key d from it.

To date, prime number factoring requires a traditional machine power that grows with the square root of the number to be factorized. The official RSA key factoring record was 768 bits in 2010, 795 bits in 2019 and 829 bits in February 2020[2229]. Even if this doesn't take into account undisclosed NSA records, it provides an idea of the problem scale. We're far from having a classical computer breaking an RSA 2048 bits code given the problem size is exponential with the size of the RSA key.

In the symmetric key realm, you'll find encryption systems using protocols like AES with usual keys of 256 bits, that is in use since 2001. These keys are shared by two parties in a channel and time that can be different from the encrypted data transmission. The best symmetric key system is called the "one time pad" with key size equaling the size of the encrypted data. It means that the key can be very large depending on the data size. But this is the best secured system. It however requires the ability to create a random and totally unpredictable key.

Quantum cryptoanalysis threats

The diagram below in Figure 727 points out the main encryption algorithms vulnerable or not to known quantum algorithms[2230]. Broadly speaking, common public key encryption systems are vulnerable. Only post-quantum cryptography systems are supposed to be resilient. But things are moving fast and some SIDH, lattice and multivariate keys are now classically broken!

Figure 727: what key generation services are quantum safe or not. Source: NIST.

[2229] This factorization of an RSA-250 digits (829 bits) and the previous RSA-240 digits (795 bits) was achieved by an international team led by French researchers from Inria: Fabrice Boudot (Université de Limoges), Pierrick Gaudry (CNRS), Aurore Guillevic, Emmanuel Thomé and Paul Zimmermann (Inria) and Nadia Heninger (University of California). Computation used 2700 core-years, of Intel Xeon Gold 6130 CPUs running at 2.1 GHz. See The State of the Art in Integer Factoring and Breaking Public-Key Cryptography by Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé and Paul Zimmermann, June 2022 (9 pages) and Factoring RSA-240 and computing discrete logarithms in a 240-digit prime field with the same software and hardware by Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé and Paul Zimmermann, Inria, March 2021 (87 slides).

[2230] Seen in IDQ: Quantum-Safe Security relevance for Central Banks, 2018 (27 slides) and slightly supplemented by some captions.

Shor's phantom menace

Peter Shor**'s** algorithm sparked interest in quantum computing when there was even no single working qubit around that was controllable by quantum gate! Shor's algorithm enables theoretically to factor integers in a reasonable time that is proportional to their logarithm. It is thus a factorization in a linear time as a function of the number of key bits. This could be detrimental to all public key-based cryptography[2231].

But this will happen only in a relatively distant future! In 2019, Google researchers published an algorithm allowing to quickly break an RSA key (of 2048 bits) and with "only" 20 million qubits having an error rate of 0.1% and with a calculation lasting 8 hours. This is more "acceptable" than the billion qubits that were needed in previous instances of Shor's algorithm. Today's quantum computers have a coherence time much shorter than a second, but the decoherence counter is reset after each error correction code that is used in the algorithm[2232].

Breaking a 2048-bit RSA key requires at least a number of logical qubits equal to twice the size of the key used +2, so 4098 qubits. Depending on the technologies used, this number should be multiplied by 30 to 20,000 for the number of physical qubits. This scalability is one of the greatest challenges for building viable quantum computers as we've seen in other parts of this book.

Moreover, as we have seen in the section on Shor's algorithm, the quantum Fourier transform underlying it uses phase controlled R-quantum gates whose implementation is far from obvious. Indeed, when the phase is an angle of 1/2048 times a 360° turn in the Bloch sphere of a qubit, the controlled rotation of the phase can be inferior to the error rate of a one or two-qubit quantum gate. We must therefore bet on the ability of error correction codes to handle this.

Is the threat assessment misplaced? At this point in time, the biggest number ever factored on a gate-based quantum computer with Shor's algorithm is 35, with an IBM QPU[2233]. Using a hybrid Variational Quantum Factoring algorithm itself based on a QAOA algorithm, Zapata Computing factored the number 1,099,551,473,989 (=1,048,589 multiplied by 1,048,601) with 5 IBM superconducting qubits in 2021[2234]. Meanwhile, the largest number factored on a D-Wave 2000Q annealer was achieved in 2019 was 376,389 using a block multiplication table method [2235].

A 762-bit RSA key close to the 2010 record would require a **D-Wave** annealer computer with 5.5 billion qubits, far from the existing 5000[2236]. A D-Wave of 5893 qubits could do the job if all qubits could be arbitrarily coupled to the other, which is not possible due to the way these 2D chipsets are designed. And trapped ions and their any-to-any connectivity won't save us since they don't seem to scale. Also, we shouldn't discount threats from quantum machine learning algorithms[2237].

[2231] See this presentation which describes in great detail how Shor's algorithm works: On Shor's algorithms, the various derivatives, their implementation and their applications by Martin Ekerå, 2019 (135 slides).

[2232] See How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits by Craig Gidney and Martin Ekerå, 2019 (25 pages).

[2233] See An Experimental Study of Shor's Factoring Algorithm on IBM Q by Mirko Amico, Zain H. Saleem and Muir Kumph, 2019 (10 pages).

[2234] See Analyzing the performance of variational quantum factoring on a superconducting quantum processor by Amir H. Karamlou et al, npj, Zapata Computing October 2021 (6 pages).

[2235] See Breaking RSA Security With A Low Noise D-Wave 2000Q Quantum Annealer: Computational Times, Limitations And Prospects by Riccardo Mengoni et al, Cineca, 2019 (8 pages).

[2236] According to High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: Application to the experimental factorization of 291311 by Nike Dattani, Xinhua Peng and Jiangfeng Du, June 2017 (6 pages).

[2237] See Capgemini and Fraunhofer IAIS lead study in quantum machine learning for it security commissioned by the German Federal Office for Information Security, November 2021.

Shor's menace was visualized in the diagram in Figure 728 from the European standardization organization ETSI[2238], based on very optimistic predictions on QPUs capabilities to exploit Shor's algorithm.

The orange part of the graph should be shifted into the future by at least 10 to 20 years, showing how the threat is usually exaggerated by cybersecurity specialists who are not aware of the various difficulties to create scalable quantum computers.

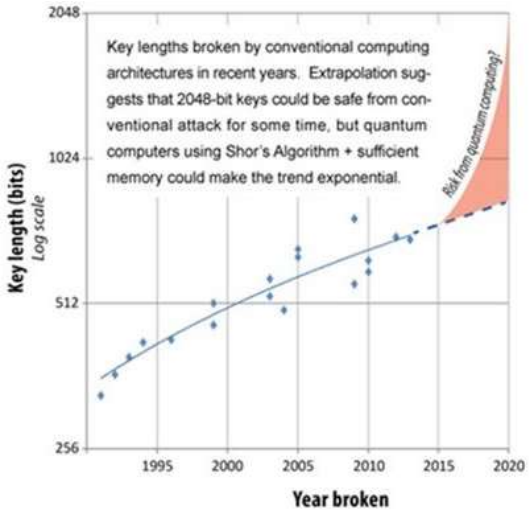


Figure 728: how Shor's risk is usually overestimated with a past example. Source: Quantum Safe Cryptography and Security, 2015 (64 pages).

Shor's algorithm applied to RSA public key breaking could however have quite a negative impact on most Internet security since being integrated in the **TLS** and **SSL** protocols that protect websites and file transfers via **HTTPS** and **FTP**, in the **IPSEC** protocol that protects IP V4 in the IKE sub-protocol, in the **SSH** protocol for machines remote access and in the **PGP** protocol that is sometimes used to encrypt emails. RSA and derivatives are also used in many **HSM** (Hardware Security Modules) such as in cars ECUs (Electronic Central Units)[2239].

The threat also deals with software **electronic signatures** and therefore their automatic updates, **VPNs** used for remote access to protect corporate networks, email security with **S/MIME,** various **online payment** systems, **DSA** (Digital Signature Algorithm, an electronic signature protocol), **Diffie-Hellman** codes (used for sending symmetrical keys) as well as **ECDH, ECDSA** and **3-DES** elliptic curve cryptography. The **Signal** protocol used in WhatsApp would also be in the spotlight. So a lot of Internet security is more or less in the line of sight.

ECC (Elliptic Curve Cryptography) is the first algorithm with elliptic curves, created in 1985 by Neal Koblitz and Victor Miller. The most common variants today are **ECDH** (Elliptic-curve Diffie-Hellman) and **ECDSA** (Elliptic Curve Digital Signature Algorithm, launched in 2005).

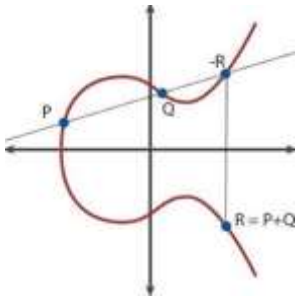


Figure 729: an elliptic curve.

These variants were deployed from 2005 and more widely only from 2015, so 30 years after the creation of the first ECC! Incidentally, the elliptic curves allowed Andrew Wiles to demonstrate the Fermat's last theorem in 1992, which has nothing to do with cryptography[2240].

One of the interests of elliptic curve-based codes is to use shorter public keys than with RSA encryption. But these elliptic curves are also theoretically breakable with quantum computing with a reasonable time because of our friend Peter Shor and the resolution of the discrete logarithm problem (DLP) [2241]. Moreover, an ECDSA backdoor was revealed by Edward Snowden in 2013, housed by the NSA in its Dual EC DRBG random number generator and not in the elliptic curve itself.

[2238] See Quantum Safe Cryptography and Security, 2015 (64 pages).

[2239] See Post-Quantum Secure Architectures for Automotive Hardware Secure Modules by Wen Wang and Marc Stöttinger, 2020 (7 pages).

[2240] As in Elliptic curves cryptography and factorization (86 slides).

[2241] As documented in Shor's discrete logarithm quantum algorithm for elliptic curves by John Proos and Christof Zalka, 2003 (34 pages). The discrete log problem consists in finding an integer k verifying a^k = b modulo p, a, b and p being known integers. This allows to break the elliptic and Diffie-Hellman curve keys.

It was then recommended by NIST in 2014 and NSA in 2015 for the transmission of sensitive information[2242].

The other reason for alternative cryptography solutions is that today's sensitive communications can be stored for a long time by private or state hackers, and exploited much later, when quantum computers are up to the task. This category of attack is named **Store Now, Decrypt Later** (SNDL). Some present day information may have some value later, whether it is financial transactions, private communications, trade secrets or other state secrets. And forward secrecy, a feature used to protect the transport layer like SSL used with HTTPS with separate keys for each session, is not enough against quantum computing-based attacks. Quantum computing is thus a veritable Damocles sword whose fall is difficult to predict and rather distant in time by at least a very long decade. Beyond that time, it is almost impossible to make educated predictions.

Many predictions are entirely wrong whether they talk about a "quantum apocalypse[2243]", an equivalent of a "nuclear threat"[2244] or when some folks predicted in 2020 that the Bitcoin security would be broken by 2022[2245]. They were confusing physical and logical qubits requirements among other mistakes! The same mistake was reiterated a year and a half later with a cybersecurity poll[2246]. The main issue with these polls is that they are asking a question to cybersecurity specialists and other commentators who have no clue about the scalability challenges of quantum computing[2247]. And that's true as well for a former NSA director[2248]! The same could said about the interpretation of a 2021 paper by Nicolas Sangouard et Elie Gouzien which stated that theoretically, a RSA-2048 key could be broken by "only" 13,436 physical qubits in 177 days provided it could exploit a 40 million modes quantum memory that is even more long term than 13,436 physical qubits[2249].

Only a few analysts think that the quantum threat is overestimated[2250]. It is the result of a mix of an unbalanced knowledge of the actual quantum threat between quantum information and cybersecurity specialists. On top of that, cybersecurity vendors have a natural interest to increase the threat perception, in order to sell PQC-based upgraded security solutions[2251]. There's a nice potential market to address with $10B by 2030[2252]. So, if quantum computers were able to scale to a point to break today's asymmetric cryptography, it would indeed create a quantum apocalypse. The question is whether it is realistic or not. There is a bigger risk to kill all electronic devices with solar flares than asymmetric cryptography with a large scale quantum computer.

[2242] See Ben Schwennesen's Elliptic Curve Cryptography and Government Backdoors, 2016 (20 pages).

[2243] See What is the quantum apocalypse and should we be scared? by Frank Gardner, BBC, January 2022.

[2244] See 'Nuclear Threat to Cybersecurity' — Post-Quantum Cybersecurity Rapidly Gains Attention of U.S. Congress, Administration by Matt Swayne, The Quantum Insider, July 2022.

[2245] See Quantum computers could crack Bitcoin by 2022 by Robert Stevens, May 2020.

[2246] See Cybersecurity Experts Say Quantum, Advanced Technology Will Break Standard Encryption Within Two Years by Matt Swayne, The Quantum Insider, December 2021.

[2247] One good example is this paper Quantum Computing Threatens to Collapse the Grid by Alexander Boulden, December 2021 that forecasts doomsday for grid management due to quantum computing threat on cybersecurity. The chart from Statistica/CBinsights is both false and outdated, showing three qubit systems that never worked: Intel 49 superconducting qubits, Google's Bristlecone 72 qubits (it ended up being 53 functional qubits with Sycamore in 2019) and Rigetti's 128 qubits that were announced in 2018 and never released. They are up to 80 qubits as of 2022.

[2248] See Podcast with Adm. Mike Rogers - former NDA director by Yuval Boger, March 2022.

[2249] See Factoring 2048-bit RSA Integers in 177 Days with 13436 Qubits and a Multimode Memory by Nicolas Sangouard and Élie Gouzien, September 2021 (20 pages).

[2250] See Quantum Cryptanalysis: Hype and Reality by Chris Jay Hoofnagle and Simson Garfinkel, February 2022 think that the quantum cybersecurity threat is overestimated.

[2251] See The race to save the Internet from quantum hackers by Davide Castelvecchi, Nature, February 2022.

[2252] See The Quantum Insider Report Forecasts Quantum Security Market Worth $10 Billion by 2030, February 2022.

The fear is also fueled by governments' paranoia and the global fight between the USA and China for quantum technology dominance. On top of that, a lot of myths abound about the NSA and its capabilities, up to many folks thinking that this organization already owns an RSA-breaker QPU in its datacenters. While you can never efficiently prove that something doesn't exist, a good understanding on the scalability challenges with quantum computing make serious people think this thing is just a bad nightmare. But if the cost of getting protected against this potential threat it is reasonable, then it makes sense to implement PQC solutions.

Mosca's inequality

Michele Mosca created an inequality that explains the time risk. It is expressed in the form $D+T>G_c$, where D is the length of time during which today's data circulating in encrypted form must be secured, T, the time needed to make my transition from its encryption systems to solutions resistant to quantum computing, and G_c, the time it will take to develop quantum computers capable of breaking the public keys of current encryption systems. You specify D. You can plan for T according to your information systems and available commercial solutions and standards. How about G_c? You must evaluate it with your gut feeling because current estimates span from 5-10 years to... never! For example, some researchers from the UK and USA tried in 2020 to predict when a FTQC would show up[2253]. With a sort of logistic regression, their model predicted that proof-of-concept fault-tolerant quantum computers will be developed between 2026 and 2033 with 90% confidence with the median in early 2030, and that RSA-2048 Shor attacks will become feasible between 2039 and 2058 with a 90% confidence and median in 2050. Making predictions with such a method for a 30 year timeframe seems preposterous.

Michele Mosca and Marco Piani from evolutionQ publish a report every year collecting the opinion of 46 respondent experts on the potential advent of a quantum threat to public-key cryptography. The 2021 edition seems to showcase similar results as in the 2020 edition[2254]. We see a broad spectrum ranging from 3 experts thinking that it would materialize in fewer than 5 years and most of them thinking it would do so before 30 years. My take is that the best prediction one should make is: "*we don't know*"! And when you are paranoid, it easily becomes "*who knows?*".

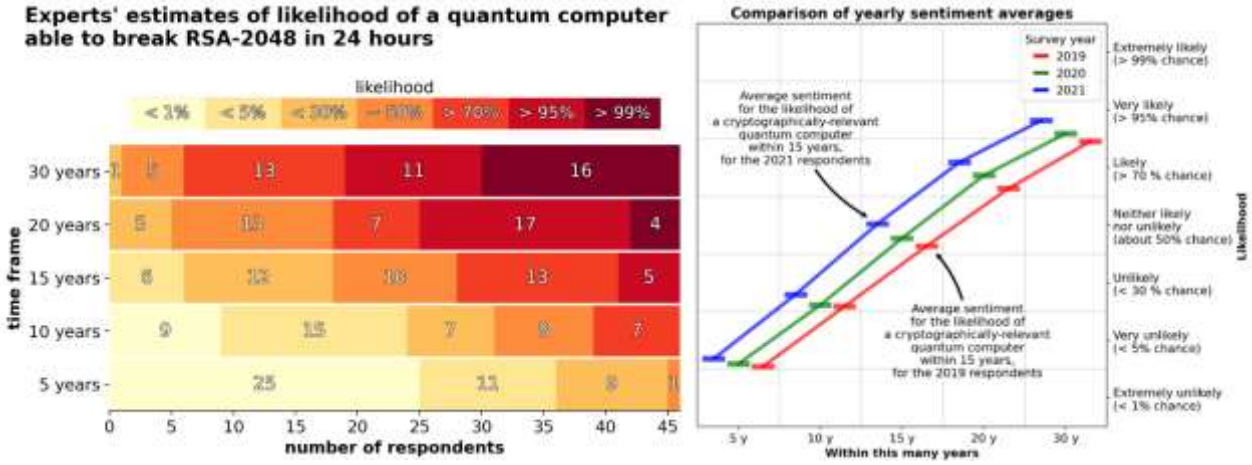


Figure 730: evolutionQ's yearly report on the quantum cyber risk as estimated by specialists from various disciplines. Source: 2021 Quantum Threat Timeline Report by Michele Mosca and Marco Piani, 2021 (87 pages).

[2253] See Forecasting timelines of quantum computing by Jaime Sevilla and C. Jess Riedel, December 2020 (23 pages).

[2254] See 2021 Quantum Threat Timeline Report by Michele Mosca and Marco Piani from evolutionQ for the Global Risk Institute, 2021.

As an illustration, a US report from 2004 prepared with the best scientists of this period planned by the year 2012 to see the implementation of a concatenated quantum error-correcting code and to obtain 50 physical qubits[2255]. These qubits came by 2019 and we don't have yet a sufficient number of qubits to implement concatenated codes. In 2012, the surface code was invented that is more efficient and has been experimented at very low scale.

Grover, Dlog and Simon threats

Symmetric cryptography systems are not affected by Shor's algorithm. These include the **Data Encryption Standard** (DES) which uses keys of 64 bits or more and is outdated, replaced by the **Advanced Encryption Standard** (AES) which has been a US government standard since 2002, with private keys ranging from 128 to 256 bits.

To date, the best quantum breaking algorithms for symmetric **AES** keys would take more than the age of the Universe (13.8 billion years) to run on 128-bit keys. With AES-256 bits, we are therefore in peace, and it is the recommended key length to be quantum resistant! They are based on mechanisms that are quite different from the mathematical problem-solving of public key ciphers.

Keys are shared upstream of the exchanges and are generally themselves encrypted with the asymmetric **Diffie-Hellman** algorithm. But this Diffie-Hellman encryption is based on elliptic curves, which is breakable by Shor's algorithm. The problem lies then with the vulnerability of the majority of encryption systems using asymmetric keys which are used to share symmetric keys.

A hash function converts data of arbitrary size such as a file to a number of fixed size. This makes it possible to do quick searches to compare files. For example, it can be used to check that a file has not been altered during transmission.

SHA algorithms (Secure Hash Algorithms) are standard hash functions that consist in replacing data of arbitrary size by a unique key size. The **SHA-1** hash algorithm is resistant to Shor's algorithm, but it has been broken by other methods and is therefore considered outdated. It is the **SHA-3** which is the most up-to-date and since 2015. The SHA algorithm could be broken by Grover's search algorithm, but with a large number of logical qubits, at least 6,000 logical qubits for common keys[2256] .

		SHA-256	SHA3-256
Grover	T-count	1.27×10^{44}	2.71×10^{44}
	T-depth	3.76×10^{43}	2.31×10^{41}
	Logical qubits	2402	3200
	Surface code distance	43	44
	Physical qubits	1.39×10^{7}	1.94×10^{7}
Distilleries	Logical qubits per distillery	3600	3600
	Number of distilleries	1	294
	Surface code distances	{33, 13, 7}	{33, 13, 7}
	Physical qubits	5.54×10^{5}	1.63×10^{8}
Total	Logical qubits	$2^{12.6}$	2^{20}
	Surface code cycles	$2^{153.8}$	$2^{146.5}$
	Total cost	$2^{166.4}$	$2^{166.5}$

Table 3. Fault-tolerant resource counts for Grover search of SHA-256 and SHA3-256.

Figure 731: the staggering level of quantum resources required to beak SHA-256 symmetric keys with Grover's algorithm.

This represents an order of magnitude close to the qubit requirements for breaking RSA keys with Shor's algorithm. For example, a hash key or fingerprint can be used to verify the integrity of content such as software or simply a password. The problem is to resist collisions, i.e., methods to find or create an object whose fingerprint would be the one you have, which is quite different from finding the original object (like an image) from its fingerprint, which is rather difficult.

The number of qubits needed to break keys depends on the size of the key. SHA-1 and SHA-2 have small key sizes that can be recovered in a reasonable time with **Grover**'s quantum search algorithm, but this is not the case for SHA-3 which exploits larger keys. This is the same logic as for AES.

[2255] See A Quantum Information Science and Technology Roadmap Part 1: Quantum Computation, 2004 (268 pages

[2256] Based on Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3, 2016 (21 pages), which is also the source of the table on this page.

At last, let's also mention **Shor's Dlog** (discrete log) algorithm that threatens Digital Signature Algorithms, Diffie-Hellman key exchanges and El-Gamal encryption. And **Simon**'s algorithm can also break Even-Mansour ciphers that are used in some disk encryption solutions, although with a lot of caveats, the attacker needing to encrypt a superposition of inputs all with the same keys[2257]. All in all, Shor is not the only quantum threat on cybersecurity!

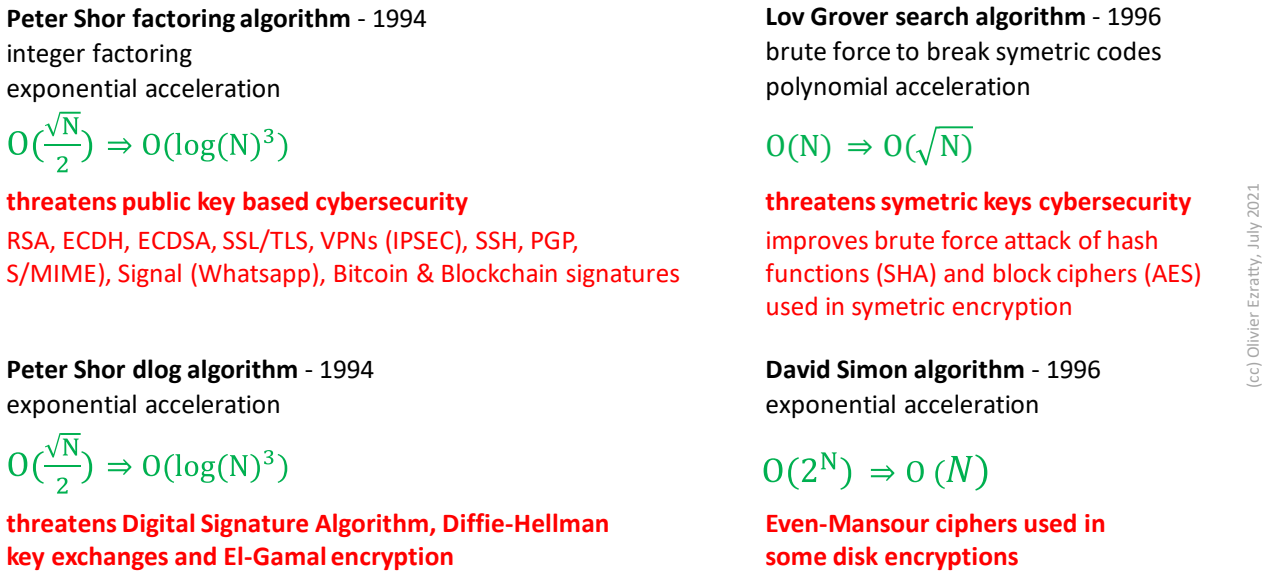


Figure 732: Shor's algorithm is not the only quantum algorithm that could threaten existing cybersecurity. (cc) Olivier Ezratty, 2021.

Blockchain and Cryptocurrencies vulnerabilities

What about **Bitcoin**, other crypto-currencies and the **Blockchain**? The answer is summarized *below* with a good inventory of the cryptosystems used by use as a starting point[2258].

Otherwise, experts have opposite views on the quantum risk, from let's forget it[2259], to it will come sooner than expected[2260].

[2257] See Breaking Symmetric Cryptosystems Using Quantum Algorithms by Gaëtan Leurent with Marc Kaplan, Anthony Leverrier and María Naya-Plasencia, 2016 (58 slides).

[2258] The answer is well documented in The Quantum Countdown Quantum Computing and The Future of Smart Ledger Encryption by Long Finance, 2018 (60 pages).

[2259] See Here's Why Quantum Computing Will Not Break Cryptocurrencies by Roger Huang, December 2020.

[2260] See Q-Day Is Coming Sooner Than We Think by Arthur Herman, Forbes, June 2021. It mentions a crack of a RSA-2048 bit encryption key in 10 seconds with 4,099 stable qubits without mentioning the source of this performance. I have searched it and didn't found the source reference of these 10 seconds mentioned in various places. The only detail is it would require a perfect quantum computer executing one million operations per second.

Basically, the Blockchain is based on a patchwork of cryptographic algorithms including AES, RSA and SHA-3. It uses a hash algorithm to ensure the integrity of the chain of trust, and a digital signature to authenticate new transactions that are incrementally added to the Blockchain.

Bitcoin uses a SHA-256 crypto hash, which is quantum resistant, and a signature that exploits ECDSA elliptic curves, which is not. In a similar manner, **Ethereum** uses a quantum resistant SHA-3 hash and a vulnerable ECDSA signature.

Table 3. Main Algorithms Types Used for Cryptography, and Uses For Smart Ledgers[19]

Type of Algorithm	General Use	Example Algorithms of This Type	Example Uses for Smart Ledgers
Symmetric	Secret communications	AES, DES, 3DES, RC4	Protection of resources stored on ledger
Public key	Secret communications (including key exchange) or digital signature	RSA, Diffie-Hellman, El Gamal, ECDSA	User authentication; signature of transactions, data or software
Hash	Generating fixed-length digest of arbitrary-length text	SHA-256, SHA-512, SHA-3	Ensuring authenticity of blockchain

Figure 733: algorithms used in cryptos and smart ledgers. Source: The Quantum Countdown Quantum Computing and The Future of Smart Ledger Encryption by Long Finance, 2018 (60 pages).

However, an Eth2 upgrade to Ethereum published in 2021 has replaced ECDSA based signatures by Lamport Q-R signatures which are quantum safe, with the inconvenient of being very large (over 200 times bigger than an ECDSA signature).

A recent review paper lists Bitcoin, Ethereum, Litecoin, Monero and ZCash as highly vulnerable to Shor's algorithm and all these, except Monero, to be moderately vulnerable to Grover search[2261].

All in all, quantum computing will not allow to alter the Blockchain, nor the proof of work used by Bitcoin which relies on the repeated use of quantum-resistant hash. The vulnerability of the Blockchain lies in the signature that relies on the ECDSA elliptic curve algorithm which can be broken with Shor's algorithm. This would make it possible to impersonate someone else in a transaction involving a Blockchain or Bitcoins. That's still whole lot of potential troubles! For example, if a Bitcoin transaction was intercepted to retrieve the sender's ECDSA signature, it could be exploited to transfer Bitcoins from that sender's wallet.

What is the "size" of the quantum computer that would break the ECDSA signature of the Bitcoin? The required number of qubits depends on the desired computing time. It would be 317 million physical qubits to break the key in one hour using a surface code, a code cycle time of 1 µs (IBM's cycle is right now at about 1 ms) and qubit fidelities 99,9% (IBM reached it with 27 qubits in 2021). In one day, the requirement is lower, at 13 million physical qubits. Whatever, as we've seen in studying the scalability of various quantum computing architecture and their enabling technologies, it's clear we are very far from seeing this threat to materialize[2262]. And like some like to asset, it doesn't matter since the Bitcoin may not outlast the current NISQ era!

Workarounds can obviously be created until a quantum threat to transaction integrity is confirmed. This can be done by encrypting the signatures used by the blockchains with a PQC system, as we'll see later[2263].

It is also possible to encrypt the data circulating in a Blockchain with a quantum computationally resistant algorithm such as AES-256, with the disadvantage that it is symmetrical and therefore requires keys to be exchanged beforehand. However, there are already some workarounds.

[2261] See Vulnerability of blockchain technologies to quantum attacks by Joseph J.Kearney et al, 2021 (10 pages).

[2262] See The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime by Mark Webber et al, September 2021 (16 pages).

[2263] See Blockchained Post-Quantum Signatures by Chalkias Browny Hearnz, 2018 (8 pages).

A protocol using a longer validation time for Bitcoin transactions would allow to bypass the use of integer factoring to break the Bitcoin electronic signature algorithm, ECDSA[2264].But this would only amplify a key flaw of Bitcoin as a currency: a lengthening of transaction times that are already far from real time!

Bitcoin mining is potentially vulnerable by Grover's algorithm although its real practical speedup on a LSQC (large scale quantum computer) is questionable. Researchers are proposing some changes in the rules (and timing) applied by miners to mitigate this threat[2265].

We can also mention the open source Blockchain project resisting quantum attacks, Quantum Resistant Ledger. It is based on the XMSS (Extended Merkle Signature Scheme) electronic signature protocol[2266].

There is also a risk of attack at the mining level, with Grover's algorithm. But here again, there are solutions available[2267].The **Long Finance** document from which this table is extracted summarizes all these risks on Smart Ledgers by separating the transactions that are relatively protected and those that rely on vulnerable electronic signatures that are not vulnerable to hacking of the SSL and TLS protocols[2268].

The Quantum Countdown
Quantum Computing And The Future Of Smart Ledger Encryption

Table 4. Risks to Blockchain Architectures from Quantum Computing

	Transactions	Data on Blockchain	Software on Blockchain
Read historical records without authorization	No (blockchains are intended to allow access to transaction information)	No, unless confidential and secured with vulnerable cryptography	No, unless confidential and secured with vulnerable cryptography
Alter historical records	No	No	May be able to run software without authorisation if signature used
Spoof ongoing records	Yes, possibly	Yes, possibly	Yes, possibly

Figure 734: Source: Source: The Quantum Countdown Quantum Computing and The Future of Smart Ledger Encryption by Long Finance, 2018 (60 pages).

This section on threats would not be complete without mentioning the disagreements between cybersecurity specialists. Some are rather conservative and consider that one should not touch too much of what works well. They think Shor's threat is exaggerated. Others, such as the NIST in the US, are more alarmist and believe that the most critical cryptographic systems should be updated as soon as possible[2269]. And we also have arguments between the compared advantages of QKD and PQC, the two systems that can protect cybersecurity from quantum computing long-term threats[2270].

[2264] It is documented in Committing to Quantum Resistance A Slow Defence for Bitcoin against a Fast Quantum Computing Attack, 2018 (18 pages).

[2265] See On the insecurity of quantum Bitcoin mining by Or Sattath, February 2019 (22 pages).

[2266] See also Blockchained Post-Quantum Signatures by Chalkias Browny Hearnz, 2018 (8 pages).

[2267] See On the insecurity of quantum Bitcoin mining by Or Sattath, February 2019 (22 pages).

[2268] For more information, see also The quantum threat to payment systems by Michele Mosca of the University of Waterloo, 2017 (52 minutes). Mosca is one of the world references in the quantum cryptography field. See also The Quantum Countdown Quantum Computing And The Future Of Smart Ledger Encryption, Long Finance, February 2018 (62 pages).

[2269] Analysts are amplifying the fear, as in Executive's Guide to Quantum Computing and Quantum-secure Cybersecurity from Hudson Institute, a US conservative think tank, March 2019 (24 pages), Preparing Enterprises for the Quantum Computing Cybersecurity Threats by CSA, May 2019 or Global Risk Report 2020 from the World Economic Forum.

[2270] See Quantum crypto-economics: Blockchain prediction markets for the evolution of quantum technology by Peter P. Rohde et al, February 2021 (12 pages) that modelize different scenarios depending on the reality of the quantum threat.

Quantum Random Numbers Generators

Quantum, post-quantum and traditional cryptographic systems are all fed by random number generators. They have been around for ages. Random numbers are also used in a large set of applications beyond classical cryptographic protocols.

It includes gaming and casinos to draw lottery winning numbers, playing card shuffling, and various bets-related numbers, statistical analysis like the ones using Monte Carlo simulations in the finance sector, selecting random samples from large data sets like with machine learning, various scientific simulations and testings (like the Wheeler which-way or delay-choice experiment we already described), and smart networks simulations.

In all these use cases, the main concern is to create truly random numbers. Namely sequences of 0s and 1s without repetitions of any sequence and a balanced proportion of 0 and 1, as in the decimals of π. These numbers generation processes must also be non-deterministic, not reproducible and with no correlations, meaning that series of randomly generated numbers must be statistically independent. We could indeed generate good random numbers but if they were similar in time, it wouldn't be satisfactory at all.

Unfortunately, most commonly used random number generators are pseudo-random and happen to be deterministic. These are branded **PRNGs** (Pseudo-Random Number Generators).

Some mathematical formula deterministically produces a series of number and some randomness is introduced by using as seed parameters some highly variable elements such as time with a millisecond precision, GPS coordinates, thermal noise or other contextual information. It still generates deterministic sequences of numbers with some repeat period, although passing regular randomness tests successfully.

Most PRNG systems now use a randomness extractor merging the output of a random entropy source and a short random seed. Despite these initialization variables and various tricks of the trade, common random number generators still create some periods within their generated numbers[2271]. Still, it may be useful to use deterministic RNGs in some cases where reproducibility is mandatory. Also, PRNGs have the advantage to be fast[2272].

To avoid determinism, we must use a truly random physical process for the generation of numbers, aka **TRNGs** (True Random Number Generators), based on some chaotic physical phenomenon. One common technique consists in measuring the thermal noise of an electronic component or the atmospheric electromagnetic noise[2273].

Thermal noise TRNGs are implemented in most microprocessors like those from **Intel** since 2013 and from **AMD** since 2015 but with various identified weaknesses[2274]. It can for example rely on voltage randomness in resistive materials (Johnson's effect), Zener noise in diodes or, more commonly, on some amplified free-running oscillator.

[2271] However, there are still other solutions for generating non-quantum random numbers that need to be equally random, although this is still questionable. See for example Scientists Develop 'Absolutely Unbreakable' Encryption Chip Using Chaos Theory by Davey Winder, 2019.

[2272] See Quantum Random-Number Generators: Practical Considerations and Use Cases Report by Marco Piani, Michele Mosca and Brian Neill, evolutionQ, January 2021 (38 pages). This is the best document I found that explains the various subtleties of QRNGs, particularly about the device dependent and device-independent species.

[2273] Atmospheric noise is used by the service random.org operated by Randomness and Integrity Services Ltd (1998, Ireland).

[2274] Since 2013, Intel processors have been using the RDRAND function that is part of their 32 and 64 bits instruction set, returning a random number generated by an on-chip thermal noise based entropy source. AMD provides support for this instruction set since June 2015.

So here come **QRNGs** (Quantum Random Number Generators), a subclass of TRNGs. They rely on quantum physics laws and one that is particularly important: Born's probability rule, based on Schrödinger's wave equation. It replaces a generic chaotic system by a non-deterministic measurement of a physical property of some quantum objects, usually individual photons. In quantum physics, a quantum object's properties measurement is intrinsically random, at least, as far as we know[2275].

Quantum is the kingdom of randomness[2276]! But this randomness is not a guarantee to obtain truly nondeterministic random numbers. There are weaknesses in all these systems, particularly with their classical or semi-classical components like the beam splitters or photon detectors it is using, or with the software part handling the so-called randomness extraction. Its consequence is an intense competition between QRNG vendors. They all claim to generate "truly" random numbers contrarily to their QRNG competitors.

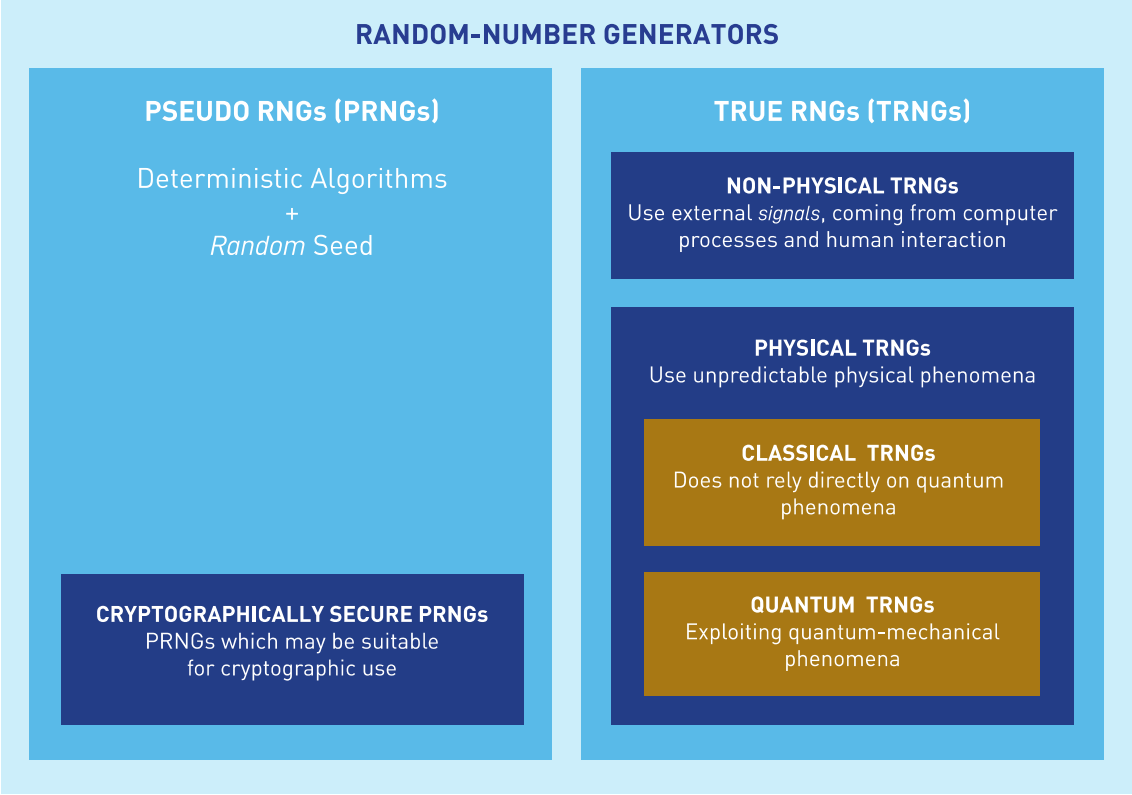


Figure 735: taxonomy of random numbers generators. Source: Quantum Random-Number Generators: Practical Considerations and Use Cases Report by Marco Piani, Michele Mosca and Brian Neill, evolutionQ, January 2021 (38 pages).

Many differentiation features are also important: the random numbers generation rate (in bits/seconds, some applications may be very demanding), the time it takes to warm up and stabilize the system (some QRNGs are slow to warm-up and may require hours to stabilize), is it device independent (impacts randomness quality but also RNG rates; but no such commercial systems are available yet), certifiability (some are black-boxes that are really difficult to audit, others are said to be self-certified) and other standard characteristics that may be important depending on the use case (weight, size, price and power drain).

[2275] See the review paper A Comprehensive Review of Quantum Random Number Generators: Concepts, Classification and the Origin of Randomness by Vaisakh Mannalath et al, March 2022 (38 pages) and Quantum Random Number Generators : Benchmarking and Challenges by David Cirauqui et al, June 2022 (15 pages).

[2276] See Can Free Will Emerge from Determinism in Quantum Theory? by Gilles Brassard and Paul Raymond-Robichaud, 2012 (22 pages). Even this is however arguable. See for example Quantum randomness is chimeric by Karl Svozil, April 2021 (16 pages) which comes back on the eternal debate of quantum measurement and its related randomness.

At last, vendor trust is a key criterion, particularly when you discover that some Switzerland cybersecurity products contained backdoors created on behalf of the CIA[2277]. It also explains why, whatever the technology used, western countries may not and probably should not rely on Chinese or Russian TRNG/QRNG vendors.

It's now up to you to understand how these systems are benchmarkable and benchmarked to figure out whether such and such QRNG is safe or not. Many different QRNG techniques have been created to date. The most commonplace are those using photons, with components that are now easy to miniaturize, even in a smartphone.

Photons counting is the most common method, based on the measurement of single photons emitted individually in series, passing through a regular balanced beam splitter and analyzed by two detectors[2278]. The series of generated 0s and 1s are theoretically random. Quantum physics mathematical formalism and experiments say so!

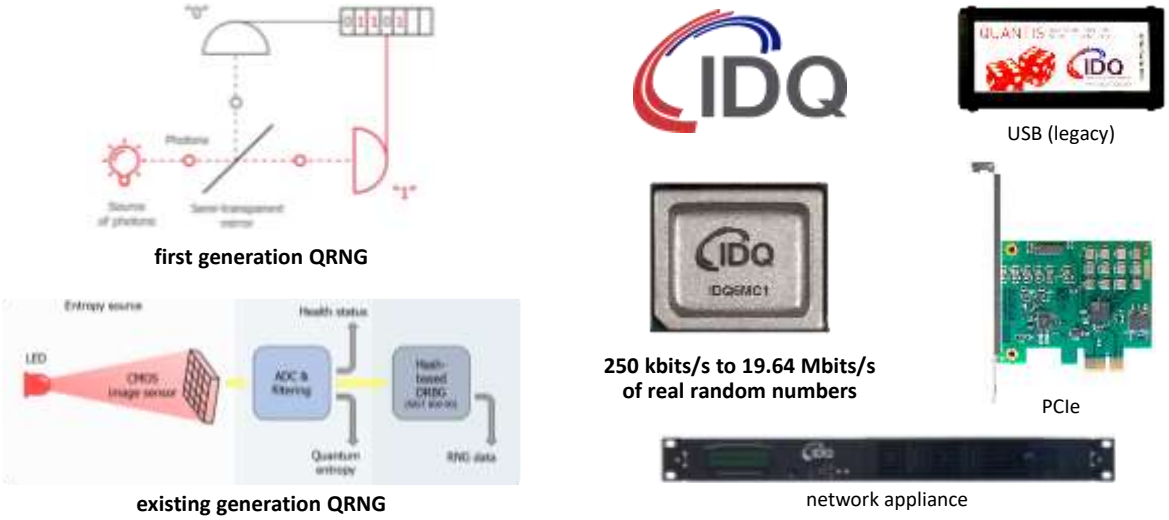


Figure 736: IDQ quantum number generators. Source: IDQ.

Each detected photon creates at most only one bit, but not all photons are detected. The detection speed is limited by the photon detectors bandwidth and their saturation level. This QRNG technique was pioneered by **IDQ** (Switzerland) in 2001. One of its shortcomings is the used light source that can't necessarily be certified. In some products, there's also some warm-up time before real random numbers can be generated. Some solutions can certify the numbers generation randomness in such situation, like using a first beam splitter and detector before photons are separated by a polarizing beam splitter[2279].

Nowadays, photon counting is (seemingly) done without a polarizing beam splitter. The light source is some LED diode, lighting a small CMOS image sensor, and generating "shot noise". That's what IDQ is now selling with its miniaturized Quantis chipset. It's adapted to mass market use cases, in smartphones, laptops and car. Such QRNG first appeared in a consumer product in 2020 in a version of the **Samsung** Galaxy A71 5G smartphone called Galaxy A Quantum, marketed by **SK Telecom** only in Korea. It probably won't change much in terms of user security, but it can make a lasting impression.

[2277] See The intelligence coup of the century' - For decades, the CIA read the encrypted communications of allies and adversaries by Greg Miller, Washington Post, February 2020. It deals with the Crypto AG company created in 1952 and dissolved in 2018.

[2278] See Quantum Random Number Generators by Miguel Herrero-Collantes, 2016 (54 pages). This setting is frequently referred to as a welcher-weg experiment, or "which way" experiment.

[2279] See Using the unpredictable nature of quantum mechanics to generate truly random numbers by Bob Yirka, 2021 that refers to Certified Quantum Random Numbers from Untrusted Light by David Drahi, December 2020 (32 pages). Its RNG output is 8.05 Gb/s.

In April 2021, Samsung announced a new version of this smartphone, the Galaxy Quantum2, adapted to 5G and with similar QRNG features using an IDQ Quantis chipset[2280]. The same chipset is found in a Vsmart Aris 5G smartphone, coming from Vietnam! **Q→NU**, **CryptaLabs** and **Qrypt** are also commercializing such type of QRNGs.

Photon arrival time aka "time bin qubits" is about evaluating the arrival time of successive single photons in a simpler setting coupling a photon source like a LED or a laser and a photon counter to a high-resolution counter, down to a couple nanoseconds[2281]. Practically, randomness comes from evaluating the variation of this arrival time compared with the decaying exponential waiting-time distribution. The system can also use a photon counting setting with a regular beam splitter and two photon detectors coupled each with a counter[2282]. It has low latency and is quickly up to speed. **Qnu Labs, PicoQuant** and **QuTools** are providers of such QRNGs. A variation of this technique recently developed uses a LED light illuminating a matrix of SPADs (single photon avalanche detectors) on a CMOS circuit, with a RNG capacity of 400 Mbit/s[2283].

Quantum vacuum fluctuations uses a balanced homodyne measurement of vacuum fluctuations of the electromagnetic field contained in the radio-frequency sidebands of a single-mode (usually 780 nm) laser diode[2284]. Two diodes compute the difference of the signals coming from the two exits of a polarizing beam splitter and the resulting signal is amplified and digitized, to be processed by a randomness extractor. Such a QRNG system is implemented in a web site run by ANU (Australian National University) with the qStream QRNG from **Quintessence Labs**, which generates keys at a >3.5Gbps rate[2285]. A record of 100 Gbps rate was obtained by a European team in 2022[2286].

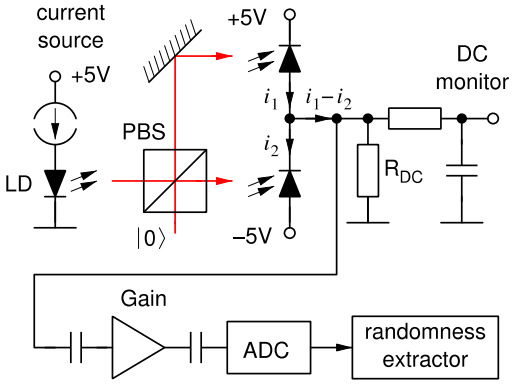


Figure 737: quantum vacuum fluctuation QRNG. Source : Random numbers from vacuum fluctuations by Yicheng Shi et al, 2016 (5 pages)

Spontaneous emission uses amplified spontaneous emission, detection and digitization of optically filtered amplified spontaneous emission noise from a light source such as superluminescent diode (SLD).

[2280] The QRNG chipset is a square of 2.5mm creating random codes by capturing noise from an LED and a CMOS sensor.

[2281] See Photon arrival time quantum random number generation by Michael A. Wayne et al, 2009 (7 pages) which describes the principles of this random numbers generation methods.

[2282] See First high-speed quantum-safe randomness generation with realistic devices, NTT, February 2021, which refers to A simple low-latency real-time certifiable quantum random number generator by Yanbao Zhang et al, 2021 (8 pages).

[2283] See A High Speed Integrated Quantum Random Number Generator with on-Chip Real-Time Randomness Extraction by Francesco Regazzoni et al, February 2021 (9 pages).

[2284] A homodyne measurement consists in extracting information encoded as modulation of the phase and/or frequency of an oscillating signal. In the mentioned case, it's the phase. See an example in Random numbers from vacuum fluctuations by Yicheng Shi et al, 2016 (5 pages) and in A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers by Francesco Raffaelli et al, University of Bristol, Quantum Science and Technology, February 2018 (10 pages).

[2285] See https://qrng.anu.edu.au/ and Real time demonstration of high bitrate quantum random number generation with coherent laser light, by T. Symul et al, 2021 (4 pages) and Maximization of Extractable Randomness in a Quantum Random-Number Generator by J. Y. Haw, 2015 (13 pages). The operations are linked to the offer of QuintessenceLabs.

[2286] See 100 Gbps Integrated Quantum Random Number Generator Based on Vacuum Fluctuations by Cedric Bruynsteen et al, September 2022 (10 pages).

Phase noise and **phase diffusion** (PD-QRNG[2287]) are variations of spontaneous emission QRNGs. It uses a photons counting method variation proposed in 2009[2288]. In one implementation, a VCSEL laser (single mode vertical cavity surface emitting laser) is associated with a phase noise measurement using a delay self-homodyne method.

The photons from the laser are traversing a beam splitter. Among its benefits are a very high-bit rate, of several tens of Gbits/s of random bits.

The technique is used by vendors like **Quside**, **QuantumeMotion** and **Kets**.

One way goes to the next beam splitter, and the other traverses a delay line, and is then merged back with the main line. An APD (avalanche photodetector), then counts the exiting photons and its signal is converted from analog to digital with an ADC[2289].

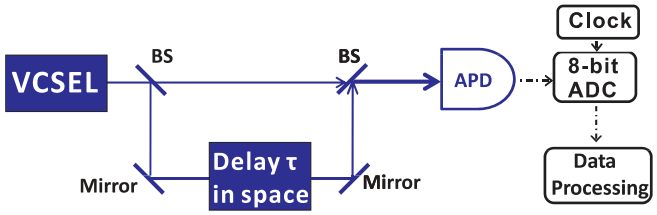


Figure 738: Source: Truly Random Number Generation Based on Measurement of Phase Noise of Laser by Hong Guo et al, Peking University, January 2010 (4 pages).

Radioactive decay was one of the first developed QRNG technologies, based on the random timing of decay of particular radioactive atoms, detected with a Geiger counter. It has limited bit rates and is not widely used, on top of being not very practical to implement given it's based on radioactive materials. There is however a vendor in that space, **EYL**.

Other various techniques are mentioned but seemingly not widely used: **laser chaos** that creates a time-delayed optical feedback via a reflector, **Raman scattering**, **attenuated pulse** and **Optical Parametric Oscillators (OPO)** and as proposed in 2022, **skyrmions**-based QRNGs[2290].

Another technique consists in merging in a single platform several QRNG methods. That's what a Chinese team released in July 2021 on an Alibaba Cloud server, mixing four types of QRNGs: single-photon detection, photon-counting detection, phase-fluctuations and vacuum-fluctuations[2291]. Three of these QRNG sources were off-the-shelf (Quantis-PCIe-16M from ID Quantique, QRG-100E from QuantumCTek and QRN-16 from MPD).

Device Independence deals with the difference between randomness and privacy. A SDI (source device independent) QRNGs ensures private randomness, where the created random numbers can't be known by any adversary. With SDI QRNGs, the randomness source is assumed to be untrusted but the measurement devices are trusted. It's more secured than a trusted device or device dependent QRNG where the device is well characterized and trusted. Device independence must also deal with detector attacks in the QRNG[2292].

[2287] See Quantum entropy source on an InP photonic integrated circuit for random number generation by Carlos Abellan et al, Optica, 2016 (7 pages) and Real-time interferometric quantum random number generation on chip by Thomas Roger et al, Journal of Optical Society, 2019 (7 pages).

[2288] In Experimental demonstration of a high speed quantum random number generation scheme based on measuring phase noise of a single mode laser by Bing Qi, Yue-Meng Chi, Hoi-Kwong Lo and Li Qian, 2009 (7 pages).

[2289] See Truly Random Number Generation Based on Measurement of Phase Noise of Laser by Hong Guo et al, Peking University, January 2010 (4 pages).

[2290] See Single skyrmion true random number generator using local dynamics and interaction between skyrmions by Kang Wang et al, Nature Communications, February 2022 (8 pages).

[2291] See Quantum random number cloud platform by Leilei Huang, Hongyi Zhou, Kai Feng and Chongjin Xie, Nature, July 2021.

[2292] See Source-independent quantum random number generator against detector blinding attacks by Wen-Bo Liu et al, April 2022 (14 pages).

These have a high bit rate in the Gbits/s range while SDI QRNGs have a much lower bit rate, in the kbits/s range due to a more complicated setup. SDI QRNG can rely on entanglement and non-locality or be based on quantum computation (this is a variation of the qubit measurement technique mentioned above). SDI QRNG enables real-time estimate of the output entropy which can quantify and certify the QRNG randomness without possessing a detailed knowledge of the entropy source device. The device independence certification comes with loophole free violation of Bell's inequalities.

A record rate of 17 GBits/s key generation with a SDI-QRNG was obtained in 2018 in an Italian lab[2293]. It was also experimented in a highly integrated photonic circuits, using a self-tested randomness expansion protocol with multi-dimensional encoding[2294].

There are also MDI-QRNGs, where the source is trusted and the measurement device is untrusted. It is for example used with time-bin QRNGs with a testing mode used to create a 4-quantum states ($|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$) tomography[2295].

Qubits measurement is a more generic way of generating quantum randomness than photon counting after traversing a polarizing beam splitter. It uses gates-based quantum processing units applied to one or several qubits and creating superposition. The simplest is a single Hadamard gate, but it's not sufficient to create enough randomness. The common practice is to create entangled states, or Bell states, which is done combining Hadamard and CNOT gates[2296]. The useful states are those where there is some correlation or anticorrelation between the qubits from a Bell pair, showing that they were random. **CQC** (UK, part of Quantinuum) is providing such a solution, named Quantum Origin, running on superconducting qubits in the cloud, in partnership with IBM and also running on Quantinuum trapped ions qubits. There are variations of QRNG exploiting computing qubits that are based on quantum walks[2297]. Still, I don't know how these solutions are certified and we're back at studying the real randomness, non-determinism and weaknesses of qubits preparation sources (microwaves, lasers) as well as qubit readout techniques (microwaves readouts, CCD/CMOS readouts for cold atoms, trapped ions and NV centers, and single photon detectors for photon qubits).

Quality. Quantum random numbers generators are not equal. The source may be a true RNG but other components may contain weaknesses and be hacked in some circumstances: the photon source[2298], the photon measurement system which could deviate or be defective, and at last randomness extractor various other weaknesses. Also, it can be difficult to distinguish classical hardware noise from the quantum randomness coming from the QRNG in evaluation tests.

Evaluation. Random series of numbers must be incompressible. This algorithmic randomness can be tested with Borel normality. An infinite sequence of binary numbers is random if every binary string of length n appearing in the sequence has a frequency of 2^{-n}.

[2293] See Source-device-independent heterodyne-based quantum random number generator at 17 Gbps by Marco Avesani et al, 2018 (7 pages). It uses a POVM measurement of continuous variable observables.

[2294] See Multidimensional quantum entanglement with large-scale integrated optics by J. Wang et al, Science, 2018 (24 pages).

[2295] See Experimental measurement-device-independent quantum random number generation by You-Qi Nie et al, China, 2016 (16 pages).

[2296] See Quantum random number generators with entanglement for public randomness testing by Janusz E. Jacak et al, 2020 (9 pages) and Reference Standard RS-EITCI-QSG-EQRNG-PROTOCOLS-STD-VER-1.0, EITCI, 2019 (21 pages).

[2297] See Quantum Walk Random Number Generation: Memory-based Models by Minu J. Bae, University of Connecticut, July 2022 (12 pages).

[2298] See for example QRNG: Out-of-Band Electromagnetic Injection Attack on a Quantum Random Number Generator by P.R. Smith et al, January 2021 (12 pages).

There are various tests of algorithmic randomness like the NIST SP 800-22 1A Test[2299]. It contains 15 tests but other tests suites exist that complement the NIST set, totaling 40 tests[2300].

Test	Defect detected	Property
Frequency (monobit)	Too many zeroes or ones	Equally likely (global)
Frequency (block)	Too many zeroes or ones	Equally likely (local)
Runs test	Oscillation of zeroes and ones too fast or too slow	Sequential dependence (locally)
Longest run of ones in a block	Oscillation of zeroes and ones too fast or too slow	Sequential dependence (globally)
Binary matrix rank	Deviation from expected rank distribution	Linear dependence
Discrete fourier transform (spectral)	Repetitive patterns	Periodic dependence
Non-overlapping template matching	Irregular occurences of a prespecified template	Periodic dependence and equally likely
Overlapping template matching	Irregular occurences of a prespecified template	Periodic dependence and equally likely
Maurer's universal statistical	Sequence is incompressible	Dependence and equally likely
Linear complexity	Linear feedback shift register (LFSR) too short	Dependence
Serial	Non-uniformity in the joint distribution for m-length sequences	Equally likely
Approximate entropy	Non-uniformity in the joint distribution for m-length sequences	Equally likely
Cumulative sums (cusum)	Too many zeroes or ones at either an early or late stage in the sequence	Sequential dependence
Random excursions	Deviation from the distribution of the number of visits of a random walk to a certain state	Sequential dependence
Random excursions variants	Deviation from the distribution of the number of visits (across many random walks) to a certain state	Sequential dependence

Figure 739: the NIST test suite for QRNG. Source: Random Number Generators: An Evaluation and Comparison of Random.org and Some Commonly Used Generators by Charmaine Kenny, April 2005 (107 pages).

Recent TRNG/QRNG benchmarking tools use machine learning techniques and a convolutional network to detect patterns in the generated numbers[2301]. However, while these tests may detect weaknesses in QRNG randomness, it won't ensure real nondeterminism. Other tests are required, like loophole free Bell tests, already mentioned.

QKD or PQC? We'll describe these two cryptography solutions later on. Which one will make use of QRNGs? Post-quantum cryptography requires large classical random keys, so QRNGs will be very useful, particularly those who have a large throughput. Quantum Key Distribution (QKD) needs randomness to select its active basis choice for each and every detected pairs of photon like their polarization angle. So again, a good and fast QRNG will be mandatory. This QRNG functionality can however be embedded in some specific QKD systems with relying on the randomness of the time between photons detection in the SPCMs (Single Photon Counting Modules)[2302]. But QRNGs have a much broader addressable market: classical cryptography and all the businesses in need of random numbers like casinos, online gaming and lotteries.

[2299] See A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications by Andrew Rukhin et al, NIST, 2010 (131 pages). Then, Experimentally probing the algorithmic randomness and incomputability of quantum randomness by Alastair Abbott, Cristian Calude and al, UGA/Institut Néel France and University of Auckland, 2018 (17 pages) and Recommendations and illustrations for the evaluation of photonic random number generators by Joseph D. Hart et al, 2017 (29 pages).

[2300] See Random Number Generators: An Evaluation and Comparison of Random.org and Some Commonly Used Generators by Charmaine Kenny, April 2005 (107 pages).

[2301] See Machine Learning Cryptanalysis of a Quantum Random Number Generator by Nhan Duy Truong et al, 2019 (13 pages) and Benchmarking a Quantum Random Number Generator with Machine Learning, 2020 (26 slides).

[2302] This is described in Practical random number generation protocol for entanglement-based quantum key distribution by G. B. Xavier et al, 2008 (10 pages).

Let's now look at the QRNG industry vendors landscape. As said before, this technique has been mastered for a long time by **ID Quantique** (IDQ), a company cofounded by Nicolas Gisin, which belongs to SK Telecom since 2018. Other players abound like **CryptoMathic**, **Crypta Labs**, **Quside**, **InfiniQuant**, **Kets**, **PicoQuant** and **Quantropi**[2303]. **Axion Technologies** (2017, Canada) also created a random number generator competing with the Swiss IDQ.

Figure 740: a map of QRNG vendors. (cc) Olivier Ezratty, 2022.

CryptoMathic (1986, Denmark) develops quantum random key generators and various keys generation systems.

EYL (2015, USA, $900K) sells radioactive isotopes-based entropy chips of 3mmx3mm and QRNG chips. They form factor is a USB key.

PicoQuant (1996, Germany) is a Berlin-based SME specialized in photonics and which markets photon counters and diode lasers. But they are here because they also offer a photon arrival time QRNG, the PQRNG 150, with a throughput of 150 Mbits/s. It is much less miniaturized than the random number generator component from IDQ that is integrated in Samsung's Galaxy 5G announced in May 2020[2304].

Qrypt (2018, USA) develops cryptographic solutions using a high speed QRNG powered by multiple entropy sources exclusively licensed from Oak Ridge National Lab and other labs. It will support NIST PQC standards when selected. Qrypt invested in Quside (Spain), which is developing high quality and high speed QRNGs.

Qnu Labs (2016, India) sells its Tropos Quantum Random Number Generation, which allows the creation of random numbers of any size and quite quickly, at a rate of up to 1.5 random Mbits/s, or even several tens of Gbits/s. It also sells a QKD solution, Armos and a quantum secure platform for key management, Hodos. They were helped by the Intel startup program.

[2303] These companies are described in the quantum telecommunication and cryptography vendors section since they provide some PQC or QKD solution on top of QRNGs.

[2304] They contribute to research projects in QKD infrastructures like in Ultrafast quantum key distribution using fully parallelized quantum channels by Robin Terhaar et al, July 2022 (13 pages)

Quside (2017, Spain) proposes a QRNG using phase diffusion, with a 400 Mbits/s key generation rate. It is a spin-off of ICFO, the Institute of Photonics of Barcelona. Quside QRNGs were used in many of the 2015 loophole-free Bell test experiments thanks to their high key rate. Their latest offering is the miniaturized QN 100 Quantum Entropy Source.

Quantum Dice (2019, UK, £2M) is a spin-off from the University of Oxford selling a "true" "self-certified" and fast QRNG device. It uses a patented DISC protocol ensuring that randomness comes only from the quantum process and is protected from external influences.

Their October 2021 £2M investment round was led by French venture capital fund Elaia Partners. They also got a £1M non-dilutive grant from the Quantum Accelerator Group led by IP Group, in partnership with Innovate UK as part of the UK national quantum plan.

Quantropi (2018, Canada) is a company created in Ottawa by James Nguyen (CEO) and Randy Kuang (Chief Scientist).

It was initially created to distribute a software generator of "lightweight ultra-high-entropy" random encryption keys. It then evolved into selling a complicated cybersecurity offering mixing custom-made PQC, a specific scheme for quantum key distribution solution, all that packaged in a gibberish marketing lingua mixing classical and quantum crypto[2305].

Their QiSpace end-to-end quantum security SaaS platform contains a lot of stuff:

- **MASQ**, their asymmetric encryption offering, with a PQC for key exchange and digital signature containing a MPPK for Multivariate Polynomial Public Key, but they also have a Quantum Permutation Pad aka QPP. These things are supposed to support NIST PQC finalists and Quantropi's own PQC.
- **QEEP**, their symmetric encryption offering, providing "quantum-secure symmetric encryption that's up to 18 times faster than AES-256".
- **SEQUR**, their "quantum entropy as a service" (QEaaS) offering which contains some form of QRNG, branded QiSpace SEQUR NGen pseudo-QRNG (so, it's not a real QRNG) and their SEQUR SynQK, a sort of QKD that is supposed to deliver 5 simultaneous Quantum-key streams over distances ranging from 4,000 to 15,000 km at 130 to 190 megabits per second. What's quantum in-here? Their "coherent-based Two-Field Quantum Key Distribution (CTF-QKD)", a signal modulation scheme using coherent optical communications hardware and infrastructure[2306].

ComScire (1994, USA) is the developer of several random number generators including PureQuantum QRNG, which creates 4 to 128 million bits per second. Is it really quantum? Not really sure!

Its entropy source seems to be coming from CMOS shot noise, using an Altera FPGA[2307]. The company also markets QNGmeter 3.6, a software tool testing the randomness and nondeterministic nature of generated numbers.

Terra Quantum (Switzerland) also provides a photonic based QRNG generated 1.2 Mb/s of random bits.

[2305] This leads to some extreme marketing claims as seen on Startup: Only Quantum Cryptography Can Save The $100 Trillion Global Digital Economy by John Koetsier in Forbes, March 2021.

[2306] It seems documented in Quantum Public Key Distribution using Randomized Glauber States by Randy Kuang and Nicolas Bettenburg et al, 2020 (7 pages).

[2307] Its functioning is described in Entropy Analysis and System Design for Quantum Random Number Generators in CMOS Integrated Circuits by Scott A Wilber, 2013 (28 pages).

Quantum Key Distribution

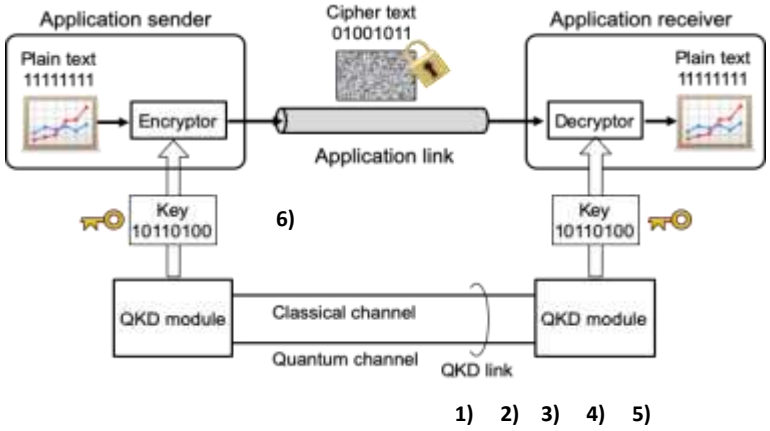
Quantum cryptography is based on "quantum key distribution" which consists in allowing the exchange of symmetrical encryption keys, by optical means (optical fiber, air link or satellite optical link) using a system to protect its transmission against intrusions [2308].

QKD protocols have the particularity of allowing the detection of any intrusion in the transmission chain and to indicate that someone has tried to read its contents or if, disturbances have occurred, "on the line"[2309].

QKD principles

One early version was the **BB84** protocol invented by **Charles Bennett** and **Gilles Brassard** in 1979 and published in 1984 [2310]. They are even the creators in 1982 of the expression "quantum cryptography"[2311]. But it wasn't yet QKD per se. This protocol is about sending photon-based information with four types of rectilinear/diagonal polarizations, *aka* non-orthogonal states: 0°, 45°, 90° and 135°. Alice & Bob exchange through a classical channel their polarization basis, used for encoding by Alice and for measurement by Bob, after the photons have been sent to make sure Bob keeps only the relevant bits where his random measurement was done in the same as the polarization basis used by Alice.

The qubits read by an intruder would modify the key, by projecting their polarization at 0° or 90°, or 45°/135° depending on the case and randomly. Any reading intrusion would be detected by Alice and Bob during their classical communication because of the inevitable disturbances it would cause. If the protocol detects an intruder, it can take this into account and block the communication of sensitive information because the encoding key has been captured and, maybe, chose another quantum channel. And there are solutions to avoid a denial of service in such a case[2312].



1) **Alice and Bob share photons created from entangled pairs.**
2) **They measure these photons properties on a random basis.**
3) **Alice and Bob exchange the used basis on a classical channel.**
4) **Alice and Bob keep the bits with matching basis. It creates a « sifted key ».**
5) **They check the statistics of measured bits, checking there was no intruder.**
6) **The generated key is used to cipher the transmitted content.**

Figure 741: general principle of quantum key distribution. Source: TBD.

[2308] See the review paper Quantum Key Distribution Secured Optical Networks: A Survey by Purva Sharma et al, September 2021 (35 pages) which contains a very good description of the various QKD technologies and protocols, their challenges and the way they are addressed and The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet by Yuan Cao, IEEE, 2021 (59 pages).

[2309] See the review paper Advances in Quantum Cryptography by Stefano Pirandola et al, 2019 (118 pages).

[2310] In Quantum cryptography : public key distribution and coin tossing, 1984 (5 pages).

[2311] Here is a general overview of QKD and PQC: The Impact of Quantum Computing on Present Cryptography, March 2018 (10 pages).

[2312] See for example A quantum key distribution protocol for rapid denial of service detection by Alasdair Price et al, from the University of Bristol, in EPJ Quantum Technology, 2020 (20 pages).

Artur Ekert then created the **E91** protocol in 1991 with using quantum entanglement and non-locality, avoiding the explicit transmission of photon information that is used in BB84 and that could be intercepted by an intruder [2313].

With E91, Alice and Bob share the photons created from entangled pairs. They can then share a randomly generated key with a sequential measurement of these photons. Like with BB84, this measurement must be done in a random orthogonal polarization basis that has to be shared afterwards between Alice and Bob. They will retain the randomly generated bits when their polarization was synchronized, creating a "sifted key". If an eavesdropper Eve intercepted the entangled photons, their projections would be different. To make sure there was no eavesdropper, Alice and Bob compute a Bell test statistic which must yield ideally a so-called Bell parameter $|S| = 2\sqrt{2}$, called Tsirelson's bound, otherwise, there was an eavesdropper.

One key difference between BB84 and E91 is the origin of randomness in the shared keys. With BB84, it must be generated by Alice with a random number generator, preferably a TRNG (true random numbers generator) and not a PRNG (pseudo-random numbers generator) as described in the earlier section on QRNGs, page 810. With E91, it comes directly from the randomness of the entangled photon pairs readouts. All in all, E91 consolidates a quantum communication protocol and a quantum random number generator.

QKD protocols have since made their way. They are at the origin of the creation of the whole field of quantum cryptography, which has now left the exclusive realm of research and experimentation to enter actual deployments like in China, even though there are still problems remaining to be fixed such as the creation of safe repeaters, to replace the commonplace unsafe trusted nodes (even in China) where the key bits are turned into classical data at each and every node station, given you need to have one of these about every 80 km.

QKD was expanded with CV-QKD (continuous variable) which modulates both the phase and the amplitude of the transmitted optical signal. It notably allows multiplexing several communications on the same optical fiber and to exploit the existing infrastructures of telecom operators. **Philippe Grangier** was one of its designers, along with **Frédéric Grosshans** from CNRS-LIP6, in 2002[2314]. CV-QKD complements discrete variables QKD (DV-QKD) as are called the previously mentioned QKD protocols, based on the properties of single photons, which requires some cooling on the single-photon detector side.

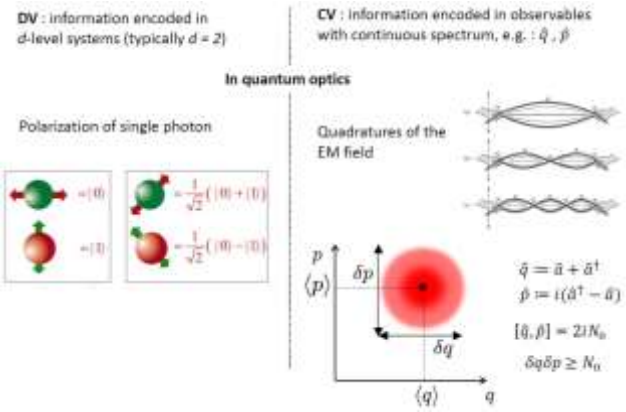


Figure 742: DV and CV in QKD. Source: TBD.

[2313] And published in the article Quantum Cryptography Based on Bell's Theorem (3 pages). Artur Ekert has been a member of Atos Scientific Council since 2016, along with Alain Aspect, Daniel Esteve, Serge Haroche, Cédric Villani and David DiVincenzo.

[2314] Their QKD protocol is baptized accordingly GG02.

Figure 743 makes a rough comparison between DV-QKD and CV-QKD. Nowadays, CV-QKD seems preferred for telecom fiber deployments.

Figure 744 describes a typical optical architecture for the implementation of a CV-QKD protocol based on BB84, without entanglement given CV-QKD can also be implemented with entanglement based protocols. It uses a simple photon source in the telecom wavelength band around 1550 nm followed by amplitude and phase modulators. On the Bob side, a homodyne detector will demodulate the signal.

	DV-QKD	CV-QKD
Quantum state	Polarization, phase, or time bin of a single photon	Quadrature components of quantized electromagnetic field
Source	Single-photon source	Coherent-state or squeezed-state source
Detector	Single-photon detector	Homodyne or heterodyne detector
Channel model	Lossy qubit channel	Lossy bosonic channel
Distance limitation	Performance of single-photon detectors	Efficiency of post-processing techniques

Figure 743: comparison between DV-QKD and CV-QKD protocols. Source: The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet by Yuan Cao, IEEE, 2021 (59 pages).

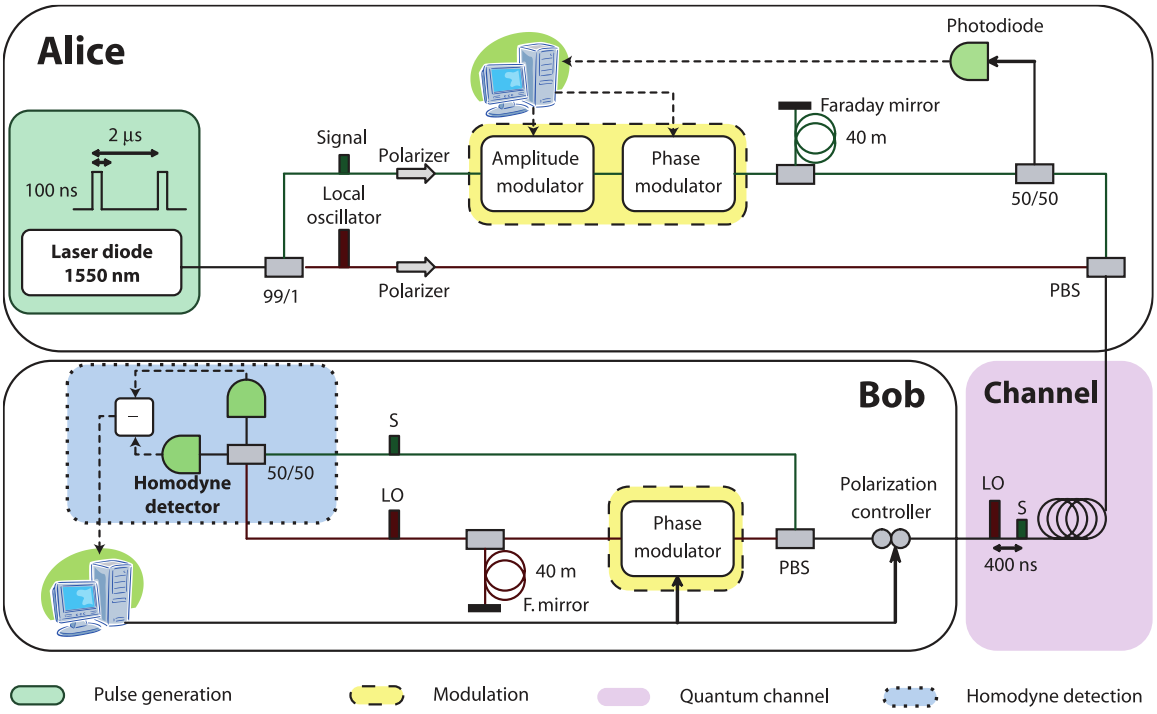


Figure 744: an example of of CV-QKD implementation of the BB84 protocol. The SECOQC quantum key distribution network in Vienna by M. Peev, C. Pacher, Romain Alleaume, C. Barreiro, J. Bouda, W. Boxleitner, Thierry Debuisschert, Eleni Diamanti, et al, 2009 (39 pages).

The integration of a QKD in conventional telecommunication optical fibers is typically done using three methods: by frequency multiplexing (WDM), for instance with a QKD signal on 1310 nm and data sent on 1550 nm, by time sharing (TDM) or by using a dedicated fiber embedded in a sheath (SDM). China has a very good experience in that domain[2315].

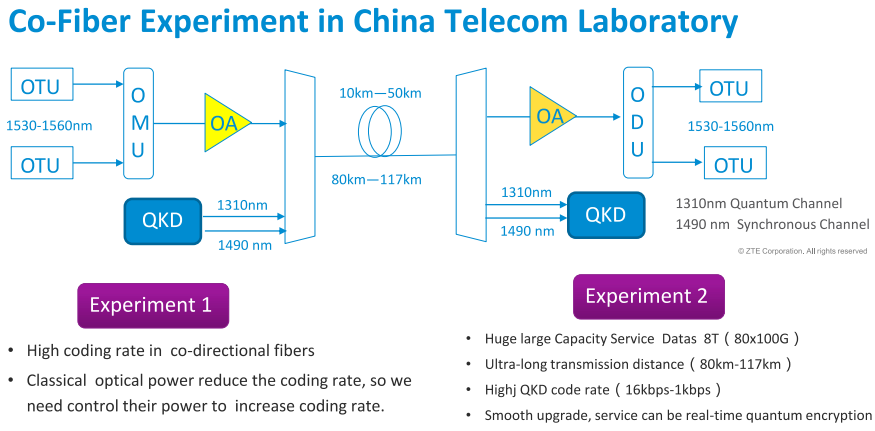


Figure 745: co-fiber experiment in China Telecom laboratory distributing quantum keys over telecom fiber lines. Source: QKD Application: Coexistence QKD Network and Optical Networking the same optical fiber network by JiDong Xu, ZTE, June 2019 (15 slides).

With entanglement-based CV-QKD protocols, the initial entanglement done before sending the two bits in the qubits avoids violating the Holevo theorem, already mentioned several times, according to which a set of qubits cannot carry more information than its equivalent number of classical bits. On the other hand, the information encrypted with the transmitted key is usually sent over a traditional channel[2316]. It is still often encrypted using SSL, which protects the relationship between your browser and the websites you visit and supports the secured https protocol.

In practice, keys transmission using a QKD is accompanied by a complex system of "key distillation" that manages the communication imperfections with classical error correction codes (which have nothing to do with the quantum error correction codes seen at the qubit level elsewhere in this document, page 216), an amplification of confidentiality and an authentication system using private keys already shared by the correspondents, making it possible to avoid so-called *man-in-the-middle* attacks by hackers pretending to be one of the interlocutors.

Error correction codes and the rest of the protocol generate on-line losses of about 80% of the quantum key communication[2317]. Implementing a QKD combines a quantum random key generator such as those from IDQ, an authenticated classical channel to exchange QKD basis information and a QKD channel to share random keys, which can generally be transported on a dark fiber from a B2B telecom operator.

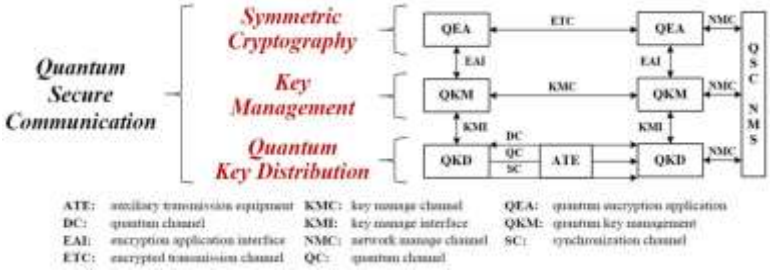


Figure 746: the three components of quantum secure communication with a symmetric cryptography, key management and a QKD. Source: Development and evaluation of QKD-based secure communication in China by Wen-yu Zhao, June 2019 (15 slides).

[2315] See QKD Application: Coexistence QKD Network and Optical Networking the same optical fiber network by JiDong Xu, June 2019 (15 slides). It's also described in Quantum Encrypted Signals on Multiuser Optical Fiber Networks Simulation Analysis of Next Generation Services and Technologies by Rameez Asif, 2017 (6 pages) and Quantum experiments explore power of light for communications, computing by Elizabeth Rosenthal, January 2020.

[2316] Classical information can take a very different path. For example, a quantum key can be transmitted by satellite and data can be transmitted terrestrially over fiber optics.

[2317] According to the excellent overview by Sheila Cobourne of the University of London Quantum Key Distribution Protocols and Applications, 2011 (95 pages).

The useful data is encrypted with the QKD generated key with classical encryption protocols like AES[2318] and transmitted over a traditional channel, which may also be a classical optical fiber or other physical communication media, even cellular communications.

This is well documented by ETSI[2319]. On arrival, a quantum key receiver and the system for decrypting the signal arriving via the traditional channel is used.

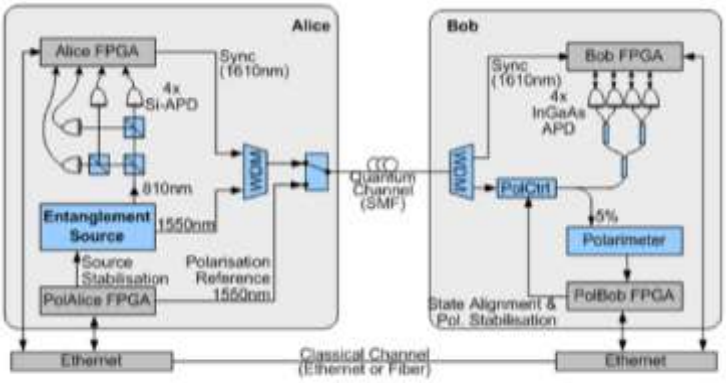


Figure 4.6: Schematic of an entanglement-based QKD system

Figure 747: Source: Quantum Key Distribution (QKD) Components and Internal Interfaces from ETSI, 2018 (47 pages).

The secret keys throughput is an important issue and is currently at its maximum in Mbits/s vs. the Tbits/s of the operators' optical links[2320]. Many optimizations must be implemented to make QKD practical, first with closing the many discovered security loopholes. Other improvements can be achieved with implementing clock synchronization without an additional dedicated channel and develop protocols to increase raw key rates[2321].

The quantum keys transfer rate can be much lower than the physical data rate available. There are fundamental bounds on how much secret keys can be generated over a noisy quantum channel.

There are also other fundamental questions about the overall architecture and topology of QKD networks, most of the time working in “point to point” and relying on so-called trusted nodes, which can be considered as “classical” repeaters [2322].

Proposals abound to create large multi-point networks and routing protocols[2323] and on entanglement distribution optimization[2324].

[2318] One-time pads encryption techniques can also be used with QKD. It consists in creating a key that is as large as the content to be encrypted. This technique makes the content uncrackable with brute force.

[2319] In Quantum Key Distribution (QKD) Components and Internal Interfaces from ETSI, 2018 (47 pages) which describes the different QKD techniques available to date. It also describes very well the photon sources used in QKDs as well as the associated quantitative and qualitative parameters.

[2320] See Experimental Demonstration of High-Rate Discrete-Modulated Continuous-Variable Quantum Key Distribution System by Yan Pan et al, March 2022 (5 pages) which describes a record of high-speed CV-QKD distribution over distances of 5 to 50 km with keys generations ranging from 288 Mbits/s to 7.6 Mbits/s. A record key rate of 1 Gbits/s with a source of entangled photons in the 1550 nm telecom wavelengths was obtained in 2022 by an Austrian team but the practical key rate would be much lower in practical use cases due to fiber attenuation over long distances. See Experimental entanglement generation for quantum key distribution beyond 1 Gbit/s by Sebastian Philipp Neumann et al, September 2022 (11 pages).

[2321] See for example Operational real field entangled quantum key distribution over 50 km by Yoann Pelet, Sébastien Tanzilli et al, July 2022 (7 pages).

[2322] See an example of trusted node deployment with Trusted Node QKD at an Electrical Utility by Philip G. Evans et al, March 2021 (10 pages).

[2323] See A Quantum Internet Architecture by Rodney Van Meter et al, December 2021 (17 pages), Cost and Routing of Continuous Variable Quantum Networks by Federico Centrone, Frederic Grosshans and Valentina Parigi, April 2022 (20 pages), A quantum router architecture for high-fidelity entanglement flows in quantum networks by Yuan Lee, Eric Bersin, Axel Dahlberg, Stephanie Wehner and Dirk Englund, npj, June 2022 (8 pages) and An Efficient Routing Protocol for Quantum Key Distribution Networks by Jia-Meng Yao et al, April 2022 (27 pages).

[2324] See 40-user fully connected entanglement-based quantum key distribution network without trusted node by Xu Liu et al, January 2022 (15 pages) and Genuinely Multipartite Entanglement vias Quantum Communication by Ming-Xing Luo et al, April 2022 (9 pages).

There are a few other varieties of QKD protocols beyond the DV-QKD and CV-QKD as shown in Figure 748 with **DI-QKD**, a more secure Device-Independent QKD [2325] and **MDI-QKD** for "measurement-device-independent" QKD [2326].

Protocol	Type	Approach	Year
BB84	DV	Prepare-and-measure	1984
E91	DV	Entanglement-based	1991
BBM92	DV	Entanglement-based	1992
GG02	CV	Prepare-and-measure	2002
DPS	DV	Prepare-and-measure	2002
Decoy-state	DV	Prepare-and-measure	2003–2005
SARG04	DV	Prepare-and-measure	2004
COW	DV	Prepare-and-measure	2005
MDI	DV/CV	Prepare-and-measure	2012
TF	DV	Prepare-and-measure	2018
PM	DV	Prepare-and-measure	2018

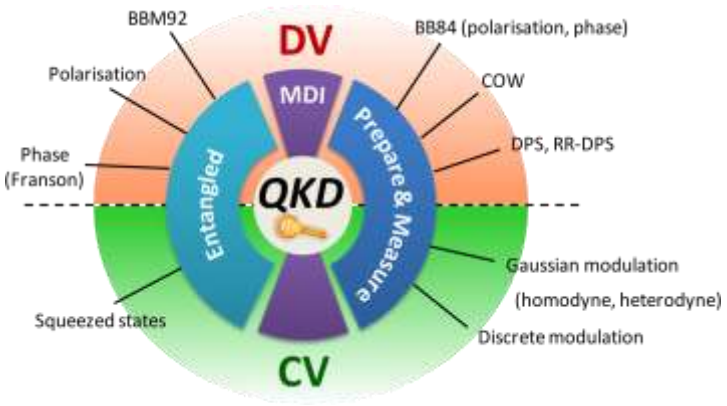


Figure 748: a map of QKD protocols between DV and CV ones. I don't cover them all in this book. Sources: Source: The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet by Yuan Cao, IEEE, 2021 (59 pages) and VSCW19-QKD-part1. https://quantum-uniqorn.eu/wp-content/uploads/2019/06/VSCW19-QKD-part.pdf .

QKD experiments and deployments

Many breakthrough symbolic experimental deployments of QKD have been done both in the open air and with optical fibers.

Open-air QKD demonstrations started in 1996 in the USA on a 75m distance, then on 144 km to connect the islands of La Palma and Tenerife in the **Canary Islands** and conducted by Austrians in 2007 and 2010[2327], in 2019 in urban areas in Italy with a distance of 145m[2328] and in India in 2022 over 300 m[2329].

An experiment took place in **Vienna** in 2008 as part of the European **SECOQC** (*SEcure COmmunication* based on Quantum Cryptography) project launched in 2004, involving some 40 research laboratories and vendors, using a "mesh" architecture and a CV-QKD optical link [2330].

This went on in Switzerland with **IDQ** with local banks. In 2007 they also set up an election vote counting system based on a QKD.

[2325] See the international review paper Advances in device-independent quantum key distribution by Víctor Zapatero et al, August 2022 (15 pages).

[2326] See Measurement-device-independent quantum key distribution by Hoi-Kwong Lo, Marcos Curty and Bing Qi, 2011 (7 pages) and this good overview of QKD and its technical challenges in Practical challenges in quantum cryptography by Eleni Diamanti et al, 2016 (25 pages).

[2327] See Second Generation QKD System over Commercial Fibers, 2016 (5 pages) et Feasibility of 300 km Quantum Key Distribution with Entangled States, 2010 (14 pages).

[2328] See Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics by Matteo Schiavon et al, July 2019 (7 pages). QKD key transmission over the 145m air link took place at 1550 nm in the infrared band that is commonly used in fiber optic transmissions and therefore compatible with many existing telecommunication equipment. They used a silicon chipset doing all the work with an error rate of only 0.5% and a data rate of 30 kbits/s. Their QCosOne ("Quantum Communication for Space-One") used telescopes with 120 and 315 mm optics for transmission and reception. It worked during daytime, but there were still problems in case of turbulence and depending on the time of day and the side effects coming from the sun. Performance was better in the evening. They used triple photon encoding: temporal, spatial and spectral.

[2329] See Indian Scientists Demonstrate Wireless Quantum Key Distribution Over 300 Meters by Matt Swayne, The Quantum Insider, February 2022.

[2330] See The SECOQC quantum key distribution network in Vienna by Romain Alléaume, Eleni Diamanti et al, 2016 (39 pages).

In 2018, the **UK** deployed its UK Quantum Communications hub between Bristol, London, Cambridge and Ipswich[2331].

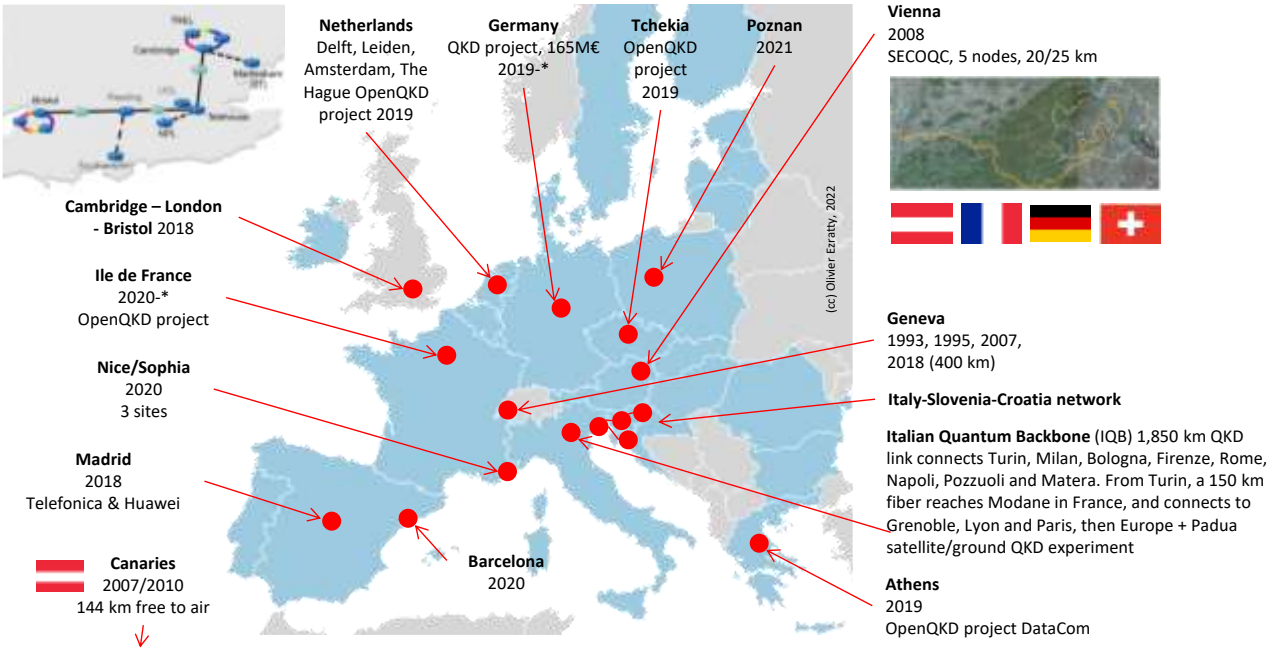


Figure 749: a map of QKD test deployments throughout Europe. (cc) Olivier Ezratty, 2022.

In France, **Orange** announced in May 2019 the launch of tests of a QKD protected communication with the University Côte d'Azur (UCA) which provides the solution via the InPhyNi laboratory. It connects the Valrose and Inria campuses in Sophia Antipolis with an access point on the Plaine du Var IMREDD campus in Nice, using dark fibers provided by the telecom operator[2332].

The test network was operational in September 2021. In particular, Orange is studying the reliability of trusted optical network nodes in such a configuration. The operator is also looking to combine QKD solutions to protect physical links and PQC solutions that could be used as a method of encrypting data transmitted in association with a QKD.

In **Denmark**, DTU launched a CV-QKD trial with Danske Bank[2333].

In **Greece**, Space Hellas and the University of Athens launched in 2022 a pilot QKD deployment after having started an OpenQKD project in 2019 with Datacom.

Cyprus announced in 2022 its deployment of a QKD network with a EuroQCI EU funding of 7.5M€ as part of the CYQCI project.

The European consortium **OpenQKD** is experimenting a terrestrial QKD network.

It prepares the ground for the launch of the **EuroQCI** network which would be an operational implementation of a terrestrial and satellite European QKD network[2334].

[2331] Seen in IDQ: Quantum-Safe Security relevance for Central Banks, 2018 (27 slides). The network was extended in Cambridge in 2019 as seen in Cambridge quantum network by J. F. Dynes et al, 2019 (8 pages).

[2332] See Experimenting quantum key exchange over the Côte d'Azur, Orange, December 2019. And for Orange's QKD projects in general: Orange and quantum technologies for secure data exchange, June 2020.

[2333] See First quantum-safe data transfer in the Nordic region by Anne Kirsten Frederiksen, February 2022.

[2334] See Nine more countries join initiative to explore quantum communication for Europe, December 2019 and Quantum communications infrastructure architecture: theoretical background, network structure and technologies. A review of recent studies from a European public infrastructure perspective by Adam M. Lewis and Petra F. Scudo, January 2022 (40 pages).

This involves in particular France, Germany, Austria, Italy, Spain, the Netherlands, Greece, Switzerland and Poland and vendors like Thales Alenia Space (satellite communication), Orange and Mellanox (a subsidiary of Nvidia). From a practical point of view, it's about deploying a large interoperable experimental QKD network on a European scale, exploited by applications in various fields (healthcare, energy grids, transportation, finance, government, education, and the likes). The consortium also intends to influence QKD standardization. And at last, as far as possible, it's also about contributing to the development of a European industry offering in QKD and associated technologies. There is at last a deployment of QKD across Italy, Slovenia and Croatia[2335]. In France, the test area will be the Paris region and its major research laboratories with the Institut d'Optique, Telecom Paris, LIP6 in Jussieu and Nokia labs in Villarceau. The project has received €15M in European funding from Horizon 2020, independently of Quantum Flagship. Thales announced in December 2021 that it was participating to the QSAFE consortium with Deutsche Telekom, Telefonica and the AIT (Austrian Institute for Technologies) to create a European quantum telecommunication infrastructure as part of EuroQCI, with both terrestrial and satellite links.

In **USA**, the first experiments were conducted in Boston by **DARPA** between 2004 and 2007. A QKD network piloted by **Battelle** was tested in Ohio in 2013[2336]. Tests were also conducted in 2015 at **MIT**, linking two sites 43 km apart. A commercial deployment of QKD on an unused 800 km fiber optic network connecting Boston to Washington DC is also being deployed by **Quantum Xchange** and **Zayo**, to connect Wall Street finance businesses with their back-offices in New Jersey. It uses some trusted node technology[2337]. An 85 km facility was also deployed in Chicago in 2019[2338]. In July 2020, the Department of Energy announced the expansion of the QKD network to link all of its research laboratory sites[2339].

In 2022, it connected the DoE Argonne and Fermi labs and enabled fast network synchronization of quantum and classical signals coexisting on the same optical fiber over a distance of 59 km[2340].

In **Canada** launched in November 2020 its Canada Quantum Network through a partnership between Xanadu, the Creative Destruction Lab and the startups service company MaRS around Toronto.

In **India**, the Defence Research and Development Organisation (DRDO) with IIT Delhi demonstrated a QKD for a distance of 100 km.

In **Japan**, Toshiba announced in September 2018 that a QKD solution co-developed with the Tohoku Medical Megabank Organization (ToMMo) at Tohoku University had achieved a QKD throughput of more than 10 Mbps during one month.

In **Singapore**, the Quantum Engineering Program (QEP, launched in 2018) from the National University of Singapore (NUS) launched the National Quantum-Safe Network (NQSN) which is starting classical and quantum network trials supporting both QKD and PQC.

[2335] See Deploying an inter-European quantum network by Domenico Ribezzo et al, March 2022 (8 pages).

[2336] See Battelle Installs First Commercial Quantum Key Distribution Protected Network in U.S., 2013.

[2337] See New plans aim to deploy the first US quantum network from Boston to Washington, DC, October 2018. Schema source: From MIT : Semiconductor Quantum Technologies for Communications and Computing, 2017, 32 slides).

[2338] See Argonne and UChicago scientists take important step in developing national quantum internet by Louise Lerner, February 2020.

[2339] See Department of Energy (DOE) Unveils Blueprint for a U.S. Quantum Internet by Doug Finke, July 2020.

[2340] See Quantum Network Between Two National Labs Achieves Record Synch by Matt Swayne, June 2022 and Picosecond Synchronization of Photon Pairs through a Fiber Link between Fermilab and Argonne National Laboratories by Keshav Kapoor et al, August 2022 (7 pages).

They plan to have 10 fiber nodes. This is done in partnership with Amazon Web Services and Thales. One of the challenges in deploying QKD is the miniaturization of its components. Whereas initially a complete rack of hardware was needed for quantum key transmitting/receiving stations, the goal is to fit everything in a photonics component a few mm long. This is what **NTU** researchers in Singapore did in 2019 to manage a CV-QKD supporting existing telecom operators' fiber infrastructures[2341]. But this miniaturization concerns here only the photonics part. These photonic circuits have to be completed by classical electronic components.

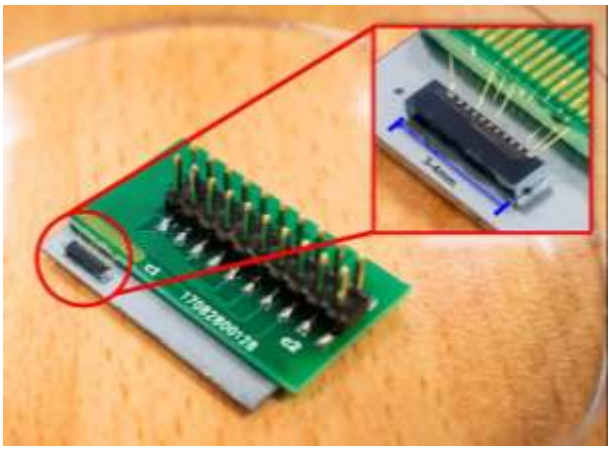


Figure 750: Source: Researchers create quantum chip 1,000 times smaller than current setups, PhysOrg, October 2019

The development of such integrated photonics components will also be supported in the framework of European Horizon Europe projects that follows Europe 2020 projects over the 2021-2027 period.

China stands out since 2016 with impressive QKD experiments and deployments. The country invests heavily in QKD with a now classical multi-pronged strategy: to protect its sensitive communications against any attacker and to develop an industry in a promising emerging technology field. A first deployment was carried out in 2012 in the Hefei area to link various Chinese government entities[2342].

It was then expanded with an installation of a QKD-secured fiber optic link between Shanghai and Beijing, covering 2,000 km. The line installed between 2013 and 2016 was deployed by a local startup, **QuantumCTek**.

The network relies on 32 transponders with secured physical access[2343]. Indeed, the signal attenuation was then too strong beyond about 50 km on one optical fiber.

Figure 751: China's QKD backbone. Source: 2019.

The entities using this line are government agencies, including various financial sector regulatory agencies and banks. The country also plans to protect its energy grid infrastructure with this network[2344].

[2341] See Researchers create quantum chip 1,000 times smaller than current setups, PhysOrg, October 2019 which references An integrated silicon photonic chip platform for continuous-variable quantum key distribution by G. Zhang et al, December 2019 (5 pages).

[2342] See Unhackable Chinese Communication Network Launches Soon by Rechelle Ann Fuertes, 2017.

[2343] Source: Security assessment and key management in a quantum key distribution network by Xiongfeng Ma, June 2019 (21 slides).

[2344] See Application In Power Industry Promotes the Development of Quantum Cryptography Technology by Yonghe Guo, June 2019 (13 slides).

China then launched in 2017 a deployment of an additional 33,000 km of the **National Quantum Secure Communication Backbone Network**, to be completed by 2025. It had started with the creation of a Hefei-Wuhan link[2345]. Hefei is the city where Jian-Wei-Pan's main quantum technologies laboratory is located[2346].

QKD by satellite, UAVs and underwater

Satellite quantum communication is another mean to distribute quantum keys that makes sense over long distance. These keys can be shared across two locations while the encrypted data may be transported in more classical terrestrial means. This would be theoretically simpler than using QKD distribution over large fiber networks full of (so far, non-existent) quantum repeaters.

One advantage is that the photon loss is much lower with satellites than with fibers. Indeed, with satellites, photon losses coming from the atmospheric absorption and scattering occurs only in the lower 10 km of the atmosphere, with about a 3 dB loss on a clear day. The rest of the distance is in near vacuum, with nearly no absorption and decoherence and the loss caused by beam diffraction is approximately proportional to the square of distance whereas the losses in fiber are mainly due to the absorption and scattering of the fiber medium, which is proportional to the exponent of the distance.

It means that for long communicating distances of several hundred km, satellite-ground channels have an advantage over fiber-based channels in terms of channel losses[2347]. China was a pilot country in that area, the use of the **Micius** satellite also named **Mozi** for a western/Chinese pronunciation and **QUESS** (Quantum Experiments at Space Scale).

It was used for running several different experiments: a satellite-to-ground decoy-state QKD with KHz keyrate over a distance of up to 1200 km and satellite-replayed intercontinental key exchange, a satellite-based entanglement distribution to two Earth locations separated by 1205 km and a ground-to-satellite qubit teleportation [2348] . The satellite weighs 640 kg and consumes 560W.

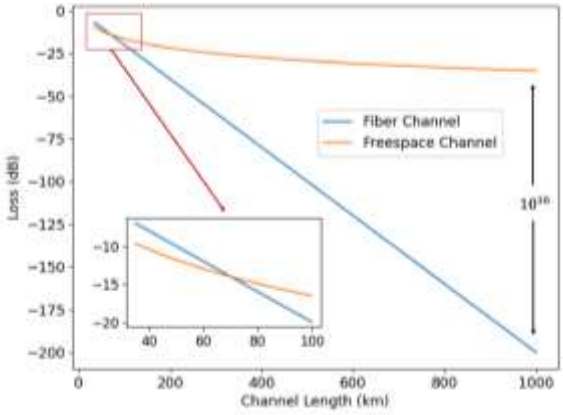


FIG. 10 Typical losses in fiber and free-space channels. The attenuation parameter of fiber is $\sim 0.2\ dB/km$. The parameters of free-space channel are based on the design of Micius satellite. The free-space channel shows advantage for a distance over ~ 70 km

Figure 752: how photon losses compare between fiber and freespace channel using satellite. Source: Micius quantum experiments in space by Chao-Yang Lu, Yuan Cao, Cheng-Zhi Peng and Jian-Wei Pan, August 2022 (53 pages).

[2345] See Towards large-scale quantum key distribution network and its applications by Hao Qin, 2019 (17 slides).

[2346] The extended BB84 based QKD network is documented in Implementation of a 46-node quantum metropolitan area network by Teng-Yun Chen et al, September 2021 (14 pages). It describes the intra-metropolitan network infrastructure deployed in Hefei, with 46 nodes.

[2347] This paragraph is largely inspired from the excellent and well detailed review paper Micius quantum experiments in space by Chao-Yang Lu, Yuan Cao, Cheng-Zhi Peng and Jian-Wei Pan, August 2022 (53 pages).

[2348] See respectively Satellite-to-ground quantum key distribution by Sheng-Kai Liao, Jian-Wei Pan et al, Nature, August 2017 (18 pages), Satellite-Relayed Intercontinental Quantum Network by Sheng-Kai Liao, Jian-Wei Pan et al, PRL, 2018 (10 pages), Satellite-to-ground entanglement-based quantum key distribution by Juan Yin, Jian-Wei Pan et al, PRL, 2017 and Ground-to satellite quantum teleportation by Ji-Gang Ren, Jian-Wei Pan et al, Nature, 2017 (16 pages). The principle was first described in 1993 in Teleporting an Unknown Quantum State via Dual Classical and EPR Channels by Charles Bennett, Gilles Brassard (from Montreal), Claude Crépeau, Richard Jozsa, Asher Peres and William Wootters. See also Quantum Communication at 7,600km and Beyond by Chao-Yang Lu and Cheng-Zhi Peng, Jian-Wei Pan, November 2018.

A 2018 experiment was about creating a videoconference between China and Austria using a quantum key sent every minute[2349]. Why with Austria? Because Jian-Wei Pan did his PhD thesis in Austria under the supervision of Anton Zeilinger, who piloted the European part of the experiment.

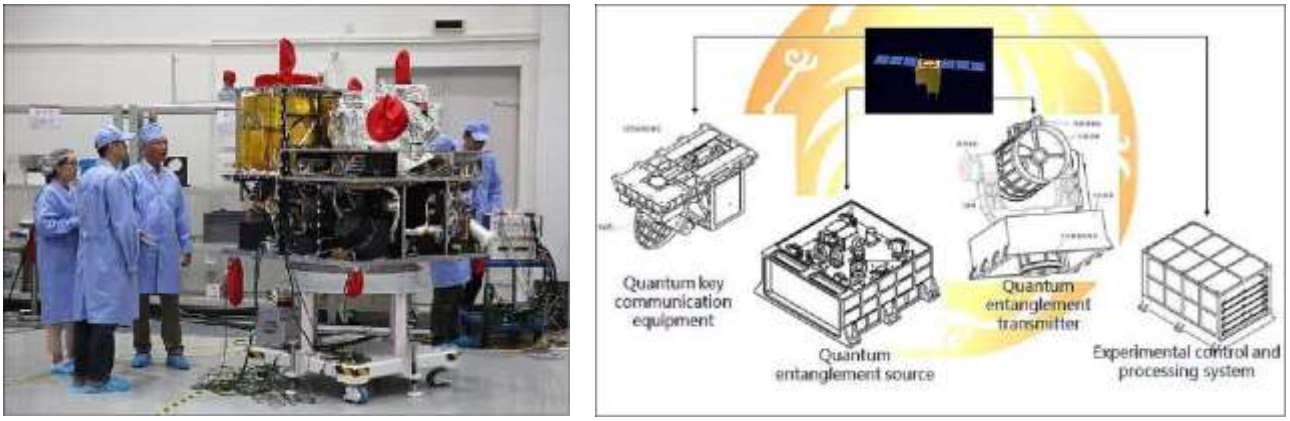


Figure 753: a QKD satellite.

China is planning to launch a cloud of satellites in low orbit by 2030 dedicated to sending quantum keys by repeating this process[2350]. If they are banking on QKD for symmetric key management, it seems that China is also investing in post-quantum cryptography but in a quieter way.

But this satellite experiment had limitations: it could handle 5.9 million pairs of entangled photons per second, but due to error corrections, only one useful photon pair was exploitable per second[2351]. As a result, Chinese scientists are studying scheduling approaches to load balance key distribution over time[2352]. Also, it works only by night!

At the beginning of 2020, China announced that it had miniaturized its ground receiving station for quantum key communication with the Micius satellite from 10 tons to 80 kg. The key bitrate was reduced, from 40Kbits/s to 4-10Kbits/s. The experiment took place on the Earth side in Jinan and Shanghai, so it seems at sea level[2353] . The Bank of China would already secure transactions by sending keys via the Micius/Mozi Beijing satellite and remote provinces.

In June 2019, Chinese researchers announced that they had demonstrated the use of optical QKD aerial links established within a network of 35 kg octocopter UAVs spaced 200 m apart during a 40-minute flight at an altitude of 100 m[2354].

[2349] See Real-world intercontinental quantum communications enabled by the Micius satellite, USTC, PhysOrg, January 2018. Experiments or equivalent experiences have been launched by European teams. See Quantum Photonics Technologies for Space, October 2018 (22 pages) and Nanobob CubeSat mission, 2018 (31 pages). This is also being done in the UK, where an experimental Cubesat micro-satellite project is planned to cover the country. See QUARC: Quantum Research Cubesat - A Constellation for Quantum Communication by Luca Mazzarella et al, 2020 (27 pages).

[2350] See some details on the satellite QKD deployment architecture in Approaches to scheduling satellite-based quantum key distribution for the quantum network by Xingyu Wang et al, 2021 (11 pages).

[2351] See A step closer to secure global communication by Eleni Diamanti, Nature, June 2020, which describes the practical conditions and limitations of these satellite key transmission experiments. And in particular the most recent one described in Entanglement-based secure quantum cryptography over 1,120 kilometers by Juan Yin et al, Nature, June 2020. The actual key bitrate was 0.12 bits per second!

[2352] See Approaches to scheduling satellite-based quantum key distribution for the quantum network by Xingyu Wang et al, 2021 (11 pages).

[2353] See China has developed the world's first mobile quantum satellite station by Donna Lu, January 2020.

[2354] See Drone-based all-weather entanglement distribution by Hua-Ying Liu et al, May 2019 (16 pages) and World's First "Quantum Drone" for Impenetrable Air-to-Ground Data Links Takes Off by Charles Q. Choi, IEEE Spectrum.

The payload handling quantum communication weighted 11.8 kg. It can still be miniaturized, since the Chinese are aiming to integrate it into mass-market UAVs.

China was also proud to announce in 2021 that they had created the world's first integrated quantum communication network, combining 700 terrestrial optical fibers with two ground-to-satellite links, achieving quantum key distribution over 4,600 km[2355]. China researchers also developed a portable ground satellite QKD station of only 100 kg[2356].

China announced yet another premiere in August 2022, with transmitting QKD keys from its **Tiangong-2** space lab to four ground stations who are also connected to Micius which is positioned in a higher orbit, thanks to using Tiangong-2 as a repeater[2357].

But China is not alone there.

Singapore and its universities and startups are working on CubeSat based tiny QKD distribution satellites[2358].

In **Europe**, there are also satellite QKD plans and architecture proposals[2359]. The EU is planning the launch of a 6B€ satellite program announced in February 2022 with QKD support, to be deployed by 2028. Eleni Diamanti's team in France is working on using adaptive optics to improve key sharing with satellite[2360]. Another project run by a 20-company consortium led by SES (Astra) and the European Space Agency with the support of the EU is planning the launch in 2024 of its EAGLE-1 QKD low-earth orbit satellite-based system.

NASA's SEAQUE (Space Entanglement and Annealing QUantum Experiment) is a small experiment being launched in the ISS to test photon entanglement distribution in space, particularly to assess self-healing solutions against radiation damages. The project has contributions from the USA, Canada and Singapore. The experiment designed by **AdvR** (2019, USA) is to be docked outside the ISS in the "Bishop airlock" that is by Nanoracks, a private in-space services company[2361].

And beyond Earth, some are even devising about how some extraterrestrial civilization could communicate with us with entangled photons. I'm just wondering how these photon sources could be detected out of the noise coming from distant stars, even using all the technologies around to detect exoplanets (transit methods, spectrography, etc.)[2362].

After space, how about distributing QKD underwater? It's not a joke. It's being investigated in Turkey and in China[2363]! The first simulations deal with 10 to 40 m distances. It's far from being sufficient to enable communications with submarines, particularly of the nuclear breed.

[2355] See Chinese Scientists Report World's First Integrated Quantum Communication Network by Matt Swayne, 2021.

[2356] See Portable ground stations for space-to-ground quantum key distribution by Ji-Gang Ren, Jian-Wei Pan and al, May 2022 (9 pages).

[2357] See Space–ground QKD network based on a compact payload and medium-inclination orbit by Yang Li et al, Optica, August 2022 (6 pages).

[2358] See A CubeSat platform for space based quantum key distribution by Srihari Sivasankaran et al, April 2022 (6 pages).

[2359] See Satellite-based Quantum Information Networks: Use cases, Architecture, and Roadmap by Laurent de Forges de Parny, Eleni Diamanti, Sébastien Tanzilli et al, February 2022 (21 pages).

[2360] See Analysis of satellite-to-ground quantum key distribution with adaptive optics by Valentina Marulanda Acosta, Eleni Diamanti et al, November 2021 (17 pages).

[2361] See NASA is launching a new quantum entanglement experiment in space by Charlotte hu, March 2022.

[2362] See Viability of quantum communication across interstellar distances by Arjun Berera and Jaime Calderón-Figueroa, June 2022 (18 pages), a fancy topic that was covered everywhere like in Mathematical calculations show that quantum communication across interstellar space should be possible by Bob Yirka, Phys.org, July 2022.

[2363] See On the Optimization of Underwater Quantum Key Distribution Systems with Time-Gated SPADs by Amir Hossein Fahim Raouf and Murat Uysal, Ozyegin University in Istanbul, June 2022 (6 pages) and Practical underwater quantum key distribution based on decoy-state BB84 protocol, by Shanchuan Dong et al, March 2022 (10 pages).

QKD photon sources and detectors

We've already covered photon sources for quantum computing and seen some of their requirements like the creation of deterministic and indistinguishable photons, on top of the even harder challenge to create large clusters of entangled photons.

The challenges with photons generation for QKD are not the same. What is required are steady streams of individual photons, preferably generated in the telecom wavelengths between 1200 nm and 1550 nm. Entanglement based QKD also requires the generation of entangled pairs of photons. At last, these sources should be lightweight and easy to integrate in telecom infrastructures. Preferably, they shouldn't be power hungry and not require cryogeny, thus a preference for ambient temperature solid-state solutions.

The breath of technologies used or investigated for photon generation is amazing. Let's mention a few of these recent advances:

- **GaAs quantum-dot** single photon sources with high-source brightness ensuring high-speed quantum communication[2364]. A record of 175 km distance was broken in 2022 using GaAs/In-GaAs quantum dots and a finite key rate of 13 kbps over 100 km[2365].
- **AlGaAs sources** with spontaneous parametric down-conversion (SPDC) enable the creation of polarization and/or frequency entangled sources of photons at telecom wavelengths[2366].
- **InAs** quantum dots embedded in GaAs with a conversion to telecom wavelength at 1550 nm generating indistinguishable photons[2367].
- **Silicon with carbon atoms defects** creating optical wavelengths photon at 1279 nm[2368].
- **Vanadium defects in silicon-carbide** operating between 100mK and 3K with the benefit from a relative long stability[2369].

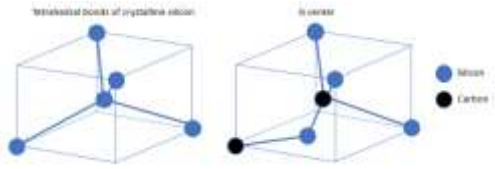


Figure 754: a G center and its two carbon atoms.

- **Si-based SPDC** to create pairs of entangled photons[2370].

[2364] See Enhancing quantum cryptography with quantum dot single-photon sources by Mathieu Bozzio et al, April 2022 (37 pages).

[2365] See Single-emitter quantum key distribution over 175 km of fiber with optimised finite key rates by Christopher L. Morrison et al, September 2022 (9 pages).

[2366] See On-chip generation of hybrid polarization-frequency entangled biphoton states by S. Francesconi, Sara Ducci, Perola Milman et al, MPQ and C2N, July 2022 (10 pages) and Broadband biphoton generation and polarization splitting in a monolithic AlGaAs chip by Félicien Appas, Sara Ducci et al, August 2022 (16 pages).

[2367] See A Pure and indistinguishable single-photon source at telecommunication wavelength by Beatrice Da Lio et al, January 2022 (7 pages).

[2368] See Single G centers in silicon fabricated by co-implantation with carbon and proton by Yoann Baron, Anais Dréau et al, April 2022 (5 pages). The electronically active G center is a complex of two substitutional carbon atoms and an interstitial silicon atom. See also the review paper on silicon defects A bright future for silicon in quantum technologies by Mario Khoury and Marco Abbarchi, 2022 (12 pages). Another intrinsic silicon defect resulting from irradiation of Si crystals is also studied, aka the W-center. See Detection of single W-centers in silicon by Yoann Baron, Jean-Michel Gérard, Vincent Jacques, Isabelle Robert-Philip, Anais Dréau et al, April 2022 (10 pages). See also Wafer-scale nanofabrication of telecom single-photon emitters in silicon by M. Hollenbach et al, April 2022 (20 pages) that covers the controllable fabrication of single G and W centers in silicon wafers using focused ion beams (FIB) with a probability exceeding 50%.

[2369] See Vanadium in Silicon Carbide: Telecom-ready spin centres with long relaxation lifetimes and hyperfine-resolved optical transitions by T. Astner et al, June 2022 (9 pages).

[2370] See Near perfect two-photon interference out a down-converter on a silicon photonic chip by Romain Dalidet, Sébastien Tanzilli, Camille-Sophie Brès et al, InPhyNi at Nice in France, EPFL and Ligentec. February 2022 (8 pages).

- **Silicon-nitride MRR** (microring resonator) that are able to generate 8 pairs of heralded entangled photons directly in the telecom wavelengths around 1550 nm [2371]. Microring resonators are tiny optical waveguides looped back onto themselves in circle or spiral, usually implemented in silicon semiconductors. They enable interference phenomena, the creation of delay lines, and the likes[2372].
- **CV-QKD squeezed states** preparation with off-the-shelf telecom equipment[2373].

Then, we have photon detectors and counters. They use various techniques depending on the QKD protocol used (entangled-based or not, etc.).

SPD (single-photon detectors) are used after the photons traverse a polarization filter. The main variants are:

- **APD**, avalanche photodiodes.
- **SPAD,** single photon avalanche photodiode which can detect single photons.
- **SNSPD**, superconducting nanowire single-photon detector, which require <4K cooling[2374].
- Silicon-based **VLPC** (visible light photon counter).

QKD nodes and repeaters

The range of QKD transmission over fiber has improved with only 30 cm in 1989 (IBM with Charles Bennett), 1100 m at the University of Geneva in 1993, then 23 km in 1995 with the BB84 protocol, all via fiber optics. China researchers created a 404 km QKD fiber connection without a repeater in 2016[2375], then extended this record in 2020 to 509 km of transmission without repeater[2376] and to 511 km using the TF-QKD protocol[2377]. The technique was improved in 2020 by a mix of British and American researchers to reach 600 km[2378].

The record was broken in 2022 with 833 km as shown in Figure 755 [2379]. In Austria, an entanglement distribution was achieved over 248 km in 2022[2380].At these large distances, the error rates are so high that it becomes impractical. The key rates are very low, getting under 10^{-7} for distances larger than 400 km. There is even a upper bound for these key rates, $-\log_2(1-\eta)$ with η being the transmissivity of the lossy quantum channel, whatever the protocol[2381].

[2371] See High-quality multi-wavelength quantum light sources on silicon nitride micro-ring chip by Yun-Ru Fan et al, September 2022 (13 pages). Works with silicon chipsets and at ambient temperature. Creates 8 pairs of frequency multiplexed heralded entangled photons.

[2372] See the review paper Silicon microring resonators by Wim Bogaerts et al, Laser & Photonics Review, 2012 (27 pages).

[2373] See Plug-&-play generation of non-Gaussian states of light at a telecom wavelength by Mohamed Faouzi Melalkia, Sébastien Tanzilli, Virginia D'Auria et al, May 2022 (6 pages).

[2374] See an example with Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution by Xiaodong Zheng et al, October 2021 (8 pages).

[2375] Documented in Measurement device independent quantum key distribution over 404 km optical fiber, 2016 (15 pages).

[2376] Seer Study achieves a new record fiber QKD transmission distance of over 509 km by Ingrid Fadelli, March 2020.

[2377] See Twin-Field Quantum Key Distribution over 511 km Optical Fiber Linking two Distant Metropolitans by Jiu-Peng Chen, Jian-Wei Pan et al, January 2021 (32 pages).

[2378] See 600-km repeater-like quantum communications with dual-band stabilization by Mirko Pittalugal et al, 2020 (14 pages).

[2379] See Twin-field quantum key distribution over 830-km fibre by Shuang Wang et al, Nature, January 2022 with a 140 dB loss!

[2380] See Continuous entanglement distribution over a transnational 248 km fibre link by Sebastian Philipp Neumann et al, March 2022 (23 pages).

[2381] See Fundamental Limits of Repeaterless Quantum Communications by Stefano Pirandola et al, 2017 (61 pages).

Quantum channels used for QKD are subject to noise and leaks. Transmitting a useful photon requires several trials and its number grows exponentially with distance. And when the photon arrives at destination, its state fidelity also decreases exponentially with distance. As a result, for large distances, we need nodes and/or repeaters. They must guarantee a good key rate and fidelity and be tolerant to errors. They are essential for distributing quantum keys over long distances, beyond 80 km[2382]. QKD networks also use classical optical switches using frequency multiplexing. It enables the routing of QKD signals from one emitter to different receivers, but once at a time. They also use SDN (software defined network) to dynamically configure the networks and their nodes, particularly trusted nodes.

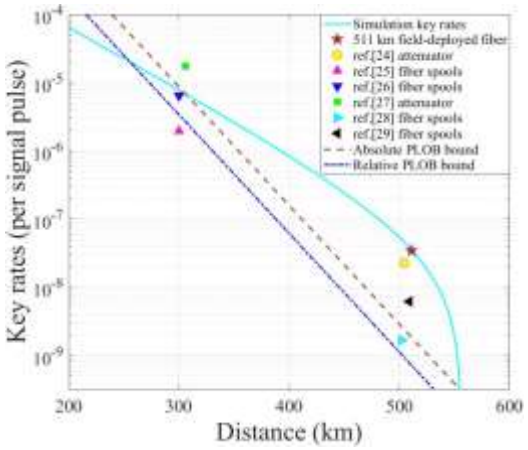


Figure 755: relationship of QKD keyrates and distance without repeaters. Source: See Twin-Field Quantum Key Distribution over 511 km Optical Fiber Linking two Distant Metropolitans by Jiu-Peng Chen, Jian-Wei Pan et al, January 2021 (32 pages).

There are three main kinds of nodes and repeaters:

Trusted node relays where keys must be revealed classically in the intermediate stations, thus the need for it to be in "trusted" locations. These nodes are mostly used with the BB84 protocol but can also work with entanglement-based QKDs. They can be implemented to create an arbitrary distance QKD connection. This is the dominant solution. It is used in the 2,000 km Beijing-Shanghai QKD line and in the various EU OpenQKD projects.

Untrusted node relays are safer than trusted node relays work but work only with the family of entanglement-based QKD protocols like MDI-QKD and for relatively short distance. It avoids security loopholes at the measurement side and allows the relay to be controlled by an eavesdropper without endangering the security of the shared keys. Complex networks can contain both trusted and untrusted nodes depending on their location and physical safety.

Quantum repeaters which are safer than trusted node repeaters. They use entanglement swapping techniques which keep the key sharing link quantum from end-to-end between Alice and Bob. They do not implement any measurement or cloning but, instead, quantum states purification which consists in keeping trusted entangled pairs selected out of many imperfect pairs. They must usually be equipped with some form of quantum memory to propagate the state of the photons to be transmitted through entanglement swapping[2383]. These quantum memories are still unproven and a field of fundamental research. These are different kinds of quantum memories than the ones that needed for quantum computing and that we covered in the quantum memory part starting page 244. These quantum memories for quantum repeaters need a single qubit per link.

[2382] Knowing that the record distance for quantum telecommunication without repeaters is 509 km as we have already seen. See also Viewpoint: Record Distance for Quantum Cryptography by Marco Lucamarini, Toshiba & Cambridge, November 2018 and Recent progress on Measurement-Device-Independent (MDI) Quantum Key Distribution (QKD) by Marco Lucamarini, 2018 (71 slides).

[2383] See Quantum Nodes for Quantum Repeaters by Hugues de Riedmatten, ICFO, January 2021 (60 slides).

It can be implemented with cold atoms[2384], trapped ions[2385], rare earth doped crystals[2386] and NV centers[2387], which can also be arranged in arrays[2388] and use all-photonic quantum processes (APQR)[2389].

These repeaters technologies are still at basic research stage and with some limitations[2390]. The DLCZ protocol created by Harvard, Austria and China scientists in 2001 made it possible to improve entanglement sharing on lossy communication channels and has been continuously improved since then[2391]. It is based on using clouds of identical atoms instead of individual atoms, beam splitters and single-photon detectors with moderate efficiencies with a communication efficiency that scales polynomially with distance.

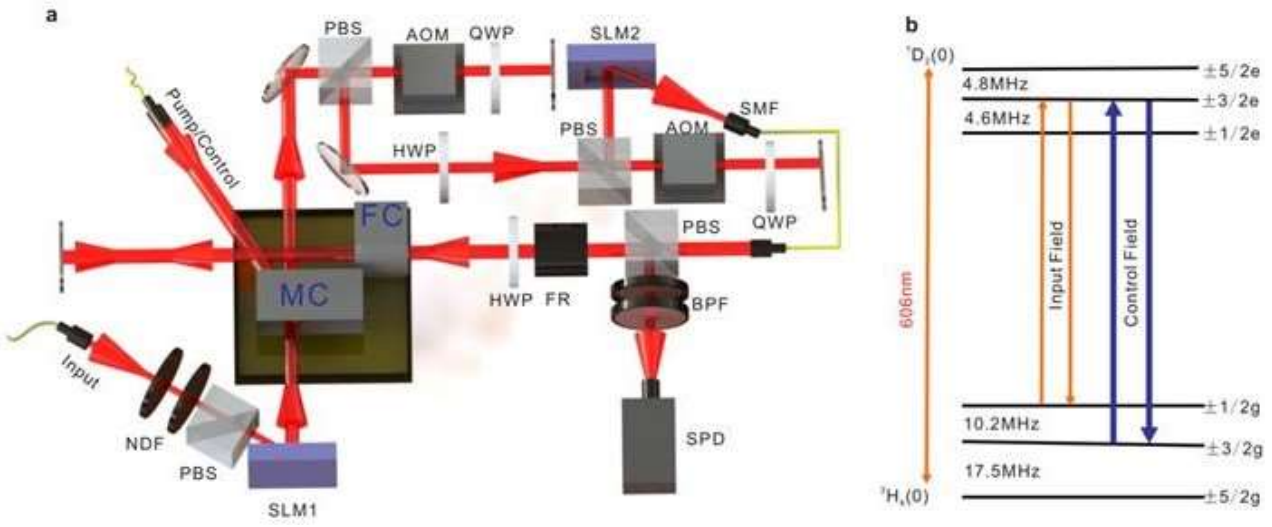


Figure 756: schematic for an atomic based quantum memory for a quantum repeater. Source: Multiplexed storage and real-time manipulation based on a multiple-degree-of-freedom quantum memory, by Tian-Shu Yang et al, China CAS, 2018 (9 pages).

[2384] See Entangling single atoms over 33 km telecom fibre by Tim van Leent et al, Nature, July 2022 (16 pages).

[2385] See the thesis A memory-based quantum network node with a trapped ion in an optical fibre cavity by Pascal Kobel, 2021 (222 pages). It uses ytterbium ions which have coherence time exceeding the second range and transitions in the microwave band. See also A telecom-wavelength quantum repeater node based on a trapped ion processor by Victor Krutyanskiy, Marco Canteri, Martin Meraner, James Bate, Vojtech Krcmarsky, Josef Schupp, Nicolas Sangouard and Ben P. Lanyon, October 2022 (31 pages),

[2386] See Storage of photonic time-bin qubits for up to 20 ms in a rare-earth doped crystal by Antonio Ortu, Adrian Holzäpfel, Jean Etesse and Mikael Afzelius, npj, March 2022 (7 pages) describes a 20 ms quantum memory using crystals doped with europium, operating near 0K, On-demand storage of photonic qubits at telecom wavelengths by Duan-Cheng Liu et al, January 2022 (11 pages) which uses erbium-yttrium crystals, Storage and analysis of light-matter entanglement in a fiber-integrated system by Jelena v. Rakonjac et al, Science Advances, July 2022 (6 pages) with praseodymium and yttrium, On-demand Integrated Quantum Memory for Polarization Qubits by Tian-Xiang Zhu et al, January 2022 (20 pages) with europium and yttrium, Remote distribution of non-classical correlations over 1250 modes between a telecom photon and a $^{171}Yb^{3+}$ Y_2SiO_5 crystal by Moritz Businger et al, Université de Genève, Chimie ParisTech and Sorbonne Université, May 2022 (8 pages) that uses ytterbium and yttrium and Multiplexed storage and real-time manipulation based on a multiple-degree-of-freedom quantum memory, by Tian-Shu Yang et al, China CAS, 2018 (9 pages).

[2387] See Proposal for room-temperature quantum repeaters with nitrogen-vacancy centers and optomechanics by Jia-Wei Ji et al, University of Calgary, March 2022 (20 pages).

[2388] See Electric-Field Programmable Spin Arrays for Scalable Quantum Repeaters by Hanfeng Wang et al, April 2022 (12 pages).

[2389] See Loss-tolerant all-photonic quantum repeater with generalized Shor code by Rui Zhang et al, March 2022 (8 pages).

[2390] See Tutorial on quantum repeaters by Rodney Van Meter and Tracy Northup, 2019 (178 slides), Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, 2018 (5 pages), An Information-Theoretic Framework for Quantum Repeaters by Roberto Ferrara, 2018 (144 pages) and Quantum Internet Protocol Stack: a Comprehensive Survey by Jessica Illiano et al, February 2022 (25 pages) which explains how entanglement is used as a resource in quantum Internet and how it is handled in quantum repeaters. Quantum repeaters, namely, devices implementing the physical process called entanglement swapping and perform a BSM (Bell state measurement). It then covers higher level quantum Internet protocols proposals.

[2391] See Long-distance quantum communication with atomic ensembles and linear optics by Lu-Ming Duan, Mikhail Lukin, Juan Ignacio Cirac and Peter Zoller, Nature, May 2001 (11 pages).

In July 2019, Chinese researchers announced that they succeeded using a photonic repeater technology based on 12-photon interferometers without any quantum memory, encoding a qubit in a cluster state and using error correction in repeaters [2392]. In mid-2019, other Chinese researchers experimented the teleportation of qutrits, allowing a transmission of more information per photons[2393]. This could be used to increase the rate of QKD key transmission.

Securing QKD

QKD is not the solution-that-fixes-all-problems. It can be subject to jamming, denial of services and various attacks which we cover later. Its safety also depends on the security of both ends of telecommunication like with any other solution.

Securing a chain depends on its weakest links and here it is the transmitters and receivers before they even exchange via a QKD. Furthermore, QKDs are not a panacea because they depend on a point-to-point link and not on a routing technique that allows several paths to be used.

Attack	Target component	Tested system
Distinguishability of decoy states A. Huang *et al.,* Phys. Rev. A **98**, 012330 (2018)	laser in Alice	3 research systems
Intersymbol interference K. Yoshino *et al.,* poster at QCrypt (2016)	intensity modulator in Alice	research system
Laser damage V. Makarov *et al.,* Phys. Rev. A **94**, 030302 (2016); A. Huang *et al.,* poster at QCrypt (2018)	any	5 commercial & 1 research systems
Spatial efficiency mismatch M. Rau *et al.,* IEEE J. Sel. Top. Quantum Electron. **21**, 6600905 (2015); S. Sajeed *et al.,* Phys. Rev. A **91**, 062301 (2015)	receiver optics	2 research systems
Pulse energy calibration S. Sajeed *et al.,* Phys. Rev. A **91**, 032326 (2015)	classical watchdog detector	ID Quantique
Trojan-horse I. Khan *et al.,* presentation at QCrypt (2014)	phase modulator in Alice	SeQureNet
Trojan-horse N. Jain *et al.,* New J. Phys. **16**, 123030 (2014); S. Sajeed *et al.,* Sci. Rep. **7**, 8403 (2017)	phase modulator in Bob	ID Quantique
Detector saturation H. Qin, R. Kumar, R. Alleaume, Proc. SPIE 88990N (2013)	homodyne detector	SeQureNet
Shot-noise calibration P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A **87**, 062313 (2013)	classical sync detector	SeQureNet
Wavelength-selected PNS M.-S. Jiang, S.-H. Sun, C.-Y. Li, L.-M. Liang, Phys. Rev. A **86**, 032310 (2012)	intensity modulator	(theory)
Multi-wavelength H.-W. Li *et al.,* Phys. Rev. A **84**, 062308 (2011)	beamsplitter	research system
Deadtime H. Weier *et al.,* New J. Phys. **13**, 073024 (2011)	single-photon detector	research system
Channel calibration N. Jain *et al.,* Phys. Rev. Lett. **107**, 110501 (2011)	single-photon detector	ID Quantique
Faraday-mirror S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A **83**, 062331 (2011)	Faraday mirror	(theory)
Detector control I. Gerhardt *et al.,* Nat. Commun. **2**, 349 (2011); L. Lydersen *et al.,* Nat. Photonics **4**, 686 (2010)	single-photon detector	ID Quantique, MagiQ, research systems

Figure 757: QKD sources of vulnerabilities. Source: QKD Measurement Devices Independent by Joshua Slater, 2014 (83 slides).

This could lead to a form of denial of service by blocking the used physical communication, but rerouting techniques are investigated[2394]. The table in Figure 757 lists a whole bunch of vulnerabilities in the QKD, many of which having since been removed [2395].

[2392] See Scientists Firstly Realize All-photonic Quantum Repeater, July 2019 and Experimental quantum repeater without quantum memory by Zheng-Da Li et al, 2019 (12 pages).

[2393] See Qutrits experiments are a first in quantum teleportation by Daniel Garisto in Scientific American, August 2019, which refers to Experimental multi-level quantum teleportation by Xiao-Min Hu et al, April 2019 (12 pages) and Quantum teleportation in high dimensions by Yi-Han Luo, June 2019 (23 pages).

[2394] On QKD vulnerabilities and methods to avoid them, see QKD Measurement Devices Independent by Joshua Slater, 2014 (83 slides).

[2395] See Certification of cryptographic tools by Vadim Makarov from Quantum Hacking Lab in Moscow, 2019 (15 slides).

All the side-channel attacks from the table in Figure 757 that can be typically fixed with countermeasures. But the more fundamental issue of device independence, linked to the need of loophole free Bell test will be very difficult to implement practically. Work is very active in the area[2396].

Cryptography is fascinating for the speed at which security devices can be broken by researchers before they are deployed en masse. Thus, QKDs would be vulnerable due to an implementation vulnerability associated with Bell's theorem that can be handled with better quality detectors[2397]. It's a never-ending race!

QKD and Blockchain

Another example is this project to use QKD to secure a Blockchain. This is obviously delicate to deploy end-to-end on a large scale. Indeed, Blockchain users don't have a satellite link in the mountains or a secured fiber on hand, even when they are mobile.

But so be it. This is the proposal of Evgeny Kiktenko of the Russian Quantum Center in Moscow[2398] and Del Rajan and Matt Visser of Victoria University of Wellington in New Zealand[2399]. Why exactly is not all data transmitted protected in the same way as the QKD? It seems at least to be limited by the low bitrate of existing QKDs. Still, JPMorgan Chase, Toshiba and Ciena are piloting a QKD network of 100 km mixed fibers (handling both QKD and classical data distribution) to secure "mission-critical Blockchain application"[2400]. If it is so critical and requires a proprietary network, why does it need a Blockchain in the first place?

Other theoretical architectures have been proposed in India that would rely on quantum computing to improve its security[2401]. There are even proposals for a sort of quantum Bitcoin and smart contracts coming from Israel[2402].

When you mix a complicated system with a couple others that are as complicated, it doesn't make it simpler to grasp. So, I'll pass on.

QKD over 5G

You may hear about plans to deploy QKD security in 5G networks. Of course, it doesn't deal with the radio portion of 5G and with your smartphone, but only about securing the backbone landline fiber networks of telecom operators[2403].

[2396] See Cryptographic Security Concerns on Timestamp Sharing via Public Channel in Quantum Key Distribution Systems by Melis Pahali et al, March 2022 (6 pages) and Improved Finite-Key Security Analysis of Quantum Key Distribution Against Trojan-Horse Attacks by Alvaro Navarrete and Marcos Curty, February 2022 (18 pages).

[2397] It is documented by Jonathan Jogenfors in Breaking the Unbreakable Exploiting Loopholes in Bell's Theorem to Hack Quantum Cryptography, 2017 (254 pages).

[2398] Documented in First Quantum-Secured Blockchain Technology Tested in Moscow, June 2017.

[2399] In Quantum Blockchain using entanglement in time, 2018 (5 pages).

[2400] See JPMorgan Chase, Toshiba and Ciena Build the First Quantum Key Distribution Network Used to Secure Mission-Critical Blockchain Application, February 2022. See also DV-QKD Coexistence With 1.6 Tbps Classical Channels Over Hollow Core Fibre by Obada Alia et al, March 2022 (7 pages) which documents the coexistence of QKD and classical communication on the same fiber.

[2401] See Quantum blockchain using weighted hypergraph states by Shreya Banerjee et al, Physical Review Research, 2020 (7 pages) and Quantum Blockchain based on Dimensional Lifting Generalized Gram-Schmidt Procedure by Kumar Nilesh and P. K. Panigrahi, January 2022 (16 pages). See The Next Generation of Blockchain: Quantum Blockchain Networks by Manan Narang from OneQuantum, March 2022, which confuses "quantum computing" and "quantum cryptography" and PQC to secure Blockchains.

[2402] See Quantum Prudent Contracts with Applications to Bitcoin by Or Sattath, April 2022 (49 pages).

[2403] See Quantum Key Distribution for 5G Networks: A Review, State of Art and Future Directions by Mohd Hirzi Adnan, Zuriati Ahmad Zukarnain and Nur Ziadah Harun, 2022 (28 pages).

Market and standards

What about the size of the QKD market? **Inside Quantum Technology** (a UK analyst company) made an estimate with a first $1B dollars reached in 2024, then an exponential growth leading to $7B in 2028[2404]. These are simplistic exponential growth curves, as usual. We'll see.

China is very active in defining a set of QKD standards[2405]. The ITU is also working on QKD standards[2406]. Europe is represented in the standardization work carried out at ISO, IEEE, ETSI and CEN-CENELEC, the European Committee for Standardization in Electronics and Electrotechnology.

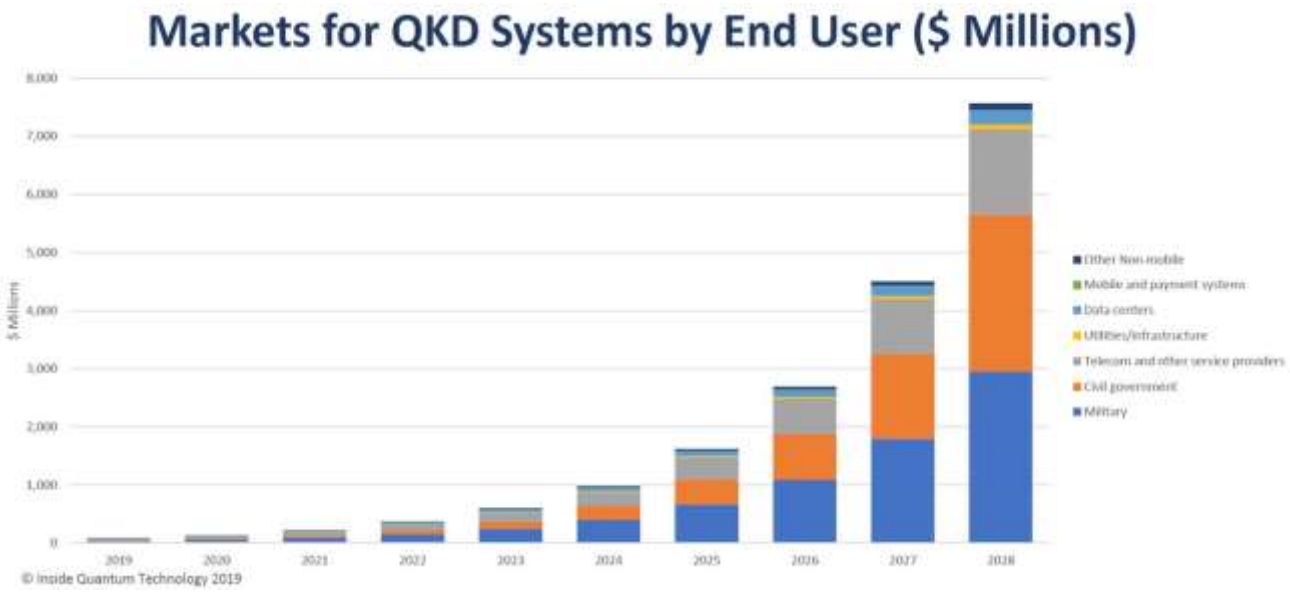


Figure 758: Inside Quantum Technology's QKD market assessment as done in 2019. Source: The Future of the Quantum Internet A Commercialization Perspective by Lawrence Gasman, June 2019 (11 slides).

Post-quantum cryptography

A physical protection of symmetric key transmission is not easily applicable in a generalized way, if only because it requires some optical link (direct free to air or by optical fiber) between transmitters and receivers. This, for example, does not work with radio links like with smartphones.

So, cybersecurity also requires the creation of cryptography systems capable of resisting the onslaught of quantum computers whether coming from Shor's or Grover's algorithms. Breaking encrypted messages - without private keys - should be an NP-Complete or NP-Hard problem to withstand future quantum assaults.

Post-Quantum Cryptography (PQC) complements Quantum Key Distribution (QKD) for this respect. It is certainly easier to deploy on a large scale because it is independent from the telecommunications infrastructures.

[2404] See The Future of the Quantum Internet A Commercialization Perspective by Lawrence Gasman, Inside Quantum Technology, June 2019 (11 slides) and The Future of the Quantum Internet A Commercialization Perspective by Lawrence Gasman from Inside Quantum Technology, June 2019 (11 slides). Seen in ITU Workshop on Quantum Information Technology for Networks.

[2405] See Introduction of Quantum secured Communication Standardization in CCSA by Zhangchao Ma, June 2019 (16 slides) and An overview of current quantum information technology (QIT) standardization by Wei Qi, June 2019 (13 slides).

[2406] See ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N), 2019.

However, it can be combined by sending PQC public keys over physical QKD links or with using some PQC for authenticating the classical link used for the exchange of the photon measurement basis[2407]. Different PQC systems differ in many parameters and have different trade-offs between signature size, processing speed for encryption and decryption, and public key size.

Let's look at the PQC timeline[2408]:

- **1978**: the first algorithm resistant to quantum computers is created by **Robert McEliece** (details below) even before Richard Feynman even mentioned the idea of creating quantum computers and the creation of both Shor and Grover's algorithms!
- **2003**: the term "post quantum cryptography" (PQC) is created by **Daniel Bernstein**[2409].
- **2006**: the first international **PQCrypto** workshop is held in Belgium to study ways to circumvent quantum computer attacks at a time when you can barely assemble two qubits. The program consists in finding successors to the quantum-resistant public key cryptography algorithms RSA and ECC[2410]. The 12-person program committee includes among others Louis Goubin from the University of Versailles and Phong Nguyen and Christopher Wolf from the ENS. From this first edition, four of the five pillars of the PQC are established with the code-based crypto, lattice codes, hash Lamport signature and multivariate cryptography. The isogenies will arrive later. Two French researchers propose two of these four tracks: Nicolas Sendrier, from Inria, with "Post-quantum code-based cryptography" and Jacques Stern from ENS with "Post-quantum multivariate-quadratic public key schemes" [2411]. These workshops have since been held every one to two years around the world. The 2013 edition took place in Limoges, France.
- **2012**: the **NIST** (National Institute for Standards & Technologies) launches its first projects and a team on PQC.
- **2014**: the **European Union** launches a Horizon 2020 call for projects on PQC. At the same time, ETSI, the European Telecoms Standardization Body, also launches its working group on PQC.
- **2015**: **NIST** organizes its first PQC workshop. ETSI published a reference document on QC[2412]. The NSA woke up and declared that the transition to PQC would become a priority[2413]. The NSA is playing two roles each time: it wants to protect itself and the sensitive communications of the U.S. government with good encryption systems but at the same time maintain the ability to break the codes of standard commercial communications and those from other countries. This relies on the brute force of giant supercomputers and a highly asymmetrical technical resources. In 2015, the European project PQCrypto coordinated by Tanja Lange is launched[2414].
- **2016**: NIST publishes QCP Progress Report (15 pages) and an associated standardization roadmap.

[2407] See Experimental authentication of quantum key distribution with post-quantum cryptography by Liu-Jun Wang et al, May 2021 (7 pages).

[2408] I extracted a piece of it from Quantum cryptanalysis - the catastrophe we know and don't know by Tanja Lange, a researcher from the Netherlands, 2017 (33 slides).

[2409] Daniel Bernstein is the author with Johannes Buchmann and Erik Dahmen of the impressive book Post-Quantum Cryptography, 2009 (254 pages) which describes well the challenges of PQC.

[2410] The proceedings are in PQCrypto 2006 International Workshop on Post-Quantum Cryptography, May 2006 (254 pages).

[2411] Source: Quantum Computing and Cryptography Today by Travis L. Swaim, University of Maryland University College (22 pages).

[2412] See Quantum Safe Cryptography and Security (64 pages).

[2413] See Commercial national security algorithm suite and quantum computing FAQ IAD (11 pages).

[2414] It is documented in Post-Quantum Cryptography for Long-Term Security (10 pages).

- **2017**: marks the end of the PQC standardization proposal submissions to NIST. By the end of 2017, 69 applicants are accepted out of 82, mainly with Euclidean networks (lattice codes) and error correction codes (code based PQC). In the same year, the 8th PQCrypto workshop was held in Utrecht, The Netherlands. These candidates had to meet increasing security levels labelled SL1, SL3 and SL5 which corresponds to key size thresholds. These key sizes are between 30 bytes and 5 KB depending on the PKI/signature and the security level.
- **2019**: 26 candidates are selected by NIST in February to move to the second stage, including 17 candidates for public key encryption solutions and 9 for signatures[2415]. These include three projects involving Worldline, which until 2019 was part of the Atos Group. For its part, Inria (France) was involved in 7 of the 26 selected projects.

2019 second round candidates,
2020 finalists and 2020 alternate candidates

BIKE	LEDAcrypt	Rainbow
Classic McEliece	LUOV	ROLLO
CRYSTALS-DILITHIUM	MQDSS	Round5
CRYSTALS-KYBER	NewHope	RQC
FALCON	NTRU	SABER
FrodoKEM	NTRU Prime	SIKE
GeMSS	NTS-KEM	SPHINCS+
HQC	Picnic	Three Bears
LAC	qTESLA	

Figure 759: NIST PQC selection in 2019.

- **2020**: results of the third round of NIST candidate selection in July, which kept 15 out of the 26 candidates from the previous round[2416]. This selection includes 7 teams that were finalists for this stage and 8 teams that propose lower quality solutions that need to be further evaluated (aka "alternate candidates"). See their list in the tables below[2417]. It must be noted that the NIST challenge embedded some constraints on intellectual property. Strictly said, NIST doesn't object to the contestants having some patents related to their submitted protocols. But they favor royalty-free ones and IP licensing without compensation, under reasonable terms (RAND) and conditions that are demonstrably free of unfair discrimination. While this could certainly accelerate their adoptions, this may indirectly favor large cybersecurity vendors who already have an existing customer base.

  In Figure 760 and Figure 761 are the participants countries, research teams and vendor organizations per project. It shows in green the solutions that were later selected in July 2022. In red are the two solutions that were found to be defective in 2022.

[2415] See NIST Post-Quantum Cryptography - A Hardware Evaluation Study, 2019 (16 pages), Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process, 2019 (27 pages) and Recent Developments in Post Quantum Cryptography by Tsuyoshi Takagi, November 2018 (38 slides).

[2416] See PQC Standardization Process: Third Round Candidate Announcement, July 2020.

[2417] The Bit-flipping Key Encapsulation (BIKE) was codeveloped by Intel. It's a public key based encryption. Decoding can be done with 1.3 million operations at 110 MHz on an Intel Arria 10 FPGA in 12 ms.

NIST finalists

	finalists	research teams	vendors teams
Public-Key Encryption/KEMs	Classic McEliece	**UK**: U. London, U. Plymouth. **Switzerland**: ETH Zurich. **USA**: U. Illinois & Chicago, U. Florida, Yale. **Europe**: U.Ruhr Bochum, U. Eindhoven, U. Southern, Denmark, MPI, Inria (France). **Taiwan**: Academia Sinica.	Google PQ Solutions PQShield
	CRYSTALS-KYBER	**USA**: SRI. **Canada**: U. Waterloo. **Europe**: Radboud U. Netherlands, Ruhr U. Bochum, ENS Lyon.	IBM Research Europe Arm, PQShield NXP Semiconductors
	NTRU	**Europe**: Radboud U Netherlands, Eindhoven U. **USA**: Brown U. **Canada**: U. Waterloo.	Qualcomm NTT Algorand, PQShield
	SABER	**Europe**: KU Leuven (Belgium). **UK**: Birmingham U.	
Digital Signatures	CRYSTALS-DILITHIUM	**USA**: Florida Atlantic U. **Switzerland**: ETH Zurich. **Europe**: CWI Netherlands, Ruhr U. Bochum, MPI, ENS Lyon.	IBM Research Europe Google, PQShield
	FALCON	**Europe**: ENS Paris, U. Rennes (France). **USA**: Brown U.	IBM Research PQShield, Qualcomm Ethereum Foundation Thales
	Rainbow	**Europe**: FAU Erlangen Nuremberg, U. Versailles. **USA**: Cincinnati U. **Taiwan**: Academia Sinica, National Taiwan U.	

Grey: 2020 selection
Green: 2022 selection
Red: broken in 2022

(cc) compilation Olivier Ezratty, 2022

Figure 760: NISQ finalists selection in 2020. In green, the 2022 selection. In red, broken PQC. (cc) Olivier Ezratty, 2022.

And the alternate candidates:

NIST alternate candidates

	finalists	research teams	vendors teams
Public-Key Encryption/KEMs	BIKE	**USA**: U.Washington, Florida U. **Europe**: U. Limoges, ENAC & U. Toulouse, Inria, U. Bordeaux (France), U. Ruhr Bochum (Germany). **IsraeL**: U. Haifa.	Intel Google IBM **Worldline France**
	FrodoKEM	**USA**: U. Michigan. Stanford U. **Netherlands**: CWI. **Canada**: U. Waterloo. **Middle-East**: Ege University (Turkey).	NXP Microsoft Research PQShield
	HQC	**France**: ISAE-Supaero, Limoges U., ENAC, U. Toulouse, Toulon U., Bordeaux U. **USA**: Florida U.	Worldline France and Netherlands
	NTRU Prime	**Taiwan**: Academia Sinica, National Taiwan U. **Australia**: U. Adelaide. **Europe**: Eindhoven U (Netherlands), Hamburg U. (Germany), Tampere U. (Finland). **USA**: Illinois U.	NXP
	SIKE	**USA**: Florida U. **Canada**: Waterloo U., Toronto U. **Europe**: Radboud U. Netherlands, U. Versailles (France).	evolutionQ Amazon Microsoft Research Infosec Global Texas Instruments
Digital Signatures	GeMSS	**France**: Inria, University of Versailles and Sorbonne Université.	CryptoNext Orange
	Picnic	**USA**: Northwestern U., GeorgiaTech, U. Maryland., Princeton U. **Europe**: Austrian Institute of Technology, TU Graz (Austria), Aarhus U. (Denmark), DTU (Denmark).	Microsoft Research Dfinity
	SPINCS+	**Europe**: U.Ruhr Bochum, KU Leuven, TU Graz, Eindhoven U, Radboud U.	Cisco, Infineon Infosec Global Genua, Taurus

Grey: 2020 selection
Green: 2022 selection
Red: broken in 2022

(cc) compilation Olivier Ezratty, 2022

Figure 761: NISQ alternate candidates selection in 2020. In green, the 2022 selection. In red, broken PQC. (cc) Olivier Ezratty, 2022.

- **2022**: in January, the Biden administration published a Memorandum and Executive Order 14028 asking all Federal administration to prepare a PQC deployment plan in 2022[2418]. It even required the deployment of PQC solutions for stored and transiting data.

[2418] See Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, January 2022.

- **2022**: in July, NIST published a first final list of 4 validated PQC standards, 1 for a PKI and 3 for a digital signature[2419]. These are in green in the above tables. In the PQC standardized signatures, Falcon is recommended for those applications requiring smaller signatures than the ones generated by CRYSTALS-Dilithium. SPHINCS+ signatures are based on a different scheme, although more complex to implement. They still plan to standardize other PQC signatures. Just before this choice was published, after some delay, one of the 2020 finalist signatures PQC, Rainbow, was broken by IBM Zurich researchers at the first security level SL1 corresponding to small sized keys and, not surprisingly, not selected[2420]. In August 2022, the SIKE PKI was also seemingly broken by researchers from Belgium[2421].

  In July 2022, the NIST NCCoE (National Cybersecurity Center of Excellence), was tasked to work with Federal agencies and industry vendors to speed up the transition to PQC. The vendors are AWS, Cisco, Crypto4A Technologies, Cryptosense, InfoSec Global, ISARA Corporation, Microsoft, Samsung SDS, SandboxAQ, Thales and VMware. These players will provide deployment recommendations and their own software and services solutions. Simultaneously, the CISA (Cybersecurity and Infrastructure Security Agency), a US federal agency within the DHS (Department of Homeland Security) announced the creation of a PQC initiative to assist other federal agencies in the deployment of PQCs. Not surprisingly, many PQC and other security vendors are already providing NIST compliant solutions! They provide some encapsulation mechanisms for third-party and/or open source PQCs in their cybersecurity management tools.

- **2025**: NIST's target date for finalizing PQC standards. Deployments of these standards would begin with the rapid deployment of commercial solutions supporting these standards. Fast, for the simple reason that the candidates are often in the standardization consortia. Some of them are already testing their solutions.

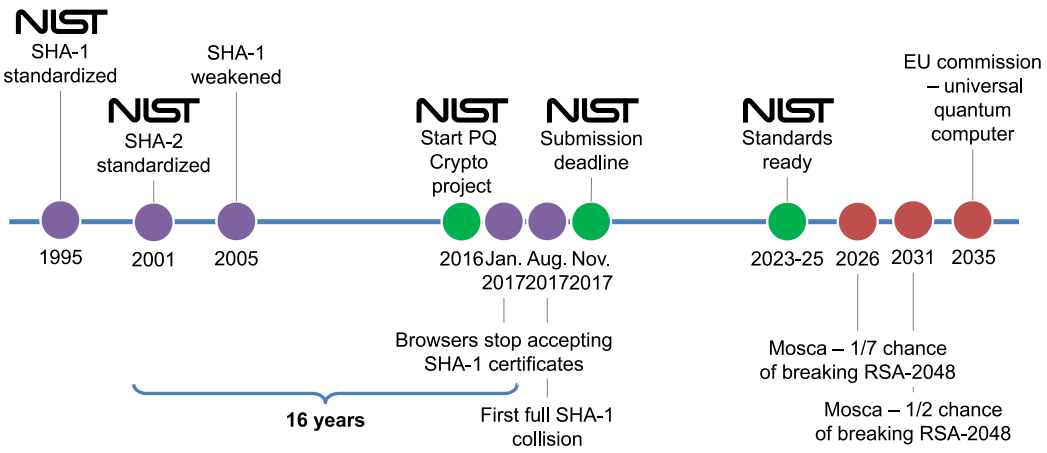


Figure 762: NISQ PQC standardization planning as of 2019. Source: Introduction to post-quantum cryptography and learning with errors, Douglas Stebila, 2018 (106 slides).

There are five distinct categories of PQC standards, as follows. I will not be able to technically describe them all except for the first category[2422]. In the last part of this section on cryptography, we will mention the case of some startups that are positioned in this market.

[2419] See NIST Announces First Four Quantum-Resistant Cryptographic Algorithms, NIST, July 2022.

[2420] See NIST PQC Finalists Update: It's Over For The Rainbow by Edlyn Teske. March 2022.

[2421] See Post-quantum encryption contender is taken out by single-core PC and 1 hour by Dan Goodin, ArsTechnica, August 2022, referring to An efficient key recovery attack on SIDH (preliminary version) by Wouter Castryck and Thomas Decru, August 2022 (15 pages). And some good explanations in "Quantum-Safe" Crypto Hacked by 10-Year-Old PC by Charles Q. Cho, August 2022.

[2422] See in particular A Guide to Post-Quantum Cryptography by Ben Perez, October 2018.

Table 2 - Comparison on encryption schemes (RSA decryption = 1, size in bits, k security strength)

Algorithm	*KeyGen (time compared to RSA decrypt)*	*Decryption (time compared to RSA decrypt)*	*Encryption (time compared to RSA decrypt)*	*PubKey (key size in bits to achieve 128 bits of security)*	*PrivateKey (key size in bits to achieve 128 bits of security*	*Cipher text (size of resulting cipher text)*	*Time Scaling*	*Key Scaling*
NTRU	*5*	*0.05*	*0.05*	*4939*	*1398*	*4939*	k^2	*k*
McEliece	*2*	*0.5*	*0.01*	*1537536*	*64861*	*2860*	k^2	k^2
Quasi-Cyclic MDPC McEliece	*5*	*0.5*	*0.1*	*9857*	*19714*	*19714*	k^2	*k*
RSA	*50*	*1*	*0.01*	*3072*	*24,576*	*3072*	k^6	k^3
DH	*0.2*	*0.2*	*0.2*	*3072*	*3238*	*3072*	k^4	k^3
ECDH	*0.05*	*0.05*	*0.05*	*256*	*256*	*512*	k^2	*k*

Note: in key scaling, the factor log k is omitted.

Figure 763: Comparison of key size of various encryption schemes. Source : Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges, ETSI, 2015 (64 pages).

Established companies are not left out. **IBM** announced in August 2019 a system for archiving information on magnetic bank that integrates post-quantum cryptography[2423]. They use encryption based on Euclidean networks. As it is usually long-term storage, it is necessary to keep the decryption software for the same length of time to avoid ending up with a pile of data that cannot be reused. IBM is also involved in the three consortia that responded to the NIST call for proposals. **Kudelski Security** (Switzerland) is also interested in PQC.

Figure 764: IBM's stance on cybersecurity. They bet on the right horse given their slides in 2019 presented 3 of the 4 2022 NIST finalists!

In France, the civil cybersecurity agency **ANSSI** published an information note in May 2020 in which it expressed certain reserves about the QKD[2424]. It highlighted the fact that it does not address a common problem, cannot guarantee perfect inviolability and requires dedicated optical infrastructures. Instead, it recommends focusing on PQC.

[2423] See IBM's quantum-resistant magnetic tape storage is not actually snake oil by Kevin Coldewey in TechCrunch, August 2019.

[2424] See L'avenir des communications sécurisées passe-t-il par la distribution quantique de clés? by ANSSI, May 2020 (6 pages).

This followed a memo of equivalent content from their British **NCSC** counterparts published in April 2020[2425]. A similar publication from the **NSA** was released in October 2020[2426]. It was renewed in 2021 and 2022.

Code-based cryptography

This cryptographic system invented in 1978 by **Robert McEliece**, long before Shor's algorithm, has since resisted all cryptanalysis attacks, either classical or designed with quantum algorithms. It is the oldest of the PQC codes which was even a PQC before its time. The method consists in multiplying the data to be encrypted, represented as binary vectors (of length k), by a public and static matrix with more columns than rows (k x n), aka a "binary Goppa code″.

This multiplication generates a vector larger than the original vector (with n bits). We then add a binary vector which adds random errors to the result but of constant value (vector z in schema with a given number of 1s). It is described as a "*uniformly random word of weight t*". It is a series of random bits containing a fixed number "t" of 1s called a Hamming weight. The public key sent by the receiver to the transmitter is the matrix Ĝ and this number of errors t.

The three matrices having created Ĝ constitute the private key. This matrix Ĝ is the multiplication of three matrices called SGP for "non **S**ingular", "generator matrix / **G**oppa code" and "**P**ermutation matrix". The message decoding uses inverses of matrix S, P and G. This is explained in this diagram. The G matrix is by designed crafted to remove the "t" errors introduced in the encryption phase.

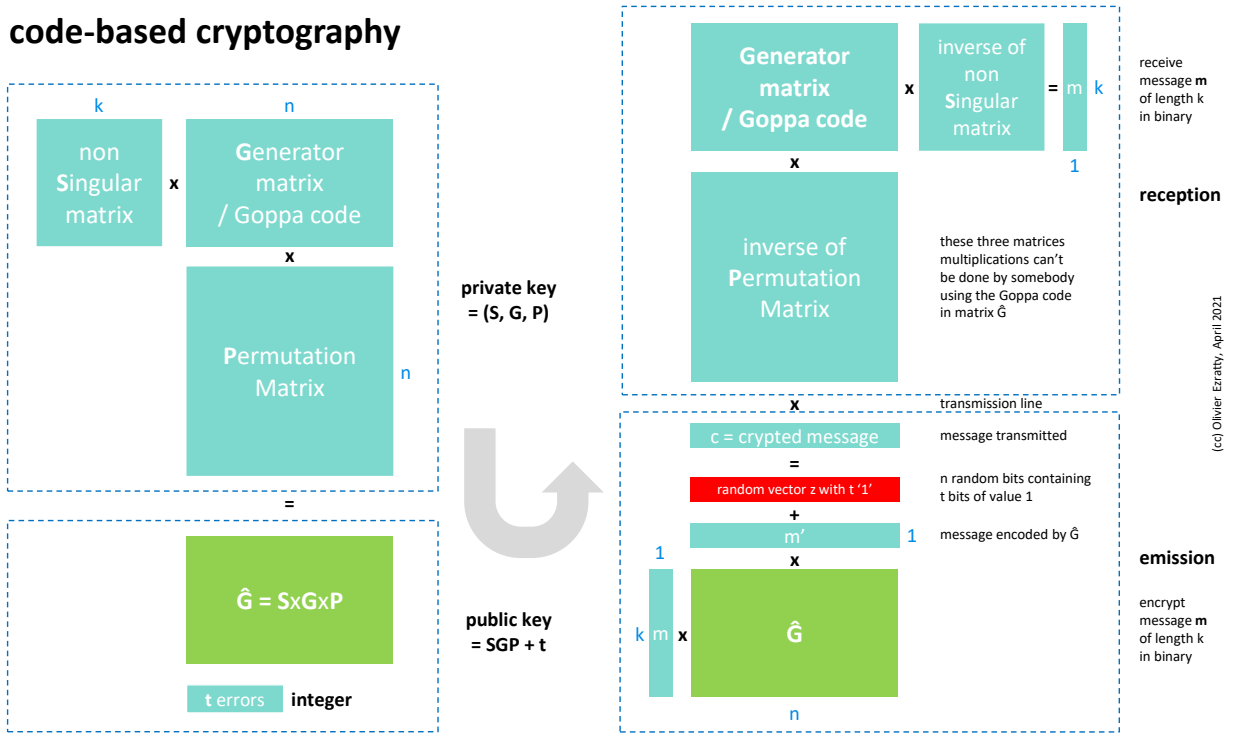


Figure 765: how a code-based PQC key generation works. It's all about mixing and matching many non-square matrices. (cc) Olivier Ezratty, from various sources. 2021.

This system generates public keys one hundred times larger than with RSA, of the order of 80 KB. It generates new vulnerabilities if you reduce their size.

[2425] See Quantum Security Technologies, NCSC, March 2020 (4 pages) and a detailed response in Quantum safe cryptography - the big picture - Fact Based Insight by David Shaw, 2020.

[2426] See NSA Cybersecurity Perspectives on Quantum Key Distribution and Quantum Cryptography, NSA, 2020.

The advantage of the PQC category is its good encryption and decryption speed. It can even be accelerated by using a dedicated FPGA chipset[2427].

Breaking this kind of encryption is an NP-Hard problem that is currently inaccessible to quantum computing, even though to resist quantum computing it would still require a fairly large key of at least 1 MB[2428].

Lattice-based cryptography or Euclidean networks

The technique was proposed in 1996 by Miklos Ajtai, a researcher at IBM, and implemented in a public key system in 2005 by Oded Regev with its LWE (Learning With Errors) system and improved since then by many researchers.

The associated literature is inaccessible for non-specialists. It is not easy to understand how this encryption method works despite the elegance of the diagrams that present the notion of Euclidean network like the one in Figure 766[2429]. Basically, it is a matrix of dots that allows to locate points according to their coordinates according to a mark of different vectors between the public and private keys.

An error is added to the coordinates generated with the public key vector. Only the coordinate vectors of the private key can be used to retrieve the coordinate of the encrypted value. Initially, it suffered from performance problems, but effective solutions appeared such as NTRU, created in 1998 by Jeffrey Hoffstein, Jill Pipher and Joseph Silverman. The method advantage is to use small public keys. Its decryption is an NP-complete problem inaccessible to quantum computing. On the other hand, it is a method protected by many patents, so it is proprietary and potentially expensive[2430].

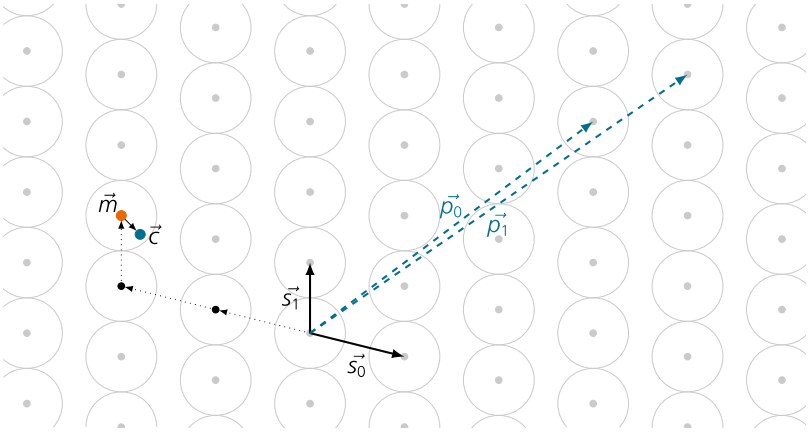


Figure 3.2: Example for lattice-based encryption in a two-dimensional lattice: The secret, well-formed base is $\{\vec{s_0}, \vec{s_1}\}$; the public, "scrambled" base is $\{\vec{p_0}, \vec{p_1}\}$. The sender uses $\{\vec{p_0}, \vec{p_1}\}$ to map the message to a lattice point $\vec{m}$ and adds an error vector to obtain the point $\vec{c}$. The point $\vec{c}$ is closer to $\vec{m}$ than to any other lattice point. Therefore, the receiver can use the well-formed secret base $\{\vec{s_0}, \vec{s_1}\}$ to easily recover $\vec{m}$ (dotted vectors); this is a hard computation for an attacker who only has the scrambled base $\{\vec{p_0}, \vec{p_1}\}$. For a secure scheme, the dimension of the lattice must be much higher than 2 as in this example.

Figure 766: Euclidean network key generation. Source: Practical Post-Quantum Cryptography by Ruben Niederhagen and Michael Waidner, 2017 (31 pages).

The PQC **New Hope** solution (CECPQ1) which was tested in 2016 for a few months by **Google** in Chrome and is based on Ring-LWE is in this class of methods. Since 2019, they have moved to CECPQ2 which includes a variant of the HRSS key exchange system that is among the bidders in the NIST competition and the selected in the last wave in the NTRU project[2431].

[2427] As seen in Code-Based Cryptography for FPGAs by Ruben Niederhagen, 2018 (73 slides).

[2428] The resistance of this method to attacks is documented in Code-Based Cryptography by Tanja Lange, 2016 (38 slides). For more information, see also Code Based Cryptography by Alain Couvreur, 2018 (122 slides) and Some Notes on Code-Based Cryptography, a thesis by Carl Löndahl, 2014 (192 pages).

[2429] See Practical Post-Quantum Cryptography by Ruben Niederhagen and Michael Waidner, 2017 (31 pages).

[2430] For more information, see the thesis Lattice-based cryptography: a practical implementation by Michael Rose, 2011 (103 pages), Lattice-based Cryptography by Daniele Micciancio and Oded Regev, 2008 (33 pages) and the slightly more pedagogical but still incomprehensible Overview of Lattice based Cryptography from Geometric by Leo Ducas, 2017 (53 slides).

[2431] See Experimenting with Post-Quantum Cryptography by Matt Braithwaite, July 2016 and then Google starts CECPQ2, a new postquantum key exchange for TLS, January 2019.

In France, a team from the IRISA-EMSEC laboratory is developing a cryptographic solution based on these Lattice base systems, also named Euclidean networks.

Damien Stehlé is another specialist of the domain, doing research at ENS Lyon. He participated to the creation of CRYSTALS - Kyber, a finalist in 2020 and 2022 of NIST's PQC competition.

Isogeny-based cryptography

This variant of elliptic curves is even less easy to grasp than all of the above. It is a "*morphism of superimposed group and finite kernel between two elliptic curves*". Piece of cake! The system was proposed in 2006 by Alexander Rostovtsev and Anton Stolbunov and then broken by quantum cryptoanalysis by Andrew Childs, David Jao and Vladimir Soukharev. This led David Jao and Luca De Feo (Inria) to propose in 2011 the use of "super-singular" curves to correct this flaw[2432].

This cryptography is used in Supersingular isogeny Diffie–Hellman key exchange (SIDH).

Software publisher **Cloudflare** has released an open source security solution based on isogenies, CIRCL (Cloudflare Interoperable Reusable Cryptographic Library). It is published on GitHub. Their SIKE key encapsulation solution has been submitted to NIST.

In January 2019, they were among the 17 finalist candidates for public key encryption or key creation solutions[2433]. In 2022, it was broken using a single computer for one hour to 21 hours depending on the key size (from SIKEp434 to SIKEp751).

Hash-based signatures

This post-quantum cryptography other method also predates the very notion of quantum computer imagined by Richard Feynman in 1982. It is based on the work of **Leslie Lamport** of the SRI in 1979 and her single-use hash-based "signatures". The method was then improved by using hash trees also called Merkle trees to sign several messages. It is based on public keys of reduced size, down to 1 kbits.

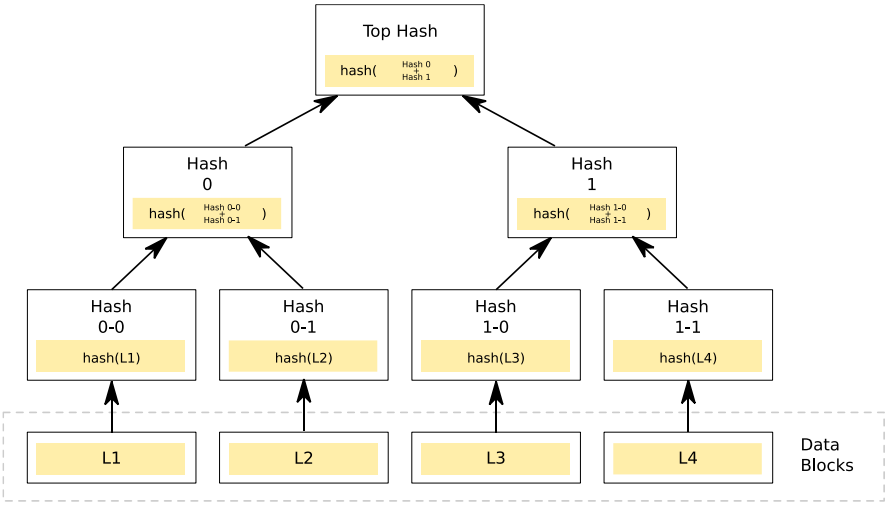


Figure 767: source: Merkle Tree, Wikipedia.

This method is mainly used for electronic signature[2434].

[2432] More on this with 20 years of isogeny-based cryptography by Luca De Feo, 2017 (84 slides), An introduction to supersingular isogeny-based cryptography by Craig Costello (Microsoft Research), 2017 (78 slides), Isogeny Graphs in Cryptography by Luca De Feo, 2018 (73 slides) and An introduction to isogeny-based crypto by Chloe Martindale, 2017 (78 slides).

[2433] See Cloudflare wants to protect the internet from quantum computing, June 2019 and Introducing CIRCL: An Advanced Cryptographic Library, June 2019.

[2434] If you are well versed in mathematics and cryptography, see Hash-based Signatures: An Outline for a New Standard (12 pages), Design and implementation of a post-quantum hash-based cryptographic signature scheme by Guillaume Endignoux, 2017 (102 pages) and SPHINCS: practical stateless hash-based signatures, 2015 (30 pages).

Multivariate polynomial cryptography

This last group of methods is reminiscent of error correction codes. The public key is a multiplication of several matrices, two of which are linear and one quadratic (with squared values), the three separate matrices constituting the private key used to reconstruct the encrypted message. As a result, the keys are extremely large.

Code breaking these keys is an NP-Hard problem, out of reach of quantum computing. The method dates from 2009 and was obviously then declined in several variants. The public keys are quite large, up to 130 KB (with the HFEBoost variant) [2435]. This encryption method is also rather used for electronic signatures.

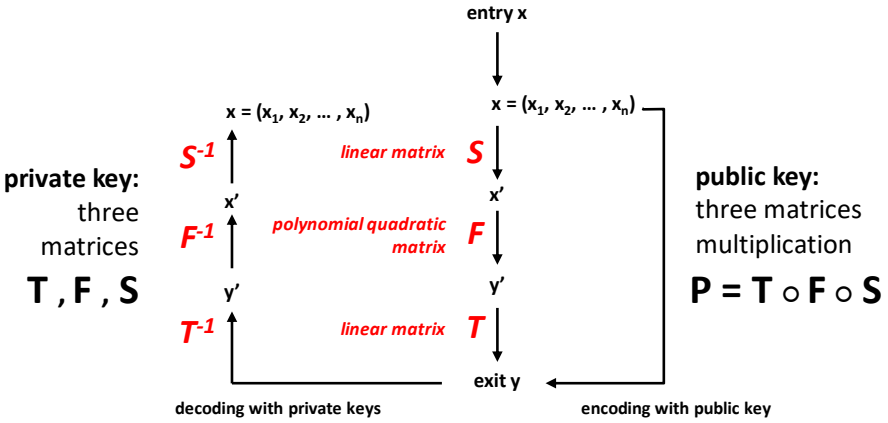


Figure 768: multivariate polynomial cryptography. Source: (cc) Olivier Ezratty, reconstructed from other sources.

The Rainbow PQC signature selected by NIST in 2020 as a finalist and broken in March 2022 was in that category.

We could imagine that QKD (physical protection of key distribution) could be combined with PQC (logical protection of encryption against quantum computer decryption). Actually, not really. QKD is rather dedicated to symmetric keys that assume protection of physical communication between correspondents, whereas PQC relies on public keys that do not need to be protected by QKD because their interception (without QKD) would already be useless to hackers.

However, QKD for key exchange can be combined with PQC for authentication and data encryption. QKD requires authentication, which can be provided upstream by PQC. On the other hand, QKD can be redundant with PQC used for key exchange[2436].

Quantum homomorphic cryptography

Homomorphic cryptography consists in encrypting data that can then pass through a conventional processing in encrypted mode and give an encrypted result that will be decipherable at the end of the processing.

In machine learning and deep learning, this mode of encryption makes it possible to distribute training and inference processing of learning machine models in the cloud without the hacking of the transmitted data revealing the data content that feeds the model or inferences.

The disadvantage of this method is that it does not work with all learning machine models and is very expensive in terms of machine time for data encryption and decryption as well as computation.

Quantum homomorphic encryption is a similar approach for encoding data that will feed a quantum computer in the cloud and then decode the result of the processing.

[2435] Note the contribution of Jacques Stern from the ENS "Post-quantum multivariate-quadratic public key schemes" at PQCRYPTO 2006.

[2436] To learn more about PQC, see in particular Post-quantum cryptography - dealing with the fallout of physics success by Daniel Bernstein and Tanja Lange, 2017 (20 pages).

It is one of the tools for implementing so-called "blind computing" in the cloud, where servers cannot understand and interpret the data they process.

Various algorithms for encrypting quantum gate control programs have been proposed but are not yet commonly used[2437]. Some of the keys can be quantum-transmitted like a QKD. This is one of the conditions to be sure that the server part cannot interpret the processing it performs[2438].

Quantum interconnect

As indicated at the beginning of this long section, QKD-based quantum cryptography is not the only application of quantum telecommunications[2439]. It is one of its applications. And, as we have already seen earlier in this book, quantum telecommunications are not about transmitting information faster than light[2440].

One application area is the creation of quantum networks linking quantum "endpoints" that are themselves quantum, which could be quantum computers and even quantum sensors[2441]. In the first case, links between quantum computers would make it possible to create distributed computing architectures, following the example of classical distributed computing architectures that exist on the Internet, in data centers and within supercomputers. This is a “scale-out” approach to grow the capacity of quantum computers, as opposed to “scale-in” approaches that consist in creating QPUs with a larger number of qubits. Since this number is limited, scale-out approaches are researched. We don’t know yet if scaling-out is going to be more or less difficult to achieve than scaling-in.

In the sensors case, networked quantum sensors can create a trusted system, improve the sensitivity of quantum sensing or even connecting quantum sensors directly with quantum computers, either for sending some form of quantum data without using conversion to classical data or to improve sensor/computer communication security[2442].

A direct link between quantum computers and quantum telecommunications would bring interesting benefits for implementing secured processing between several parties like a small quantum computer delegating some tasks to a larger one in a secured manner[2443]. This the concept of "blind computing" associated to the BFK protocol created in 2009 by Anne Broadbent, Joe Fitzsimons and Elham Kashefi[2444].

[2437] See Classical Homomorphic Encryption for Quantum Circuits by Urmila Mahadev, 2018 (7 pages), Quantum Fully Homomorphic Encryption With Verification, 2017 (30 pages and slides, 28 slides), Quantum Homomorphic Encryption: A Survey, 2017 (11 pages) et Quantum homomorphic encryption for circuits of low T-gate complexity by Anne Broadbent et Stacey Jeffery, 2015 (35 pages).

[2438] As indicated in On the implausibility of classical client blind quantum computing by Scott Aaronson, Elham Kashefi et al, 2017 (43 pages).

[2439] See the excellent Quantum internet: A vision for the road ahead by Stephanie Wehner et al, October 2018 (11 pages).

[2440] Let’s remind at least two key explanations: first, entanglement and non-locality is about having a correlation between two distant quantum objects values when measured sequentially, but this value is random by essence. You can’t set one quantum value at one end (Alice) and then measure it at the other location (Bob’s). You just decide to measure random values at both end that happen to be correlated. On a more practical reason, the teleportation algorithm that can send a qubit state to another location with using entanglement needs two classical communications links. So, we’re stuck with the speed of light. See No, We Still Can't Use Quantum Entanglement To Communicate Faster Than Light by Ethan Siegel, February 2020.

[2441] See Repeater-enhanced distributed quantum sensing based on continuous-variable multipartite entanglement by Yi Xia et al, 2018 (9 pages).

[2442] See one example of quantum sensors interconnect proposal in An elementary quantum network of entangled optical atomic clocks by B. C. Nichol et al, Nature, November 2021-September 2022.

[2443] See Equivalence in delegated quantum computing by Fabian Wiesner, Jens Eisert and Anna Pappa, June 2022 (43 pages).

[2444] See Universal blind quantum computation by Anne Broadbent, Joseph Fitzsimons and Elham Kashefi, 2008 (20 pages) and the associated presentation (25 slides), Blind quantum computing can always be made verifiable by Tomoyuki Morimae, 2018 (5 pages), Experimental Blind Quantum Computing for a Classical Client, 2017 (5 pages) and Blind Quantum Computation by Charles Herder (5 pages).

The principle consists in preparing computation in a quantum way at the starting point and sending it by a quantum link by teleportation to the remote quantum computer. It is a bit the quantum equivalent of the homomorphic encryption used in distributed machine learning.

However, connecting quantum computers is not an easy task. It's not about inputs/outputs or memory and storage sharing like with classical scale-out architectures. It should indeed be possible to convert the qubit state of these machines into quantum states of photons - usually in the infrared range at 1550 nm - for optical transmission. Apart from the photon-based systems case, qubits are most often electrons spins or atoms energy states. Hence the numerous efforts to make conversions between these qubits states and qubits encoded in transmissible photons. And setting up some quantum connectivity is not just about sending one photon from one computer to the other, but to connect them with entanglement resources and use the teleportation algorithm[2445].

So far, there are three known approaches to connect quantum computers: microwaves, photons and shuttling electrons or ions. In that space, there's a clear difference in photon-based solutions which could scale at a large level, leveraging fiber optics telecommunication infrastructures and other options (microwave, shuttling electrons of ions) which are by design "on premise" and won't rely on telecommunications infrastructures[2446].

Microwaves interconnect

This type of QPUs interconnect is adapted to qubits that are driven by microwaves, so in order of priority, superconducting, silicon spin and to some extent trapped ions and cold atoms qubits.

But so far, it has been investigated mostly with superconducting qubits. This technology is adapted to relatively short range connectivity and could have a high efficiency.

Superconducting qubits belong to the field of circuit quantum electrodynamics (cQED) and are driven by microwave pulses. Microwaves are used for qubit readout so we know how to convert the state of a qubit into microwaves, which are in the 4-8 GHz range. These microwaves can be used for short distance communication between processing units as was first realized by an international team led by the University of Chicago in 2020.

They connected two nodes of three superconducting qubits, each arranged as an entangled GHZ state, and managed this entanglement transmission with microwaves on a distance of one meter on a niobium-titanium coax cable.

The entanglement transmission was done with a fidelity of 65% and 91% for a single qubit transmission. It's a first promising step[2447].

Figure 769: Source: Deterministic multi-qubit entanglement in a quantum network by Youpeng Zhong, Audrey Bienfait (ENS Lyon), et al, November 2020 on arXiv and February 2021 in Nature (38 pages).

[2445] See Distributed Quantum Computing: A path to large scale quantum computing by Stephen DiAdamo, August 2021.

[2446] See Development of Quantum InterConnects for Next-Generation Information Technologies by David Awschalom, Sophia E. Economou, Dirk Englund, Liang Jiang, Mikhail D. Lukin, Christopher Monroe, Jelena Vučković, Ronald Walsworth et al, 2019 (31 pages) which positions well different QPU interconnect technologies.

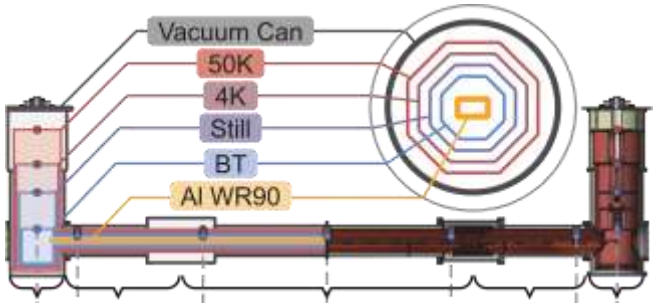
[2447] See Deterministic multi-qubit entanglement in a quantum network by Youpeng Zhong, Audrey Bienfait (ENS Lyon), et al, November 2020 on arXiv and February 2021 in Nature (38 pages).

Another team led by Andreas Wallraff from ETH Zurich with the University of Sherbrooke in Canada connected several superconducting units using connected cryogenic systems.

This enabled the connection between these units with microwave waveguides[2448]. The two processing units were separated by a 5 meters cryogenic link where the microwaves are transmitted. I don't know of any superconducting hardware vendor that plans to adopt this architecture.

Figure 770 above and below, ETH Zurich 5 meter cryogenic microwave link. Source: Microwave Quantum Link between Superconducting Circuits Housed in Spatially Separated Cryogenic Systems by Paul Magnard, Alexandre Blais, Andreas Wallraff et al, PRL, December 2020 (13 pages).

In another experiment, a team from the Technical University of Munich with colleagues from RIKEN in Japan and Aalto University in Finland tested a microwave entangling connection of 45 cm between two superconducting qubits. They used two microwave parametric amplifiers (JPA) to create a pair of entangled and squeezed microwave photons to connect "Alice" & "Bob" qubits.



The resulting teleportation fidelity was of 69%. We'll see if that scales well with a growing number of qubits[2449].

Now, what is needed is way more sophisticated. Connecting different qubit chipsets would require to connect at least one qubit of nearby chipsets to each other. This would create a limited connectivity between the chipsets. The example using a simple hexagonal qubit topology typical of IBM's superconducting chipsets would require the connections in red. But this is for 27 qubit chipsets, not thousand qubit chipsets[2450]!

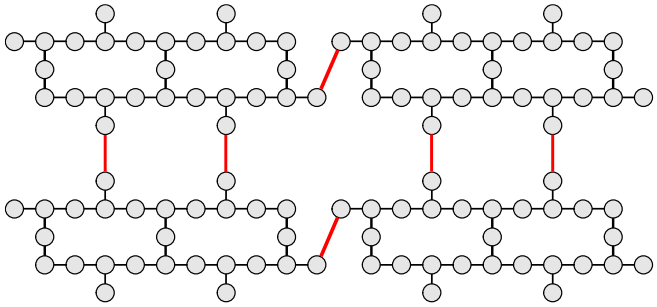


Figure 771: Source: Short-Range Microwave Networks to Scale Superconducting Quantum Computation by Nicholas LaRacuente et al, January 2022 (22 pages).

That's also what a team from the Universities of Pittsburgh and Illinois with ENS Paris proposed in 2021, using a microwave router and a SWAP gate to connect several chipsets [2451].

[2448] See Microwave Quantum Link between Superconducting Circuits Housed in Spatially Separated Cryogenic Systems by Paul Magnard, Alexandre Blais, Andreas Wallraff et al, PRL, December 2020 (13 pages). Paul Magnard now works for Alice&Bob.

[2449] See Experimental quantum teleportation of propagating microwaves by K. G. Fedorov et al, December 2021 (7 pages).

[2450] See Short-Range Microwave Networks to Scale Superconducting Quantum Computation by Nicholas LaRacuente et al, January 2022 (22 pages).

[2451] See also A modular quantum computer based on a quantum state router by Chao Zhou, Matthieu Praquin et al, Universities of Pittsburgh and Illinois and ENS Paris, September 2021 (11 pages). With Praquin from ENS Paris. About linking transmon qubits with microwaves, starting with implementing SWAP gates between 4 single-qubit modules with relatively slow gates (750 ns). Quote: "*For atomic scale qubits communicating using optical frequency states, it is infeasible to couple photons into a communication channel with* ***very high efficiency****. This loss of information precludes light from simply being transferred from module to module, instead one must* ***herald instances*** *in which transmission is successful*". This doesn't bode well for photons interconnect.

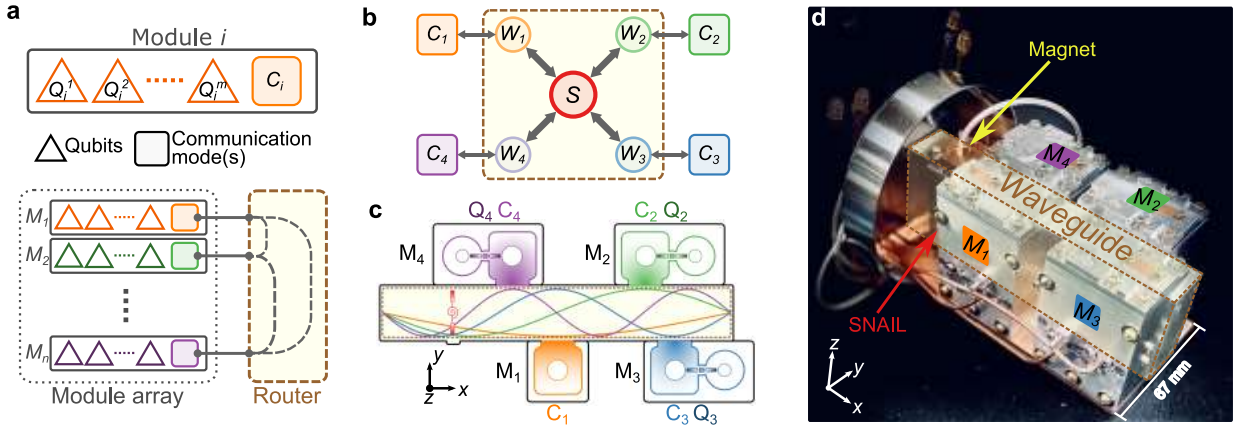


Figure 1. **Schematic representation and picture of the modular quantum computer device** (a) Basic structure of our modular quantum computer, in which a number of quantum modules are connected via their communication modes to a quantum state router. (b) Coupling scheme between the router and four communication modes. The brown dashed square represent the router with four waveguide modes ($W_1 - W_4$) and a SNAIL (S). Each waveguide mode is dispersively coupled to a single communication cavity mode ($C_1 - C_4$). (c) Schematic drawing of the full system consisting four modules and the central quantum state router. The colored curves inside the router represent the E (electric) field distribution of the first four waveguide $TE_{10n} (n = 1, 2, 3, 4)$ eigenmodes. The SNAIL chip (represented in red) is placed at a location where it couples to all the waveguide modes being used. Each module (for M_2 to M_4) consists of a qubit ($Q_2 - Q_4$), a communication cavity ($C_2 - C_4$) and a readout cavity (for module M_1 the qubit has been omitted). (d) Photograph of the assembled device.

Figure 772: Source: A modular quantum computer based on a quantum state router by Chao Zhou, Matthieu Praquin et al, Universities of Pittsburgh and Illinois and ENS Paris, September 2021 (11 pages).

Another way would be the creation of more complicated many-to-many connectivity. If you have for example two superconducting chipsets ala Google Sycamore with, let's say, NxN qubits, you will first need to create N connections between the edge of the first chipset and the edge of the nearby second chipset.

Then, with entanglement sharing, you will have to make sure you can create two-qubit gates with these nearby connected qubits[2452]. What gate would be mandatory to enable a real scale-out? At least SWAP gates[2453]. You'd need to adopt a full stack approach, from the qubits, the QPUs interconnect and all related software concerns[2454].

Microwaves-based interconnect is also investigated to create quantum link between electron spin-based qubits[2455].

[2452] See Quantum transfer of interacting qubits by Tony J. G. Apollaro et al, May 2022 (24 pages) which addresses this point of N qubits connectivity between nearby chipsets.

[2453] See A modular quantum computer based on a quantum state router by Chao Zhou et al, April 2022 (21 pages) with all-to-all couplings among four independent quantum modules of superconducting qubits. They handle full-iSWAP time of 760 ns and average inter-module gate fidelity of 97% and Co-Designed Architectures for Modular Superconducting Quantum Computers by Evan McKinney et al, University of Pittsburgh, May 2022 (14 pages) which uses a superconducting nonlinear asymmetric inductive element (SNAIL) modulator and $\sqrt{iSWAP}$ gates. Hypercube 3D connections.

[2454] See Will Quantum Computers Scale Without Inter-Chip Comms? A Structured Design Exploration to the Monolithic vs Distributed Architectures Quest by Santiago Rodrigo et al, 2020 (6 pages) which makes some fully-stack architecture proposals. See also Towards a distributed quantum computing ecosystem by Daniele Cuomo et al, University of Naples, Italy, March 2020 (6 pages).

[2455] See Resonant microwave-mediated interactions between distant electron spins by F. Borjans, Jason Petta et al, Nature, December 2019 (6 pages) and Strong coupling between a photon and a hole spin in silicon by Cécile X. Yu, Simon Zihlmann, José C. Abadillo-Uriel, Vincent P. Michal, Nils Rambal, Heimanu Niebojewski, Thomas Bedecarrats, Maud Vinet, Etienne Dumur, Michele Filippone, Benoit Bertrand, Silvano De Franceschi, Yann-Michel Niquet and Romain Maurand, June 2022 (6 pages).

In August 2021, **AMD** published a patent designed to handle a local scale-out capacity for quantum computers, with a teleportation-based multi-SIMD architecture. SIMD stands for "Single Instruction Multiple Data" and is heavily used in parallel classical hardware architectures like vector processors or tensor processors and GPUs. Here, teleportation would be used to handle coordination between several quantum processing units and reduce both the number of qubits and quantum gates needed to run an algorithm. Unfortunately, this patent doesn't describe in any way a real quantum process, contains no physics, no maths, no compiling trick, no timing analysis and nothing about teleportation implementation and about any quantum algorithm parallelization. It also mentions a "global memory" like if creating qubits memory was some standard off-the-shelf technology. On top of that, none of the patent holders seem to have a quantum computing background and they never published any quantum-related paper visible on arXiv[2456].

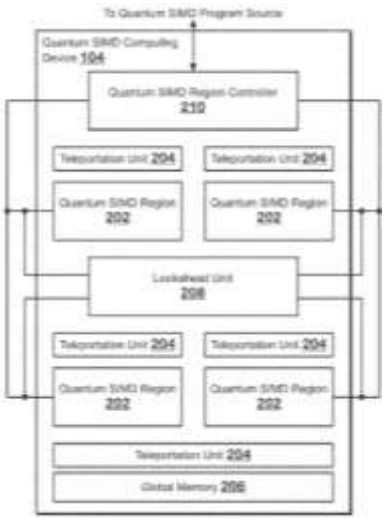


Figure 773: AMD's weird patent.

This has the flavor of a PR-driven approach that only a few scientists can fact-check, if not of a patent-troll. And it unfortunately worked[2457]!

In June 2022, **Huawei** also published a patent in China numbered CN114613758A related to the production of quantum computing chipsets and their scale-out. It describes M subchips of N qubits[2458]. In the provided schematics, you can see four qubits subchips (20), four coupling structures (30) and a central one with no connectivity with the others that is the cavity mode suppression structure of undetermined nature, shape and form (40). The asserted benefit from this architecture is resilience to manufacturing defects more than a scale-in architecture. These have undetermined internal structures and connections, nor any physical or experimental data attached. This wouldn't pass any scientific paper peer-reviewing process! Needless to say that like with AMD, this is borderline patent troll.

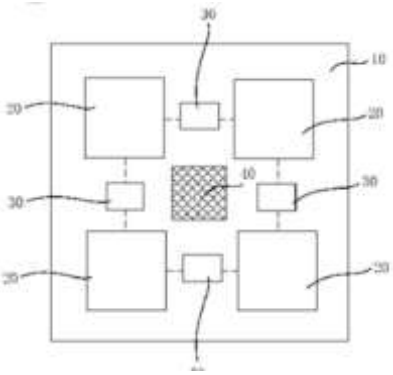


Figure 774: Huawei also weird patent.

Photons interconnect

The most generic way to interconnect QPU, particularly over arbitrary distance, would be with photons and fiber optics. It requires a couple things like creating deterministic or heralded sources of entangled photons connecting qubits, qubits-to-photon or microwave-to-photon[2459] quantum state conversion, photons conversions to telecoms wavelengths[2460] and, most of the time, some form of quantum memory for synchronization purpose.

[2456] See New AMD Patent Proposes Teleportation to Make Quantum Computing More Efficient by Francisco Pires, August 2021.

[2457] See for example AMD patent reveals revolutionary teleportation-based quantum computer by Bogdan Solca, Notebook Check, August 2021.

[2458] See Huawei publishes patents related to Quantum chips and Quantum computers by Amit, Huawei, June 2022.

[2459] See Large-bandwidth Transduction Between an Optical Single Quantum Dot Molecule and a Superconducting Resonator by Yuta Tsuchimoto, Andreas Wallraff, Martin Kroner et al, PRX Quantum, 2022 (13 pages).

[2460] See Quantum frequency conversion of memory-compatible single photons from 606 nm to the telecom C-band by Nicolas Maring, Dario Lago-Rivera et al, IFCO, 2021 (7 pages).

It seems better adapted to either photon qubits (which don't need any conversion) and qubits that are controlled by photons in the visible or near visible spectrum like cold atoms, trapped ions and NV centers[2461]. Trapped ions and cold atoms are controlled by lasers, but converting their quantum state into a photon is no small matter. Silicon qubits use the spin of one or two electrons. Spin-to-charge and charge-to-photon conversions can then be performed.

At some point, as presented in a custom drawing below, interconnect architectures may someday mix various techniques, with short-range interconnect techniques using microwaves and longer range techniques based on photons entanglement.

Some photon-based interconnect experiments have also been done with silicon spin qubits[2462]. Another option to interconnect superconducting qubits is to entangle them first with NV centers spin qubits which themselves are then easier to interconnect with photons[2463]. Another option is to couple a SiV vacancies electron spin acting as a communication qubit to a ^{29}Si nuclear spin acting as a memory qubit[2464].

Other researchers are looking for ways to encode quantum information differently in transmitted photons.

Instead of using a classical polarization encoding, researchers from Caltech experimented quantum teleportation of time-bin qubits (with "time of arrival" encoding) using a standard telecommunication wavelength of 1536.5 nm with an average success superior to 90%[2465].

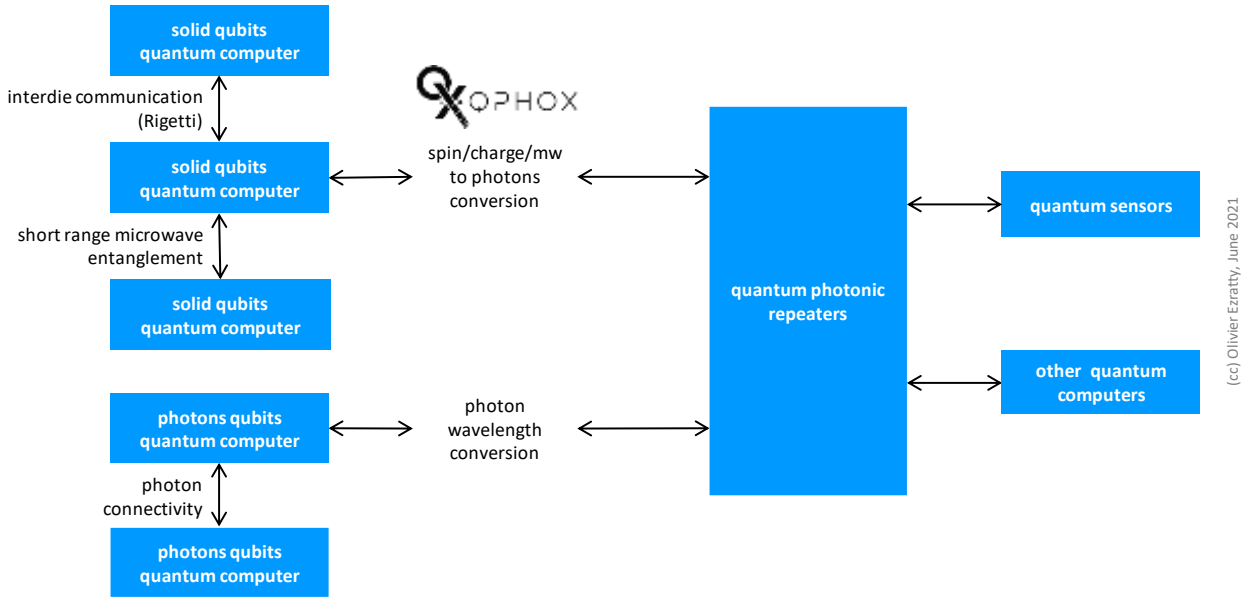


Figure 775: various interconnect architectures. (cc) Olivier Ezratty, 2022.

[2461] In 2021, a team from Qutech and TU Delft connected three NV centers qubits quantumly in an entangled GHZ state, beyond the traditional two nodes existing experiments. See Realization of a multi-node quantum network of remote solid-state qubits by Matteo Pompil, Sophie Hermans, Stephanie Wehner et al, February 2021 (28 pages).

[2462] See for example First chip-to-chip quantum teleportation harnessing silicon photonic chip fabrication by the University of Bristol, December 2019 which refers to Chip-to-chip quantum teleportation and multi-photon entanglement in silicon by Daniel Llewellyn et al, 2019 (48 pages). And the exaggerated version in The first "quantum teleportation" between two computer chips by Valentin Cimino, December 2019.

[2463] See Anisotropic rare-earth spin ensemble strongly coupled to a superconducting resonator by S. Probst et al, 2021 (7 pages).

[2464] See Robust multi-qubit quantum network node with integrated error detection by Pieter-Jan Stas, Mikhail D. Lukin et al, Harvard, July 2022 (24 pages).

[2465] See Teleportation Systems Toward a Quantum Internet by Raju Valivarthi et al, Caltech, 2020 (16 pages).

Trapped ions can also be interconnected with photons. It's the main scale-out plan for startups like IonQ[2466]. A European team succeeded in interconnecting trapped ions with photons over a distance of 230 m in 2022[2467].

Given it's still the dominant architecture, superconducting to photons connectivity is an intense field or research. In that case, microwaves are converted to another frequency range while keeping the quantum state.

This conversion can be done with opto-electromechanical systems[2468]. TU Delft researchers led by Simon Gröblacher experimentally achieved this in 2018, at 20 mK, close to superconducting qubits operating temperature[2469].

This led to the creation of **QPhoX** (2021, Netherlands, 8.9M€) by Simon Gröblacher, a startup seed funded by Quantonation. The research project turned into a "quantum modem for the quantum Internet"[2470]. Although QPhoX is a startup, it seems still operating in a field a fundamental and experimental research[2471]. In September 2022, the startup announced a partnership with IQM to scale-out superconducting qubit quantum computers.

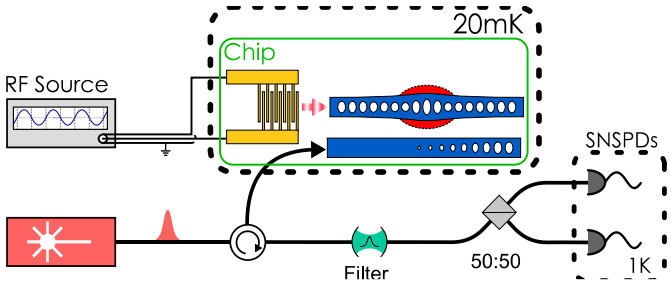


Figure 776: Source: Microwave-to-optics conversion using a mechanical oscillator in its quantum ground state by Moritz Forsch et al, 2019 (11 pages).

Next Generation Quantum (2019, USA) is CUNY university spin-off created by Shaina Raklyar (CEO) and German Kolmakov (CTO) developing commercial quantum computing applications and a hardware and software solution interconnecting multiple quantum computers to create quantum computer clusters.

They plan to manage this connection with photons and to use cavity polaritons, photons dressed with charges in a semiconductor optical microcavity that are sensitive to electric fields.

WeLinQ (2022, France, 5M€) is a startup created by Tom Darras (CEO), Jean Lautier-Gaud (COO), Julien Laurat and Eleni Diamanti (both scientific advisors).

It is a spin-off from two laboratories from Sorbonne Université: the Laboratoire Kastler Brossel and the Laboratoire d'Informatique de Sorbonne Université.

[2466] See Large Scale Modular Quantum Computer Architecture with Atomic Memory and Photonic Interconnects by Chris Monroe, July 2013 (16 pages), A high-fidelity quantum matter-link between ion-trap microchip modules by M. Akhtar, Igor Caron, Sylvain Gigan et al, March 2022 (8 pages).

[2467] See Entanglement of trapped ion qubits separated by 230 meters by V. Krutyanskiy, Nicolas Sangouard, Tracy Northup, August 2022 (22 pages) with a fidelity of 88% but a very low success rate of 4×10^{-5}.

[2468] See also A quantum microwave-to-optical transducer by Thibaut Jacqmin of LKB, 2019 (17 slides) which describes opto-electromechanical mechanisms for state conversion of superconducting qubits into transportable photons on optical fibers.

[2469] See New horizons for connecting future quantum computers into a quantum network, October 2019 which references Microwave-to-optics conversion using a mechanical oscillator in its quantum ground state by Moritz Forsch et al, 2019 (11 pages).

[2470] See The widely anticipated quantum internet breakthrough is finally here by Maija Palmer, May 2021 and A perspective on hybrid quantum opto- and electromechanical systems by Yiwen Chua and Simon Gröblacher, 2020 (7 pages). Simon Gröblacher also created Nenso Solutions, a quantum technology consulting company.

[2471] See Optomechanical quantum teleportation by Niccolò Fiaschi, Simon Gröblacher et al, Nature, October 2021 (9 pages) and Coherent feedback in optomechanical systems in the sideband-unresolved regime by Jingkun Guo and Simon Gröblacher, June 2022 (12 pages).

They develop a unique full stack (hardware and software) quantum link solution to interconnect quantum processors to enable the scale up of quantum computing. Their quantum links are based on world record cold atom quantum memories. They enable the efficient interconnexion of quantum processors to increase their computational power and the implementation of world's first quantum repeaters to enable a secure access to quantum computing at a distance.

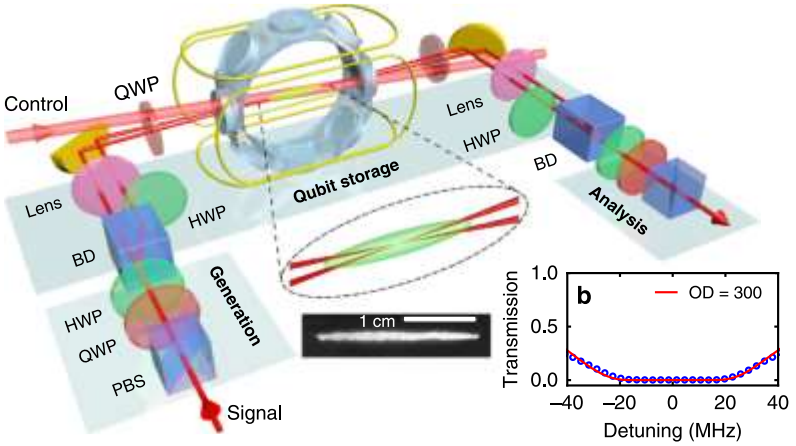


Figure 777: Source: Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble by Pierre Vernaz-Gris, Julien Laurat et al, Nature Communications, 2018 (6 pages)

Their first product, called *QDrive*, is a robust, compact, and transportable highly efficient quantum memory which will be deployed in quantum computing infrastructures to perform first proof of concepts with providers of quantum computing. Their memory technology is based on an elongated quasi-2D magneto-optical trap of alkali atoms cooled at a temperature close to 20 µK.

It enables the on-demand (i.e., the storage time is adjustable by the user) and efficient storage of photonic qubits and entangled states with a world record efficiency of 90%, qubit fidelity above 99% and a storage time of 15 µs[2472]. This is becoming a real commercial product.

In September 2022, WeLinQ announced a partnership with ixBlue for the procurement of lasers adapted to their needs.

In the quantum memory realm, Chinese researchers succeeded in 2019 to entangle two rubidium atom ensembles quantum memories via entangled photons at a distance of 50 km[2473]. But ensemble atoms are not perfect qubits for computing.

PhotoniQ (2021, Israel) is a startup developing quantum interconnection systems based on cold atoms chips. Its founder is Ron Folman, a quantum researcher from Ben Gurion Negev University. The system would be used both for quantum repeaters and for connecting several quantum processing units. This is still at the research stage and the startup is still stealth.

Other efforts are undertaken to connect heterogeneous quantum networks with hybrid entanglement swapping between DV and CV photonic systems[2474]. More classically, qubits can be distantly connected through a photonic link, as MPQ researchers in Germany did show in 2021[2475].

[2472] See Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble by Pierre Vernaz-Gris, Julien Laurat et al, Nature Communications, 2018 (6 pages) and Connecting heterogeneous quantum networks by hybrid entanglement swapping by G. Guccione, Tom Darras, Julien Laurat et al, April 2021 (15 pages) where they describe a higher-level interconnect architecture based on their technology.

[2473] See New Record: Researchers have entangled quantum memory over 50 kilometers by Stéphanie Schmidt, February 2020. The feat comes from Hefei's Jian-Wei Pan laboratory in China. This refers to the article published in Nature: Entanglement of two quantum memories via fibers over dozens of kilometers by Jian-Wei Pan et al, February 2020 and previously on arXiv in March 2019: Entanglement of two quantum memories via metropolitan-scale fibers (19 pages).

[2474] See Quantum Networking Demonstrated for First Time par Dhananjay Khadilkar, November 2018, referencing Connecting heterogeneous quantum networks by hybrid entanglement swapping by Giovanni Guccione, Tom Darras et al, May 2020 (7 pages).

[2475] See Quantum systems learn joint computing - MPQ researchers realize the first quantum-logic computer operation between two separate quantum modules in different laboratories, February 2021.

Entangled Networks (2020, Canada) is a startup developing a set of protocols and software for multi-QPU environment (multi-qubit gates implementation across distributed QPUs, performance optimization).

The hardware part requires optical quantum interconnect solutions including a high-resolution optical collection system and a low loss Bell state analyzer. The company was created by Aharon Brodutch (CEO) and Ilia Khait (CTO), two Israeli researchers established in Toronto. It was acquired by IonQ in January 2023.

Bohr Quantum Technology (2022, USA) is a stealth startup working on a quantum interconnect system based on some Caltech and Fermilab research. It is supposed to enable quantum computing scaley-out architectures with interconnecting QPUs and/or quantum memories.

The company was created by Paul Dabbar (CEO, a former Under Secretary for Science of the DoE who oversaw DoE research labs during the whole Trump administration) and Conner Prochaska (Chief of Strategic Partnerships, also coming from the DoE). No CTO or Chief Scientist? Bad omen. Their LinkedIn profiles tout that the company "*has developed and built the world's first commercial ready quantum networking system*".

Electrons and ions shuttling

Electrons shuttling is a technique envisioned to enable interconnection of silicon spin qubits[2476]. It would have a very short range.

QUASAR is a semiconductor-based project using shuttling electrons with a QuBus (*pictured next*), a quantum bus to transport electrons and their quantum information over distances of 10 µm. The partners are Infineon, HQS, Fraunhofer (IAF, IPMS), Leibnitz Association (IHP, IKZ) and the Universities of Regensburg and Konstanz. The project will run until 2025 to create 25 coupled qubits. The resulting computer is to be deployed at JUNIQ.

Jülich is also participating to the European Flagship QLSI project driven by CEA-Leti in France. QUASAR got a 7.5M€ funding from BMBF. The resulting computer is to be deployed at JUNIQ. Jülich is also participating to the European Flagship QLSI project driven by CEA-Leti in France. QUASAR got a 7.5M€ funding from BMBF[2477].

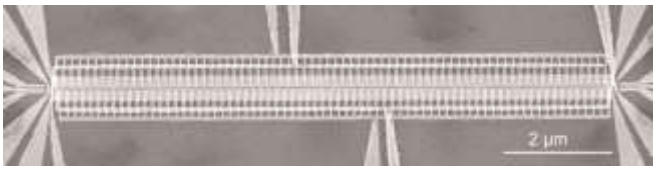


Figure 778: an electron shuttling waveguide. Source: Quanten-Shuttle zum Quantenprozessor "Made in Germany" gestartet, Jülich, February 2021.

Ion shuttling is an interconnect technique that we already quickly described with IonQ and Quantinuum.

At last, let's mention another interconnect technique, that ties superconducting qubits together with phononic communication using surface acoustic waves with the advantage that it fits into a solid-state circuit[2478].

[2476] See Multicore Quantum Computing by Hamza Jnane, Simon Benjamin et al, Quantum Motion, January 2022 (24 pages) which deals with interconnecting silicon based QPUs with microwaves or electrons shuttling.

[2477] See Quanten-Shuttle zum Quantenprozessor "Made in Germany" gestartet, Jülich, February 2021.

[2478] See Quantum Communication with itinerant surface acoustic wave phonons by E. Dumur, Audrey Bienfait, et al, University of Chicago and ENS Lyon, December 2021 (5 pages).

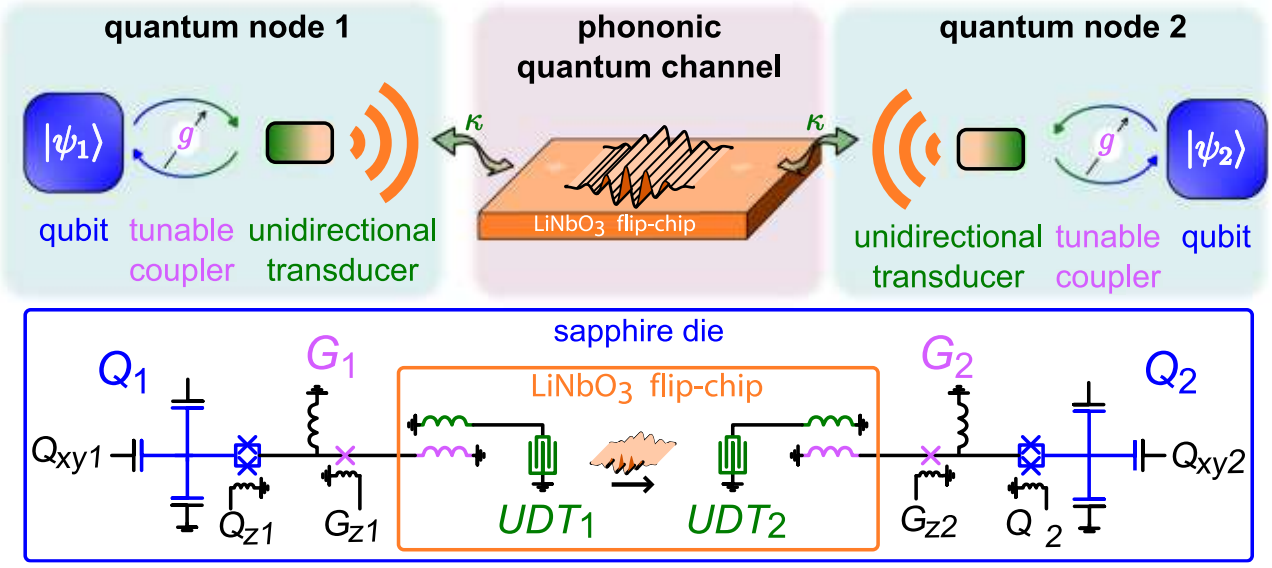


Figure 779: Source: Quantum Communication with itinerant surface acoustic wave phonons by E. Dumur, Audrey Bienfait, et al, University of Chicago and ENS Lyon, December 2021 (5 pages).

Quantum telecommunications infrastructures

Three other areas must make progress to enable the deployment of quantum telecommunications networks: protocols[2479], repeaters[2480], switches[2481], quantum memories[2482], distributed quantum error correction schemes[2483] and also compiler and other various software tools to distribute processing over several QPUs[2484].

In the network layout domain, a team led by British and Austrian researchers established an any-to-any quantum communication link with 8 network nodes using dense wavelength division multiplexers (DWDM) and a single source of polarization-entangled photon pairs[2485]. Is this a "quantum Internet"? It's still a marketing buzzword since many-nodes technologies are not really available and quantum entanglement distribution is an additional feature and not a replacement for existing classical networks.

[2479] Let's mention the Quantum Protocol Zoo initiative launched by LIP6 and VeriQloud which inventories about 56 quantum telecommunication and cryptography protocols. See Protocol Library. See also Benchmarking of Quantum Protocols by Chin-Te Liao, Elham Kashefi et al, July 2022 (16 pages).

[2480] See Adaptive bandwidth management for entanglement distribution in quantum networks by Navin B. Lingaraju et al, 2021 (5 pages).

See Telecom-heralded entanglement between multimode solid-state quantum memories by Dario Lago-Rivera et al, Nature, IFCO, June 2021 (7 pages).

[2481] See Development of Quantum InterConnects (QuICs) for Next-Generation Information Technologies by David Awschalom et al, 2019 (31 pages) and Quantum Switch for the Quantum Internet: Noiseless Communications Through Noisy Channels, 2020 (14 pages).

[2482] See this general overview of quantum memories used in quantum networks: Optical Quantum Memory and its Applications in Quantum Communication Systems by Lijun Ma et al of NIST, 2020 (13 pages). The schema of this page on the Quantum Internet is derived from it. See also Towards real-world quantum networks: a review by Shi-Hai Wei et al, January 2022 (71 pages) that discusses the links between quantum computing resources and quantum memories.

[2483] See Quantum teleportation of physical qubits into logical code spaces by Yi-Han Luo, William J. Munro, Anton Zeilinger, Jian-Wei Pan et al, July 2021 (5 pages).

[2484] See Optimized compiler for Distributed Quantum Computing by Daniele Cuomo et al, December 2021 (15 pages) and Distributed Shor's algorithm by Ligang Xiao, July 2022 (15 pages).

[2485] See A trusted node–free eight-user metropolitan quantum communication network by Siddarth Koduru Joshi et al, September 2020 (9 pages) and the subsequent work Flexible entanglement-distribution network with an AlGaAs chip for secure communications by Félicien Appas, Eleni Diamanti, Sara Ducci et al, NPJ Quantum Information, July 2021 (12 pages).

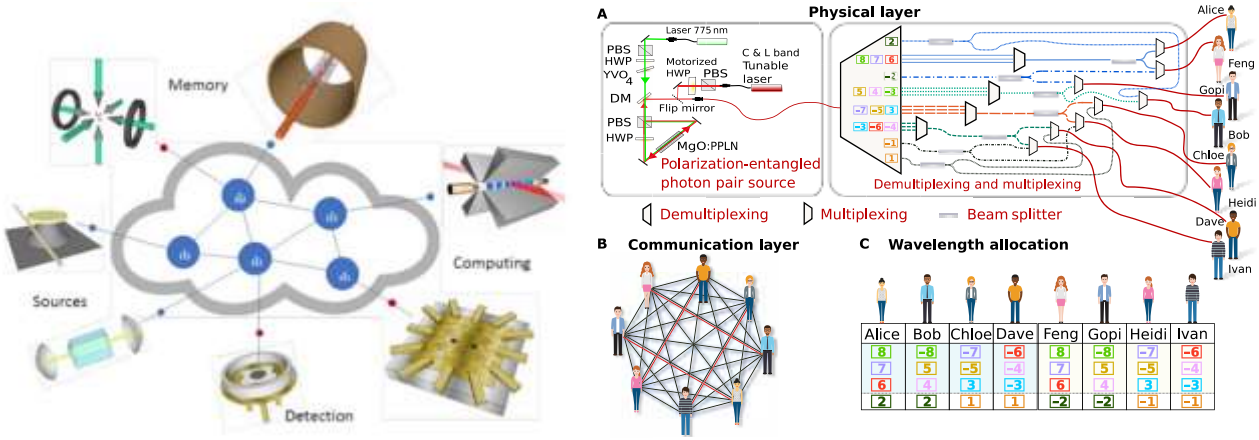


Figure 780: Source: A trusted node–free eight-user metropolitan quantum communication network by Siddarth Koduru Joshi et al, September 2020 (9 pages).

Other applications of quantum telecommunications should be mentioned in addition to distributed computing:

- **Quantum electronic signatures** that authenticate classic messages. They are transferable to third parties, non-repudiable and non-forgeable.
- **Connecting quantum sensors** which could be useful when it makes sense to consolidate quantum states from various quantum sensors, to improve their precision, like with telescopes interferometry, and also protect their content[2486].
- **Transmission of anonymous data**. It allows two nodes in a quantum network to communicate with each other without one node being able to identify the other node and also without the other nodes not involved in the protocol being able to identify the sender and the recipient. The communications leave no trace and are therefore not auditable. This replaces traditional anonymization proxies. It can be used as a basis for distributed processing, coupling this with classical or quantum data encryption. It is a means of ensuring the anonymization of the transmission of data such as survey or health data.
- **Quantum money** that applies a concept of Stephen Wiesner (1942-2021, Israeli) from 1970, and improved in 1983. It is based on tokens of verifiable integrity that can only be used once[2487].
- **Clock synchronization** which has been tested in the early 2000s and is useful for telecommunication networks and GPS operations[2488].
- **Detecting Extra-Terrestrial life**. Well, sort of. That's the plan from SETI who wants to analyze "quantum communications" coming from exoplanets, which would bear some differentiated signature. One can wonder how such communications could be sorted out from the planet's star random photon streams, but who knows[2489].

About the relationship with inter-QPU connectivity and data-transfer speed? Could these connections enable faster data-transfer than classical data links? Well, yes and no. If it's about transmitting classical data, an inter-QPU or quantum telecom link won't make things faster.

[2486] See one example with Distributed quantum sensing with optical lattices by Jose Carlos Pelayo, Karol Gietka and Thomas Busch, Okinawa Institute of Science and Technology Graduate University, August 2022 (7 pages).

[2487] A recent proposal of quantum money co-authored by Peter Shor is in Publicly verifiable quantum money from random lattices by Andrey Boris Khesin, Jonathan Z. Lu and Peter Shor, July 2022 (15 pages). It's still highly theoretical.

[2488] See Distant clock synchronization using entangled photon pairs by Alejandra Valencia et al, 2004 (10 pages).

[2489] See We could detect alien civilizations through their interstellar quantum communication by Matt Williams, April 2021 referring to Searching for interstellar quantum communications by Michael Hippke, April 2021 (14 pages).

Inter-QPU connectivity is mainly about creating a (much) larger QPU than the separate QPUs. The resource is entanglement. When you have two interconnected QPUs of N qubit each, the Hilbert space managed by the interconnected QPUs has a size of 2^{2N} complex numbers whereas the isolated QPUs handle only $2*2^{N}=2^{N+1}$ complex numbers. But in the end, when reading out the qubits in these isolated or consolidated QPUs, you don't capture more than 2N classical bits. But teleportation may be useful to teleport at a very fast rate an entangled state from one location to another. Let's say that while the data is quantum, interconnect and teleportation can bring some speed advantage. This could be the case when connecting quantum sensors and quantum computers.

Quantum Physical Unclonable Functions

qPUF are not the most talked about quantum technologies. It is at the crossroads of quantum cryptography, QRNGs, embedded systems and sensors.

Generically, Physical Unclonable Functions (PUF) are systems containing a piece of classical hardware that contain some unique signature related to the random aspect of matter and physical disorder[2490]. This unique signature can't be reproduced. It can also be dynamically generated and always be different.

A PUF is implemented as a unique function and is hard to physically and logically clone. They operate on a challenge/response basis: a challenge is fed into the PUF, which generates a unique binary response coming from the hardware module, which is based on its unique material imperfections.

The physical imperfections used in PUF are manyfold: reflection of optical materials, random scattering of light, ring oscillators, coating materials capacitance up to some random characteristics of electronic components like SRAM and DRAM memories. The most common PUFs are using silicon IC and their various defects and variations that are even greater as their integration nodes become smaller, now down to 5 nm.

The generated binary strings are used in as keys or identifiers in cryptography systems and as anti-counterfeiting systems. These can also serve as generic true random number generators, either standalone or combined with other entropy sources. But these security systems are not perfect and are prone to various attacks[2491], done with various methods including machine learning, side attacks and even, potentially, quantum computing[2492].

qPUFs are quantum equivalents of PUF that are based on quantum states and their physical unclonability. There's even a variation with Quantum read-out of PUF (QR-PUF) which reads-out quantumly a non-quantum physical disorder in a physical device. These qPUFs are better than classical PUFs but their resistance to forgery depends on their detailed level of unforgeability, which can be "existential" and "selective"[2493].

[2490] See Physical One-Way Functions by Papu Srinivasa Ravikanth, 2001 (154 pages) and Physically Unclonable Functions - a Study on the State of the Art and Future Research Directions by Roel Maes and Ingrid Verbauwhede, 2010 (36 pages).

[2491] A side-channel attack collects information from a security system or influence its execution in an indirect manner, by collecting in a stealth way some data on hardware operations (quantity of data processed in a computer, heating, amount of gas in a car tank). Side-channels may be power dissipation, operations timing, system temperature, acoustic, radio or optical emissions or a mix of these.

[2492] Samsung Galaxy S10 launched in 2019 contains an Exynos 9820 chipset with PUF technology, for crypto wallets, associated with Samsung Knox, a built-in storage hardware for security keys used with Blockchain services and cryptocurrencies like Ethereum. According to Samsung, the Exynos "*PUF generates an unclonable key for data encryption by using the unique physical characteristics of each chip*" but this characteristic is not specified. Looks like this PUF was replaced in some subsequent Samsung smartphones by a QRNG coming from IDQ.

[2493] See Quantum Physical Unclonable Functions: Possibilities and Impossibilities by Myrto Arapinis, Elham Kashefi et al, June 2021 (32 pages) and A Unified Framework For Quantum Unforgeability by Mina Doosti, Mahshid Delavar, Elham Kashefi and Myrto Arapinis, March 2021 (47 pages), all from the University of Edinburgh and CNRS LIP6 Paris. See also On the Connection Between Quantum Pseudorandomness and Quantum Hardware Assumptions by Mina Doosti, Elham Kashefi et al, March 2022 (33 pages) which deals with the conditions of unforgeability in relation to quantum pseudorandomness.

What is the physical form of qPUFs? It can be based on photonic features and polarized prepared devices and multiple scattering medium.

Quantum Base (2014, UK, $1.1M) offers various quantum product authentication solutions such as the Q-ID Optical, an optically readable "atomic" fingerprint solution that uses Physically Unclonable Functions (PUFs) in the form of physical tags that cannot be copied at the atomic scale level[2494].

The tag exploits a thin 2D layer of graphene that contains unique irregularities at the atomic scale that cannot be cloned. These irregularities would be amplified by unspecified quantum phenomena. Moreover, these tags can be dynamically activated and deactivated.

The project stems from the work of Lancaster University of Robert Young who is the co-founder of the startup. The whole is integrated in a home-made random number generator (Q-RAND) based on a semiconductor diode, which can be integrated in a chipset (video)[2495]. They also propose the Q-ID Electronic, a unique identifier generator.

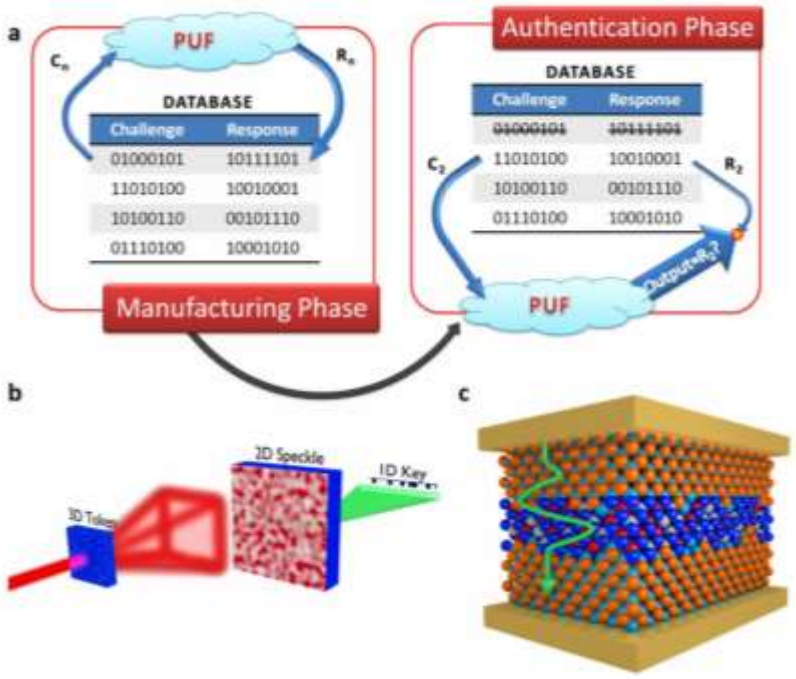


Figure 781: a qPUF made with photon and a scattering media.

Vendors

Let's now review the startups in this vast sector of activity of quantum and post-quantum cryptography, trying to describe the nature of their offer and their differentiation when the information is publicly available! I have only kept here startups offering technology solutions and not integrated consulting and integration companies.

Note that on the market size side, the market for quantum and post-quantum cryptography is modest for the moment. A 2017 report estimated it at $2.5B by 2022[2496]. However, it is expected to gain momentum from this period onward, following the finalization of standardization by NIST and ETSI.

[2494] This is documented in the USPTO patent US10148435B2 Quantum Physical Unclonable Function filed in 2015 (11 pages) and validated in 2018. It evokes a semiconductor component based on gallium arsenide, aluminum and antimony that generates a random spectral response that differs from one component to another. The process is described in Using Quantum Confinement to Uniquely Identify Devices by Robert Young et al, 2015 (8 pages).

[2495] The *resonant-tunnelling diode* (RTD) process is documented in Resonant-Tunnelling Diodes as PUF Building Blocks, by Ibrahim Ethem Bagci et al, 2018 (6 pages).

[2496] See New CIR Report States Quantum Encryption Market To Reach $2.5 Billion Revenues By 2022: Mobile Systems Will Ultimately Dominate, 2017.

In addition to startups, commercial offers in quantum and post-quantum cryptography are also proposed or about to be proposed by various large IT players such as **Battelle**, **Infineon**, **Raytheon**, **IBM**, **Atos**, **Gemalto** (part of Thales group), **Cisco**[2497], **Infineon**[2498], **Microsoft**[2499], **Intel**[2500], **NEC**, **Toshiba**, **Huawei**[2501], **KT** and **Samsung**. Even **Amazon** announced in 2022 the creation of its own quantum networking center in Boston and a partnership with Harvard University[2502].

Figure 782: the big map you were expecting on QKD (left) and PQC (right) vendors. (cc) Olivier Ezratty, 2022.

IBM created a set of PQC protocols and participated to the NIST PQC competition. They were finalists of round 3 of the NIST selection in July 2020 for both lattice-based CRYSTALS-KYBER (secure key encapsulation mechanism) and CRYSTALS-DILITHIUM (secure digital signature). These were developed in partnership with **ENS Lyon** (France), **Ruhr-Universität Bochum** and **Radboud University** (Germany). These PQC solutions are embedded in an IBM TS1160 tape drive system with a modified firmware in combination with symmetric AES-256 encryption. It enables a secured long-term data storage. In November 2020, IBM also announced it would integrate these protocols in its cloud offering.

Microsoft also works on PQC algorithms. It includes FrodoKEM and SIKE which are PQC based key exchanges protocols. Then, qTesla and Picnic, PQC based signatures protocols.

[2497] Cisco's Quantum Research is led by Alireza Shabani with three full time researchers. The company is even organizing a yearly event, Cisco Quantum Summit.

[2498] With its Optiga TPM SLB 9672, a hardware trusted module supporting AES and SHA2-384 encryptions that are quantum resistant.

[2499] See the Microsoft site that describes their activity in the PQC.

[2500] Intel participated to the creation of the BIKE PQC PKI that was preselected in 2020 by NIST but is not so far a finalist, per the 2022 4 selected PQCs, including only one PKI. Intel PQC research is done at their Crypto Frontiers Research Center that was launched in 2021. This collaborative effort with Universities is plan to last only until 2024. See Intel Labs Establishes Crypto Frontiers Research Center, 2021.

[2501] See Continuous-Variable Quantum Key Distribution with Gaussian Modulation, the Theory of Practical Implementations, 2018 (71 pages). The Huawei team working on the QKD is partly located in their research center in Dusseldorf.

[2502] See Announcing the AWS Center for Quantum Networking by Denis Sukachev and Mihir Bhaskar, June 2022 and Announcing a research alliance between AWS and Harvard University by Antia Lamas-Linares, Mihir Bhaskar, and Denis Sukachev, September 2022.

Let's also mention **Toshiba**'s ambitions in QKD deployments, announced in October 2020. They are deploying a QKD based network for **NICT** (National Institute of Information and Communications Technology) in Japan, on top of a similar deployment undertaken with BT and their Openreach network in the UK in 2020 and demonstrations done with **Verizon** and **Quantum Xchange**.

Their hardware offer includes the "Multiplexed QKD system" which can transmit QKDs at a key rate of 40 kb/s over 70 km, and high-speed data on the same fiber. The "Long Distance QKD System" has similar features with a key rate of 300 kb/s and a range of up to 120 km but requiring two fibers. These solutions using the (quite old) BB84 protocol are manufactured in Cambridge, UK and fit in a 3U 19" rack format.

ABCMintFoundation (2017, Switzerland) created by Jin Liu and Jintai Ding is tasked with creating a quantum resistant Blockchain using a Rainbow Multivariable Polynomial Signature Scheme. It is a community driven open source project. It uses keys that can be as large as 1.7MB.

Abelian (2022, USA) is providing a Blockchain infrastructure enabling "gold 2.0" that is based on a lattice PQC. It secures financial transactions in smart contracts and so-called DeFI (decentralized finance based on a Blockchain). It even deals with the Metaverse and Web3 applications. The company is organized as a foundation and its founders are anonymous[2503].

AegiQ (2019, UK, $4,3M) is developing quantum cryptography systems based on III-V single-photon source semiconductors. It was created by Max Sich (CEO), Scott Dufferwiel (CTO) and Andrii Iamshanov (CFO) as a spin-off of the University of Sheffield. They plan to equip telecommunication data centers for their fiber optical infrastructures upgrades to QKD. They are also building a satellite-based QKD offering.

AgilePQ (2014, USA) provides a software platform for "post-quantum" security of communication between connected objects and the cloud, such as drones.

It includes AgilePQ C-code, a piece of software that runs on connected object microcontrollers and consumes little power, and AgilePQ DEFEND, an adaptive size-based key generation system. DEFEND generates codes that are harder to break than AES 256 and with 429 orders of magnitude difference. Specifically, we go from a key space of 10 to the power of 77 to 8*10 to the power of 506 (factor of 256)[2504] . The system that is patented seems to be a variant of linear random codes but with keys of reasonable size. It has been standardized at NIST and interfaces with SCADA (Supervisory control and data acquisition) control and supervision systems. The company is a Microsoft Azure partner.

American Binary or **Ambit** (2019, USA) sells PQC solutions to governments, enterprise customers and consumer products companies, including a VPN.

Anametric (2017, USA, $1.9M), formerly bra-ket science, is a startup that wants to create information storage systems in qubits operating at room temperature. It seems they are focused on quantum telecommunication systems.

[2503] See Abelian (ABEL) – A Quantum-Resistant Cryptocurrency Balancing Privacy and Accountability by Alice, Bob, Eve, and λ, February 2022 (140 pages).

[2504] See AgilePQ DEFEND Cryptographic Tests (11 pages).

Agnostiq Inc (2018, Canada, $2.5M) is a startup created by Oktay Goktas coming out of the Creative Destruction Lab accelerator in Toronto. They offer Covalent, a Python-based workflow management tool to submit and scale jobs on hybrid quantum computers, cloud privacy and quantum obfuscation tools and pre-built applications in the finance sector for portfolio optimization and options pricing. It supports all classical AWS cloud services.

Alternatio (2016, Poland) develops a post-quantum cryptography IP core to be integrated in chipsets for the industry and connected objects.

ArQit (2016, UK, $70M) is developing QuantumCloud, a cloud-distributed symmetric keys mixing keys generation in local agents and key distribution via low earth orbit satellites and QKD.

They also claim, through a patent, that they can implement terrestrial QKD without trusted nodes or repeaters, which was debunked by an international team of researchers[2505]. In May 2021, the company announced a funding round of $400M using an IPO through a special purpose acquisition company like IonQ, this time with Centricus Acquisition Corp. As a result, the company published in May 2022, a revenue of $12.3M for H2 2021 with an operating loss of $14.3M, with $5,3M in H1 2022, compared to a loss of $5.5M in H2 2020. They also published a "myth busting" presentation[2506].

BLAKFX (2017, USA) develop quantum resistant software solutions around their Helix22 SDK that provides five layers of symmetric keys protections for end-user to end-user communications (AES1, TwoFish, AES2, ThreeFish, Snow3G). With sufficiently long keys, symmetric keys are quantum resistant.

BraneCell Systems (2015, Cambridge Massachusetts and Dusseldorf, $1.8M) is a startup launched by Wassim Estephan and Christopher Papile.

It started to develop a cold atom based QPU[2507]! They have filed a few patents, including USPTO patent 9607271, validated in March 2017[2508]. They however later pivot on creating an atom-based repeater.

Ciena (1992, USA) is an equipment manufacturer in the field of optical telecommunications. They integrate IDQ's offers in their solutions, and, their optical random key generators.

[2505] See Long-range QKD without trusted nodes is not possible with current technology by Bruno Huttner, Romain Alléaume, Philippe Grangier, Hugo Zbinden et al, npj, September 2022 (5 pages).

[2506] See Arqit Myth Busters by Arqit, 2022 (10 pages). I'd say OK with most myths, but not for their assessment of the quantum computing threat on classical security which, like all cybersecurity vendors, they tend to exaggerate.

[2507] Their communication is cryptic to say the least, as BraneCell Systems Presents Distributed Quantum Information Processing for Future Cities, April 2018 and a partnership announced with the US government service provider, AST, in July 2018 in AST and BraneCell Announce Their Partnership to Improve Critical Government Functions Through the Power of Quantum Computing. They do not provide any technical or popularization information about their solution, qubits and error rates. They were also aiming for an ICO that would have been the first of its kind for a quantum computing startup. Their main goal was to create a secure communication system. They target the financial, energy, health, chemical and public sectors. A Quantum Theranos? At the very least, we have the right to doubt.

[2508] Here is the patent description: "*The subject matter relates to multiple parallel ensembles of early stage spherical pulses radiated through engineered arrays forming the foundation for quantized computer processors taking advantage of integer thermodynamics. The materials, architecture and methods for constructing micro- and/or nano-scale three-dimensional cellular arrays, cellular series logic gates, and signature logic form the basis of small- and large-scale apparatuses used to execute logic, data bases, memory, mathematics, artificial intelligence, prime factorization, optical routing and artificial thought tasks not otherwise replicated in electron-based circuits*".

Although they do not yet have a structured QKD offering, they are very interested in standardizing it. In particular, they are participating in the Quantum Alliance Initiative launched in 2018 in the USA by the Hudson Institute, a conservative think tank, which is working towards this goal and creating proposed standards for QKD and QRNG (quantum random number generation).

Crypta Labs (2013, UK, $300K) develops post-quantum encryption solutions adapted to connected objects. In particular, they propose quantum random number generators that can be integrated into a cell phone (such as IDQ) and also work in space. The QRNG uses a LED or laser light source and a camera sensor. They are working with the University of Bristol.

Crypto4A Technologies (2016, Canada) offers an encryption solution based on a random number generation.

It includes a 19-inch QAOS format appliance server for generating entropy random numbers (without specifying the technology used) and another that generates quantum safe PQC encryption, the QxEdge Hardware Security Module (HSM). The PQC generation module is called QASM (Quantum Assured Security Module), which duplicates the quantum development language of the same name.

It is based on quantum safe hash-based signatures (HBS). These appliances are equipped with four Intel Core i7 chipsets, 16 GB of memory and 256 GB of SSD and run on a hardened version of Linux. They support algorithms certified by the NSA in the USA ("suite B") and future NIST PQC standards.

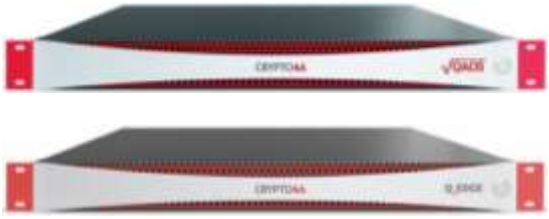


Figure 783: CryptoAA QRNG based HSM products.

CryptoExperts (2008, France) develops homomorphic encryption and post-quantum cryptography, and also offers services based on these technologies.

CryptoNext Security (2019, France) is a startup that develops a post-quantum cryptography solution. They were founded by Ludovic Perret (CPO, ex Inria, who left the company in 2022) and Jean-Charles Faugères (CTO, ex LIP6 Sorbonne) with Florent Grosmaitre as CEO.

Their software solution is developed in C language and assembler for performance reasons. It combines multivariate polynomials and hashing. Their solution can be integrated into RSA/ECC schemes by hybridization. CryptoNext is also one of the French teams who submitted a PQC proposal to the NIST which has been selected as an alternative candidate in 2020's round 2, GeMSS, which consolidates contributions from CryptoNext, Inria, Orange, University of Versailles and Sorbonne Université.

PQC standardization processors are used in practice by many organizations such as ISO, ITU (X509), IETF (TLS) and ETSI (algorithms). Their PQC should be integrated into R3's CORDA blockchain solution for banks. Note that China is also organizing a competition with a faster selection schedule than the NIST one. CryptoNext equips French special forces with their PQC, running on secure mobiles using Android.

Crypto Quantique (2016, UK, $8M) is a startup offering a cryptography solution to secure communication with connected objects targeting various markets ranging from automotive to finance. It uses a chipset that is installed in the object. It is a "quantum processor" in silicon technology that is used to generate a unique identification key for the object, which is tamper-proof and tamper-proof. It probably exploits photonics with a random number generator similar to the Swiss IDQ technologies.

Their technology is called Quantum Driven Physically Unclonable Function (QD-PUF) but they do not explain how it works or what encryption model is used[2509]. The founders are of Iranian, Italian and Greek origins, a beautiful patchwork. In July 2022, they announced that their platform was supporting the only selected PKI by NIST the same month, CRYSTALs-Kyber.

Cyph (2014, USA, $1M) sells PQC solutions. The company was created by Ryan Lester and Joshua Boehm, two engineers from SpaceX. Mars not interesting anymore?

Dencrypt (2013, Denmark) is a cybersecurity software provider protecting smartphone communications. They are working on creating PQC based solutions in partnership with the Technical University of Denmark (DTU).

evolutionQ (2015, Canada, $5.5M) is a startup that stands out especially for the pedigree of its creator, Michele Mosca, a specialist in post-quantum cryptography known for his Mosca scale to assess the risk of quantum computing on classical cybersecurity.

He is also the founder of the Institute for Quantum Computing at the University of Waterloo in Canada. The company provides what is known as "service equipped" to support companies in the adoption of post-quantum and quantum cryptography. It begins with a six-phase Quantum Risk Assessment product[2510]. Is it really a product? It looks more like a methodology to be implemented with consultants. The rest is of the same cream with integration and training services to evolve the company's cryptographic systems.

In July 2022, SandboxAQ announced a strategic partnership with evolutionQ including some funding in a series A round. It will help complement SandboxAQ's PQC offering with evolutionQ's QKD software platform, BasejumpQDN.

Flipscloud (2013, Taiwan) creates "quantum level" encryption software targeting IoT, cloud services and the big data market. It seems it is using some unspecified PQC and AES 256 bits keys. Software runs on embedded systems using Arm cores and Imagination CPUs.

fragmentiX (2018, Austria) offers a secure data storage management system that uses the technique of fragmentation and distribution of data on different physical media. All this is supplied in the form of appliances.

The distributed data is of course encrypted, but in a classical way. This is another way to create data protection that is resistant to Shor's algorithm. It is not the only company positioned in this niche.

They combined their appliances with QKD equipment from IDQ and Toshiba that was available at AIT. The theoretical proposal comes from researchers of TU Darmstadt in Germany and it has already been implemented a couple of years ago in Tokyo.

GoQuantum (2018, Chile) is willing to provide "*a post-quantum secure data transmission solutions through quantum-based hardware and radio link layer encryption*.". Translation: it's using PQC encryption algorithms with a photonic based QRNG for key generation.

HaQien (2019, India) designs post-quantum cryptography (PQC) solutions. But it is not quite clear because they also seem to use a random number generator to create classical keys.

[2509] See Physically Unclonable Functions: a Study on the State of the Art and Future Research Directions by Roel Maes and Ingrid Verbauwhede (36 pages) and Quantum readout of Physical Unclonable Functions by B. Skoric (21 pages).

[2510] It is documented in A Methodology for Quantum Risk Assessment, published in 2017.

Hub Security (2017, Israel, $55M) sells quantum secure FPGA based Hardware Security Module (HSM). These HSM modules contain QRNGs and support quantum-resistant algorithms acceleration in hardware (PQC).

IDQ (ID Quantique) (2001, Switzerland, $74.6M) is one of the oldest companies in the sector, cofounded by Swiss researcher Nicolas Gisin, a specialist in photonics and quantum entanglement.

The company offers a complete range of random number generators and QKD management systems as well as a high-efficiency (>95%) superconducting nanowire single photon detector (SNSPDs) as well as single-photon avalanche detectors (SPADs). These photon detectors are controlled by the ID1000 Time Controller Series introduced in January 2022.

Its Quantis random number generator, already described at the beginning of this section, is complemented by Cerberis, a QKD solution to protect the generation of encryption keys in a 6U rack and Centauris, a range of encryption servers supporting 100 GBits/s optical links. This FPGA-based server currently supports elliptic curve-based systems as well as AES-256, pending the standardization of PQC (post-quantum-crypto) protocols.

As of 2022, IDQ's Cerberis XG (enterprise market) and XGR (research market, supporting OpenQKD) Series was the fourth generation of this product line in a 1U form factor for both ends supporting various network topologies (ring, hub and spoke, meshed). It supports a 1.GHz key generation rate and includes a QRNG system for photon basis readout selection.

Since the beginning of 2018, the company belongs to the Korean group SKT Invest which is the Corporate Venture branch of **SK Telecom**. The fund invested $65M in what was modestly presented as a partnership while it's actually a takeover with a 51% ownership.

IDQ's QKD offer is notably deployed in Korea to protect the 5G backbone of the operator SK Telecom. They are also partnering with Toshiba in Cambridge and in the OpenQKD project.

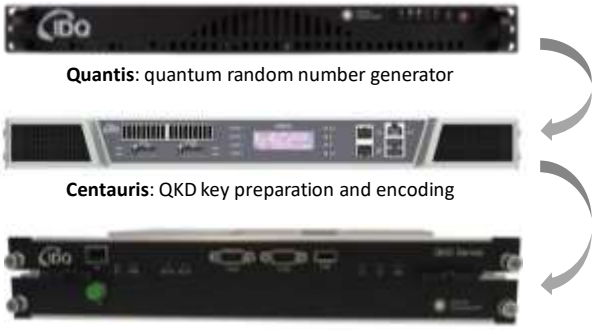


Figure 784: IDQ's QKD offering.

Keequant (2017-2020, Germany, $1.7M), formerly InfiniQuant, is a spin-off from the Max Planck Institute for the Science of Light with 14 employees as of November 2022. They develop CV-QKD solutions for telecom operators.

They work on miniaturizing their QKD systems in miniaturized plugable QKD+PQC hybrid boards costing less than 10K€. The startup is also working on a quantum random number generator.

Infotecs (1991, Russia) is a cybersecurity specialist historically specialized in VPN creation. It has developed a PQC solution in 2016, with an awkward communication that could make it look like QKD[2511].

But they develop many QKD solutions. In 2018, they launched their "ViPNet Quantum Phone", using their ViPNet VPN (ViPNet Client and ViPNet Connect) and a hardware QKD solution developed at Moscow University. What they call a "phone" is in fact a PC with an external box with a fiber optic link connecting it to a QKD key server[2512].

[2511] See Infotecs At The Forefront Of Quantum Cryptography, 2017.

[2512] See Infotecs has presented its ViPNet Quantum Phone, January 2018.

ISARA (2015, Canada, $27M) develops post-quantum encryption software solutions and PQC implementation consulting with "ISARA Radiate Security Solution Suite" which provides public keys and encryption algorithms.

They are visibly based on hash trees and combine PQC (post-quantum crypto) and traditional PKI (public-key infrastructure)[2513]. One of their investors is the Quantum Valley Investments fund, managed by Mike Lazaridis, co-founder of Blackberry RIM. He reinvested his Blackberry-related fortune in the development of the Canadian scientific and entrepreneurial ecosystem, particularly in quantum, where he has invested a total of $450M[2514].

KETS Quantum Security (2016, UK, £5.1M) develops a quantum random number generator (QRNG) and a QKD quantum key generator, all integrated in a single component miniaturized photonic and packaged in PCI cards.

All this is combined with a consulting activity for the deployment of the solutions. The company was founded by photonics researchers from the University of Bristol. They target the financial and public sector markets. They are prototyping UAVs with Airbus for QKD implementation in military or public security applications, with Airbus Defense. Their QKD chipset can also equip Cubesat-type microsatellites.

Ki3 Photonics (Canada) is a spin-off of the National Institute of Scientific Research on energy, materials and telecommunications from Montreal created by Yoann Jestin (CEO) and Piotr Rozgtocki (CTO)

It develops compact and energy efficient QKD hardware solutions to ease its deployment over standard telecommunications links with using signals multiplexing using frequency combs.

Knot Communications / **Artedys** (France) wants to launch a network of satellites to operate some sort of quantum blockchain satellite phone. They plan to launch a satellite between 2024 and 2027. This looks a little farfetched.

LuxQuanta (2021, Spain) is a spin-off of ICFO that develops CV-QKD solutions supporting distances up to 40 km. They deployed a 30 km pilot project in Spain in 2022.

MagiQ (1999, USA, $7.5M) is a startup that initially started in 2003 with the creation of a QKD system. For about ten years, this company seems to have repositioned itself in the US service and defense industry. They have developed the Agile Interference Mitigation System (AIMS), a system for reducing electromagnetic communication interference.

MtPellerin (2018, Switzerland) is a startup specialized in the management of crypto assets via a dedicated mobile application ("Bridge Wallet"). They have created a quantum safe with IDQ, "The Quantum Vault", which is based on IDC's random number generator and QKD system.

NodeQ (2021, UK) is a software and service company dedicated to the deployment of quantum cryptography and telecommunications solutions. It was created by Stefano Pirandola and Samuel L. Braunstein. Stefano Pirandola pioneered continuous variable quantum cryptography, routing strategies on quantum networks using arbitrary topology, quantum repeaters, entanglement distillation and quantum computing optimization.

[2513] This is documented in the white paper Enabling Quantum-Safe Migration with Crypto-Agile Certificates, 2018 (7 pages).

[2514] See The Co-Inventor of BlackBerry Is Building Canada's Quantum Brain Trust, Blomberg, 2018.

After working as a MIT researcher, he became a professor of quantum computing at the University of York (UK). Samuel L. Braunstein also worked on quantum teleportation with continuous variables and quantum teleportation networks.

He also worked in quantum sensing and introduced the first bosonic model for universal quantum computing with Seth Lloyd in 1998[2515]. Both created the hybrid quantum Internet concept, association direct and continuous variables[2516].

NuCrypt (2003, USA) develops optical technologies for quantum communications and metrology, including entangled photon sources, optical pulse generators, single photon detectors, polarization analyzers and associated software.

Nu Quantum (2018, UK, £4.3M) is a spin-off from the University of Cambridge developing QKD optical links and satellite systems using proprietary single-photon components. They also created their own source of single photons and have some ambition to create a photon-based quantum computer of their own. The startup is co-founded and directed by Carmen Palacios-Berraquero.

Origone (2014, UK) develops cryptography solutions based on D-Wave computers. It targets the defense market as well as the railway industry. Their quantitative/post-quantum cryptography activity is an evolution of a traditional cybersecurity business.

Patero (2018, Germany) is a software PQC software and service vendor addressing the national security, critical infrastructures and supply chain markets.

It's bound to protect customers after "Q Day", the (elusive and very long term) moment when some quantum computer will break existing public-key based cryptography. It covers various parts of the IT stack: gateways, virtual cloud and edge computing. The company was cofounded by Henning Schiel who is their CTO.

Post-Quantum or **PQ Solutions** (2009, UK, $10.4M) is a startup initially created under the name SRD Wireless that created the secure PQ Chat messaging using the random linear codes invented by Robert McEliece.

The company was renamed as Post-Quantum or PQ Solutions Limited in 2014, or PQ Group. They offer a line of security products integrating post-quantum crypto algorithms. One of the co-founders, Martin Tomlinson, has developed the Tomlinson-Harashima pre-encoding, which corrects interference in telecommunication signals and various error correction codes. Their products also include PQ Guard, a post-quantum encryption system. Their CEO, Andersen Cheng is also the CEO of **Nomidio** (2020, UK), a provider of quantum-proof identity solutions, the Nomidio Private Identity Cloud.

PQSecure Technologies (2017, USA) is a provider of isogeny-based PQC solutions. It is a spin-off from the University of Florida Atlantic launched by Reza Azarderakhsh. Their SIKE algorithm is a finalist in the NIST PQC call for proposals.

PQShield (2018, UK, $26.9M) is Oxford University spin-off that develops PQC solutions, including HSM (hardware security modules).

[2515] See Quantum computation over continuous variables by Seth Lloyd and Samuel L. Braunstein, 1998 (9 pages).

[2516] See Physics: Unite to build a quantum Internet by Stefano Pirandola and Samuel L. Braunstein, Nature, 2016 (3 pages).

They participate to several finalist teams in the PQC competition launched by NIST including the CRYSTALS-Kyber PKI and CRYSTALS-Dilithium's signature that were selected in July 2022. They have developed a licensed SoC (system on chip) that integrates their in-house Euclidian networks based PQC. Bosch is one of their first customers.

Qaisec (2019, Bulgaria) develops cryptographic solutions targeting the AI, finance and telecommunications sectors. They seem to offer first a security audit service and then cryptography solutions that use quantum random number generators for keys. They are also creating a PQC-based blockchain.

QANPlatform (2019, USA) was cofounded by Johann Polecsak (CTO) and is developing a quantum-proof Blockchain relying on a Lattice-based PQC implemented in the RUST programming language.

QuantLR (2018, Israel) is a developer of an affordable QKD software solution that is supposed to reduce the cost of QKD deployment by 90% with "*no specific hardware*".

The startup was cofounded by Hagai Eisenberg, a professor at Hebrew University of Jerusalem. When looking at a recent paper he coauthored[2517], you get an idea of what they may be doing.

It consists in using a high-dimensional QKD architecture that can work on existing binary QKD hardware on distances of up to 40 km, thanks to using some time-bin encoding programmed on a FPGA component.

They also partner with a telecom equipment manufacturer, **PacketLight Networks** (2000, $18M), also based in Israel, which provides optical fiber WDM (wavelength-division multiplexing) equipment. They also tested their solution with **Medone**, an Israeli datacenter service provider. In a sense, the startup's go-to-market is original, relying on Israeli local players when many Israeli startups usually directly go and reach international players and partners, particularly in the USA.

Qabacus (2019, USA) is developing quantum computing and cryptography technologies and a complete cyber-security software stack.

Qasky (2016, China) commercializes research coming out of the Chinese Academy of Sciences. Funding comes from Wuhu Construction and Investment Ltd and the China University of Science and Technology.

They offer solutions for post-quantum crypto, QKD and photonics components. Their name is derived from CAS Key laboratory, CAS = China Academy of Sciences.

QEYnet (2016, Canada, $7M) is developing a QKD quantum cryptography satellite network. Funding for the startup comes from the Canadian government.

QNu Labs (2016, India, $5.3M) develops QKD-based solutions. They also offer their own quantum random number generator and are also working on the creation of a QKD solution operating on Li-Fi, W-Fi that uses the frequencies of visible light.

Qrate Quantum Communications (2015, Russia) sells QRate Key Distributor, a BB84 protocol-based QKD quantum key distribution solution in a 4U rack with a range of up to 100 km.

[2517] See Fast and Simple One-Way High-Dimensional Quantum Key Distribution by Kfir Sulimany, Hagai Eisenberg, Michael Ben-Or et al, May 2021 (7 pages).

They also market a single-photon avalanche diode detector (SPAD) operating at 1550 nm and a quantum random number generator (QRNG).

QSpace Technologies (2017, Russia, $1M) is a developer of QKD satellites that is building a CubeSat with a QKD system transmitter, to be launch in 2023. It is a spin-off from the Russian Quantum Center, itself coming out of QRate in 2021.

QuantiCor Security (2017, Germany) develops PQC solutions, particularly for Blockchain applications and connected objects, via offerings with Quantum-Multisign and Quantum IDEncrypt.

That they are supposed to be cheaper than traditional PKIs. They come from TU Darmstadt and target the healthcare market in particular.

Quantum Blockchains (2018, Poland) wants to create a quantum resilient blockchain based on QKD. That's an interesting long-term bet given the infrastructure required to make it happen at a large scale.

QuDoor (2016, China, $7,8M) aka **Qike Quantum**, aka **Quantum Door**, aka **Guokai Quantum Technology** designs various products for QKD distribution, a trapped ion quantum processor supposed to reach someday 100 qubits (Tiansuan 1) and a laser-based vibration quantum sensor. QuDoor's cofounder and R&D track record include a commercial QKD system (2003), a waveform generator (2007), ion trapping (2012), quantum computing sensing (2015) and ion-phonon-photon entanglement function (2018).

Quantum Collective (2021, Netherlands) is a European company created by Fabien Bouhier, Sebastien Le Goff and Floris Drupsteen that provides post-quantum security solutions. They name this "Quantum Security Solutions" but it's classical quantum-resilient security covering PKI, VPN and eMail security.

QuantumCTek (2009, China) is a provider of end-to-end quantum cryptography solutions: QKD, QKD repeaters, optical routers. The company is a spin-off of Hefei National Laboratory for Physical Science at Micro-scale (HFNL) and the University of Science and Technology of China (USTC).

They are behind the creation in 2014 of the "Quantum-Safe Security Working Group" with ID Quantique and Battelle, which promotes PQC. As we saw above, they have deployed the 2000 km QKD-protected link between Shanghai and Beijing. They ran an IPO (Initial Public Offering) in China in July 2020.

Quantum Impenetrable (2018, UK) is a Scottish startup that develops a security module (HSM) using a quantum random number generator and resistant to quantum key-breaking algorithms.

Quantum Xchange (2016, USA, $23.5M) distributes Phio Trusted Xchange, a key distribution system supporting both PQC and QKD.

They partner with the telecom infrastructure operator Zayo Group, from which they operate their dark fibers and use ID Quantique's QKD solutions. They began by deploying a 1,000-kilometer QKD network from Boston to Washington via New York and New Jersey[2518].

[2518] See Quantum Xchange Breaks Final Barriers to Make Quantum Key Distribution (QKD) Commercially Viable with the Launch of Phio TX, September 2019.

Since 2021, they also partner with **Cisco** for the support of the Cisco Secure Key Integration Protocol implemented in enterprise routers, for the non-quantum part of their hybrid key distribution architecture.

In 2022, they announced a partnership with **Thales** for the delivery of security keys with Thales High Speed Encryptors (HSEs) that supports QRNGs, QKDs and PQCs[2519].

Quantum eMotion (2007, Canada), formerly Quantum Numbers Corp**,** develops a cryptographic system based on a quantum random number generator (branded QNG2) and targets in particular mobile uses. It mainly communicates on the filing of an associated patent.

Let's hope it won't be a patent troller! The company seems to be licensing its technology to electronic component designers. It exploits research work from the Department of Physics at the University of Sherbrooke in Quebec. One of the patents relates to the generation of random numbers based on the random noise generated by some electron tunneling effect through a potential barrier[2520]. The QRNG speed reaches 1 Gbits/s and fits in USB key form factor. The company is listed on the Canadian Venture Exchange (CVE). The company expect to release a Blockchain using their QRNG in 2023.

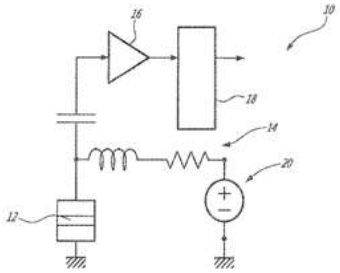


Figure 785: a patented QNRG.

Quantum Trilogy (2016, USA) created a secure communications solution based on applications (including for mail and voice communication) protected by an unspecified encryption, a QRNG to create real entropy in generated keys and servers that are protected at some level by a QKD.

QuBalt (2015, Germany) is a startup established between Germany and Latvia that develops solutions for post-quantum cryptography (PQC) and quantum algorithms.

Qubit Reset (2018, USA) develops quantum repeaters for QKD arrays. The company was founded by two Argentinians based in Miami. It is not listed in the Crunchbase and does not seem to have raised any funds, which seems to be a bad omen.

Quintessence Labs (2006, Australia, $49,3M) proposes a quantum random number generator and a QKD system. They use the CV-QKD technique which allows the use of existing fiber optic infrastructures of very high-speed telecom operators.

Qunnect (2017, USA, $12.4M) is a spin-off from Stony Brook University of Long Island created by Mehdi Namazi, Eden Figueroa, Noel Goddard and Mael Flament, Quantonation being one of their investors[2521]. Qunnect is developing a quantum product suite that enables long range quantum entanglement distribution protecting against photons loss.

[2519] See Quantum Xchange Collaborates with Thales to Enable Quantum-Safe Key Delivery Across Any Distance, Over Any Network Media, November 2021.

[2520] I found the complete PDF of USPTO patent 10437559 on https://www.pat2pdf.org/.

[2521] They received $1.5 million of funding in April 2020 from the US Department of Energy under the Small Business Innovation Research Awards (SBIR) program. See Qunnect receives $1.5M award from the DoE - Swiss Quantum Hub, April 2020.

Their repeaters are based on a quantum memory operating at room temperature, using warm rubidium vapor and without any requirement for vacuum- and/or cryogenic- support[2522]. This memory provides 100s of µs of coherence time. They also develop their multi-laser multi-wavelength locking references and Qu-Source, a SFWM-based generated of entangled pairs of photons.

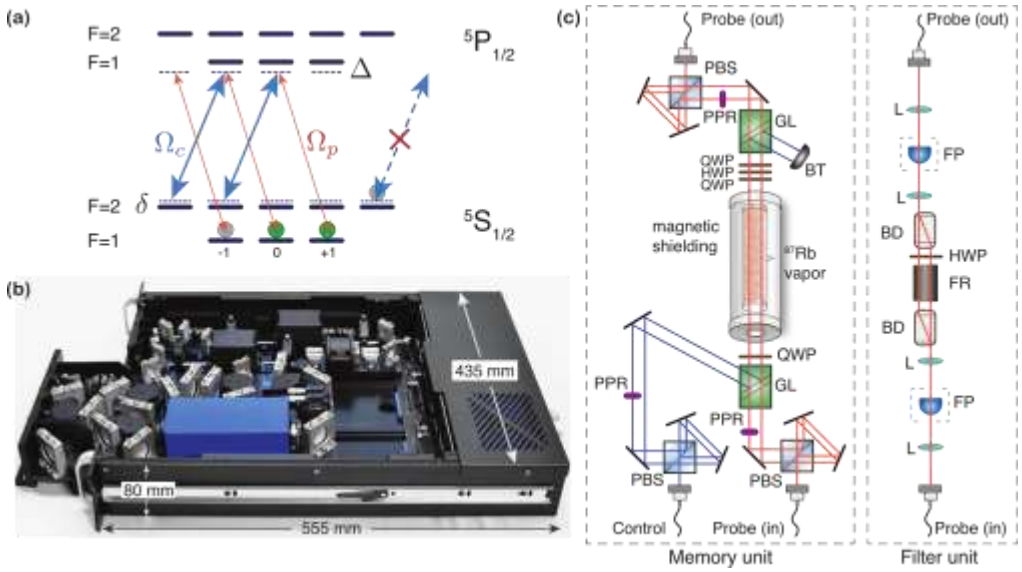


Figure 786: Qunnect repeater architecture. Source: Field-deployable Quantum Memory for Quantum Networking by Yang Wang, Alexander N. Craddock, Rourke Sekelsky, Mael Flament and Mehdi Namazi, May 2022 (16 pages).

In May 2022, the company got two SBIR awards from the US DoE for $1.85M to fund the development and commercialization of their quantum repeater product suite. In October 2022, the startup got a series A funding of $8M led by Airbus Ventures Qunnect officially announces its Series A financing of over $8 million. The round was led by Airbus Ventures with Quantonation, SandboxAQ, NY Ventures, Impact Science Ventures and Motus Ventures as other investors.

The company partners with various technology vendors like Exail, WeLinQ, Toptica, Q-CTRL, ColdQuanta and Single Quantum.

QuSecure (2019, USA, $1.7M) develops a secure blockchain solution that is resilient to quantum code breaking.

It seems that they are also developing a Blockchain that would be secured via QKD, and Blockchain security testing protocols. The startup is also doing cybersecurity consulting and, in particular, audits for the deployment of PQC. It was founded by Rebecca Krauthamer, who also founded the **Quantum Thought** startup mentioned above. In 2022, they were awarded a SBIR Phase III contract to become, surprisingly, the sole-source provider of PQC for over a dozen US federal agencies with their QuProtect solution.

Ravel Technologies (2018, France) offers Ravel Homomorphic Encryption, a post-quantum and homomorphic encryption solution. The company was founded by Mehdi Sabeg.

SandboxAQ (2022, USA, >$300M) is a spin-out of Alphabet's Google AI that has a large breadth of activities, mostly around quantum related software applications and PQC software solutions.

[2522] See Field-deployable Quantum Memory for Quantum Networking by Yang Wang, Alexander N. Craddock, Rourke Sekelsky, Mael Flament and Mehdi Namazi, May 2022 (16 pages). See also an explanation video, Quantum Memories for long distance quantum networking (3:40mn) and Quantum Repeaters which explains how it is deployed.

Their first product offering is a multifunction Security Suite supporting PQC cryptography. They were selected in July 2022 as one of the 12 NIST partners to help the industry in the PQC migration path. The company also works on various quantum algorithms and on classical machine learning tools to exploit content from quantum medical image sensors The company's CEO is Jack Hidary, a serial entrepreneur and book writer ("Quantum Computing: An Applied Approach") and its chairman is Eric Schmidt. In 2022, they made a strategic investment in evolutionQ and acquired Cryptosense (2013, France, $5.7M).

Secure-IC (2010, France) is the leader of the RISQ project, which aims to create a French post-quantum crypto solution.

The company develops security hardware and software solutions that are used to evaluate the robustness of security solutions. The company is a spin-off from the Institut Mines-Télécom.

SECQAI (2021, UK) is a quantum cybersecurity company with a very broad goal to "*provide world leading technologies to organisations of all sizes*".

More precisely, they're in to "*bringing together their own quantum and AI tech to create disruptive data and security products and services for organisations looking to gain a commercial advantage*". The company was created by Rahul Tyagi, Dave Worrall and Martin Rudd. Rahul Tyagi developed a patented room temperature QRNG when he as the CEO of LyfGen. The patent USPTO 10606561 was filed in August 2018 and validated in March 2020. It's based on using slits-based diffraction and scattering entropy.

Smarts Quanttelecom (1991, Russia) proposes a quantum cryptography solution based on CV-QKD which exploits standard fibers of telecom operators.

Smarts was until 2015 a Russian mobile telecom operator. It has since become a telecom services operator with an offer of secure telecom links and data center and cloud services. Their QKD solution comes from Quanttelecom, a subsidiary of Smarts, developed jointly with the ITMO University of Saint Petersburg.

Sonora Gold and Silver Corp (2019, Canada) acquired in June 2021 a newly created startup, BTQ, that works on creating some quantum-safe Bitcoin solutions. BTQ was created in March 2021 in Lichtenstein.

SpeQtral Quantum Technologies (2017, Singapore), formerly S-Fifteen Space Systems, specializes in the distribution of QKD via satellite. They promote the work of the University of Singapore in the design of CubeSat-type pico-satellites for QKD key distribution. In September 2022, they started a partnership with Thales Alenia Space to test in 2025 a QKD distribution between their SpeQtral-1 satellites and Thales Alenia Space ground stations.

SSH Communications Security (1995, Finland, 14.1M€) is a cybersecurity company selling cybersecurity and SSH solutions. They sell NQX, a PQC-ready encryption solution among other cybersecurity solutions. In 2022, they released Tectia Quantum Safe Edition, a PQC protected SSH solution that protects remote access, file transfers and tunneling connections against the future quantum threat.

Surrey Satellite Technology or SSTL (1985, UK) wants to deploy a QKD-based quantum communications satellite built by Airbus Defense & Space (they are part of the Airbus group). The project is conducted in partnership with Eutelsat and ESA. The launch of the satellite was planned for 2020.

Synergy Quantum (2019, Switzerland) is a post-quantum encryption product and service startup that also supports data storage in a facility located in a former military bunker in the Swiss Alps.

They target governments, financial services, healthcare, smart Cities, energy and telecom sectors. The company is run by Jay Oberai (CEO), Arun K. Pati (Chief Scientific Officer), Mayank Sharma (VP Engineering), Vipin Kumar Rathi (VP Technology Architecture) and Manu Khullar (Chief Operating Officer). Any non-Indian there? Yes, with John Paukulis (CMO, USA) and Sasha Lazarevic (Head of Government Partnerships) and Jake Hwang (Head of Business Development and Investor Relations). It launched in 2022 a joint venture with the Quantum Technology Hub of the Indian Government. Not a coincidence. They seem to also offer some services in the QKD realm, including as part of this deal in India.

Taqbit Labs (2018, India) sell solutions for QKD. Their website and communication are so vague that it's impossible to understand whether they sell third party QKD products with some integration service of develop QKD hardware products of their own, and if so, in what category given most vendors don't reinvent the wheel to become full-stack vendors.

ThinkQuantum (2021, Italy) is a spin-off of the University of Padua which develops QKD and QRNG solutions for simple fiber optics deployments as well as for free space and satellite QKD.

Ultimaco (1983, Germany) sells lattice-based PQC embedded in Hardware Security Modules (HSMs). This solution is based on Picnic, one of the alternate candidate PQC digital signatures selected by the third round of the NIST PQC challenge in July 2020.

VeriQloud (2017, France) is a startup created by Elham Kashefi, and Marc Kaplan (France) and Joshua Nunn (UK). It is specialized in the creation of quantum software solutions adapted to quantum telecommunications for both QKD and distributed quantum processing.

Their offer is based on the Qline, a software solution that enables the deployment of a multi-point quantum network with a lower cost in hardware infrastructure. With this architecture, nodes that are very expensive can be replaced by simple modulators that are much more affordable. The operation is based on a kind of "time-sharing" of the line. This lowers the hardware addition by about two thirds on a typical installation below with two intermediate stations in the network. At both ends of the line there is on one side a laser and modulator-based photon generator and on the other side a single photon detector, the most expensive part of the equipment ranging from 20K€ to 100K€. The solution is deployable on networks totaling 100 to 200 km.

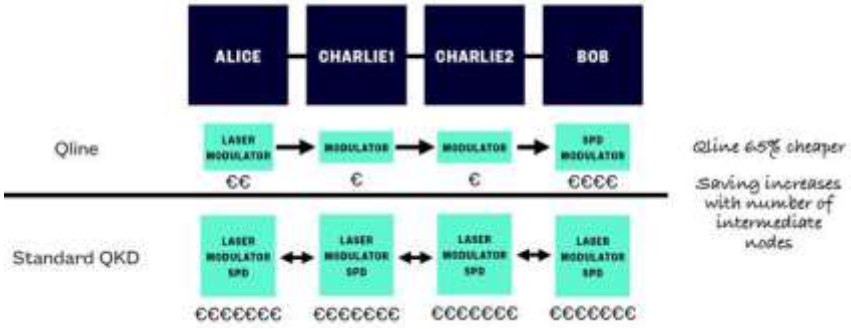


Figure 787: VeriQloud qline architecture. Source: VeriQloud.

The first application is QKD quantum key distribution. They can interoperate with classical QKD networks. Initially, secure file transfer and instant messaging are targeted as applications associated with QKD. The system can also be used to generate disposable masks[2523].

[2523] See How to build quantum communication networks at a small scale by Marc Kaplan from VeriQloud, May 2020.

The VeriQloud solution is also relevant for securing data storage.

XT Quantech (2017, China) specializes in CV-QKD distribution equipment after initially focusing on DV-QKD solutions. The CV-QKD is essential because it can coexist in the fiber links of telecom operators.

They offer server appliances for QKD key encoding and decoding gateways. Its full name is Shanghai Xuntai Information Technology Co. The company also sells a QRNG, their XT-QRNG100 that is certified in … China.

ZY4 (2014, Canada) develops post-quantum cryptography solutions based on their in-house concept of the Shannon Event Horizon which would be a new class of PKI and random number generation[2524].

Quantum telecommunications and cryptography key takeaways

- Quantum computing poses a theoretical threat to many existing cryptography systems, particularly those using public key distribution in asymmetric cryptography. This is due to Peter Shor's integer factoring algorithm that breaks RSA public encryption keys. But other algorithms than Shor are creating various threats, including for symmetric key distributions.
- As a result, two breeds of solutions have been elaborated. The first one is based on quantum key distribution, requiring a photonic transmission channel (airborne or fiber-based), and using sometimes quantum entanglement. Beware of a common misconception: these solutions are not based on quantum computers. Quantum computers are not (yet) making cryptography safer.
- The second option is to create classical cryptographic protocols generating public encryption keys that are not breakable by quantum computers. The USA NIST launched in 2016 an international competition to standardize a set of post-quantum cryptography (PQC) protocols. Four finalists were selected as NIST standard in July 2022, one for a public key interface (PKI) and three for signatures. Solutions deployments should happen next and be done way before the quantum computing menace will materialize, if it does some day. NIST may select other PQC solutions in the future.
- Quantum random numbers generation is/will be used for classical cryptography, and quantum cryptography. It provides sources of both random and non-deterministic numbers used in cryptography systems. It has other used cases when randomness is mandatory in classical computing like with lotteries and various simulation tools.
- Quantum telecommunications can also use quantum entanglement to enable communications between quantum computers and/or quantum sensors. Distributed quantum computing has two potential benefits: scale quantum computing beyond the capacity of individual quantum computers and enable safe communications between quantum computers. Distributed quantum sensing can enable better accuracy sensing.
- Quantum Physical Unclonable Functions are cryptographic solutions used to authenticate physical objects in an unfalsifiable quantum way. It is however still an unmature technology.
- There are already many startups in the QKD and PQC scene. Deployments have already started worldwide, particularly in China.

[2524] See their white paper Introducing the Shannon Event Horizon, 2019 (20 pages).

Quantum sensing

Quantum sensing is about the various precision measurement solutions that rely on second generation quantum technologies and go beyond the limits of classical measurements systems. It also often allows non-invasive measurements to be carried out on various solid or organic materials. The main physical values measured are time, distances, gravity, magnetism, temperature and electromagnetic spectrum analysis.

Quantum sensing use-cases and market

Many applications use these technologies like radars, sonars, very high sensitivity microphones or the field of imaging in general and particularly in medical imaging[2525].

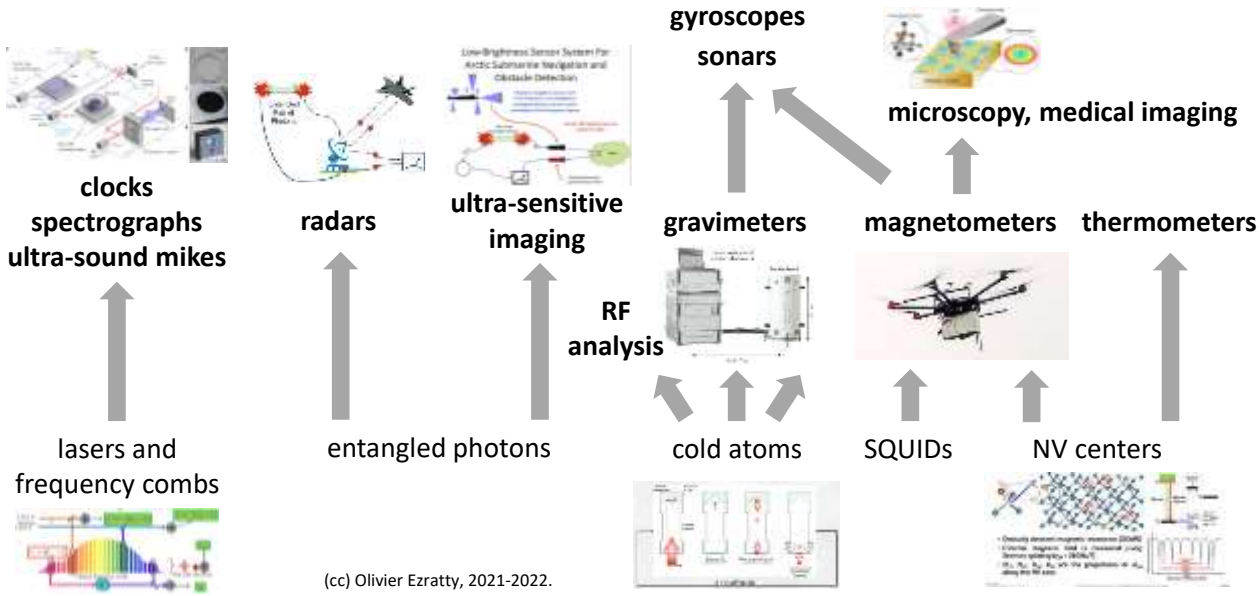


Figure 788: a map of various quantum sensing basic technologies and use cases. (cc) Olivier Ezratty, 2022.

Some of these technologies have commonalities with the various qubit types we have already explored in detail. This is particularly the case for cold atoms, NV centers and superconducting qubits. Precision magnetometers use NV centers as well as SQUIDs (Superconducting Quantum Interference Device), which also measure the direction of current in superconducting flux-type qubits and are used in particular by D-Wave in quantum annealers.

Many of these quantum measurement technologies make extensive use of photonic tools, either directly based on photons (lasers, frequency combs, entangled photons) or exploiting cold atoms and even NV centers, whose state is then evaluated by measuring their fluorescence.

[2525] See Quantum Sensing Use Cases 2022, SRI for QED-C, September 2022 (36 pages), a report on quantum sensors which makes an interesting inventory of use cases and market readiness, with an eye on national security issues. It is focused on four types of sensors, for time, inertial, magnetic field and electric field measurement. It doesn't cover other sensors categories reviewed in this part like frequency monitoring sensors, quantum radars (which may be mythical objects), quantum pressure sensors, quantum chemical sensors and quantum thermometers.

Some of these technologies are already commercially viable and continue to progress steadily. It is still a niche market made of many sub-niche markets, evaluated at around $1B and expected to double in a decade. The two largest applications markets are transportation and medical imaging.

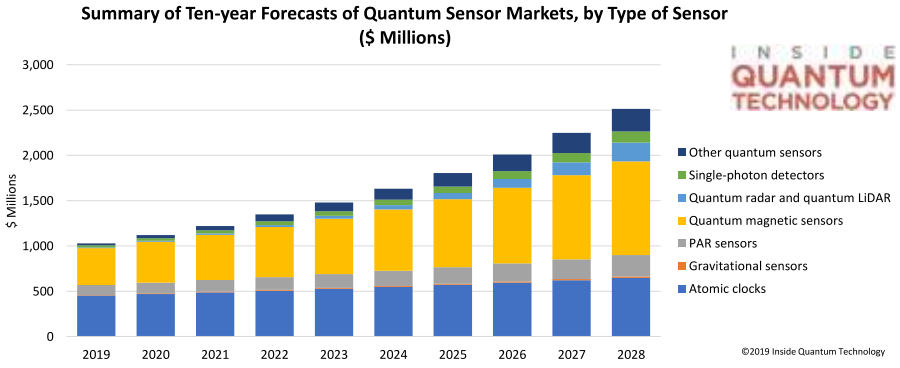


Figure 789: Source: Quantum Sensors: Ten Year Market Projections by Lawrence Gasman, 2019 (7 slides).

But these forecasts may become wrong since some use cases might at some point become mainstream and drive more market growth. This is the case of GPS without satellite links using micro-magnetometers. It could for example someday equip many classical and autonomous vehicles.

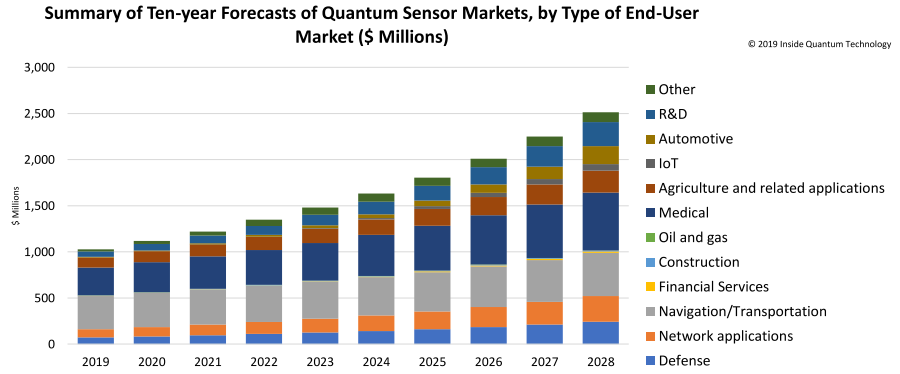


Figure 790: Source: Quantum Sensors: Ten Year Market Projections by Lawrence Gasman, 2019 (7 slides).

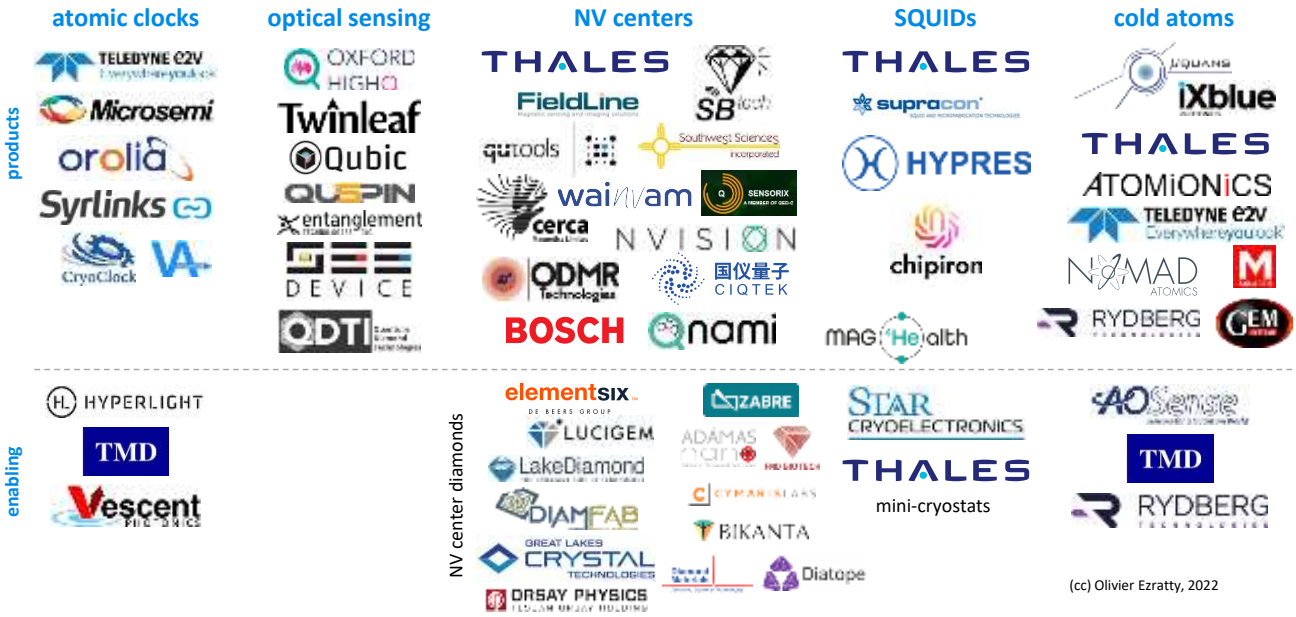


Figure 791: and now ladies and gentlemen, here is the magnificent market map for quantum sensing, including some of their enabling technologies. (cc) Olivier Ezratty, 2022.

Various other markets are relevant for quantum sensing: the energy and utilities sector[2526], telecoms, space and astrophysics research[2527], high-energy particles research[2528], civil engineering, manufacturing industries using many sensors like for quality control and non-destructive testing and control, and of course, the aerospace and defense.

International System of Measurement

Sensing cannot be discussed without being connected to the **International System for Measurement** (or International System of Units, aka SI). It was recast after a unanimous vote on the Versailles Metre Treaty signed at the 26th General Conference on Weights and Measures (CGPM) in November 2018[2529]. Its implementation started on May 20, 2019.

The new 2019 SI updates the definition of the kilogram, ampere, kelvin and mole. It is built around seven fixed constants: a number of hyperfine transitions of cesium 133, the speed of light in vacuum[2530], the Planck constant, the elementary charge of an electron, the Boltzmann constant, the Avogadro number or constant and the luminous efficiency. From these constants are derived the seven basic units of the system: kilogram, meter, second[2531], ampere, kelvin, mole and candela.

It no longer relies on materials that are degrading over time, such as the standard kilogram kept at the BIPM in Saint-Cloud, or on the triple point of water (gel) which defined the kelvin, and which depended on its isotopic composition.

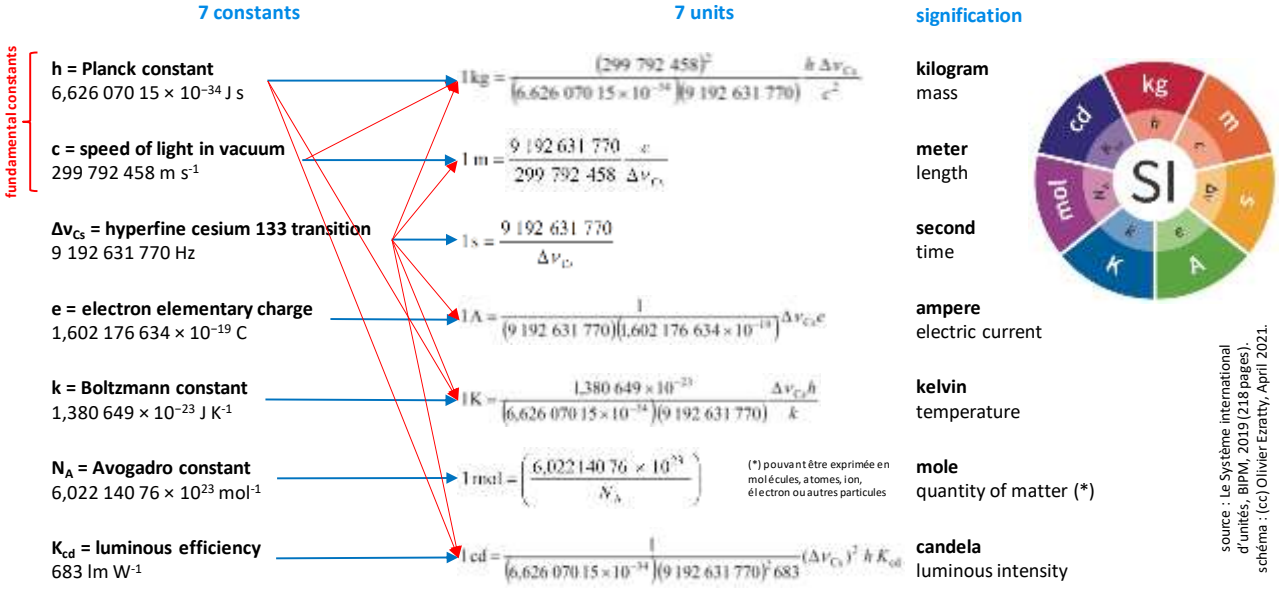


Figure 792: reconstruction of the SI constants, units and their signification. Source: (cc) Olivier Ezratty, 2021.

[2526] See Quantum Sensing for Energy Applications: Review and Perspective by Scott E Crawford, Roman Shugayev, Hari P. Paudel and Ping Lu, June 2021 (33 pages).

[2527] See Quantum Communication, Sensing and Measurement in Space by Baris I. Erkmen et al, 2012 (136 pages).

[2528] See High energy physics: Quantum Sensing for High Energy Physics by Zeeshan Ahmed, Yuri Alexeev, Giorgio Apollinari and Asimina Arvanitaki, March 2018 (39 pages) and Snowmass 2021: Quantum Sensors for HEP Science -- Interferometers, Mechanics, Traps, and Clocks by Daniel Carney et al, March 2022 (29 pages).

[2529] See The International System of Units (SI), NIST, 2019 (13 pages) and The International System of Units, BIPM, 2019 (218 pages).

[2530] The definition of the speed of light at 299 792 458 m s^{-1} dates from 1983.

[2531] The second was defined with 9 192 631 770 periods of the hyperfine transition of cesium 133 at a temperature close to 0K since the 13th CGPM of 1967. Previously, it was a fraction of the solar day, which was not stable.

The mole was previously defined on the basis of 0.012 kg of ^{12}C [2532]. The standard meter, which is kept in the Archives in Paris, was no longer the reference since 1960. All other units of measurement such as hertz, joule, coulomb, lumen or watt are derived from constants and base units. This measurement system is branded as being "quantum" because it is based on the measurement of fundamental phenomena that bring us back to quanta, in particular for the definition of the second, which uses quantized energy transitions in the cesium atom, and that of the kilogram, which uses the Planck constant, itself a foundation of quantum physics.

Numerous quantum physics works related to these evolutions of the international measurement system, notably at NIST, have a link with the commercial devices discussed in this section.

Quantum sensing taxonomy

Reusing a definition found on C.L. Degen et al's 2017 review paper[2533], quantum sensing describes the use of quantum systems, quantum properties and phenomena to measure physical quantities. The first quantum sensors were SQUID magnetometers, atomic vapors and atomic clocks. Then, the field was expanded to cover magnetic and electric fields, time and electromagnetic waves frequencies, mechanical rotations, temperature and pressure.

New "second generation" sensors work at the single-atom and spin level and may use quantum entanglement as a resource for increasing sensitivity.

Quantum sensing can use either or the following phenomenon corresponding to type I, II and III quantum sensors:

- **Type I**: using a quantum object to measure a physical quantity, characterized by quantized energy levels.
- **Type II**: using quantum coherence, wave-like spatial or temporal superposition states to measure a physical quantity.
- **Type III**: using quantum entanglement to improve the sensitivity or precision of measurement. It is sometimes labelled as "quantum metrology", "quantum-enhanced sensing" or "second generation quantum sensing".

By the way, the difference between quantum sensing and quantum metrology is not that clear in the scientific literature. For some people, it's the same. For others, quantum metrology is used for devices measuring units or fundamental constants such as an atomic clock or an atom interferometer measuring the fine structure constant, or constants that were used to create the last SI[2534]. Quantum metrology can have at least two other meanings: study of quantum-based precision measurements and quantum sensing using entanglement as seen in the above type I/II/III taxonomy.

The table in Figure 793 lists several types of known quantum sensors with their type, the physical nature of the measuring object ("qubit nature") and the measured physical quantities. For example, charged systems like trapped ions are sensitive to electrical fields while spin-based systems mainly respond to magnetic fields. Some quantum sensors may respond to several physical parameters or measure indirectly some physical quantity, which is the case for quantum thermometry with NV centers. Most of the time, quantum sensing exploits changes in the transition frequency or the transition rate in response to an external signal.

[2532] With the new SI, one gram of matter contains N_A multiplied by the number of nucleons (protons and neutrons) of the element in question (atom, molecule). This comes from the fact that in an atom, the majority of the weight is in the atom nucleus. Electrons have a mass equivalent to 1/1836 times that of a single nucleon.

[2533] See Quantum sensing by C. L. Degen, F. Reinhard and P. Cappellaro, June 2017 (45 pages).

[2534] See What is the difference between quantum sensing and quantum metrology?, 2020.

sensor type			qubit nature	type I	type II	type III	rotation	acceleration	force	pressure	displacement	time	frequency	refractive index	magnetic field	electric field	voltage	temperature	mass
neutral atoms		atomic vapor	atomic spin		X	X	X					X	X		X				
		cold atom clouds	atomic spin		X	X		X				X	X		X				
Rydberg atoms			Rydberg states		X	X										X			
trapped ions			electronic state		X	X	X			X		X	X						
			vibrational mode		X				X							X			
solid state	spin ensembles	NMR	nuclear spins		X										X				
		NV/SiC center ensembles	electron spins		X		X			X					X	X		X	
	single spins	P donor in Si	electron spins		X										X				
		quantum dot	electron spins	X	X										X	X			
		single NV center	electron spins		X		X			X					X	X			
superconducting circuits		SQUIDs	supercurrent	X	X										X				
		flux qubits	circulating current		X										X				
		charge qubits	charge eigenstates		X											X			
single electron transistor			charge eigenstates	X												X			
optomechanics			phonons	X				X	X						X		X		
interferometer			photons, atoms		X	X	X				X			X					

(cc) Olivier Ezratty, 2022, based on Quantum sensing by C. L. Degen, F. Reinhard and P. Cappellaro, June 2017

Figure 793: quantum sensing taxonomy. Source: table reconstructed from Quantum sensing by C. L. Degen, F. Reinhard and P. Cappellaro, June 2017 (45 pages).

The rest of this quantum sensing part is mostly organized along the first row and its green/blue measured values: gravity, time, magnetism, temperature, radiofrequencies and then to higher-level applications like imaging, radars and lidars and chemical sensors.

Quantum sensors are a bit paradoxical: after a measurement of a quantum sensing qubit, the only information you retrieve is a single classical bit (0 or 1). So how to you get a floating number with a large precision?

The answer is simple for the most basic cases: you make many measurements and average their results. But there are other subtleties. With NV centers sensors, you create a spin resonance spectrum with repeat measurements and the shape of the resulting curve enables you to determine the detected magnetic field with computing the distance between two curve peaks. It is an indirect measurement.

A quantum sensor measurement precision will depend on several parameters: the sampling rate (how many measurements are made with the same sensors or similar sensors in parallel), the sensor noise and the sensor sensitivity.

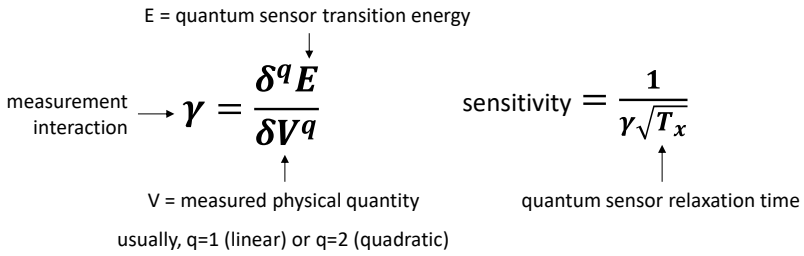


Figure 794: calculating a quantum sensor precision.

When using classical light as a measurement tool, the best precision possible with quantum measurement is the standard quantum limit (SQL) and it scales with $1/\sqrt{N}$, with N being the mean detected photon number. This threshold can be surpassed with using nonclassical states of light and nonstandard measurements, aka squeezed states, which can lower the precision down to the Heisenberg limit, with a better scaling of 1/N, generating a gain of $1/\sqrt{N}$ in precision[2535].

[2535] This is well explained in Basics of atomic clocks by Andrei Derevianko, University of Nevada, 2021 (77 slides).

At last, let's mention a developing field: quantumly networked sensors. This networking could have several benefits like connecting ensembles of quantum sensors to collectively improve their sensitivity[2536], to connect them to some quantum computers to help these directly capture some quantum data and accelerate the processing of sensed data, and also, to separate in a trusted way the state preparation, parameter encoding, measurement and data collection tasks[2537].

Quantum gravimeters, gyroscopes and accelerometers

Quantum gravimeters measure gravity with a very high accuracy. These are useful in many scenarios: in seismic detectors and volcanoes monitoring, for precision autonomous navigation complementing GPS in airplanes, ships, submarines, and drones, for gravity field mapping, for detecting subterranean holes before undergoing constructions, for detecting groundwater, ice mass change, for oil and mineral exploration (well, to be restrained) and for the detection of gravitational waves in astronomy. One talked-about use case is the detection of nuclear submarines, which would destabilize or neutralize nuclear deterrence used by nuclear countries owning these submarines, but its practicality is still questioned[2538].

There are two categories of gravimeters. Absolute gravimeters measure the gravity per se measuring the free trajectory of a test mass in vacuum, and now, with cold atoms, their interferences. Relative gravimeters measure the variation of gravity over space and also time. They are usually calibrated using absolute gravimeters. The most precise relative gravimeters are superconducting based, but are not considered as quantum gravimeters.

The quantum measurement of gravity is generally performed with cold atom interferometers (CAI), taking advantage of the wave-particle of cold atoms[2539]. The technique has been developed since 1991 and perfected since then[2540]. The principle consists in creating a source of cold atoms free falling in suspension, generally rubidium, preparing their state with lasers, then passing them through a three-stages laser-controlled atom interferometer and then analyzing the results.

In the USA, NIST and NOAA in partnership with Institute for Applied Geodesy (IFAG), Germany, developed the FG5 absolute gravimeter that was tested starting in 1993. It was using a free falling rubidium atoms vacuum chamber and an interferometer. Stanford created a cold atom gyroscope in 2006 which led to the creation of AOSense. In France, SYRTE developed a six-axis inertial sensor using two magneto-optical-traps (MOTs), also in 2006.

A related field is gradiometry, which measures horizontal or vertical gravity gradients. It is used for the measurement of the variations or anomalies in the Earth's gravity field with creating gravity maps over the earth to either improve geopositioning or to detect changing underground features over time.

[2536] See Distributed quantum sensing with a mode-entangled network of spin-squeezed atomic states by Benjamin K. Malia, Mikhail Lukin, Ronald L. Walsworth et al, May 2022 (7 pages) and Quantum Logic Enhanced Sensing in Solid-State Spin Ensembles by Nithya Arunkumar, Ronald L. Walsworth et al, March 2022 (7 pages).

[2537] See Quantum Metrology with Delegated Tasks by Nathan Shettell and Damian Markham, December 2021 (20 pages).

[2538] An airborne array of SQUIDs magnetometry detection of submarine was supposedly prototyped in China in 2017. It requires cooling but that's not a big deal for such a use case. See China's quantum submarine detector could seal South China Sea by David Hambling, New Scientist, 2017. Found in Quantum Technology and Submarine Near-Invulnerability by Katarzyna Kubiak, European Leadership Network, December 2020 (18 pages).

[2539] See Experimental gravitation and geophysics with matter wave sensors by Philippe Bouyer, LP2N, 2018 (234 slides).

[2540] See Atomic Interferometry Using Stimulated Raman Transitions by Mark Kasevich and Steven Chu, PRL, July 1991 (4 pages) and Young double-slit experiment with atoms: A simple atom interferometer, from Olivier Carnal and Jürgen Mlynek, 1991 (6 pages) which describes a Young's double-slit interferometry experiment with helium atoms. See also Experimental gravitation and geophysics with matter wave sensors, LP2N, 2018 (234 slides).

It requires specific settings and techniques to reduce noise and vibrations within the gravimeter[2541].ONERA launched gravimetry experiments in 2009 (GIRAFE project) and in 2014-2016 (GIRAFE2)[2542]. It will be tested by the French Navy in a surface vessel in 2023 and deployed on 4 vessels by 2026/2027. The goal is to create a map of underneath the oceans.

Related sensing fields are rotation measurement and gyroscopes which are implementing it. Quantum gyroscopes can be implemented with optical interferometry[2543] and, surprisingly, with superfluid ^{4}He[2544].

The figures of merits of quantum gravimeters are their **sensitivity** (smallest detectable change in gravity, measured in m/s^2 or cgs gals, for centimeter-gram-seconds, in reference to Galileo), **accuracy** (measurement uncertainty in reference to an absolute standard, is a %) and **stability**. Operational figure of merits are weight, size and warm-up time (which can last one hour). Best-in-class cold atom absolute gravimeters have a sensitivity of 10^{-9} m/s^2. Interesting miniaturization designs are also proposed, although they lead to a lower sensitivity measurement[2545].

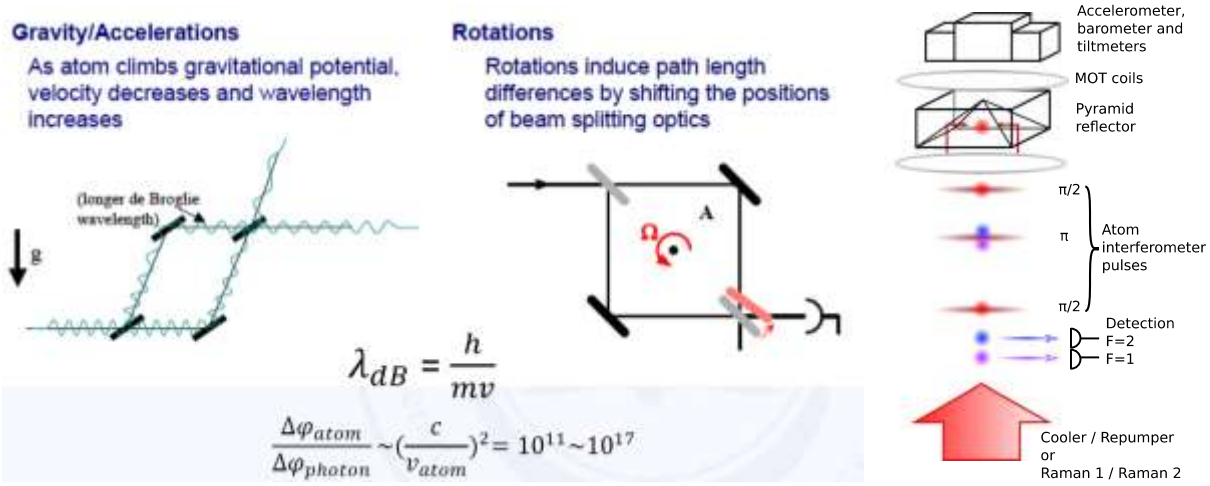


Figure 795: how cold atom interferometry works to measure both gravity, accelerations and rotations. Source: Compact and Portable Atom Gravimeter by Shuai Chen, University of Science and Technology of China, June 2019 (22 slides) and Muquans.

Other cold atom use case include magnetic field measurement in earth monitoring and temperature measurement. Hybrid sensors can associate electrostatic and cold atom acceleration sensors. Cold atom interferometry will even be used for gravitational waves detection in the MIGA experiment being setup in France[2546].

Here are the various vendors also positioned in this market, given many are still in the product development phase and don't have yet a commercial offering.

[2541] See recent advances with Quantum sensing for gravity cartography by Ben Stray, Kai Bongs et al, Nature, February 2022 (14 pages), Position fixing with cold atom gravity gradiometers by Alexander M. Phillips, April 2022 (10 pages) and Circulating pulse cavity enhancement as a method for extreme momentum transfer atom interferometry by Rustin Nourshargh, Kai Bongs et al, December 2021 (9 pages).

[2542] See ONERA invents with SHOM the "atomic" precision gravity mapping, February 2016. SHOM is the Hydrographic and Oceanographic Service of the French Navy.

[2543] See Quantum optical gyroscope by Lin Jiao and Jun-Hong An, January 2022 (7 pages).

[2544] See Superfluid helium-4 whistles just the right tune by Robert Sanders, UCBerkeley, 2005

[2545] See A Compact Cold-Atom Interferometer with a High Data-Rate Grating Magneto-Optical Trap and a Photonic-Integrated-Circuit-Compatible Laser System by Jongmin Lee, July 2021-September 2022 (21 pages). It uses a compact titanium vacuum package with a grating chip inside a tetrahedral grating magneto-optical trap (GMOT) using a single cooling beam. The sensitivity is 2x10-6.

[2546] See A gravity antenna based on quantum technologies: MIGA by B. Canuel, Philippe Bouyer et al, April 2022 (4 pages) and Exploring gravity with the MIGA large scale atom interferometer by B. Canuel, Philippe Bouyer et al, Nature Scientific Reports, 2018 (23 pages).

AOSense (2004, USA) creates and sells quantum gyroscopes, commercial optical clocks and develop a quantum gravimeter. It also provides instrumentation equipment with cold atom generators and laser frequency comb generators

They collaborate with IonQ for their quantum computers based on trapped ions. It is a spin-out from Stanford and a pioneer in the sector who is now highly diversified.

M Squared (2006, UK, $56M) has been developing a cold atom quantum gravimeter for a long time now.

They work in partnership with the University of Birmingham and Imperial College London (UCL). The project was funded under the UK government's Quantum Initiative launched in 2013. Their last generation gravimeter has a precision of 10^{-8} m/s^2. It operates at 5 µK.

The original business of the Scotland startup is their range of SolsTiS lasers covering the spectrum from 200 nm to 4000 nm. These lasers are used in industry and in optical clocks.

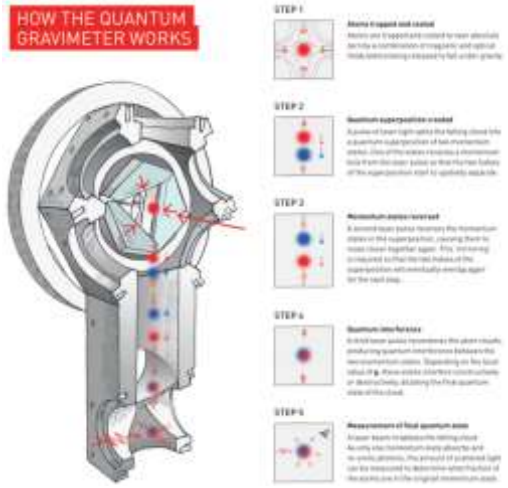


Figure 796: M Square cold atom gravimeter. Source: M Squared quantum gravimetry (4 pages).

In November 2022, M Squared announced it was entering the neutral atoms quantum computing market with its Maxwell system as part of a collaborative UK government funded project. Maxwell is supposed to be a "state of the art breakthrough system" but… with undisclosed characteristics (number of controlled atoms, gate/simulation model, algorithms examples).

exail (2000, France), formerly **iXblue** specializes in the design and manufacture of inertial and sonar power plants, with 700 employees.

It also develops lithium niobate optical modulators, microwave amplifiers and modulator bias controllers for the control of Mach-Zehnder interferometers. Their components are manufactured at their site in Lannion, Brittany and at Besancon. They are involved with the LP2N of Bordeaux in the creation of Ixatom, a quantum inertial sensor based on cold rubidium atoms[2547]. iXblue Photonics was the result of the acquisition of two companies: iXFiber in 2011, a specialist in passive optical components (FBG fiber grating filters, Fiber Bragg Gratings). Then Photline Technologies in 2013, a spin-off of the Femto-ST laboratory created in 2000 in Besancon. In May 2021, iXblue acquired **Muquans** and **Kylia** (a photonic equipment specialist, with its polarizers, delay line interferometers and multiplexers/multiplexers). In March 2022, Groupe Gorgé made the acquisition of iXblue to merge it with its subsidiary of **ECA Group**, a security, defense, and industry security technologies provider. It became **exail** in November 2022.

Muquans (created in 2011, France) is based at the Institut d'Optique in Bordeaux. They use joint research work done with the CNRS. Their quantum gravimeter is a commercial product that targets, for example, the detection of cavities in construction, oil exploration and the monitoring of volcanoes such as Etna in Italy[2548].

[2547] See iXAtom - LP2N and iXblue Cold Atoms joint laboratory.

[2548] See Detecting Volcano-Related Underground Mass Changes With a Quantum Gravimeter by Laura Antoni-Micollier, Bruno Desruelle et al, June 2022 (9 pages).

Here is how their Absolute Quantum Gravimeter and other similar atom-based quantum gravimeters work. The usual description looks like the image in Figure 797 from Muquans. It's associated with a lot of schematics in the scientific literature that are quite hard to reconcile for the non-specialist.

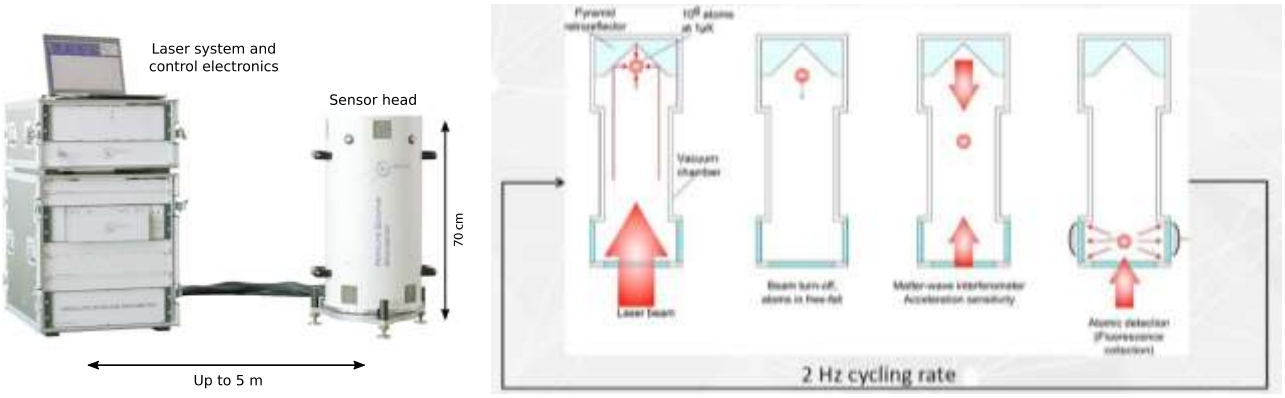


Figure 797: how atom interferometry works, continued. Source: Muquans.

I will decompose the various steps involved here:

① **Heating source**: a heated source at the top of the system prepares a small cloud of about 10^6 atoms of rubidium ^{87}Rb. The source of the atoms also contains an accelerometer that corrects the phase of the lasers in real time.

② **Magneto-optical trap**: a MOT as shown in Figure 798 is used to confine and cool the prepared source of atoms at 1µK using three pairs of counter-propagating laser beams in three orthogonal directions, applying the Doppler effect, and two anti-Helmholtz coils which magnetically trap the atoms[2549].

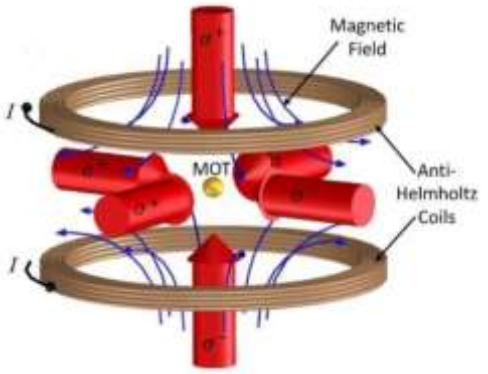


Figure 798: a typical Magneto-Optical Trap used to cool and confine neutral atoms. Source: Cold atom interferometry sensors physics and technologies by Martino Travagnin, 2020 (47 pages).

③ **Inverted pyramid retroreflection**: an inverted mirrors-based pyramid sits around the MOT and orient the prepared atom cloud downward in the instrument as shown in Figure 797.

④ **State preparation**: a laser beam coming from the bottom controls the atom cloud position. It is switched off and the cloud starts a freefall.

⑤ **Atom interferometer**: in their freefall, the atom cloud is exposed by two counter propagating vertical lasers pulses in three successive steps each generating a Raman transition with different durations and polarizations creating the equivalent of π/2, -π and -π/2 gates (H, X and H)[2550]. The first step will have the effect of a coherent beam splitter and create two streams of atoms in ground and excited state whose proportion depends on the ambient gravity. The second step will have the effect of two mirrors like in an optical interferometer and inverse the population of ground and excited states. The third step will focus the two atom beams and create a coherent beam mixing. And each step changes the phase of the atom matter wave!

⑥ **Detection**: one or two other lasers excite the two streams of atoms exiting the interferometer, generating a fluorescence effect that is detected by two sets of several diodes.

[2549] The Muquans process is documented in Gravity measurements below 10^{-9}g with a transportable absolute quantum gravimeter, 2018 (12 pages) and highlighted in Digging Into Quantum Sensors by Stewart Wills in Optics & Photonics, September 2019.

[2550] Double-photon Raman cooling uses two lasers. One excites the atoms to reach a high excited state and the other de-excites the atom to bring it down to a higher excited state than the initial state. This technique also contributes to cool atoms below a micro-Kelvin.

These diodes enable the measurement of the proportion of atoms in each interferometer output (excited/non excited). Their proportion will help compute the phase difference accumulated by the two atom streams, which itself will help calculate the ambient gravity. The process is repeated twice per second and a classical computer averages the results. ixBlue's gravimeters have a precision of 10^{-9} m/s^2.

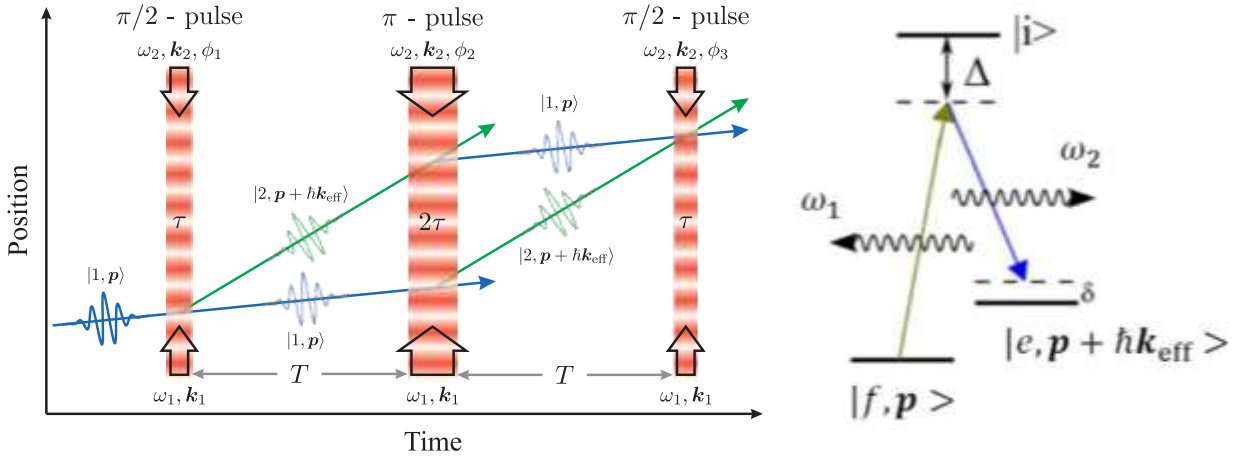


Figure 799: the three steps of cold atoms interferometry used in a gravimeter. The figure is somewhat confusing since the position axis (Z) goes up as the atom falls. So, it's inverted. Otherwise, how would you measure atoms at the bottom of the gravimeter? Two counterpropagating lasers are used, one coming from the top at frequency $\omega_1$and a wave vector k_1 and one from the bottom at ω_2 and a wave vector k_2 to create a double-photon Raman transition that will modify displacement for a share of the atoms that depends on the gravity. The diagram on the right shows the Raman transitions created by lasers with pulses ω_1 and ω_2. f corresponds to the fundamental or ground state, e to the excited state. p is the atom momentum and its difference in the excited state is $\hbar k_{eff} = \hbar(k_1 - k_2)$. The width of the laser pulse τ (about 10 ms) corresponds to its duration which generates a superposition like a Hadamard gate in gate-based computing in step 1 and 3, and a population inversion in step 2 with a duration of 2τ. Meaning, the excited atoms (green lines) are turned in ground state atoms (blue line) and vice-versa, and also inverting their vertical velocity. If the lasers were used continuously, they would create a Rabi oscillation creating continuous change in the proposition of atoms in the ground and excited state over a couple ms. Sources: Mobile and remote inertial sensing with atom interferometers by B. Barrett et al, November 2013-August 2014 (63 pages) and Cold atom interferometry sensors physics and technologies by Martino Travagnin, 2020 (47 pages).

iXblue is involved in the ESA's **NAVISP** program which plans to provide a supplementary navigation solution using gradiometry. The control of cold atoms has other applications[2551]. For example, Muquans participates in the European flagship project **Quantum Internet Alliance** to create hardware to extend the reach of QKD systems and with the French startup **Pasqal** which creates quantum processors based on cold atoms.

THALES

Thales Research & Technology (France) is developing miniaturized cold atom accelerometer, gyrometer and clock designed to be embedded. The whole with a "BEC on chip" component (for "Bose Einstein condensates on chip") in collaboration with the Charles Fabry laboratory of the Institut d'Optique (LCFIO). Atoms are vaporized in a glass cage glued to the chip, in which a good vacuum has been created. They are laser-cooled and trapped by a magnetic field and controlled by electromagnetic fields. This research project started around 2014.

Photo credit: Ecliptique - Laurent Thion.

Figure 800: a Thales BEC on chip.

[2551] See Fifteen years of cold matter on the atom chip promise, realizations, and prospects by Mark Keil, Ron Folman et al, 2019 (46 pages) which makes a good inventory of scientific applications of cold atoms and Micro-fabricated components for cold atom sensors by J. P. McGilligan et al, Review of Scientific Instruments, September 2022 (28 pages).

Atomionics (2018, Singapore, $2.5M) is currently developing Gravio, a cold atoms interferometry based sensor measuring acceleration, rotations and gravity variations.

It can be used for navigation and resource exploration. It can also be used as an underground GPS.

Other laboratories are working on the same technology, such as the **Leibniz University** of Hannover[2552]. **Aquark Technologies** (2020, UK) is a spin-off from the University of Southampton developing small vacuum chambers and simpler atoms trap system avoiding magnets. **AtomSensors** (2015, Italy) is a spin-off of the University of Florence which also develops cold atoms-based quantum sensors, including gravimeters. They also provide laser sources for spectroscopy and laser cooling of atoms. The Chinese are also in this field, but without having gone so far in miniaturization[2553].

Teledyne e2v (UK, a subsidiary of Teledyne US) is developing quantum gravimeters to maintains infrastructures with the detection of underground obstacles or cavities before construction works, and also do geothermal energy and groundwater reserves searches.

They are also involved in the creation of **CASPA** (Cold Atom Space PAyload), a small satellite weighing 14 kg and containing 6 CubeSat in a volume of 30x20 x10cm, including a cold atom gravimeter, which would be the first to operate in space. It was to be launched by ESA in 2020.

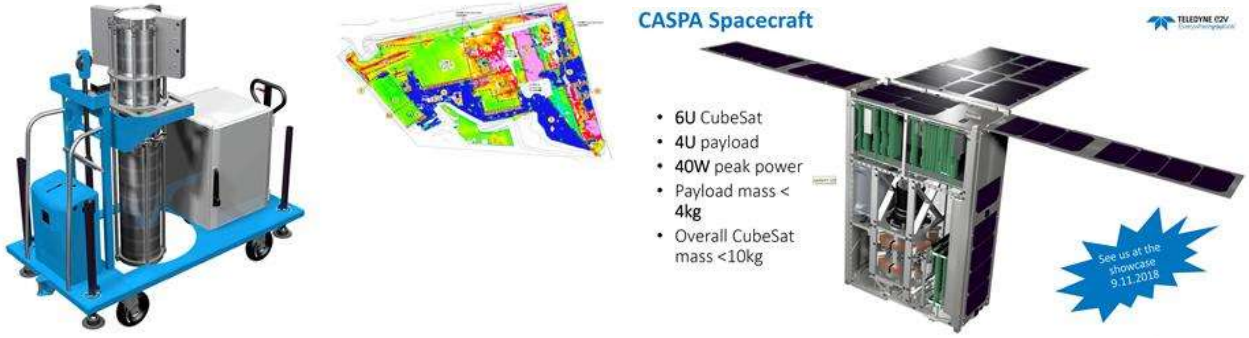


Figure 801: Teledyne e2v cold atom sensors to be embedded in a satellite that was to be launched in 2020.

Nomad Atomics (2018, Australia) develops compact cold atom-based quantum gravimeters and accelerometers. The company was launched by Kyle Hardman, Christian Freier and Paul Wigley, respectively researcher and postdocs at the Australian National University.

Innoseis (2020, Netherlands) was created by Mark Beker and Johannes van den Brand (who worked on gravitational waves detections instruments like those from LIGO), from Maastricht University. They develop MEMS based quantum gravimeters targeting seismic surveying.

Zero Point Motion (2020, UK, £2.58M) is a quantum optical inertial sensors company created by Ying Lia Li (Imperial College and University College London).

Their hybrid sensors use quantum photonics and cavity opto-mechanics to read the motion of MEMS masses. The product is being developed at the Quantum Technologies Innovation Centre at Bristol University with commercialization to start in 2024.

[2552] See Gravity measured using a Bose-Einstein condensate on a chip by Hamish Johnston, 2016 mentioning the work of Ernst Rasel of the Leibniz University of Hannover who refers to Atom interferometry and its applications by S. Abend et al, 2020 (48 pages).

[2553] See Compact and Portable Atom Gravimeter by Shuai Chen, 2019 (22 slides).

OK Quantum (2022, USA) or Oklahoma Quantum is a startup created by Saesun Kim (CEO) and Shan Zhong (Chief Scientist) who both come from the Center for Quantum Research and Technology (CQRT) of the University of Oklahoma.

They design and manufacture cold atom based quantum inertial sensors. Given their web site, they don't sell it yet.

Rafael Advanced Defense Systems (Israel) also has a department creating quantum sensing solutions, mainly gravitation sensors, with the Weizmann Institute of Science.

Microg LaCoste (1939, USA) develops absolute quantum gravimeters based on interferometry and free fall dropped mirrors, using a rubidium based atomic clock.

Draper Labs (1932, USA) also designs cold atoms sensors, mostly, gravimeters and accelerometers for navigation systems.

Trumpf (Germany) develops cold-atoms and VCSEL (lasers) based gyroscopes for satellites as part of the QYRO project funded by the German government and along with its subsidiary Q.ANT.

Wideblue (2006, UK) creates MEMS gravimeters. It's a consulting and engineering company.

Quantum accelerometers are also investigated to equip autonomous or assisted drive vehicles. German equipment manufacturer **Bosch** announced in February 2022 the creation its own quantum gyroscope for this purpose, aka IMU for inertial measurement unit as part of its new Bosch Quantum Sensing Unit, an internal startup led by Katrin Kobe and with a team of 15 people.

Finally, let's also mention a very special category of microgravimeters: the LIGO microgravimeters that are used to evaluate gravitational waves. They are based on optical interferometers of very high precision but of a size incompatible with all other imaginable uses[2554].

Quantum clocks

Atomic clocks used in GPS provide resilience for navigation systems when standard satellite GPS signals are unavailable. They are also used in telecommunication infrastructure for the Internet and mobile communications, particularly with high-speed broadband landline and mobile infrastructures. Many industry sectors also rely on precision time measurement, like the financial sector and utilities power grids. Fundamental research and astrophysics also heavily rely on precision clocks.

Time measurement steadily progressed since the first mechanical clocks used between the 14th and 19th centuries. Quartz clocks appeared between the two World Wars. They were based on the piezoelectric effect demonstrated by Pierre and Jacques Curie in 1880. With a frequency of 2^{15} Hz, time is counted with using frequency dividers, with a drift of a few hundred microseconds per day.

The first cesium atomic clocks dates from the 1950s. They had a frequency of the order of 9 GHz and provide a time measurement accuracy ranging from 10^{-13} and recent generations can reach 10^{-16}. The second is defined since 1967 as the duration of 9,192,631,770 periods of the radiation corresponding to the transition between the two "hyperfine" levels of the fundamental electronic state of cesium 133. The recent variants of these clocks are "fountain clocks". They operate at very low temperature, with laser cooling bringing the atoms at 1 µK, way much colder than superconducting qubits that are at 15 mK, but is however easier to obtain than with a dilution refrigerator. A frequency oscillator generates a transition between two levels of cesium energy. The frequency is locked with a servo loop.

[2554] See Advanced LIGO Just Got More Advanced Thanks To An All-New Quantum Enhancement by Ethan Siegel, December 2019. And a description of the quantum squeezing technique used in the latest version of LIGO: NIST Team Supersizes 'Quantum Squeezing' to Measure Ultrasmall Motion, 2019.

The precise measurement of frequencies has many applications: time measurement, synchronization of various devices on the Internet, even if only servers or scientific instruments, synchronization of moving objects to measure their position, astronomy (like with exoplanets and gravitational waves detection), absorption or emission precision spectroscopy, fiber optic transmissions and the generation of radio waves of arbitrary shape.

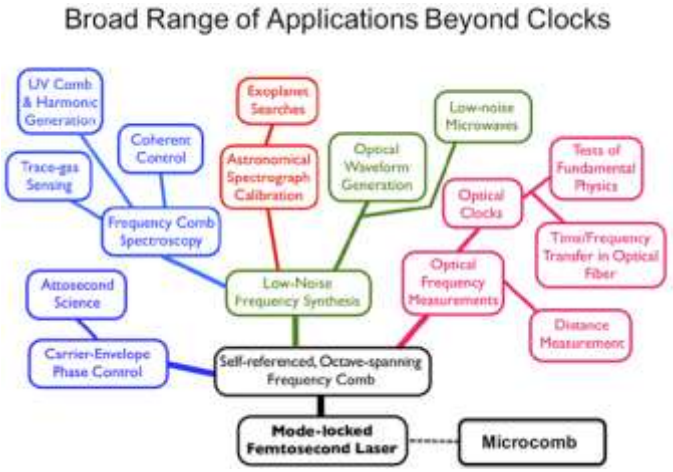


Figure 802: femto lasers use cases in quantum sensing.

However, a better accuracy may be needed, thus the need for quantum clocks [2555]. For about 20 years, time measurement was implemented with optical measurement of frequencies and time.

The measurement of atomic vibrations can be replaced by the measurement of light waves generated by lasers and at 10^{15} Hz. It allows a gain in accuracy of five orders of magnitude (10^5). It was demonstrated in 2000 to generate an accuracy of a femtosecond. This earned the Nobel Prize in Physics in 2005 to **Theodor Hänsch** (1941, German) and **John Hall** (1934, American).

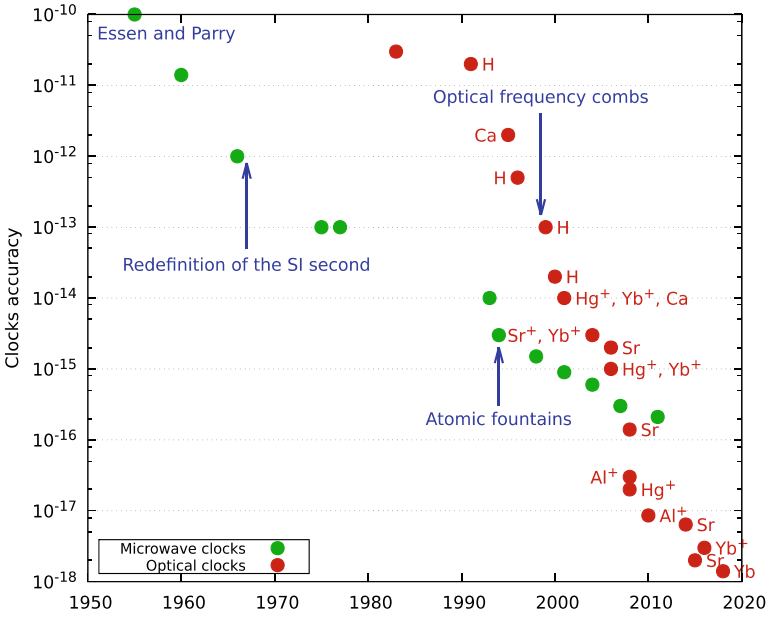


Figure 803: how quantum clocks accuracy evolved over time. Source: Chronometric Geodesy: Methods and Applications by Pacome Delva, Heiner Denker and Guillaume Lion, 2019 (61 pages).

In the USA, the **Chip Scale Atomic Clock** (CSAC) program funded by DARPA with NIST participation[2556] led to the creation of highly compact vapor-cells cesium based atomic clocks manufactured by Microchip (mentioned later, with a size of 1.6"x1.4"x0.45") after a decade of work starting in 2000 and $100m spent. It generates pulses of 4596.3xMHz with a frequency tuning resolution of $1x10^{-12}$s [2557].

Figure 804: a CSAC chipset.

Atomic clocks use microwave frequency transitions while the new generation of quantum clocks are based on higher electromagnetic wave frequencies in the optical spectrum.

[2555] See Time and Quantum Clocks: a review of recent developments by M. Basil Altaie et al, 28 April 2022 (39 pages) and Quantum clocks are more precise than classical ones by Mischa P. Woods et al, February 2022 (75 pages).

[2556] See MEMS Atomic Clocks by Svenja Knappe, NIST, Comprehensive Microsystems, 2008 (45 pages).

[2557] CSAC are just one type of atoms chipsets, which have a broader spectrum of use cases in inertial sensing and electromagnetic field sensing. See Fifteen Years of Cold Matter on the Atom Chip: Promise, Realizations, and Prospects by Mark Keil, Ron Folman et al, 2016 (44 pages).

They use the technique of frequency combs. Since these frequencies are higher, these clocks can have a better precision, with a 3 orders of magnitude gain compared to classical atomic clocks.

Frequency combs were discovered with the first mode-locked lasers by Logan Hargrove in 1964[2558]. Before optical combs, light frequency harmonic generators were used with a combination of several lasers in complicated setups. To measure light high frequencies, these clocks use optical frequency combs, which subdivided optical (high) frequencies into microwave (lower) frequencies for frequency measurement and timekeeping. It uses blocked-mode lasers that generate very short pulses, which can be as short as a few femtoseconds.

The frequency decomposition of this kind of signal gives a Gaussian-shaped frequency comb with each tooth regularly spaced at a frequency equivalent to that of the laser pulse. This is related to the fact that the length of the laser cavity is a multiple of the length of the electromagnetic waves emitted by the laser. The greater the multiple, the greater the frequency generated.

The frequency spectrum resembles a Gaussian curve. Its envelope is equal to the envelope of the spectrum of an isolated pulse, which is continuous. The width of the frequency spectrum covered can be narrow, a few nm in wavelength, or cover the entire visible spectrum, thus a few hundred nm.

A calculation is used to determine the very high frequencies of the frequency comb (f_n). It uses several parameters: the reference frequency f_{rep} of the laser pulses which is of the order of 250 MHz to 1GHz, n, the number of frequencies detected via spectroscopy (there can be hundreds of thousands) and the emission phase of the blocked mode laser which is added to each pulse and generates the frequency offset f_0, which is evaluated with a method described below and which is also of a lower order than GHz.

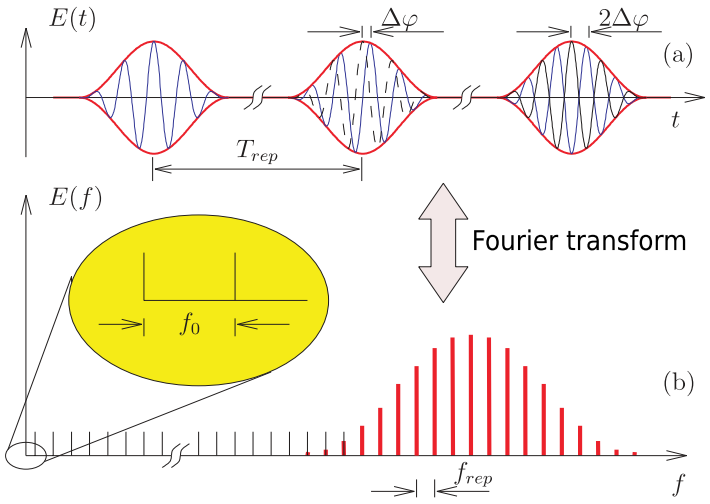


Figure 805: how a frequency comb works. Source: Ultra-short light pulses for frequency metrology, CNRS (6 pages).

The measurement of radio frequencies in the MHz/GHz wave range results in the measurement of frequencies in tens and hundreds of THz to the nearest Hz. The system thus acts as a frequency multiplier. The measurement of light frequencies is impossible with traditional electronics because of the frequencies used, which are several tens or hundreds of tera-Hertz.

These calibrated frequency combs are also used to measure a frequency difference with this standard[2559].

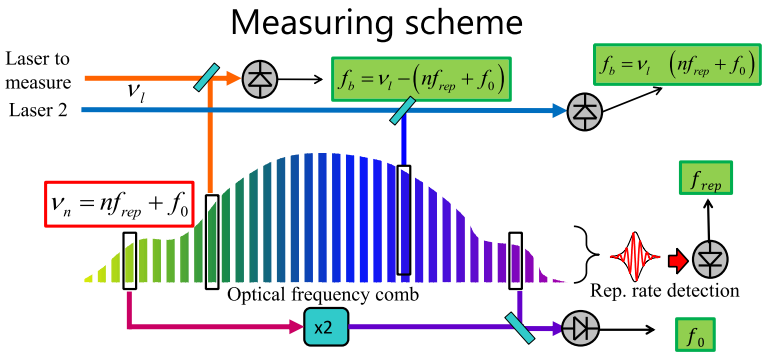
[2558] See Nobel Lecture: Defining and measuring optical frequencies by John Hall, 2006 (17 pages) and Light rules: frequency combs by Steven Cundiff, Jun Ye and John Hall in Pour la Science, 2008 (8 pages). John Hall describes frequency combs as the intersection of four initially independent fields of research: ultra-stable lasers, fast pulse lasers, nonlinear optical materials, and precision laser spectroscopy. This is a reflection of quantum computing and its many scientific and technological sources.

[2559] See Phase Coherent Vacuum-Ultraviolet to Radio Frequency Comparison with a Mode-Locked Laser by J. Reichert et al, 2005 (5 pages), Direct Link between Microwave and Optical Frequencies with a 300 THz Femtosecond Laser Comb by Scott Diddams et al, 2000 (4 pages), Fundamentals of frequency combs What they are and how they work by Scott Diddams (46 slides), Optical frequency combs and optical frequency measurements by Yann Le Coq, 2014 (38 slides) and Chip-scale Optical Atomic Clocks and Integrated Photonics by Matthew Hummon, NIST, 2018 (35 slides).

The frequency comb covers an octave, from one frequency (n) up to its double (2n). The evaluation of f_0 is done by extracting the frequency f_n, and doubling it with a crystal. By adding this frequency doubled with f_{2n}, we obtain a beat at the frequency of f_0.

$$2(f_0 + n \times f_{rep}) - (f_0 + 2n \times f_{rep}) = f_0$$

This is called **heterodyne detection**. The frequency comb becomes a kind of graduated ruler which is then used to position a frequency to be measured relative to the ruler. With that, you can build a new generation atomic clock[2560]!



If we know n (and we are sure of the signs in the equations),
→ the system is mathematically well determined

In practice, we may

- impose values to the different f with phase lock loops (multiplier scheme : ϕ-lock frep, divider scheme: ϕ-lock f_b) (narrow line...)
- measure them with frequency counters
- and/or use clever tricks (exemple : $f_b \otimes f_0$ → BPF → $\nu_l - nf_{rep} - f_0 + f_0 = \nu_l - nf_{rep}$

Figure 806: frequency comb and heterodyne detection. Source: Optical frequency combs and optical frequency measurements by Yann Le Coq, 2014 (38 slides), slide 11.

The readout of spectroscopy results using frequency combs can use CCD or CMOS cameras depending on the frequencies used in or around visible light[2561]. This measurement accuracy evolves with the use of lasers using a high pulse frequency.

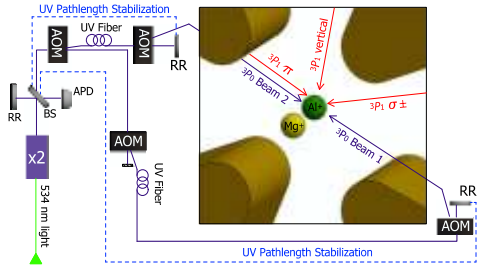


FIG. 1. Simplified schematic of the quantum-logic clock experimental setup. A frequency-quadrupled Yb-doped fiber laser is locked to the $^1S_0 \leftrightarrow {}^3P_0$ transition ($\lambda \simeq 267$ nm) by alternating the probe direction between two counterpropagating laser beams (shown in violet). An enlarged view of the trapping region is shown on the right. Three nominally orthogonal beams used for micromotion measurements are shown in red. Acousto-optic modulator (AOM), beam splitter (BS), retro-reflector (RR), frequency doubling stage (x2).

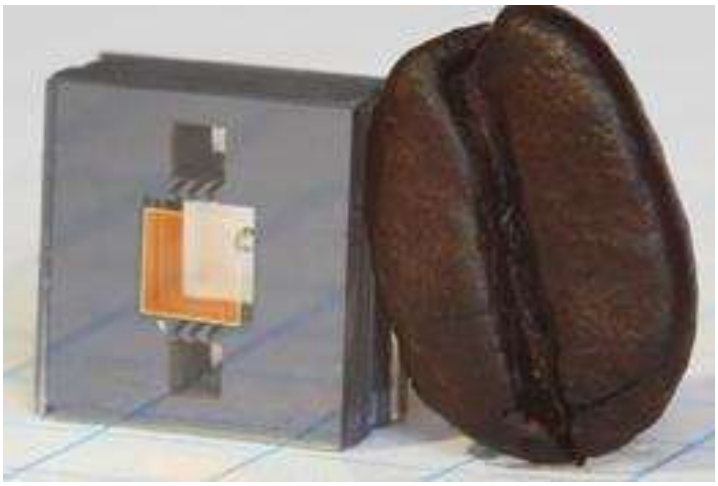


Figure 807: Source: (right) Illustration source: [27]Al+Quantum-Logic Clock with a Systematic Uncertainty below 10-18, 2019 (6 pages).

To date, the record for the accuracy of an atomic clock using spectroscopy is that of **NIST.** It is built with an aluminum ion associated with a magnesium anon. The aluminum ion is excited by two ytterbium lasers. Measurement is carried out using a quantum logic spectroscopy which is using the frequency combs seen in Figure 807, *left* [2562]. The clock reaches an accuracy of 10^{-18} seconds, a drift of one second per 33 billion years, 2.5 times the age of the Universe[2563].

[2560] This is explained in Optical Atomic Clocks by Andrew Ludlow, Martin Boyd, Jun Ye, E. Peil and P.O. Schmidt, 2015 (65 pages) and Optical atomic clocks by N. Poli et al, 2014 (70 pages). See also Photonic integration of an optical atomic clock by Z. L. Newman et al, November 2018 (12 pages).

[2561] See Frequency comb spectroscopy by Nathalie Picqué and Theodor Hänsch, 2019 (27 pages) which describes the many methods and use cases of frequency comb based spectroscopy.

[2562] See this explanation: Quantum Logic for Precision Spectroscopy by Piet Schmidt et al, 2009 (6 pages).

[2563] See [27]Al+Quantum-Logic Clock with a Systematic Uncertainty below 10-18, 2019 (6 pages).

In this market for optical quantum clocks, there are many research laboratories that produce their own equipment. These are usually based on titanium-sapphire with pulses of a few femtoseconds (10^{-15} to 10^{-14} seconds).

NIST is also working on an atomic clock that would fit into a component the size of a coffee bean, using a double frequency comb and rubidium gas (in Figure 807, *right*). The whole thing consumes only 275 mW. This project was co-funded by DARPA[2564]. However, for the moment, the precision obtained is not yet satisfactory for industrialization.

One of the projects of the European Quantum Flagship, **iqClock** (Netherlands, €10M), also aims to create very high-precision, portable quantum clocks. The consortium brings together six universities and six private partners including Teledyne EV (USA), Toptica (Germany), NKT Photonics (Denmark), AckTar (Israel) and Chronos (UK).

Let's now look at some vendors in high-precision quantum time measurement.

In the private sector, **Teledyne** sells Minac (cesium atomic clock), T-CSAC (also cesium, integrated in a chip) and Synchronicity (ytterbium-based).

UK aircraft carrier HMS Prince of Wales has been fitted with the world's first atomic clock of its kind to help ensure pinpoint accuracy wherever she goes provided by BP and Teledyne e2v.

MicroSemi (1960, USA) sells its Quantum SA.45s, a miniaturized chip-scale atomic clock (CSAC). Among other use cases, it can be used in portable IED (improvised explosive devices) jammers. The company is a subsidiary of MicroChip Technology (1989, USA).

HyperLight Corp (2018, USA), based in Cambridge, near Boston, develops nanophotonic integrated circuits such as frequency combs or resonators that are used in quantum sensing.

Cryoclock (2016, Australia) develops sapphire-based cryogenic oscillators. The company was co-founded by John Hartnett. Applications include trapped ion quantum processors and atomic clocks.

Orolia (2005, France) creates atomic clocks with cesium, or based on rubidium oscillators. They mainly target the aerospace industry and provide the Galileo GNSS service.

Syrlinks (2011, France) develops miniature atomic clocks based on MEMS and cesium for embedded applications. Their MMAC is 40 x 35 x 22 mm and consumes less than 0.3 W.

With Thales, and with the help of CNRS (SYRTE lab) Syrlinks is developing Chronos, new quantum clocks for civil and military applications with error inferior to 1 second per tens of thousands of years. It will enable geolocalization when GNSS like GPS and Galileo are not available.

TMD (1969, UK) sells microwave amplifiers. They also develop atomic clocks and instrumentation for the manipulation of cold atoms.

VectorAtomic (2018, USA) markets rubidium atomic clocks for quantum inertial navigation systems that can then avoid using GPS.

[2564] The project is documented in Architecture for the photonic integration of an optical atomic clock, 2019 (6 pages).

Vescent Photonics (2002, USA) offers optical frequency comb generators for use in atomic clocks. They also master the laser-based technique used for controlling cold. They are based in Colorado.

In June 2022, **ColdQuanta** was announcing it was working for the US Navy with **LocatorX** (USA) to create an atomic clock using the Solid-state Miniature Atomic Clock (SMAC) technology created by LocatorX under license of Oxford University[2565]. The system is using fullerene molecules (C60) doped with nitrogen. It is not relying on cold atoms, the core technology mastered by ColdQuanta. It seems the two vendors are combining lightweight atomic clocks and more precise ones using cold atoms.

Finally, let us mention again **Muquans,** which also uses its cold atoms expertise to sell an atomic clock, the MuClock, designed in partnership with the LP2N laboratory in Bordeaux and the LNE-SYRTE. It is positioned as an alternative to cesium atomic clocks. The instrument weighs 135 kg and consumes 200W.

Quantum magnetometers

Quantum magnetometers are used to detect small variations or levels of magnetism with high spatial accuracy. There are many uses cases: navigation, mineral exploration, current detection, magnetocardiography, magnetoencephalography, orientation of drones and autonomous vehicles in tunnels where GPS does not work[2566], sonar, detection of moving metal objects such as vehicles and cellular imaging[2567].

Different techniques are available for high-precision magnetometry including Bose condensates and **atomic spins in vapors** [2568], **SQUIDs** (superconducting effect with a Josephson junction as in superconducting qubits[2569]), **NV-centers** solid-state systems, particularly using optically detected magnetic resonance (ODMR), with a sensitivity (or noise) usually ranging from 10^{-9} to 10^{-15} $T/\sqrt{Hz}$ and decreasing as the signal frequency increases, and even **SiC-vacancies** (silicon vacancies in silicon carbide)[2570].

Measuring magnetism with NV centers exploit the variation of the spin resonance spectrum in the diamond cavity, which depends on the ambient magnetic field (see the chart above on the right on spin resonance spectrum). The distance between the two fluorescent light pulses (Y) generated is measured as a function of the electromagnetic excitation frequency used (X)[2571]. The spins preparation is performed with a laser and its modification with 3 GHz microwave pulses. NV-center based magnetometers can use large unordered ensembles of NV centers[2572] or individual NV centers[2573].

[2565] See ColdQuanta and LocatorX Partner to Build Next Generation of Atomic Clocks by ColdQuanta, June 2022.

[2566] A UAV solution using GPS in a tunnel is proposed by the startup Hovering Solutions (Spain).

[2567] See Nitrogen-vacancy centers in diamond for nanoscale magnetic resonance imaging applications by Alberto Boretti et al, 2019 (24 pages).

[2568] See the Rydberg atom technique described in Quantum sensing using circular Rydberg states by Rémi Richaud, LKB, November 2018 (41 slides). See also the thesis Rubidium vapors in high magnetic fields by Stefano Scotto, November 2017 (168 pages). See also Brief Review of Quantum Magnetometers by Ivan Hrvoic and Greg M. Hollyer, GEM Systems, not dated (15 pages).

[2569] See this presentation of SQUID applications: SQUID Fundamentals and Applications by Robin Cantor, 2017 (48 slides).

[2570] See Fiber-integrated silicon carbide silicon vacancy-based magnetometer by Wei-Ke Quan et al, CAS and Sichuan University, August 2022 (13 pages) which describes a proposal of silicon carbide vacancy-based room temperature ODMR magnetometer using a fiber for results measurements.

[2571] After optical magnification, fluorescence can be analyzed by a CCD image sensor.

[2572] See for example Picotesla magnetometry of microwave fields with diamond sensors by Zhecheng Wang et al, June 2022 (7 pages).

[2573] See for example Scanning gradiometry with a single spin quantum magnetometer by W. S. Huxter et al, 2022 (9 pages).

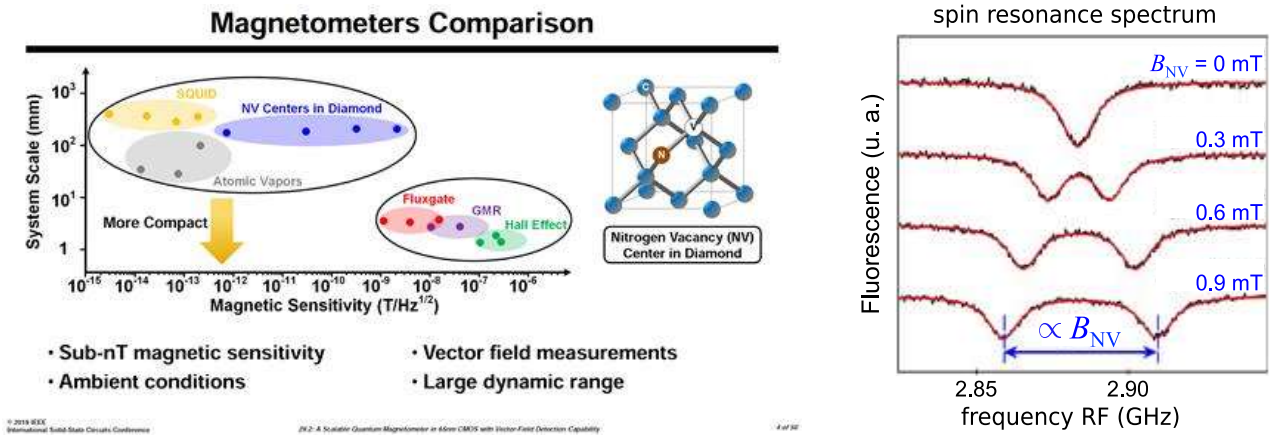


Figure 808: NV center magnetometry principle using spin resonance spectrum analysis. The two energy gaps enable the evaluation of the current magnetic field. Sources: A Scalable Quantum Magnetometer in 65nm CMOS with Vector-Field Detection Capability by Mohamed Ibrahim from MIT 2019 (51 slides) and NV Diamond Centers: from material to applications by Jean-François Roch, Collège de France, 2015 (52 slides).

The accuracy of magnetism measurement can reach a pico-Tesla, billions of times less than terrestrial magnetism[2574]. NV centers provide a lesser precision than cold atoms, but their use is more practical because the instrument is easier to miniaturize and most of them work at ambient temperature[2575]. Scanning probes magnetometers use a diamond nanocrystal containing a single cavity and a nitrogen atom, which ensures the accuracy of the measurement. The probe can be moved in space and used to analyze the magnetism of a material in 2D.

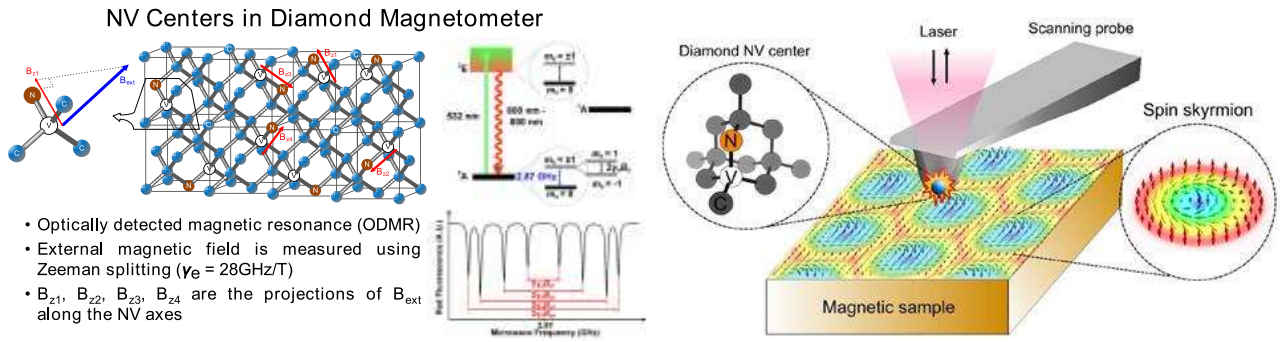


Figure 809: NV centers used in ODMR for medical imaging of materials inspection. Sources: A Scalable Quantum Magnetometer in 65nm CMOS with Vector-Field Detection Capability by Mohamed Ibrahim from MIT 2019 (51 slides) and Probing and imaging nanoscale magnetism with scanning magnetometers based on diamond quantum defects, 2016 (35 slides).

The NV-centers technique appeared in 2009. It is notably developed in France by **Thales**[2576].

[2574] The accuracy of magnetometry with NV centers is evaluated with the formula $1\mu T/\sqrt{Hz}$. See Picotesla magnetometry of microwave fields with diamond sensors by Zhecheng Wang et al, August 2022 (7 pages) which describe a heterodyne measurement technique enabling picotesla precision.

[2575] See A Scalable Quantum Magnetometer in 65nm CMOS with Vector-Field Detection Capability by Mohamed Ibrahim from MIT 2019 (51 slides) which describes a miniaturization process of a quantum magnetometer combining a 65 nm CMOS circuit manufactured by TSMC and a diamond NV-center based system.

[2576] ASTERIQS (France, €9.7M) or "Advancing Science and Technology through diamond Quantum Sensing" is a European Quantum Flagship project launched in 2018 and led by Thales, which is expected to advance techniques for measuring magnetic, electric, temperature and pressure fields. There are many applications, such as sensors for vehicle battery monitoring, high-resolution sensors for nuclear medical imaging (NMR, nuclear magnetic resonance) or for creating radio frequency spectrum analyzers. The Swiss startup Qnami is involved in the project and provides artificial diamonds.

Laboratories in Bristol, the University of Ulm in Germany and Microsoft are working on the use of NV Centers techniques coupled with machine learning and Bayesian inference methods to correct the noise found at higher temperatures[2577].

Quantum magnetometry can also rely on mixed optomechanics-photonics systems, like in a 2022 proposal from a China research team. It couples a thin SiN mechanical membrane to Terfenol-D rods[2578] with a height that is sensitive to a static magnetic field. The membrane position modifies the phase a laser-originated photon that is reflected in a cavity containing the membrane. The magnetic field s converted in the photon phase which is measured with homodyne detection using a local oscillator. The sensitivity of this sensor could be excellent, reaching 10^{-15} to 10^{-17} $T/\sqrt{Hz}$ [2579].

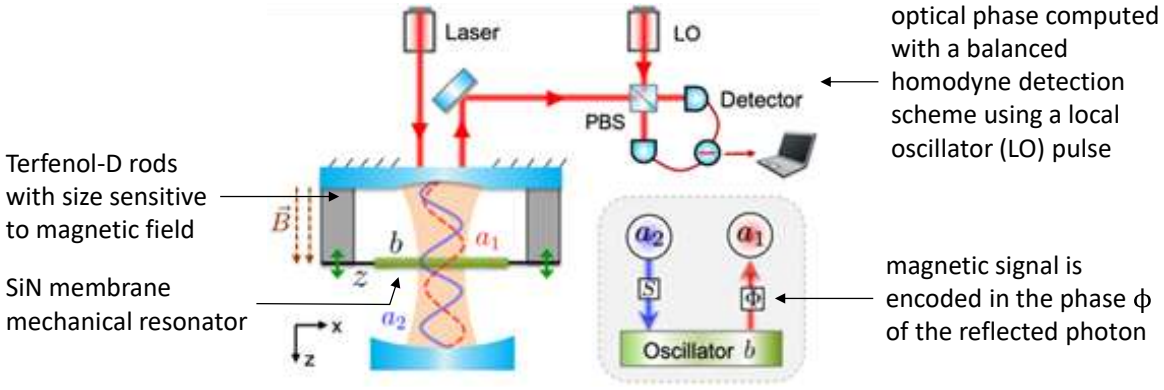


Figure 810: Source: Quantum Magnetometer with Dual-Coupling Optomechanics by Gui-Lei Zhu et al, May 2022 (7 pages).

Another amazing use case for NV center magnetometry is the precise measurement of battery charge and discharge[2580].

Let's look at some vendors in the quantum magnetometry space.

qdm.io (2021, USA) is a stealth company based in Maryland that creates NV centers sensors.

Qubic (2019, Canada) is a startup from the Institut Quantique from the University of Sherbrooke in Quebec that is working on microwaves-based quantum sensing tools for sensing, imaging and communications. It is led by Jérôme Bourassa.

Qutools (2005, Germany) offers its quNV quantum magnetometer kit, based on diamond NV-centers as its name suggests. It fits in a 3U rack. They also sell an interferometer for interferometric displacement measurement.

Figure 811: a quantum magnetometer from qutools.

[2577] See Magnetic-Field Learning Using a Single Electronic Spin in Diamond with One-Photon Readout at Room Temperature by Raffaele Santagati et al, 2018 (18 pages).

[2578] Terfenol-D is a magnetostrictive material made from an $Tb_xDy_{1-x}Fe_2$ ($x \approx 0.3$) alloy. Its name comes from terbium, iron (Fe), Naval Ordnance Laboratory (NOL, who developed the material in the 1970s), and D for dysprosium. The material is used to produce sonar systems.

[2579] See Quantum Magnetometer with Dual-Coupling Optomechanics by Gui-Lei Zhu et al, May 2022 (7 pages).

[2580] See High-precision robust monitoring of charge/discharge current over a wide dynamic range for electric vehicle batteries using diamond quantum sensors by Yuji Hatano et al, Nature Scientific Reports, September 2022 (10 pages)

Also in Germany, the University of Stuttgart is working with the Fraunhofer Institute to transfer NV-centered magnetometry technology as part of the **QMag**[2581] project.

Supracon (2001, Germany) manufactures magnetometers based on SQUIDs (Superconducting Quantum Interference Devices). It is a spin-off of the Leibnitz Institute of Photonics in Jena. It sells its sensors to astrophysics research laboratories and for geophysics prospection.

Great Lakes Crystal Technologies (2019, USA) is a supplier of diamonds for use in NV center applications, especially for quantum magnetometers. It is a spin-off from the University of Michigan and Fraunhofer USA.

FieldLine Inc (2020, USA) develops NV centers quantum sensing systems, particularly for medical brain imaging and non-destructive materials testing.

Q-Sensorix (2019, USA) develops NV centers magnetometer-based gyroscopes, launched by Alexey Akimov, Vladimir Shalaev and Yuri Lebedev. These are alumni of the University of Buffalo in New York State.

Twinleaf (2007, USA) develops precision magnetometers based on alkali metal lasers. The company is headed by Elisabeth Foley, a specialist in the field, and Thomas Kornack (CSO), both Princeton alumni.

Cerca Magnetics (2018, UK) is a spin-out from the UK Sensors and Timing Quantum Technology Hub at the University of Nottingham. It develops a wearable brain scanner magnetoencephalography (MEG) system, avoiding the use of cryogeny like heavy MRI scanners.

It uses an optically pumped magnetometers measuring weak magnetic fields. These are made with a laser illuminating a small glass cell containing a pressured gas of rubidium or cesium. A diode detects the transmitted light that depends on the local magnetic field perpendicular to the laser beam[2582]. The technology is competing with SQUIDs based MEGs.

CIQTEK (2016, China, $15M) manufactures quantum sensors targeting quantum computation, healthcare, food safety, chemistry and material science markets. These sensors are NV center magnetometers.

At last, the **Ivar Giæver Geomagnetic Laboratory** (IGGL) in Norway also uses SQUIDs to detect underground magnetism for paleomagnetic applications, to measure the magnetic remanence of ancient rocks. Using SQUIDs, their magnetometer must be cooled to 4K with a pulsed tube[2583].

GEM Systems (1980, Canada) is selling quantum magnetometers using optically pumped potassium (K-Mag).

ODMR Technologies (2015, USA) is a stealth spin-off from Berkeley which designs a magnetic resonance spectroscopic analysis system based on NV centers.

[2581] See Quantum Magnetometers for Industrial Applications, April 2019.

[2582] See Optically pumped magnetometers: From quantum origins to multi-channel magnetoencephalography by Tim M. Tierney et al, 2019 (12 pages).

[2583] See Instruments for Paleomagnetic Measurements WSGI (2G) Model 755 Superconducting Rock Magnetometer (SRM).

Elta Systems (1967, Israel) is a subsidiary from the IAI consortium. The company develops various electromagnetic sensors and radars for defense and intelligence.

They develop quantum magnetic sensors in collaboration with Israeli research groups and industry partners. These sensors can help detect IEDs (improvised explosive devices, unexploded ordinance, geophysical structures, vehicles and ships). They also work on quantum optical magnetometry and sub-pico-Tesla atomic magnetometers which can be used in medical imaging (MEG).

Wainvam-E (2020, France) is providing a set of magnetometry solutions based on NV centers targeting nondestructive measurement of various materials like steel and oxidation characterization in live cells.

Quantum thermometers

NV centers have another use: temperature measurement with an accuracy of a few mK and with a very high spatial resolution, all with highly miniaturized sensors. It is currently the most powerful temperature measurement technology for these different dimensions. It allows, for example, to determine the temperature within living cells and organisms with a sub-mm precision [2584].

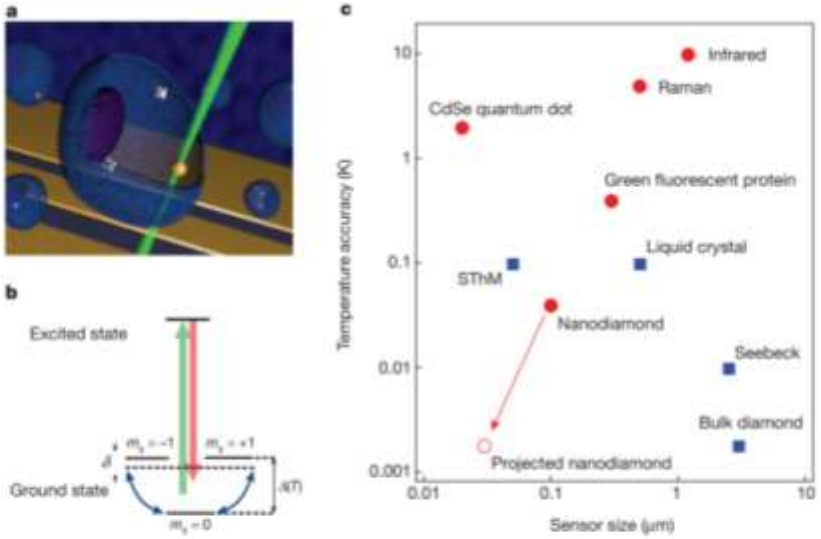


Figure 1 | Nitrogen–vacancy-based nanoscale thermometry. **a**, Schematic image depicting nanodiamonds (grey diamonds) and a gold nanoparticle (yellow sphere) within a living cell (central blue object; others are similar) with coplanar waveguide (yellow stripes) in the background. The controlled application of local heat is achieved by laser illumination of the gold nanoparticle, and nanoscale thermometry is achieved by precision spectroscopy of the nitrogen–vacancy spins in the nanodiamonds. **b**, Simplified nitrogen–vacancy level diagram showing a ground-state spin triplet and an excited state. At zero magnetic field, the $|\pm 1\rangle$ sublevels are split from the $|0\rangle$ state by a temperature-dependent zero field splitting $\Delta(T)$. Pulsed microwave radiation is applied (detuning, δ) to perform Ramsey-type spectroscopy. **c**, Comparison of sensor sizes and temperature accuracies for the nitrogen–vacancy quantum thermometer and other reported techniques. Red circles indicate methods that are biologically compatible. The open red circle indicates the ultimate expected accuracy for our measurement technique in solution (Methods).

Figure 812: Source: Nanometre-scale thermometry in a living cell, 2013 (6 pages).

Quantum thermometry also has applications in very low temperatures measurement, such as within cryostats and physics experiments. Quantum thermometers sensitivity is assessed in $K/\sqrt{Hz}$ meaning it increases with the number and frequency of measurements.

[2584] See Nanometre-scale thermometry in a living cell, 2013 (6 pages) and Real-time nanodiamond thermometry probing in vivo thermogenic responses by Masazumi Fujiwara et al, September 2020 (10 pages).

How are these NV center quantum thermometers working? Several methods are used like spin-based thermometry with ODMR (optically detected magnetic resonance) spectrum measurement using microwave excitement. The diamond containing NV centers can be attached to a fiber[2585]. There are even hybrid thermometers associating NV centers and more classical magnetic nanoparticle thermometers[2586].

It uses the fact that the zero-field splitting frequencies are linearly dependent on the ambient temperature. All-optical methods use the correlation between the NV center ZPL (zero-phonon lines) and temperature[2587].

There are solutions for temperature measurement in biological matter by fluorescence that are based on quantum dots[2588].

In 2017, NIST produced a quantum photonics thermometer of very small size for optically measuring the surface temperature of metals. However, the picture does not show the control electronics associated with the sensor[2589].

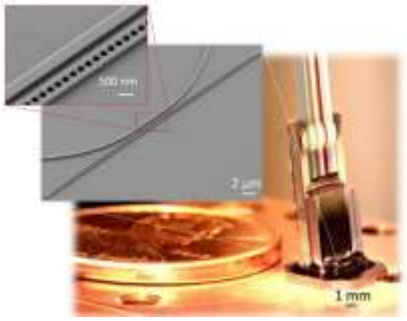


Figure 813: quantum photonic thermometer from NIST.

Southwest Sciences (1985, USA) develops optical temperature sensors based on NV centers for use in cryogenic systems. The company was founded by Alan C. Stanton and Joel A. Silver.

Quantum frequencies sensing

Radio frequency analysis is an old matter, but it is also progressing thanks to quantum technologies often associating optronics with cold atoms. Wideband frequency quantum sensing can be implemented with neutral atoms and NV centers.

Neutral atom-based sensors paired with optical readout using coherent spectroscopy can analyze electromagnetic waves frequencies from direct current (0 Hz) to the THz range. This is due to their so-called high-energy Rydberg states which can help measure high-frequency electro-magnetic waves thanks to their strong dipole. It can help reduce the size of various antennas, improve radio frequency filtering and extend the range between mobile communications cellular towers. This sort of broadband spectrum analysis can have multiple use cases, particularly in the military and intelligence sectors. These systems don't necessarily showcase high-precision and can be used as "heads-up" spectrum analysis tools before more specialized tools are used for specific parts of the electromagnetic spectrum. But some progress is made to improve these neutral atom-based electromagnetic spectrography system, noticeably in the MHz bands[2590].

[2585] See Temperature dependence of nitrogen-vacancy center ensembles in diamond based on an optical fiber by Ke-Chen Ouyang et al, November 2021 (17 pages).

[2586] See Ultra-sensitive hybrid diamond nanothermometer by Chu-Feng Liu and al, 2019-2021 (9 pages

[2587] See the review paper Diamond quantum thermometry from foundations to applications by Masazumi Fujiwara and Yutaka Shikano, April-September 2021 (24 pages).

[2588] See Intracellular thermometry with fluorescent sensors for thermal biology by Kohki Okabe et al, 2018 (15 pages).

[2589] See Thermodynamic miniaturized sensors and standards and the quantum SI by Gregory F. Strouse, 2016 (39 slides).

[2590] See Highly sensitive measurement of a MHz RF electric field with a Rydberg atom sensor by Bang Liu et al, June 2022 (7 pages) and Quantum sensing of weak radio-frequency signals by pulsed Mollow absorption spectroscopy by T. Joas et al, 2017 (6 pages).

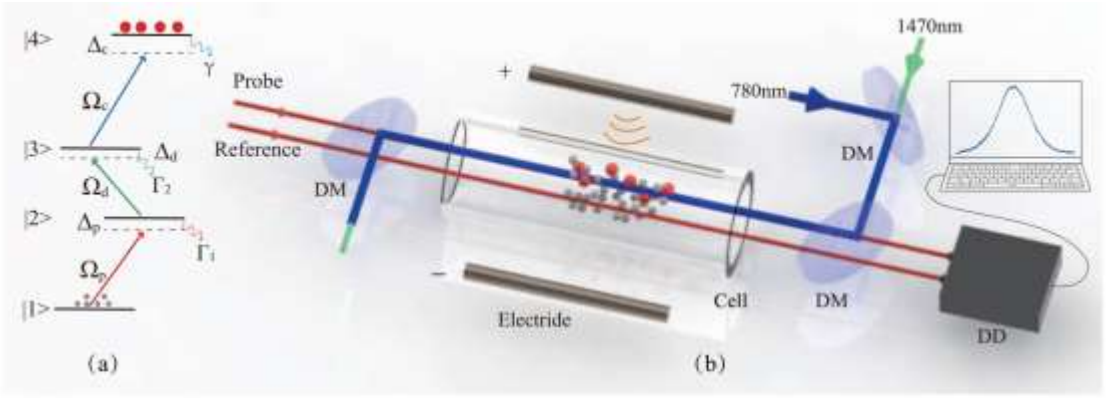


Figure 1. (a) Ladder-type four-level atomic energy diagram consisting of a ground state $|1\rangle$, two low-lying excited states $|2\rangle$ and $|3\rangle$, and a Rydberg state $|4\rangle$. An 852-nm probe light drives the transition $|1\rangle = |6S_{1/2}, F = 4\rangle \rightarrow |2\rangle = |6P_{3/2}, F = 5\rangle$, a 1470-nm dressing light couples the transition $|2\rangle = |6P_{3/2}, F = 5\rangle \rightarrow |3\rangle = |7S_{1/2}, F = 4\rangle$, and a 780-nm coupling light drives the transition $|3\rangle = |7S_{1/2}, F = 4\rangle \rightarrow |4\rangle = |55P_{3/2}\rangle$ of cesium atoms. (b) Overview of the experimental setup. The probe light and the reference light propagate in parallel through a Cs vapor cell. The probe light (red) overlaps the counter-propagating coupling light (blue) and dressing light (green) to form an EIT configuration. The transmission difference between the probe and reference lights is detected by a differencing photodetector. Two electrode rods are placed parallel to each other on both sides of the vapor cell 4 cm apart. Labels: DM - dichroic mirror; DD - differencing photodetector.

Figure 814: how cold atoms are used to measure electromagnetic waves frequencies spectrum in a highly sensitive solution developed in China, using a hot vapor cell of cesium atoms excited by lasers in their Rydberg states. The grey electrodes are connected to an RF antenna. Source: Highly sensitive measurement of a MHz RF electric field with a Rydberg atom sensor by Bang Liu et al, June 2022 (7 pages).

A quantum sensor based on alkaline Rydberg atoms can analyze the radio spectrum from 1 kHz to 100 GHz [2591]. Other quantum sensors can analyze radio waves in the 1 THz band, that is intermediate between infrared and microwaves bands, with potential applications in the measurement of thickness of thin layers of heterogeneous materials[2592].

NV centers sensors can also help run RF signals spectral analysis, from 0 to 40 GHz with the advantage of being more lightweight than most neutral atoms sensors. NV centers sensors can even be arranged in sensor arrays enabling both a wideband spectrum coverage and a high-precision analysis of a target band[2593].

Some pure optics techniques can be used to implement frequency sensing in the THz range[2594].

Figure 815: RF spectrum analyzer with rare-earth doped crystals. Source TBD.

And surprisingly, it can also work, in a different fashion, to create quantum optical microphones with the benefit to improve the quality of AI-based speech recognition[2595].

[2591] See Highly sensitive measurement of a MHz RF electric field with a Rydberg atom sensor by Bang Liu et al, June 2022 (7 pages) and Quantum sensing of weak radio-frequency signals by pulsed Mollow absorption spectroscopy by T. Joas et al, 2017 (6 pages). See also Assessment of Rydberg atoms for wideband electric field sensing by David H Meyer et al, January 2020 (16 pages). See also another less impressive performance from the same lab and published later: Waveguide-Coupled Rydberg Spectrum Analyzer from 0 to 20 GHz by David H. Meyer, 2021 (10 pages).

[2592] See Researchers demonstrate first terahertz quantum sensing, March 2020, which refers to Terahertz quantum sensing by Mirco Kutas et al, 2020 (9 pages).

[2593] See Sensing of Arbitrary-Frequency Fields Using a Quantum Mixer by Guoqing Wang et al, MIT, PRX, June 2022 (22 pages).

[2594] See Terahertz quantum sensing by Mirco Kutas et al, March 2020 (8 pages).

[2595] See A Quantum Optical Microphone in the Audio Band by Raphael Nold et al, April 2022 (7 pages).

Rydberg Technologies (2015, USA) provides cesium or rubidium specimens for cold atom-based radio frequency sensing solutions.

They sell Rydberg lasers, a Rydberg atoms-based radio-frequency probe, a RFMS (Rydberg Field Measurement System) covering the 1MHz-100 GHz frequency range, and Rydberg vapor cells [2596]. Their technology is also integrated in AM and FM radio-frequency receivers as well as in radars.

Thales is developing a real-time radiofrequency spectral analyzer *aka* a Quantum Diamond Signal Analyzer (Q-DiSA) with a bandwidth of 10 MHz to 25 GHz and a frequency resolution of 1 MHz, based on NV centers[2597]. The frequency adjustment is done with controlling the distance of the NV center with a small 1.3 cm magnetic sphere. The system is using a 532 nm laser and a CMOS sensor.

At last, we should mention **quantum antennas** where some non-classical phenomenon can occur like the creation of squeezed states[2598]. It is an emerging field that can address particular needs, like field shaping, quantum radars, quantum imaging and creating antennas for THz electromagnetic fields using quantum dots[2599]. Since 2022, **BAE Systems** (UK) is developing quantum antennas on behalf of DARPA.

Quantum imaging

Quantum sensing is enlarging the scope of what is possible to do in imaging, at both the microscale and nanoscale levels, and in the biology and material inspection realms. These new tools are based on various techniques that we'll cover here: **SQUIDs**, aka superconducting qubits[2600], **NV-centers** based magnetometry to implement NMR spectroscopy which tend to dominate the market nowadays thanks to their space resolution and readout precision, and **OPMs**, aka optical-pumped magnetometers which are mainly used for neuron imaging (MEG, magnetoencephalography). We'll also have a look at some mysterious "ghost imaging" systems that take pictures of objects with a single pixel sensor and other special quantum sensors.

SQUIDs are classically used in MRI systems which require helium-4 based cryogeny. They are also implemented in various specific use case like in sub-mm astronomy and infrared (IR) imaging. One such imager with 10,000 pixels is embedded in the NIRSpec near-infrared telescope in the JWST (James-Webb Space Telescope)[2601].

NV-centers imagers can be used to analyze organic molecules with excellent spatial resolution. It makes use of electron spin resonance spectroscopy (ESR) at cryogenic temperature which allows to examine atoms and molecules at the level of their electron spin. This enables NMR (nuclear magnetic resonance) detection[2602]. The technique is usually integrated in scanning tunneling microscopes as well as in atomic force microscopes (AFM). The electron spin of the examined materials is excited by a magnetic field and microwaves.

[2596] See A vapor-cell atomic sensor for radio-frequency field detection using a polarization-selective field enhancement resonator by D. A. Anderson et al, 2018 (11 pages).

[2597] See A quantum radio frequency signal analyzer based on nitrogen vacancy centers in diamond by Simone Magaletti, Ludovic Mayer, Jean-François Roch and Thierry Debuisschert, Nature Communications, February-July 2022 (8 pages).

[2598] See the review paper Quantum Antennas by Gregory Ya. Slepyan, Svetlana Vlasenko and Dmitri Mogilevtsev, June 2022 (70 pages).

[2599] See Generating tunable terahertz radiation with a novel quantum dot photoconductive antenna by Andrei Gorodetsky, Ksenia A. Fedorova, Natalia Bazieva and Edik U. Rafailov, Aston University Birmingham, 2016.

[2600] See Magnetometry of neurons using a superconducting qubit by Hiraku Toida et al, NTT Research Labs, June 2022 (6 pages).

[2601] Seen in Micromachined Quantum Circuits by Teresa Brecht, 2017 (271 pages)

[2602] See Advances in nano- and microscale NMR spectroscopy using diamond quantum sensors by Robin D. Allert et al, May 2022 (42 pages).

The NV-center technique allows the examination of a hard disk and semiconductors defects with a probe equipped with a single NV-center in Figure 816 and Figure 818.

It is also used for the characterization (quality control) of integrated circuits working with millimeter frequencies such as in 5G[2603]. Others are working on NV centers-based microscopy of living cells[2604].

There is even an application to qualify malaria patients by analyzing hemozoin nanocrystals appearing in red blood cells affected by the disease parasite[2605]. These techniques are used with confocal microscopy. This generates images with a very shallow depth of field of about 400 nm, creating optical sections of the sample to analyze. With modifying the position of the depth focal plane, a series of images are created which are then assembled to generate a 3D view of the analyzed sample. The light source is reflected or obtained by fluorescence in reaction to a laser beam. The result is a Confocal Laser Scanning Microscope (CLSM). NV-centers can also improve the accuracy of adaptive optics, which are used in astronomy[2606].

Imaging can also exploit an array of small NV centers that provide much better resolution than imaging systems based on SQUIDs magnetometers. The examples in Figure 818 show its architecture[2607].

The second was made to study bacteria that contain magnetic microelements. In other cases, magnetic markers can be used to attach themselves to the cells to be detected, typically in oncology.

NV centers could also be used in heart monitoring using magnetocardiography. It was tested on rats in Japan, as shown in Figure 817 [2608].

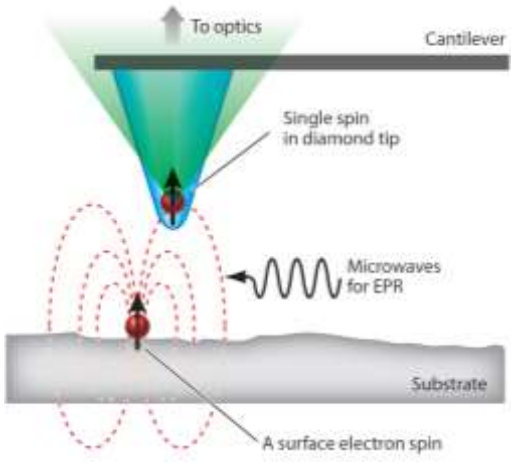


Figure 816: a typical NV center in a diamond tip for various imaging applications. Source: Nitrogen-Vacancy Centers in Diamond: Nanoscale Sensors for Physics and Biology by Romana Schirhagl, Kevin Chang, Michael Loretz and Christian L. Degen, ETH Zurich, 2014 (27 pages).

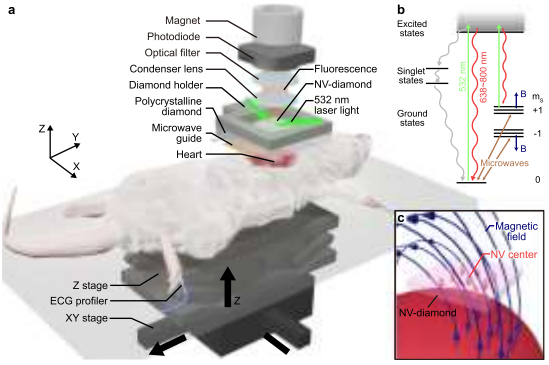


Figure 817: NV center based magnetocardiography experiment on rats. Source: Millimetre-scale magnetocardiography of living rats with thoracotomy by Keigo Arai et al, Nature Communications Physics, August 2022 (10 pages).

[2603] See Microwave Device Characterization Using a Widefield Diamond Microscope, 2018 (10 pages) which involves in particular the LSPM of Paris.

[2604] See A fluorescent nanodiamond foundation for quantum sensing in cells, 2018 (147 pages) which discusses microscopy of living cells.

[2605] See Diamond magnetic microscopy of malarial hemozoin nanocrystals by Ilja Fescenko et al, September 2018 (17 pages),

[2606] See Nanodiamonds enable adaptive-optics enhanced, super-resolution, two-photon excitation microscopy, 2019 (7 pages).

[2607] See Enhanced widefield quantum sensing with nitrogen-vacancy ensembles using diamond nanopillar arrays by D. J. McCloskey, 2019 (7 pages). The NV centers matrices are 100 µm wide. The illustration comes from other work published in 2013, cited in the conference Magnetic imaging using NV-diamond: techniques & applications by Ronald Walsworth, 2015 (51 min). Notably Optical magnetic imaging of living cells, Le Sage et al, Nature, 2013 (11 pages). See also Principles and Techniques of the Quantum Diamond Microscope by Edlyn V. Levine et al, 2019 (47 pages) and Atomic Scale Magnetic Sensing and Imaging Based on Diamond NV Centers by Myeongwon Lee et al, 2019 (17 pages).

[2608] See Millimetre-scale magnetocardiography of living rats with thoracotomy by Keigo Arai et al, Nature Communications Physics, August 2022 (10 pages).

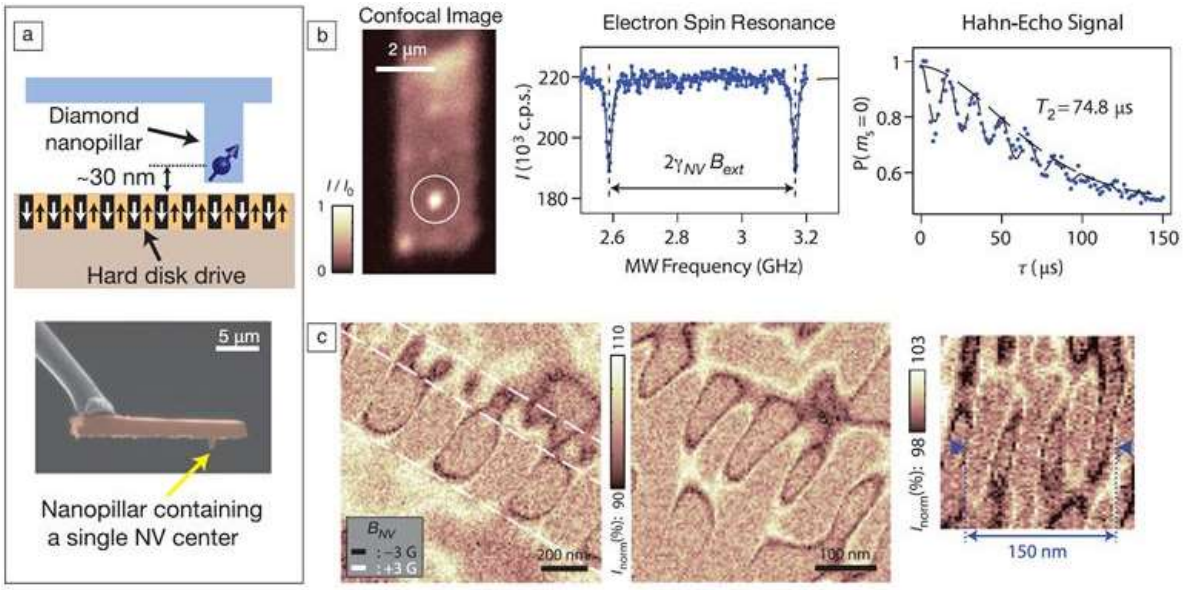


Figure 4. (a) Schematic of a monolithic diamond nanopillar probe (top) and representative SEM image of the nanopillar probe (bottom). (b) Characteristics of a nanopillar probe device. Confocal image of the device (left) clearly shows a localized fluorescence spot from a single NV center at the position of the nanopillar. Electron spin resonance (middle) was acquired with an enhanced fluorescence of 220,000 photons/sec. The coherence time of the measured Hahn-echo signal (right) is 74.8 µs, an order of magnitude longer than a typical Hahn-echo coherence time of commercial diamond nanocrystals (~5 µs). (c) Magnetic images of a hard disk drive acquired by the nanopillar probe. Alternating magnetic bits were imaged with varying sizes down to 25 nm (right), indicating the distance between a single NV center at the probe and the hard disk sample is roughly within 25 nm. Adapted with permission from Reference 19. © 2012 Nature Publishing Group.

Figure 818: Source: Nitrogen-Vacancy Centers in Diamond: Nanoscale Sensors for Physics and Biology by Romana Schirhagl, Kevin Chang, Michael Loretz and Christian L. Degen, ETH Zurich, 2014 (27 pages).

The European Quantum Flagship includes **MetaboliQs** (Germany, €6.7M), a diamond-based nuclear magnetic resonance cardiac medical imaging project. It also detects atrial fibrillation, a common cardiac pathology, with a rubidium-based atomic magnetometer[2609]. Another Flagship project, **PhoG** (United Kingdom, €2.6M) or Sub-Poissonian Photon Gun by Coherent Diffusive Photonics, is about creating stable light sources for various applications, particularly in quantum sensing. It involves researchers from Belarus, Germany and Switzerland.

Optically-pumped magnetometers (OPMs) are scalar-type quantum sensors enabling the measurement of very weak magnetic fields and based on the Zeeman effect[2610]. These sensors have emerged in the 1970s and expanded since the 2000s thanks to a better sensitivity, on par with SQUIDs.

One of their main use case is MEG (magneto-encephalography) to examine brain activity[2611] but it can also be used for materials inspections[2612]. OPMs are competing with MRI and NMR imaging systems. They are more lightweight, can be wearable, and don't require any cryogeny like with MRIs that are based on SQUIDs. OPMs can for example help track some neurodegenerative diseases like dementia, Alzheimer's and Parkinson's with tracking patients' brain waves and how their change over time[2613].

OPMs principle of operation is rather simple. A small laser beam which can be a vertical-cavity surface emitting lasers (VCSEL) illuminates a heated alkali atoms vapor (rubidium, cesium or potassium) trapped in a millimeter-scale glass cell whose size determines the sensor spatial resolution.

[2609] See New quantum technology could help diagnose and treat heart condition, March 2020.

[2610] See the review paper Optical magnetometry by Dimitry Budker and Michael Romalis, Berkeley, Nature Physics, 2007 (8 pages).

[2611] See Optically pumped magnetometers: From quantum origins to multi-channel magnetoencephalography by Tim M. Tierney et al, 2019 (11 pages).

[2612] See Optically Pumped Magnetometer Measuring Fatigue-Induced Damage in Steel by Peter A. Koss et al, 2022 (11 pages).

[2613] See Improved spatio-temporal measurements of visually evoked fields using optically-pumped magnetometers by Aikaterini Gialopsou et al, Nature Scientific Reports, November 2021 (11 pages).

The atoms nuclear and electron spin are influenced by the ambient magnetic field, which changes the vapor optical properties that will absorb more or less light depending on the probed magnetic field. Light is then measured by a photodetector after traversing a polarizing beam splitter[2614].

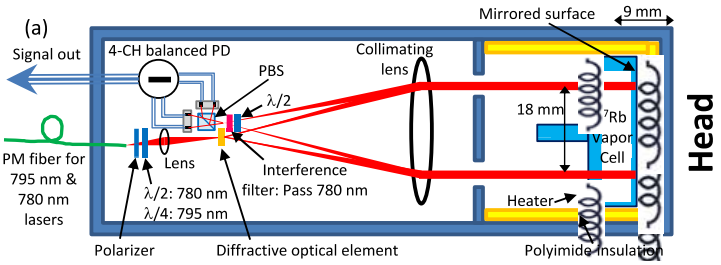


Figure 819: Source: Four-channel optically pumped atomic magnetometer for magnetoencephalography by Anthony P. Colombo et al, 2016 (15 pages).

Other quantum optical imaging techniques using **laser interferometry** make it possible to examine molecules at the atomic level in their environment and not in a vacuum and cryogenic cold[2615].

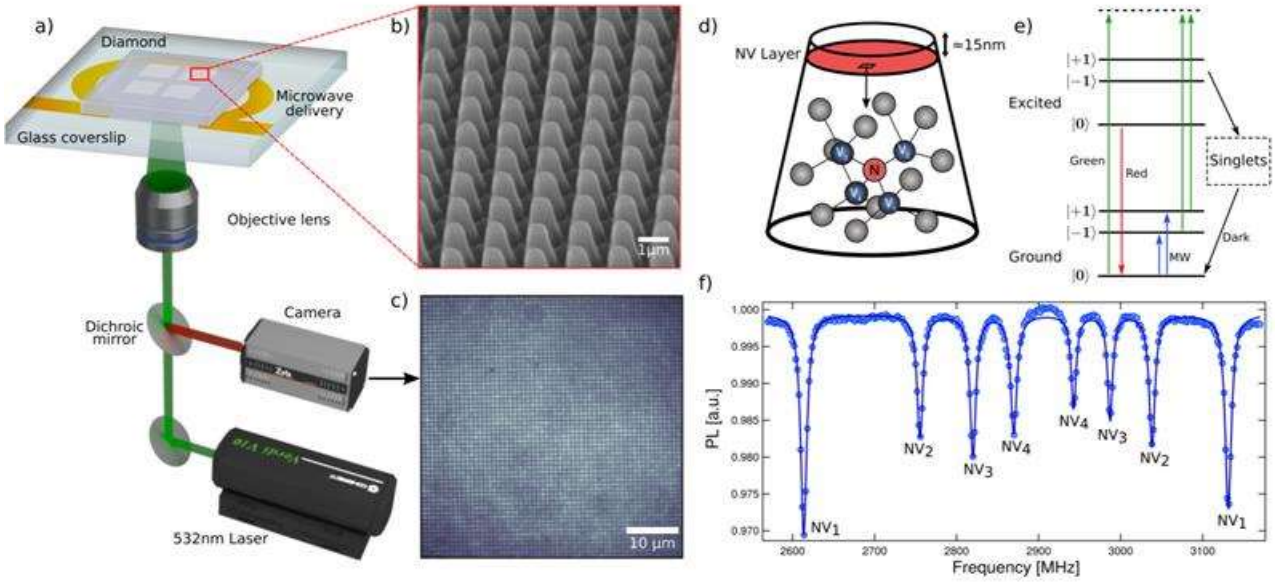


Figure 820: a widefield array of NV centers to improve their sensitivity, developed in Australia. Source: Enhanced widefield quantum sensing with nitrogen-vacancy ensembles using diamond nanopillar arrays by D. J. McCloskey, 2019 (7 pages).

The China laboratory of Jian-Wei Pan has developed a camera that analyzes the reflection of a single photon per pixel on the object to be observed. This is associated with algorithms filtering out the noise. Imaging is done in the infrared at 1550 nm and with polarized photons. This could be integrated in observation satellites[2616].

There is also a broad field of imaging that can be implemented with free electrons illumination and nanophotonics but it is at best in type I quantum sensors[2617].

[2614] See Four-channel optically pumped atomic magnetometer for magnetoencephalography by Anthony P. Colombo et al, 2016 (15 pages).

[2615] See An Entanglement-Enhanced Microscope by Takafumi Ono, Ryo Okamoto, Shigeki Takeuchi, 2014 (8 pages).

[2616] See A new camera can photograph you from 45 kilometers away, May 2019 which refers to Single-photon computational 3D imaging at 45 km by Zheng-Ping Li et al, April 2019 (22 pages). And the presentation Single Photon LiDAR by Feihu Xu, June 2019 (25 slides).

[2617] See the review paper Free-electron-light interactions in nanophotonics by Charles Roques-Carmes, August 2022 (34 pages). **Astrahl** (2022, USA) is a startup created out of the MIT which creates nanophotonics imaging systems based on free electrons scintillation. See A framework for scintillation in nanophotonics by Charles Roques-Carmes et al, Science, February 2022 (14 pages).

QLM Technology (UK, $14,64M) developed a "Quantum Gas Imaging Lidar", a quantum magnetometer solution that detects methane leaks in pipelines up to 100 meters away. The measuring system weighing a few kg can be embarked in a large drone flying at 50 km/h. They use a laser that illuminates a gaseous medium of variable opacity and a photodetector.

IDQ is involved in the creation of the solution at the LiDAR level. Their solution will be embedded in "Schlumberger End-to-end Emissions Solutions" (SEES), a product line that detects and eliminates oil and gas industry's polluting methane and flaring emissions. Their "Quantum Gas Imaging Lidar" will be embedded in "Schlumberger End-to-end Emissions Solutions" (SEES), a product line that detects and eliminates oil and gas industry's polluting methane and flaring emissions.

Figure 821: an airborne LIDAR to detect gas leaks.

SeeDevices (2017, USA) develops a quantum imaging system, the PAT-PD (Photon Assisted Tunneling Photo Detector), which exceeds the performance of traditional CMOS imagers.

This imager contains photosites using the tunneling effect that can detect single photons in a wide range of wavelengths from near infrared (1800 nm) to ultraviolet (up to UVA1, at 350 nm). This can be used for seeing in the dark and for medical imaging, like for detecting blood vessels in the infrared range.

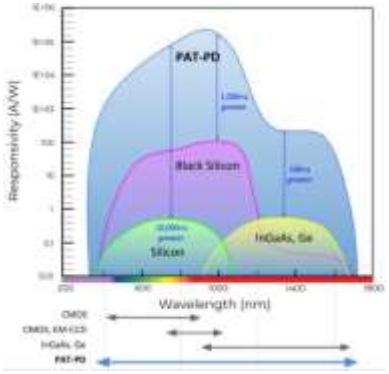


Figure 822: SeeDevice covered wavelengths.

QDTI (2012, USA) is the only known startup initially engaged in the development of a quantum computer based on NV Centers. Created by a team from Harvard University, it is logically based in Boston.

The startup is now focused mainly on medical imaging systems also using these NV centers, with the creation of precision magnetometers combined with MRI and immunological tests.

Nvision Imaging (2015, Germany) is developing an NV centers-based MRI medical imaging solution.

SBQuantum (2019, Canada) also known as SBTech and Shine Bright Technologies develops NV centers-based quantum magnetometers. They target the automotive market but are also working on integrating their technology into Cubesat-type satellites. It is also a startup coming from the Institut Quantique from the University of Sherbrooke.

They have developed a tri-axial version of their system that measures magnetism in the three X, Y and Z axis. Research on this product was funded by the NIH (National Health Institute). The product is mainly targeting magnetoencephalography (MEG) brain imaging.

Chipiron (2020, France) develops a portable and helium-free 2D and 3D MRI system using stacked SQUIDs quantum detectors (superconducting / Josephson effect based). The startup created by Dimitri Labat and Evan Kervella is first targeting osteoporosis and brain diagnosis. The product is to be sold by 2024[2618].

Qnami (2017, Switzerland, $7.3M) is a spin-off from the Quantum Metrology Research Laboratory at the University of Basel. Among other things, they produce artificial diamonds for various photonics applications.

Their targeted first the quantum sensing market with their Quantilever MX nano-diamonds probes.

They then launched in 2019 the ProteusQ range of NV center confocal microscopes, used to analyze ferromagnetic materials, based on the Quantilever probe.

Quantonation and Runa capital are among their investors. And one of the co-founders and the CEO, Mathieu Munsch, came from Grenoble Phelma and worked at the CEA in Grenoble and did his PhD at CNRS Institut Néel.

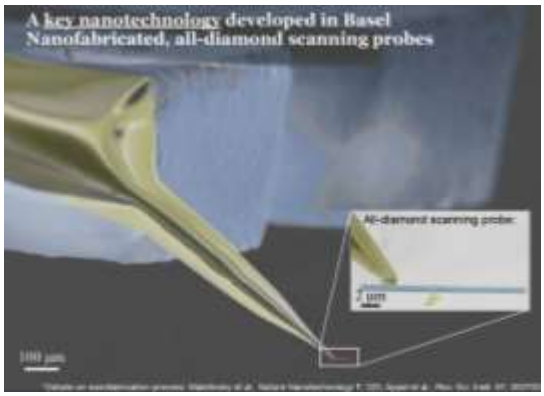


Figure 823: Qnami NV center based imaging system.

Mag4Health (2021, France) is a spin-off from CEA-Leti who develops a helium optically-pumped magnetometer based magnetoencephalography (MEG) system, working at room temperature[2619].

It is using quantum sensors that were developed at CEA-Leti. These record the brain's electromagnetic activity in real time, helping neuronal diseases diagnosis. Mag4Health MEGs are much lighter (about 150 kg) than classical systems using large superconducting magnets (5 tons).

QuSpin (2012, USA) is proposing an optical magnetometer (OPM) for neuroimagery.

Siloton (2020, UK, £470K) is developing optical coherence tomography (OCT) solutions for the assessment of age-related macular degeneration.

The company is the first investment from the Quantum Exponential Group launched by Steven Metcalfe. Their chip devices are designed by VLC Photonics in Spain and manufactured by Ligentec in Switzerland. OCT uses low-coherence light to capture micrometer-resolution, 2- and 3-dimensional images from within optical scattering media like the retina. It is also used in nondestructive testing (NDT) in the industry. It makes use of low-coherence interferometry with near-infrared light that easily penetrate the inspected medium. It probably belongs to Type I quantum sensing.

[2618] See Chipiron Ultra-low field MRI with SQUID detection by Dimitri Labat, February 2022 (13 pages).

[2619] See Performance Analysis of Optically Pumped 4He Magnetometers vs. Conventional SQUIDs: From Adult to Infant Head Models by Saeed Zahran et al, Mag4Health, Inserm and CEA, April 2022 (18 pages).

Quantum imaging could also use the curious technique of ghost imaging or quantum phantom imaging. It exists in many variations. The first one used a generator of infrared photons in 1995[2620]. One half of the photons illuminates the object and the other half a photo sensor, by crossing an optical delay line[2621]. The photons illuminating the object are entangled with those illuminating the camera, which has not seen the object at all! The obtained image is very noisy and requires some appropriate processing.

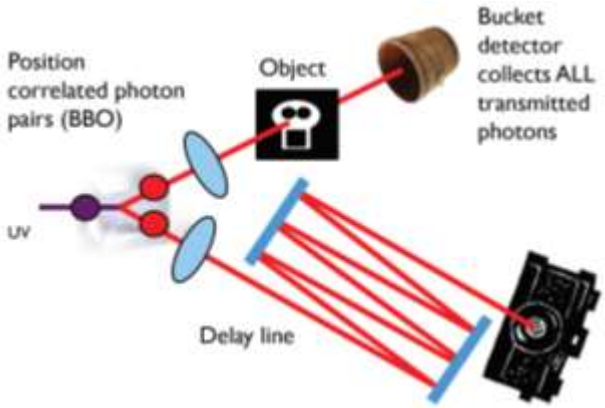


Figure 824: ghost imaging principle. Source: An introduction to ghost imaging: quantum and classical by Miles Padgett and Robert Boyd, 2016 (10 pages)

What is the purpose of this? Mainly to analyze objects with a very low photon number to avoid that they modify the object to be analyzed. This can be interesting in microbiology[2622]. The analyzed objects are seemingly always very small[2623].

Other non-quantum techniques use a single-pixel color imager that uses 1300 structured lights per second to illuminate the object for a few seconds, with up to one million iterations. The sensor prototyped at the University of Glasgow in 2013 contains four photodiodes positioned at different locations[2624]. This makes it possible to generate a 3D view of the object.

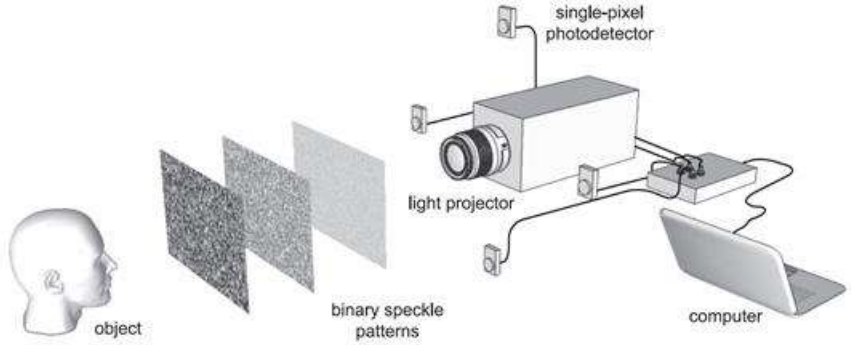


Fig. 1. Experimental setup used for 3D surface reconstructions. The light projector illuminates the object (head) with computer-generated random binary speckle patterns. The light reflected from the object is collected on four spatially separated single-pixel photodetectors. The signals from the photodetectors are measured and used to reconstruct a computational image for each photodetector.

Figure 825: Source: 3D Computational Imaging with Single-Pixel Detectors, 2013 (4 pages).

Finally, quantum imaging can also rely on the illumination of the object by entangled microwaves, using the principle of quantum radar that we will see in a following section. It is interesting for analyzing objects with low reflectivity, which would be useful in medical imaging as well as for creating short-range radars[2625]. Entangled photon can also be used to create holograms, as recently discovered by a team of physicists from the University of Glasgow[2626].

[2620] See Optical imaging by means of two-photon quantum entanglement by Yanhua Shih et al, 1995 (4 pages), University of Maryland. And Observation of two-photon 'ghost' interference and diffraction by Yanhua Shih, 1995 (4 pages).

[2621] See An introduction to ghost imaging: quantum and classical by Miles Padgett and Robert Boyd, 2016 (10 pages) provides a good overview of the subject. See also Quantum Ghost Image Identification with Correlated Photon Pairs, 2010 (4 pages).

[2622] See The Dawn of Quantum Biophotonics by Dmitri Voronine et al, 2016 (30 pages).

[2623] See this panorama of many ghost imaging methods: The promise of quantum imaging by Robert Boyd, 2016 (53 slides).

[2624] See Fast full-color computational imaging with single-pixel detectors by Stephen Welsh et al, 2013 (7 pages). Also seen in 3D Computational Imaging with Single-Pixel Detectors, 2013 (4 pages) which extends this to the capture of 3D objects using four single-pixel sensors. The video projector creates patterns that illuminate the object and alternate with its negative. See finally Imaging with a small number of photons by Peter Morris et al, 2014 (9 pages) and Quantum-inspired computational imaging, 2019 (9 pages).

[2625] See Experimental Microwave Quantum Illumination by S. Barzanjeh, S. Pirandola et al, August 2019.

[2626] See Polarization entanglement-enabled quantum holography by Hugo Defienne et al, Nature, 2021 (31 pages).

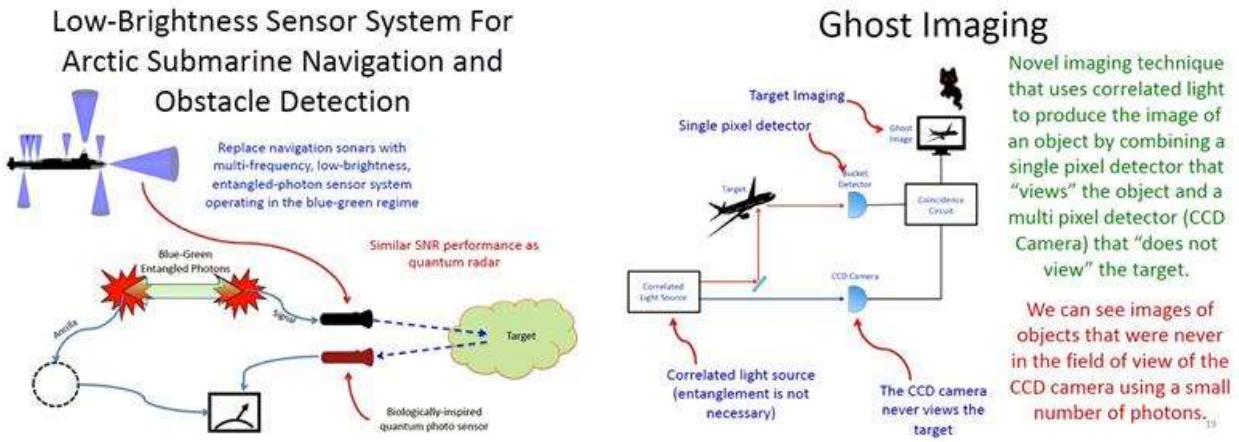


Figure 826: ghost imaging. Source: [The Future of Quantum Sensing & Communications](#) by Marco Lanzagorta of the US Naval Research Laboratory (USA), September 2018 (37 minutes).

Another envisaged technique is the generation of **ghost images**, generated by a system coupling a camera that does not see the object to be captured and a single pixel sensor that sees the object. This kind of technique can be based on the entanglement of photons or of twister pairs of photons in the visible between the two sensors[2627].

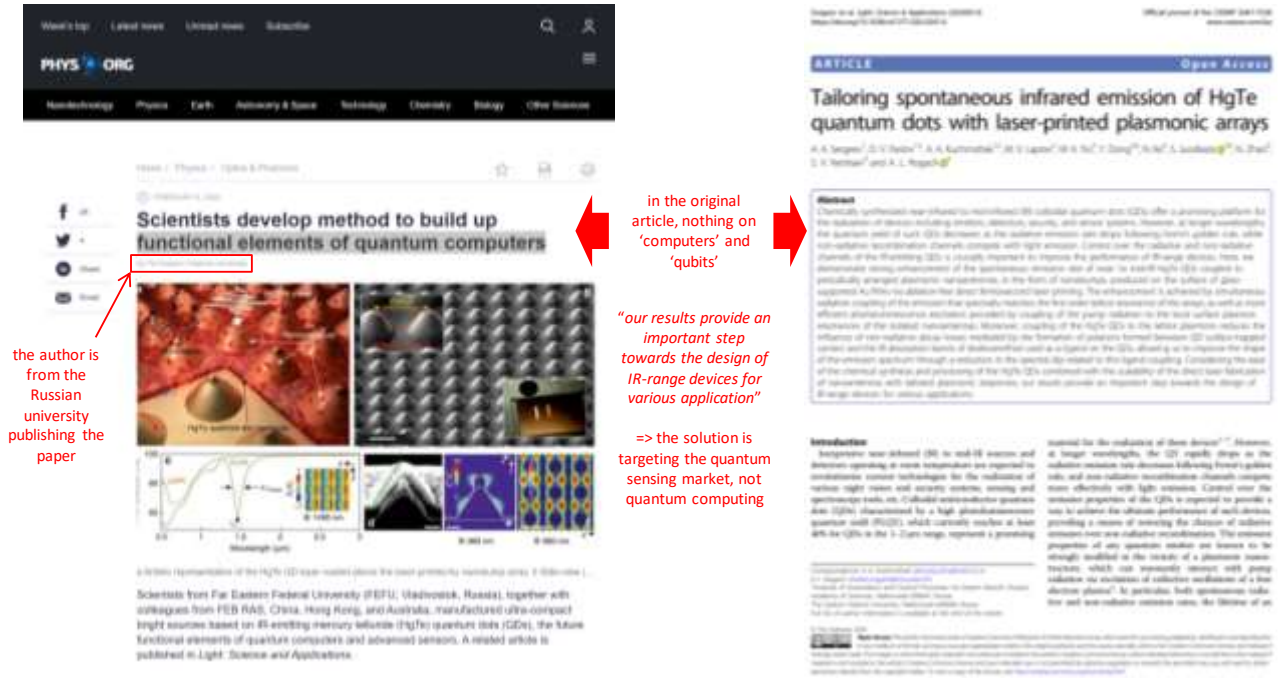


Figure 827: another example of how some research works gets hype to an incredible extend. Source: [Scientists develop method to build up functional elements of quantum computers](#) by Far Eastern Federal University, February 2020 and [Tailoring spontaneous infrared emission of HgTe quantum dots with laser-printed plasmonic arrays](#) by A. A. Sergeev et al, 2020 (10 pages).

Note that the topic of quantum imaging can sometimes be confusing. This is eloquent with this promotion of a particular type of quantum dot, confused with some fancy quantum computing technique (*above in* Figure 827).

[2627] See [An introduction to ghost imaging](#) by Miles John Padgett and Robert W. Boyd, 2017 (11 pages) and [Quantum imaging exploiting twisted photon pairs](#) by Dianzhen Cui et al, June 2022 (6 pages).

And here, it was not a problem with some journalist since the "wrong" article comes from the laboratory promoting the research results[2628].

Quantum pressure sensors

Quantum sensing also works with pressure measurement. Most pressure sensors are type I, not using superposition or entanglement features. They are used to measure pressure in specific conditions.

We have for example very thin ultra-high sensitivity pressure sensors used in medical monitoring[2629], for the measurement of low pressures using light interacting with helium gas and pressure dependent refractive index of helium[2630], high-pressures measurement up to 4 GPa using the shift of the optical spectra of quantum-wells made of III/V GaAs/AlGaAs materials[2631], with quantum dots used to measure pressure in liquids[2632], and with using SiV and GeV color centers to measure ultra-high pressure up to 180 GPa[2633].

Quantum radars and lidars

Quantum radars are slowly emerging from research. The idea initially came from Seth Lloyd from the MIT in 2008 when he devised the concept of quantum illumination[2634]. They rely on photons in the visible spectrum, and in three different ways:

- The radar emits classical photons in the visible and receives the photon reflected by the target. This does not work very well because of clouds and light noise surrounding the object.
- Radar emits photons but uses quantum photo-sensitive sensors to improve its performance. It does not work better enough.
- The radar prepares pairs of entangled photons. One is sent to the target and reflected and the other remains in the radar. The reflected photon is compared with the one that remained in place. As they have a common past, it is possible to sort the photons received by the radar to keep only the photons reflected by the target.

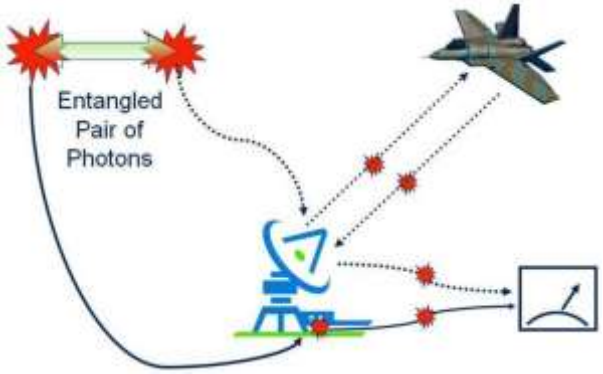


Figure 828: the principle of quantum radar. Source: Quantum Radar by Marco Lanzagorta, 2012 (141 pages).

[2628] See Scientists develop method to build up functional elements of quantum computers by Far Eastern Federal University, February 2020, which refers to Tailoring spontaneous infrared emission of HgTe quantum dots with laser-printed plasmonic arrays by A.A. Sergeev et al, 2020 (10 pages). Quantum dot seems to be more suited for night vision than for quantum computing. It is not a source of single photons. And the words "computer" and "qubit" are absent in the article.

[2629] See Quantum effect-based flexible and transparent pressure sensors with ultrahigh sensitivity and sensing density by Lan Shi et al, Nature Communications, 2020 (9 pages) that is based on thin films and spin-coating with carbon spheres dispersed in polydimethylsiloxane.

[2630] See Quantum-Based Photonic Sensors for Pressure, Vacuum, and Temperature Measurements: A Vison of the Future with NIST on a Chip by J Hendricks et al, NIST, 2021 (4 pages).

[2631] See Quantum-well pressure sensors by Witold Trzeciakowski, 1994.

[2632] See Quantum dots to probe temperature and pressure in highly confined liquids by Sayed M. B. Albahrani et al, RSC Advances, 2018 (12 pages).

[2633] See Optical properties of SiV and GeV color centers in nanodiamonds under hydrostatic pressures up to 180 GPa by Baptiste Vindolet, Jocelyn Achard, Alexandre Tallaire, Jean-François Roch et al, ENS, September 2022 (7 pages).

[2634] See Quantum Radars and Lidars - Concepts, realizations, and perspectives by Gregory Slepyan et al, June 2022 (21 pages) and A Study on Quantum Radar Technology Developments and Design Consideration for its integration by Manoj Mathews, Rowan University in New Jersey, May 2022 (8 pages) are relatively up-to-date theoretical papers on quantum radars.

It is in fact a variant of the third way which is studied[2635]. It consists in converting the photons sent to the target into a radio wave photon, while preserving their quantum state. A conversion of the same kind takes place for the photon remaining in the radar. This allows the radar waves to pass through bad weather, what photons in the visible cannot do.

This technique is expected to improve the accuracy of traditional radars and to improve its resistance to noise and interference. This kind of radar could theoretically detect stealth aircraft, modulo the fact that their flat reflective surfaces reduce their radar signature whatever the radar frequency[2636].

Entangled photons could also make it possible to effectively resist jamming systems. The first concepts saw the light of day in 2015[2637].

China is very interested in this technology and is working hard on it to be able to detect American stealth fighters or bombers like the F-22 and B-2. They announced a test of their first quantum radar in 2016, which was to become a prototype in 2018, produced by the government company **China Electronics Technology Group**[2638], with a range exceeding 100 km.

Other labs and companies are developing such radars, such as the **Institute for Quantum Computing** at the University of Waterloo in Canada[2639]. This project is funded by the Canadian Department of Defense for $2.7M.

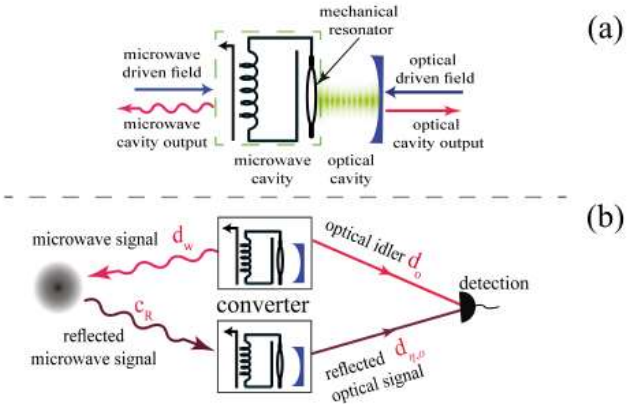


FIG. 1. (a) Schematic of the electro-opto-mechanical (EOM) converter in which driven microwave and optical cavities are coupled by a mechanical resonator. (b) Microwave-optical QI using EOM converters. The transmitter's EOM converter entangles microwave and optical fields. The receiver's EOM converter transforms the returning microwave field to the optical domain while performing a phase-conjugate operation.

Figure 829: converting radar RF waves to/from photons. Source: Microwave Quantum Illumination by Shabir Barzanjeh et al, 2015 (5 pages).

There are also some similar projects in Austria at the Institute of Science and Technology in Klosterneuburg. In the USA, **Lockheed Martin** is also invested in this emerging field. Specialists such as Marco Lanzagorta of the US Naval Research Laboratory believe that QKD satellites launched by the Chinese like Micius would have military applications of this type[2640]. In Europe, the Quantum Flagship **QMiCS** is dedicated to creating quantum microwave technologies operating at the single photon level that could help build quantum radars.

[2635] Another scenario proposes to use microwaves entanglement and a dual-receptor scheme to improve the angular detection of a target, in Entanglement-assisted multi-aperture pulse-compression radar for angle resolving detection by Bo-Han Wu et al, University of Arizona, Jul 2022 (18 pages).

[2636] See Can quantum mechanics improve radar technology? by Giacomo Sorelli and Nicolas Treps, November 2020. Which was maybe inspired by Quantum Flashlight Pierces the Darkness With a Few Percent as Many Photons by Adrian Cho, 2020.

[2637] See Focus: Quantum Mechanics Could Improve Radar, 2015, Microwave Quantum Illumination by Shabir Barzanjeh et al, 2015 (5 pages) and Enhanced Sensitivity of Photodetection via Quantum Illumination by Seth Lloyd, 2018 (4 pages).

[2638] See China's claim of developing "quantum radar" for detecting stealth planes: beyond skepticism by Ashish Gupta, 2016 (4 pages) and The US and China are in a quantum arms race that will transform warfare by Martin Giles, MIT Technology Review, January 2019. Some scientists, "under the radar", find that quantum radars features are overstated.

[2639] See Quantum radar will expose stealth aircraft, April 2018.

[2640] See The Future of Quantum Sensing & Communications by Marco Lanzagorta of the US Naval Research Laboratory (USA), September 2018 (37 minutes). He is the author of the book Quantum Radar by Marco Lanzagorta, 2012 (141 pages) which has been translated into Chinese by China, and officially bought the rights.

But quantum radars are still very theoretical devices[2641] that are currently plagued by photon losses, noise and detection issues[2642].

This technology could however be used in **LiDARs** to verify that the inbound photons correspond to those emitted by its own laser, avoiding unwanted optical interference from other LiDARs. Without malicious interference, this will be very useful when many autonomous vehicles equipped with LiDARs will have to coexist on the road[2643]. Quantum LiDARs can also have an improve resolution[2644]. Single-photon LiDARs could be used for remote wind detection at high resolution. It has been developed in China since 2014 and is used in transportable radars, including UAVs[2645].

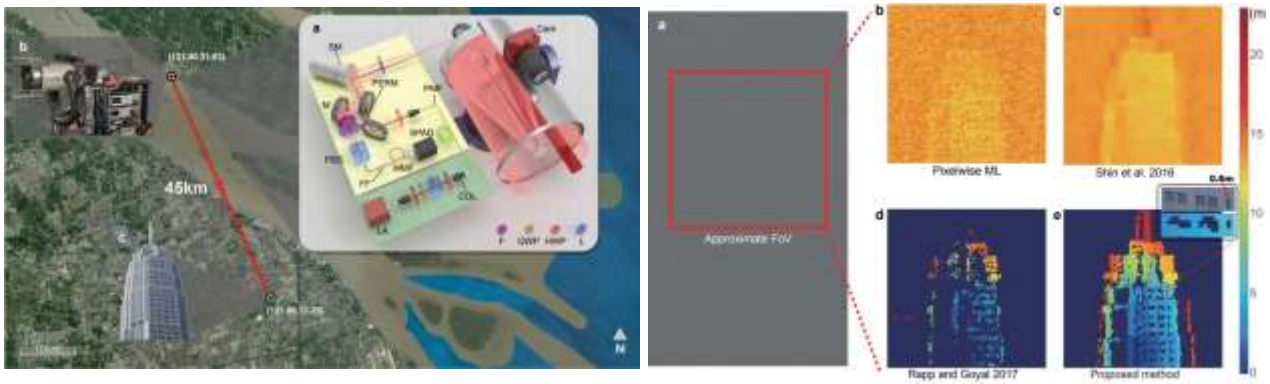


Figure 830: Source: Single Photon LiDAR by Feihu Xu, June 2019 (25 slides).

In a domain close to radar, **quantum sonars** could also emerge, so to speak. They use photons in the blue-green zone of the visible spectrum and would be usable for navigation in the Arctic Ocean. It would be a kind of quantum LiDAR. These systems could also implement optical communication with submarines via satellite, to replace radio waves that do not penetrate underwater well and are exploitable for very low-speed links.

On the other hand, one day, it may be necessary to find countermeasures against "quantum" coatings that allow the infrared signature of objects to be removed or reduced[2646].

Quantum chemical sensors

Quantum sensing is also applicable with chemical sensors used to analyze the chemical composition of various materials and substances. It is commonly used with optical interferometers[2647].

Many such solutions could use NV centers, like:

- The detection of paramagnetic species in biological samples using a fiber equipped with an NV center detection probe[2648].

[2641] Like for example in Quantum-Enhanced Doppler Radar/Lidar by Maximilian Reichert et al, March 2022 (23 pages).

[2642] See Detecting a target with quantum entanglement by Giacomo Sorelli, Nicolas Treps, Frédéric Grosshans and Fabrice Boust, May 2020 (30 pages).

[2643] This approach has been studied since at least 2009. See Quantum Lidar - Remote Sensing at the Ultimate Limit, 2009 (97 pages).

[2644] See Two-photon interference LiDAR imaging by Robbie Murray and Ashley Lyons, 2022 (7 pages).

[2645] See Single-Photon Lidar for atmospheric detection by Haiyun Xia et al, June 2019 (22 slides).

[2646] See Camouflage made of quantum material could hide you from infrared cameras by Kayla Wiles, December 2019 which refers to Temperature-independent thermal radiation by Alireza Shahsaf et al, September 2019 (17 pages).

[2647] See Quantum Optical Technologies for Metrology, Sensing, and Imaging by Jonathan Dowling, 2014 (20 slides) and 12 pages, Advanced Micro- and Nano-Gas Sensor Technology: A Review by Haleh Nazemi et al, 2019 (23 pages).

[2648] See Nanodiamonds based optical-fiber quantum probe for magnetic field and biological sensing by Yaofei Chen et al, February 2022 (21 pages).

- A concentration sensors using NV center to detect electrochemical signals emerging from an electrolyte solution, and using the inhomogeneous dephasing rate of the electron spin of the NV center ($1/T_2^*$) as a signal[2649]. It is still theoretical work.
- Another theoretical NV center sensor, dedicated to the fast, cheap and low error (<1%) detection of the covid virus in biological samples. The NV sensor would be coated with cationic polymers such as polyethyleneimine (PEI), which can form reversible complexes with viral complementary DNA sequences. The detection is fairly indirect. A complicated biological reaction creates a RNA compound which diffuses in the solution, increasing the distance between magnetic molecules and the nanodiamond. The NV centers then senses less magnetic noise and has a longer T_1 time, which turns into a larger fluorescence intensity[2650].
- Various quantum sensing techniques, again, including NV centers, could help detect various breed of organic molecules[2651].

The University of Glasgow has developed and sells under license **IndiPIX**, an improved and simplified ambient temperature mid-wave infrared (MWIR) imager using indium antimonide (InSb) photodiodes on gallium arsenide (GaAs) transistors. It can detect outdoor gas leaks and plumes, mitigating explosion risks and reduce environmental impact[2652].

Ultracold chemical reactions could be used in cold atom sensors to detect very weak signals like in dark matter detection[2653].

Oxford HighQ (2017, UK) is a spin-off from the University of Oxford developing chemical and nanoparticles sensors using optical microcavities.

Entanglement Technologies (2010, USA) is a spin-off of Stanford and Caltech.

It sells the AROMA (Autonomous Rugged Optical Multigas Analyzer) quantum gas detector that uses lasers and optical resonators similar to those used to detect gravitational waves in the LIGO, with a spectroscopy technique (CRDS: Cavity Ring-Down Spectroscopy). It allows the detection of dangerous gases in industry, especially in the extraction of fossil fuels. They were funded by EDF, via their Environmental Defense Fund.

Figure 831: Entanglement Technologies AROMA.

Quantum NEMS and MEMS

Nano or micro electromechanical structures are widely used in long-connected objects, such as accelerometers. They use many quantum phenomena, notably photonics-based, with mechanical resonators whose motion is analyzed by lasers and diodes.

[2649] See Sensing electrochemical signals using a nitrogen-vacancy center in diamond by Hossein T. Dinani et al, February 2021 (17 pages).

[2650] See SARS-CoV-2 Quantum Sensor Based on Nitrogen-Vacancy Centers in Diamond by Changhao L et al, University of Waterloo and MIT, December 2021 (14 pages).

[2651] See A molecular approach to quantum sensing by Chung-Jui Yu et al, April 2021 (12 pages).

[2652] See IndiPIX: Paving the way towards compact, portable, and cost-effective mid-wave infrared systems imaging systems, University of Glasgow (7 pages).

[2653] See Quantum metrology with ultracold chemical reactions by Seong-Ho Shinn et al, August 2022 (28 pages).

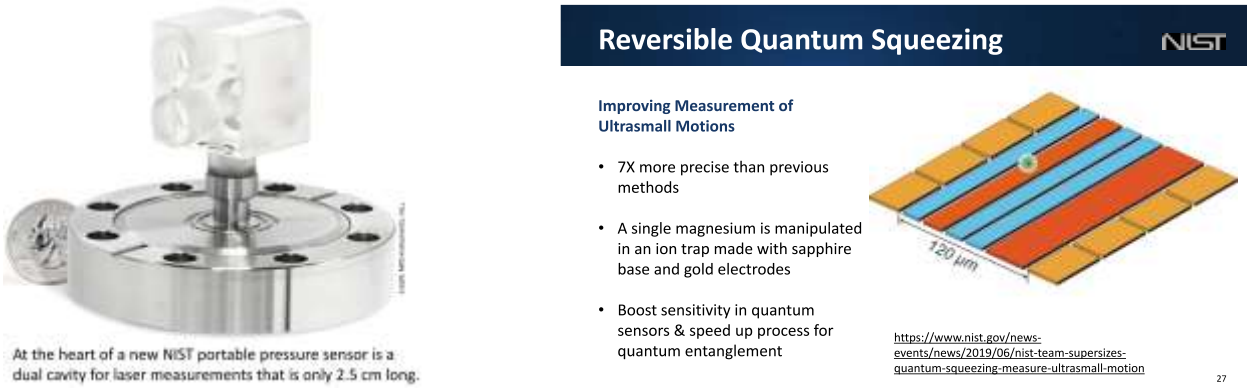


Figure 832: quantum pressure sensors and quantum motion sensors. Sources: FLOC Takes Flight: First Portable Prototype of Photonic Pressure Sensor, February 2019 and Quantum Information Science & NIST - Advancing QIS Technologies for Economic Impact, 2019 (39 slides).

They are found in quantum pressure sensors[2654] and motion detectors, both from NIST (*in* Figure 832[2655]). Other sensors are used to detect electrical resistance, temperature, mass and force, vacuum or voltage[2656] .

Finally, let's mention the European Quantum Flagship project **macQsimal** (Switzerland, €10.2M) or "Miniature Atomic vapor-Cells Quantum devices for SensIng and Metrology Applications", for the creation of quantum sensors aimed at the market of autonomous vehicle piloting and for medical imaging. This includes the creation of atomic clocks, gyroscopes, magnetometers, imaging systems using microwaves and electromagnetic fields in the tera-Hertz waves as well as gas detectors. In short, a fairly generalist approach. It is based on the use of cold atom vapor integrated in MEMS, a technique that Thales is also using.

Quantum sensing key takeaways

- Quantum sensing is the most mature and underlooked market of quantum technologies.
- Quantum sensing enables better precision measurement of nearly any physical parameter: time, distance, temperature, movement, acceleration, pressure and gravity, magnetism, light frequency, radio spectrum and matter chemical composition.
- Quantum sensing has been extensively used to update the new metric system put in place in 2019.
- Lasers and the frequency combs technique is used to measure time with extreme precision, beyond atomic cesium clocks. It is based on blocked-mode lasers generating very short pulses, aka femtosecond-lasers.
- The most used quantum sensing technology is based on NV centers. It helps measure variations of magnetism and has applications in many domains like in medical imaging and non-destructive control. Indirectly, measuring magnetism can help measure many other physical parameters like temperature and pressure.
- Another one is cold atoms based interferometry that is implemented in micro-gravimeters, accelerometers and inertial sensors. It can also be used to analyze the radio frequency spectrum.
- China supposedly built some quantum radars using photons entanglement and up/down converts between visible photons and radar frequencies but the real performance of these devices is questionable and is driving a lot of skepticism in the Western world. But the related research is still going on.

[2654] See FLOC Takes Flight: First Portable Prototype of Photonic Pressure Sensor, February 2019.

[2655] See Quantum Information Science & NIST - Advancing QIS Technologies for Economic Impact, 2019 (39 slides).

[2656] See Quantum electro-mechanics: a new quantum technology by Konrad Lehnert from NIST JILA lab (47 slides), From micro to nano-optomechanical systems: light interacting with mechanical resonators by Ivan Favero (45 slides) and Progress of optomechanical micro-nano sensors a review, by Xinmiao Liu et al, 2021 (40 pages).

Quantum technologies around the world

Quantum computing in the broadest sense is a strategic technology domain for various reasons. In cryptography, states sovereignty is at stake with the protection of sensitive communications. Quantum computing has critical applications that will extend the scope of digital computing beyond what is feasible today, particularly in the fields of healthcare, the environment and artificial intelligence.

In terms of maturity, quantum and post-quantum cryptography represent more established fields with economic players and commercial solutions, even if the standardization of post-quantum cryptography is not yet complete. However, it has fewer scientific and engineering unknowns compared to scalable quantum computing.

Quantum computing is much less mature. The feasibility of commercially and useful quantum computers remains an open question. There are significant technological challenges to overcome, including the thorny issue of qubits noise, quantum error correction, and how to scale the number of physical qubits by several orders of magnitude. So, quantum computing is full of scientific and technological uncertainties even before being economical and market ones. How countries deal with that is a good revelator of their innovation and forward-looking culture.

For the time being, fundamental research is mainly funded by governments in most countries, then from very large IT players who entertain many technology bets in parallel (IBM, Google, Microsoft, Intel, Honeywell, Alibaba), and a more or less well-funded startups, mainly in North America (D-Wave, IonQ, Rigetti, PsiQuantum, Xanadu) and, way behind, in Europe (IQM, OQC, Pasqal) and in other regions (SQC in Australia, Quantum Machines in Israel, etc).

The quantum computers software industry is in its infancy. The major players and startups creating quantum computers have all invested the software arena, starting with the low-level supporting tools and sometimes, for developing quantum applications.

Some systems are already available in the cloud, directly or through cloud services provides like Amazon, Microsoft and Google. Most of these and Atos also sell cloud access to classically run quantum emulators. One way of looking at things is coming from **Yuri Alexeev** of the Argonne National Laboratory in the USA, who draws a parallel between the history of quantum computing and that of artificial intelligence and anticipates the arrival of two winters, the first which occurred in the late 1990s, the second he expected in 2020 and the next around 2030[2657].

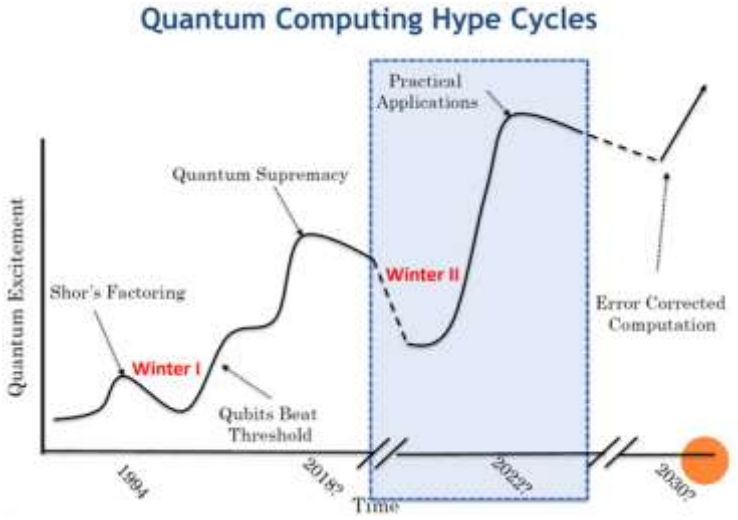


Figure 833: one view of the quantum computing hype cycle. Source: Quantum Computing Trends by Yuri Alexeev, August 2019 (42 slides).

Since this excitement is a somewhat fuzzy wave function and difficult to evaluate, it doesn't mean much. We can however anticipate at least a small winter with the startups of the sector and large customers engagements.

[2657] See Quantum Computing Trends by Yuri Alexeev, August 2019 (42 slides). You can also find an historical comparison with many other technology hypes in Mitigating the quantum hype by Olivier Ezratty, February 2022 (26 pages).

Hardware startups will have a hard time delivering useful machines, while software startups will not have a large enough addressable market due to the lack of hardware. But this will not prevent public research laboratories and large tech companies from doing fundamental and applied research.

Quantum computing startups and SMEs

Mapping these vendors is a bit easier than in other deep techs like in artificial intelligence because there are not so many. There are many methods to inventory worldwide quantum startups and small businesses. I have accounted about 450 such companies, more than the 265 I had in store in September 2020 and their total funding is about $4.7B as of October 2021.

The increment comes mostly from existing quantum enabling technologies companies that I uncovered. I added them when and if I found that they were enabling "second quantum revolution" solutions. As a consequence, metal cutting lasers and classical telecommunications photonics are out!

This ecosystem began to take shape even before quantum computers were working on a small scale. It is fascinating to discover startups that make long-term bets, particularly with hardware. Software startups rely on a still limited hardware infrastructure but often reduce their risks by also supporting traditional computing architectures like Nvidia GPGPUs in machine learning. Their customers are large companies who test algorithms on a small scale to get their hands on quantum programming, often on D-Wave annealers and sometimes with IBM who is very pushy in its quantum evangelism efforts. To date, no application seems to have been deployed in production. We are therefore in the field of applied research and small scale prototyping within client companies. The software ecosystem is to be monitored closely. It will probably expand once hardware works on a larger scale, particularly with NISQ computers and quantum simulators[2658].

For their part, quantum cryptography systems are operational and correspond to a very separate market, just like the quantum sensing market that is more mature technologically but still in its infancy.

The stakes for many startups in this field are common with those of deep techs: how to develop real products with economies of scale, how to expand internationally rapidly, how to avoid falling into models that are too "service-oriented" and at last, how to resist what some people are already calling the quantum winter. Enabling technologies niche companies (photon sources, cryostats, ultra-vacuum, various sensors, electronics) can do well by reaching out diversified markets, notably targeting several different branches of research, telecommunications, military or aerospace applications.

Investors

Quantum technologies investments may be impressive for the large rounds like those from PsiQuantum and IonQ and the associated "FOMO" factor ("*fear of missing out"*). But it's still small in volume in the technology sphere. The first investment funds more or less specialized in quantum technologies have already emerged with:

- **Quantonation**, a French seed fund created by Charles Beigbeder and managed by Christophe Jurczak, a physicist who got his PhD with Alain Aspect. They have already invested in over a dozen startups[2659].

[2658] See Some Teams Go For NISQ-y Business Some are NISQ-Averse by Doug Finke, February 2020.

[2659] Quantonation invested in LightOn (France), Spark Lasers (France), which offers laser sources not specifically dedicated to quantum computers, Pasqal (France, cold atoms), Quantum Benchmark (Canada, software), Kets Quantum Security (UK, QKD component), Orca Computing (UK, hardware, photonics-based computing), CryptoNext Security (France, PQC), Qunnect (USA, repeaters for QKD), Quandela (France, photon source), Qubit Pharma (molecular simulation), Qnami (Switzerland, NV center-based metrology), Orca Computing (photon qubits, UK), Foqus (Canada, quantum sensing software), Qu&Co (Netherlands, software), QPhoX (Netherlands, communications between quantum computers), HQS (Germany, software), Qubit Pharmaceuticals (France, software), evolutionQ (Canada, software), Inspek (France, chemical sensors), Multiverse (Spain, software), Pixel Photonics (Germany, single photons detector).

They organize quantum meetups and hackathons in Paris (with **QuantX**, the quantum alumni association from Ecole Polytechnique), the first edition having taken place in October 2018. It participated to the launch **Le Lab Quantique**, which was jointly created with **Bpifrance**. It is federating the country vendor and user quantum ecosystem.

- **Quantum Valley Investments** (QVI), a $100M Canadian investment fund, raised in 2013, dedicated to quantum technologies. Their founders had invested in 1984 in Blackberry / RIM. They do not disclose their investments, except in ISARA Corporation, part of which are spin-offs from the Canadian research laboratory Institute for Quantum Computing at the University of Waterloo in Ontario.
- **Black Quant** (Germany) is a quantum technologies dedicated investment fund created in 2022 by the QBN Network and CM-Equity, an investment company with teams in Germany, Slovenia and Croatia. They don't have any participation as of January 2022.
- **Quantum Exponential** (UK) invested £450K in May 2022 in Universal Quantum who plan to build a million qubit quantum computer. It also invested in Arqit, Siloton, Aegiq,
- **Quantum Ventures** is a quantum investment company launched in 2016. Its "Quantum Revolution Fund" is managed from London and Switzerland. It aims to raise €100M.
- **Quantum 1 Group** is an American investment fund specializing in quantum technologies since 2015.
- **Summer Capital** is a Dutch investment fund specialized in quantum technologies, data and finance. Their investments include Horizon Quantum Computing, Rigetti and Turing.
- **Parkwalk Advisors** is a British deep tech fund. As of 2021, they have invested in Phasecraft, Quantum Motion Technologies, Riverlane, nu quantum, nu nano and Oxford Quantum Circuits. This fund is part of IP Group Plc since December 2016.
- **Runa Capital**, created by Serguei Beloussov (Russian with a Singapore nationality, founder of Acronis) is an investor in many deep tech startups, including IDQ, Qnami, Qu&Co and Pasqal.
- **Phystech Ventures**, previously Quantum Wave Fund, created by Russians in the Silicon Valley, including Serguei Beloussov, and having already invested in the IDQ and Nano-Meta Technologies. Their fund is not 100% specialized in quantum. They also invest in robotics, drones, sensors and connected objects.
- **Machine Capital**, a UK fund focused on quantum and AI, which has so far invested in **QuantumX Incubator,** an incubator for quantum software projects launched jointly with **Cambridge** startup Quantum **Computing,** which specializes in the development of quantum software, with a 20-week incubation period.
- **SpeedInvest** is an Austrian investment fund specializing in deep tech start-ups, which invests among others in quantum technologies. They invest in seed stage with up to 1M€. They have invested in **QPhoX** and **Kets**.
- **Airbus Ventures** is an investment fund, headquartered in Silicon Valley, that operates independently from the Airbus Group which is one of its limited partners among several others. They invested in QCWare, IonQ, Q-CTRL, C12 and Qunnect.
- **BlackQuantFund** is an investment fund created in Germany by QBN and CM-Equity that is raising 100M€ and invested in seed in Aegiq[2660].

[2660] See QBN and CM-Equity Sets Up €100 Million Quantum Technologies Fund by Matt Swayne, January 2022.

- **2xN** (UK) launched in August 2022 a dedicated $120M fund focused on quantum computing startups with $3M to $5M pre-seed to Series A tickets. It was created by Lars Fjeldsoe-Nielsen and Niels Nielsen. Limited partners include the Danish Growth Fund and some family offices.

You then have generalist funds who invested in one or two startups, like the Canadian pension fund **PSP Investments** that invested in D-Wave with seats in the board, **UVC Partners** who invested in HQS in Germany, **Supernova Invest**, **Elaia Partners** and **Breega Capital** in Alice&Bob in France, **Omnes** in Quandela again in France. And of course, corporate venture funds like **TotalEnergies Ventures** and **Tencent Investments**.

Figure 834: a few of the key investors in quantum technologies. (cc) Olivier Ezratty, 2022.

The Quantum Insider produced in early 2020 an inventory of investors in quantum technologies startups. Here is an excerpt with general and specialized VC investors. It contains a few mistakes such as Worldquant which is positioned as an investor specialized in quantum technologies whereas it is a generalist investment company created in 2007. The use of the word quantum or a piece of quantum is not a guarantee of specialization.

Figure 835: a map of investors in quantum technologies by The Quantum Investor.

We must also describe the **SPAC** funding mechanism that was used by IonQ, Rigetti, D-Wave and Arqit. A SPAC is first an investment fund that is created before it finds where to invest the money[2661]. It plans to invest the money in one company. When the company is found, the SPAC buys shares of the company, usually with other limited partner investors like Corporate venture funds. At last, the SPAC puts the fund on the stock market and is traded with using the acquired company name. The process is a bit complicated. The SPAC business model is fairly unbalanced.

[2661] See What is a SPAC: the step by step process going public, May 2021.

The SPAC fund takes a significant cut of the deal and has a significant upside when the company IPO takes place, whatever the subsequent outcome in the stock market. There were hundreds of SPACs until 2022 but the phenomenon has dried up, particularly with assets reallocations in investors as inflation popped up after the start of the Ukraine war[2662].

IonQ and Rigetti's stock value trended down after their IPO as shown in the charts on the right, due to significant overpromises in their investor pitch decks. D-Wave's IPO in August went well but we'll have to wait and observe the stock value after a couple quarterly reports! But fears of a quantum investment winter are not limited to these ill-fated SPACs[2663].

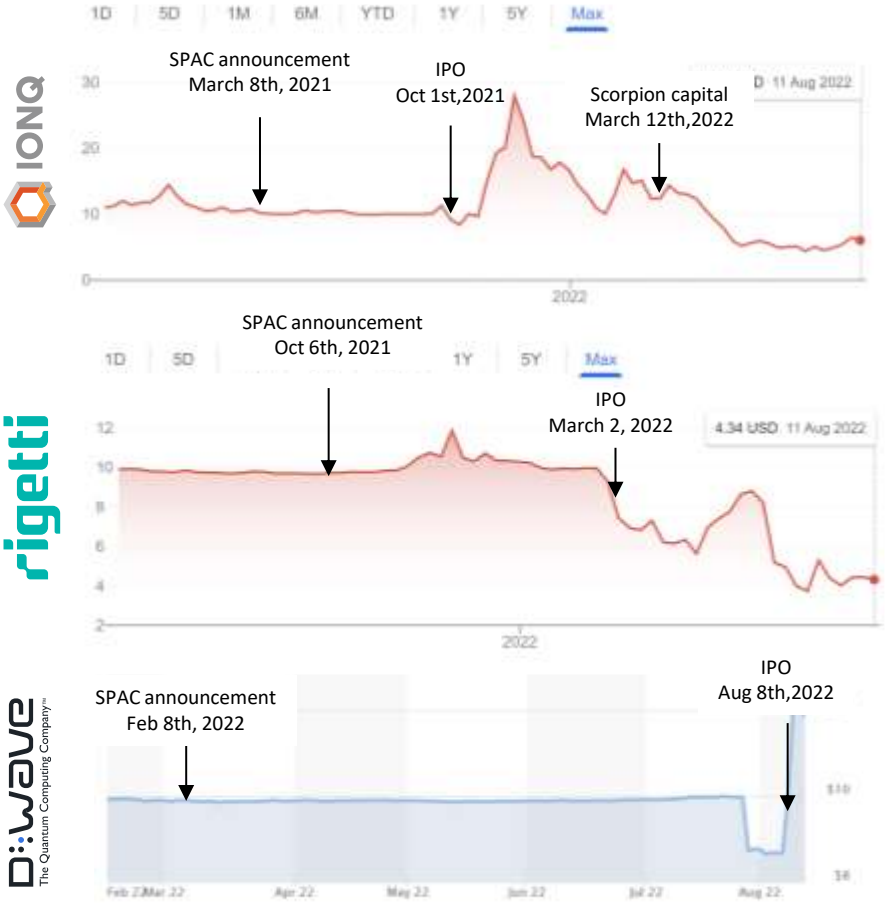


Figure 836: evolution of the value of the SPACs of IonQ, Rigetti and D-Wave. (cc) Olivier Ezratty, August 2022. Source: Google Finance, MarketWatch.

First, we had a sluggish start for 2022 with large fund rounds[2664]. Then, the current post-Covid/Ukraine war recession may drive assets reallocations unfavorable for long-term risky investments[2665]. This explains indirectly why governments and their aggressive national quantum plans find sideways to fund their local startups, like with creating an artificial market with public orders of non-existent or low performance experimental quantum hardware. And I don't account for the crooks in that market like this investment advisor in quantum technologies that selected 5 companies out of which only two happened to be in the quantum business (Rigetti, IonQ)[2666]. What a joke! What is going to happen? I'm not an oracle. Things will probably be tougher for some startups in their various rounds of investment, particularly in series B and C. The winning startups who'll escape the crisis will have good fundamentals: excellent teams, respected roadmap milestones, some IP and preferably some orders and/or revenue.

[2662] See SPACs out, the quantum community react by Karina Robinson, The Quantum Insider, June 2022.

[2663] See Is quantum computing headed for a financial reckoning? by Dan O'Shea, May 2022.

[2664] See Shifting Quantum Investment Dynamics by Russ Fein, The Quantum Leap, July 2022.

[2665] See How the recession will affect quantum tech vendors by André M. König, June 2022.

[2666] See 5 Quantum Computing Stocks to Watch towards 2022, December 2021.

Now, looking at the current revenue streams of these three companies, you find out that Rigetti, IonQ and D-Wave made respectively $2.1M, $2.6M and $1.3M in Q2 2022, probably with selling computing time in the cloud either directly or through cloud vendors like AWS, Microsoft and Google. Their cash burn rate is about $38M, $37M and $44M per year which corresponds to 4.8 and 10 years of "air supply" for Rigetti and IonQ. It is unclear for D-Wave when looking at their accounting[2667].

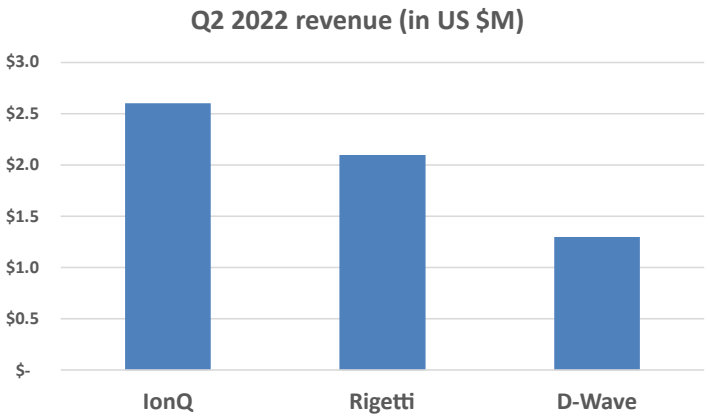


Figure 837: IonQ, Rigetti and D-Wave Q2 2022 quarterly revenue. Source: their quarterly reports.

Startup maps

An inventory of quantum startups is available on the Quantum Computing Report website. It allowed me initially to identify a good number of the startups mentioned in this section. Some startups broadcast so little information about them that one may wonder if they are not scams. This lack of communication may simply be due to the fact that many creators may be uncommunicative researchers, that they are poorly funded, and that their projects have business prospects that are too remote and risky. Also, many times, they are so early-stage that they can't talk about anything that would drive interest, such as "*I have two functioning qubits*".

Many of the startups mentioned here are not yet in the "pure" form of the startupian model, i.e. they are far from having a scalable model or even, just a product. They are often either industrial small businesses targeting very low-volume niche markets, or startups where the scientific and technological risk is still very high before they can sell anything. And often, with a combination of both. They can then finance themselves with contract research and various consulting services for large companies or public institutions.

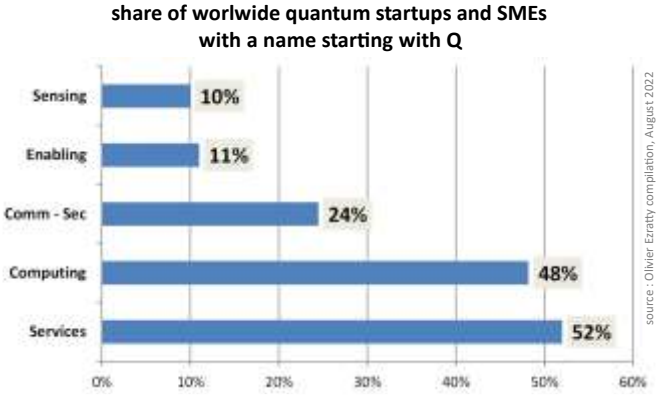


Figure 838: fun fact: in some fields like telecommunications, cryptography and consulting services, quantum startups branding shows a lack of creativity with many names starting with a Q.

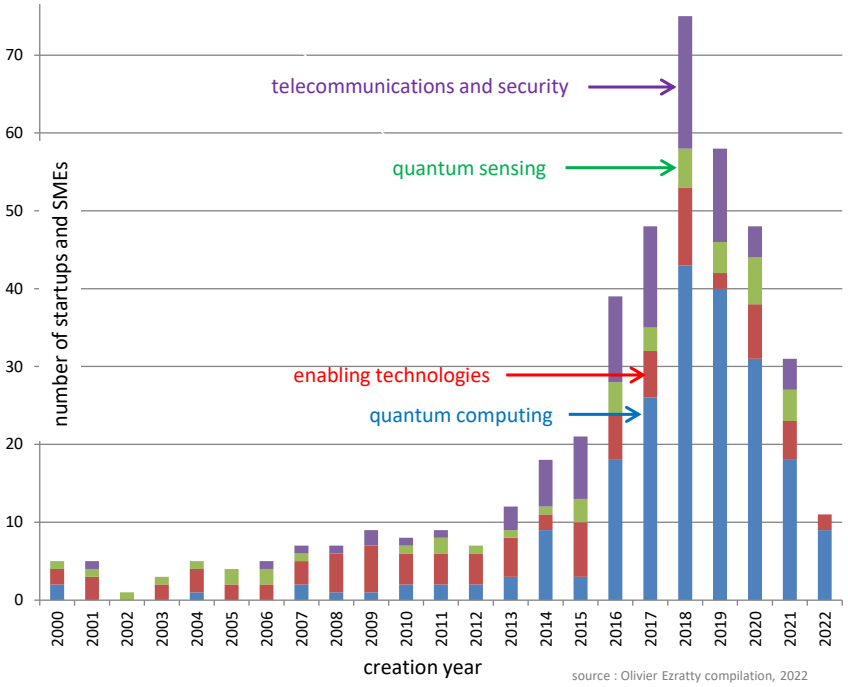
In the vast majority of cases, I relied on public information available on the Internet to describe what these startups do in the various parts of this book. One way to find out what these startups do is to identify their founders, if they are researchers, and find their original laboratories, their past scientific publications, and their PhD thesis if it is available. Finally, search for possible patents filed by the startups. This is technology intelligence using open sourced information (OSINT). Of course, you can also meet with entrepreneurs, live or distantly.

This mapping also does not include companies that seem to offer only service and consulting in quantum computing, without having their own technology or products. We inventory some of them in an earlier section on Service vendors.

As far as data is concerned, here are some charts extracted from my database of startups and SMBs. The first one provides an indication of the number of startup creations per year. The second provides a breakdown by country.

[2667] Data source: Rigetti Q2 2022 quarterly report, IonQ Q2 2022 quarterly report and D-Wave Q2 2022 quarterly report.

Of course, other sources will publish different charts[2668]! As of October 2022, my database had 552 companies. The difference comes from both new startups and existing companies, mainly in the enabling technologies space, that happen to target "second quantum revolution" technologies use cases. The selection is sometimes not obvious, like in the very large photonics supplier sector. At least you can sort things out with these company creation date as shown in Figure 839.



Country	Computing	Enabling	Sensing	Services	Comm - Sec	Total
USA	58	40	19	4	25	146
UK	20	11	8	5	18	62
France	10	27	10	4	5	56
Canada	31	6	4		11	52
Germany	16	19	4	1	6	46
India	11			3	4	18
Switzerland	3	8	1		4	16
Netherlands	7	4	1	1	2	15
China	6		1		6	13
Japan	10	2		1		13
Spain	7	3			1	11
Finland	4	3		2	2	11
Israel	4	2	2		3	11
Australia	6		3	1	1	11
Denmark	3	6			1	10
Singapore	5	1	1	1	1	9
Italy	2	3	1	1		7
Sweden	2	4				6
Russia		2			4	6
Poland	3				2	5
Austria	3				1	4
Turkey		1	1			2
Bulgaria	1				1	2
Tchekia				1	1	2
Estonia	2					2
UAE	2					2
Greece	2					2
Belgium		1				1
Bielorussia	1					1
South-Korea	1					1
Hong-Kong	1					1
Uruguay	1					1
Taiwan					1	1
Ukraine	1					1
Chile					1	1
Lybia	1					1
Luxembourg		1				1
Norway	1					1
Columbia	1					1
Total	226	144	56	25	101	552

Figure 839: chart of the creation year of small business and startups in "second revolution" quantum technologies. (cc) Olivier Ezratty, August 2022.

Another chart in Figure 840 shows a different breakdown by country that highlights the largest funding. As usual, we see a significant financing gap between North America and Europe. One of the reasons is that European startups were created later or are more traditional small business which don't rely on venture capital for their development[2669]. The other is of course a different access to capital and markets. The size of the US market has always been an advantage for US-born companies although it doesn't prevent some worldwide leaders to emerge elsewhere in the world like ASML or SAP.

60% of worldwide startups funding went to the top seven startups: IonQ, PsiQuantum, Rigetti, D-Wave, Xanadu, Quantinuum all from the USA and Canada, plus Arqit from the UK[2670], while Europe has an equivalent number of companies compared to North America. If there are as many quantum startups and small businesses in mainland Europe than in North America, their visible equity funding represents only 10% of worldwide funding while North American companies got a hefty 70% as of August 2022, but it was 5% a year ago in September 2021. This doesn't include the investments from large IT corporations like IBM, Amazon, Microsoft, Google and Intel.

This funding discrepancy explains for example why PsiQuantum which was created out of UK became a US company. As a result, directly or indirectly, it could raise over $700M which a record to date in the quantum industry.

[2668] See The landscape of the quantum start-up ecosystem by Zeki Can Seskir et al, May and October 2022 (15 pages) that used this book as one source among others to create its own database of quantum companies with a total of 441 companies.

[2669] See New record looms in VC funding of quantum startups by Michel Kurek, September 2020 and The European Quantum Computing Startup Landscape by Alex Kiltz, October 2020.

[2670] Arqit's SPAC funding of $450M was not finalized as of January 2022.

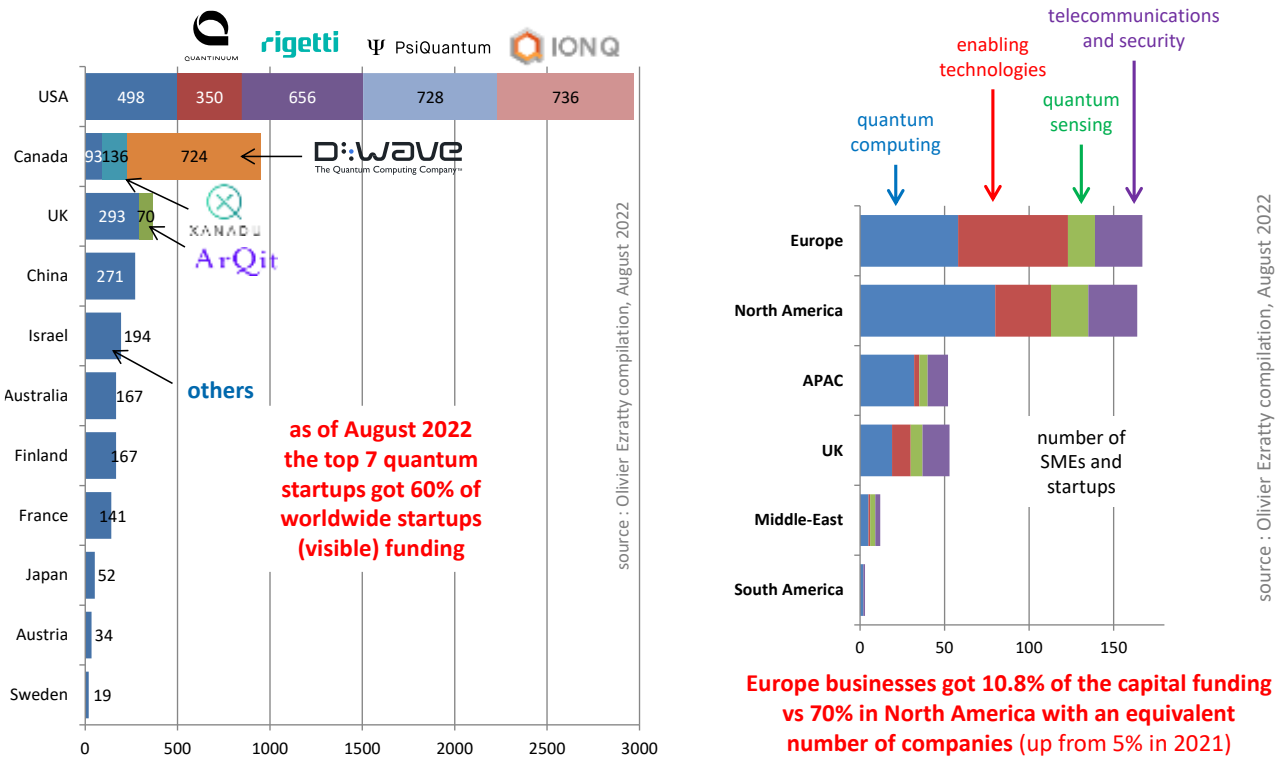


Figure 840: chart showing where the investment money went by country and its concentration. (cc) Olivier Ezratty, 2022.

David Shaw from Fact Based Insight (UK) created a very complete map of all quantum technologies in the global quantum ecosystem chart below[2671]. We cover most of these companies in different parts of this book, split between quantum computing (page 142), enabling technologies (page 464), software (page 740), telecommunication and cryptography (page 859) and sensing (page 875).

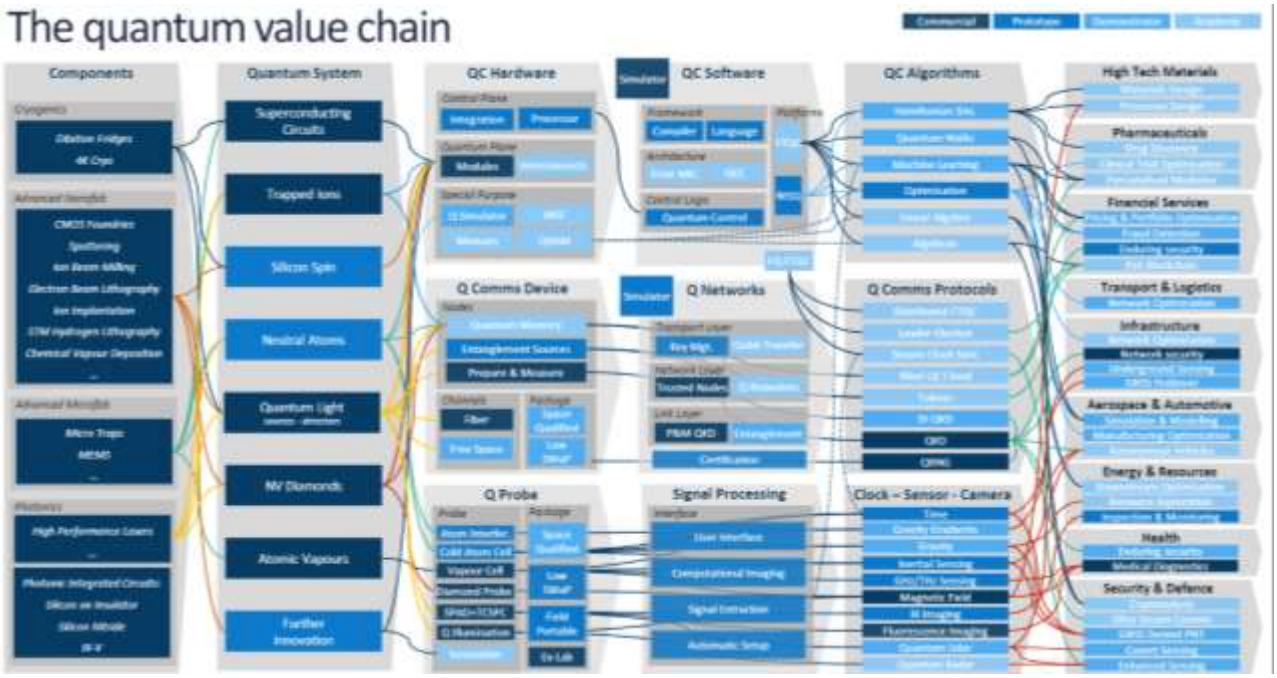


Figure 841: David Shaw's quantum value chain. Source: Quantum Value Chain Overview, by David Shaw, Fact Based Insight, April 2021.

[2671] See Quantum Value Chain Overview, by David Shaw, Fact Based Insight, April 2021.

Quantum Startup incubation and acceleration

There are already a few incubation and acceleration programs for deep tech startups which host quantum startups in the world. One of the most famous is the **Creative Destruction Lab**, based in Toronto and other cities in Canada. **Xanadu** and **North** came out of it. Similarly, **Unit DX** is a deep tech incubator based in Bristol, UK, which started in the biotech industry and also helped some quantum startups[2672]. **Duality** is a quantum dedicated startup accelerator in the USA with a sponsorship from Amazon. **Quantum Startup Foundry** is the University of Maryland accelerator which was completed in 2022 by **Q-Cat** (Quantum Catalyzer), a startup studio.

In France, the **HEC Challenge+** program and the **Deeptech Founder** program created by the team behind the deep tech Hello Tomorrow event, accelerated a big share of France's quantum startups like Quandela, Pasqal and Alice&Bob. To create such acceleration programs, you need to be close to critical mass pool of talents, such as a dynamic academic and research zone.

Disappeared startups

How about startups who disappeared? You would guess that there are many given the technology immaturity of the sector. Well, there aren't so many out of the 300 to 400 hundreds and so created so far.

Quantum Factory (Germany) was closed in January 2021. They were building trapped ions computers. **NextGenQ** (France) was pursuing the same goal and was also closed in 2021. The company had just a founder with not quantum physics skills nor any funding.

SeQureNet (2008-2017, France) was a spin-off of Telecom ParisTech specialized in the distribution of long distance CV-QKDs. It had been funded within the framework of the European research project SECOQC (secure communication based on quantum cryptography). The startup was based on work done by Philippe Grangier's team at the Institute of Optics and the Thales TRT laboratory in Palaiseau. The company closed down in 2017. It had been launched a little too early compared to the maturity of the market.

Black Brane Systems (2016, Canada) was a startup focused on the development of quantum machine learning solutions. They startup as a very "stealthy" company, got some undisclosed funding in 2018 and then closed their business.

We also have acquired startups like **CQC** (Quantinuum in 2021), **Labber Technology** and **Quantum Benchmark** (Keysight, 2020 and 2021), **Muquans** (ixBlue, 2021), **QxBranch** (Rigetti, 2019), **Qu&Co** (merged with Pasqal in 2022) and **Super.tech** (ColdQuanta, 2022). So far, no quantum startup was acquired by a large IT vendor like IBM, Google and Microsoft. But to some extent, the investment of SandboxAQ, a spin-off from Alphabet, in August 2022, is a first[2673].

Global investments

What about global investments in quantum computing? A 2015 McKinsey study provided an overview of investments that likely compiled public research budgets. At that time there were 1500 researchers worldwide with a total budget of $1.5B. This number has since increased much. The USA and China were obviously leading that space. But the distribution of these investments, which probably include both quantum cryptography and quantum computers, is intriguing for other countries. As usual, Europe was fragmented with Germany, France, The Netherlands, Finland, Italy, Spain, the United Kingdom (then, in the European Union) and Switzerland (geographically in Europe). And we have strong quantum countries in other regions like Canada, Japan, Singapore and Australia.

[2672] See Incubators & Accelerators: Launchpads For Quantum Success? by James Dargan, 2020.

[2673] See SandboxAQ Announces a Partnership with evolutionQ as part of its New Strategic Investment Program, August 2022.

Quantum technologies have become a geopolitical issue, almost like nuclear deterrence[2674]. Governments are motivated to invest in quantum for strategic reasons: both in the idea of being able to decrypt existing or past telecommunications in the context of the activities of their intelligence services and to protect their own via quantum or post-quantum cryptography. More than almost any other digital technology, quantum is therefore a tool for the states strategic sovereignty[2675]. The public authorities in these different countries have mobilized in very different ways on quantum. Most developed countries governments coordinate efforts in the quantum field. Plans with up to $2B over 5 or 10 years periods have been announced here and there.

It's still quite difficult to compare these investments between countries and for a couple reasons:

- What is the **existing run-rate investment**? It's sometimes not easy to capture this data, particularly with highly decentralized research like in the USA and most European countries.
- What are the **undisclosed investments** in military and intelligence? It may be high in the USA and Russia. But lower in Europe, given these countries don't allocate a great share of their GDP to military expenses.
- Is the publicized funding **incremental** or includes existing investments? You can easily embellish things with the latter accounting method, or create misleading rankings of country investments like when McKinsey did showcase a chart with Germany investing more than the USA which was not true at all[2676].
- Are there any **double bookings** in the showcased investments? This can easily generate misleading information.
- Are some countries **overinflating** their investment? This is a hypothesis for China's investments which have been highly confusing. We provide as accurate data for this regard here.

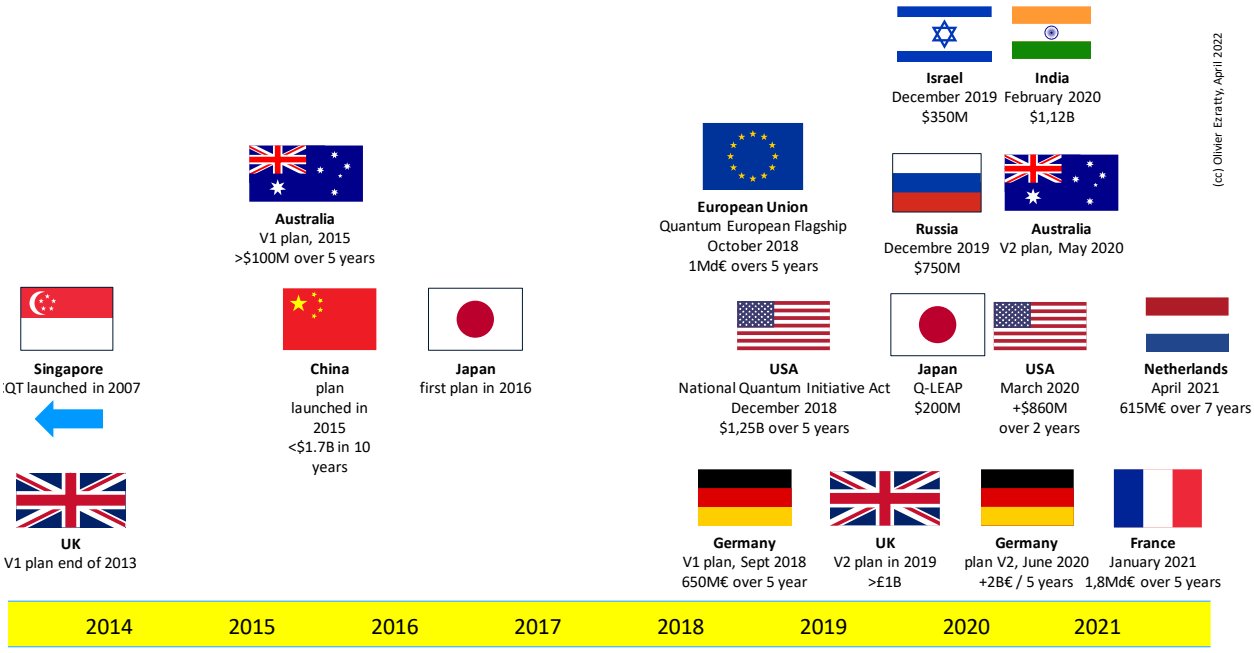


Figure 842: national quantum initiative plans across the years. (cc) Olivier Ezratty, 2022.

[2674] See Quantum, AI, and Geopolitics (3): Mapping The Race for Quantum Computing by Hélène Lavoix, December 2018.

[2675] See the forum Europe: Keys to Sovereignty by Thierry Breton, August 2020. He cites three pillars of this sovereignty: computing power, data control and secure connectivity. Quantum technologies have a key role to play in the first and third! However, the means cited to obtain this sovereignty are classic and relate to public funding for R&D. We know that this is clearly insufficient.

[2676] See A quantum wake-up call for European CEOs, McKinsey, December 2021.

Where's government money (your taxes) going? It usually funds the following in these various national quantum initiatives:

- Incremental **public research** funding efforts. This comes from both the country governments and sometimes, from local governments, like in Germany.
- Growing the **education effort** and addressing the skills shortage. This is particularly important as it deals with very highly skills roles, with a strong scientific background.
- Creating **quantum hubs** that consolidate quantum research and sometimes startup creation. These are handled within universities or public labs (like the DoE in the USA) and regions (like in Munich in Germany) or across several of them in a thematic way (UK). This may involve some real estate and building construction.
- Create **hybrid quantum-classical supercomputing centers**, based on existing supercomputing capacities, which is being done nearly everywhere, in the USA, Europe, etc.
- Create a **quantum technologies industry** with both encouraging startups creation and existing industries to adopt quantum technologies, like in the sensing domain or just, in software development. This goes with putting in place public/private funding mechanisms for long-term investments.
- Handle **procurement** with local startups with countries indirectly funding their local quantum computing startups champions through local procurement like in Finland with IQM, Australia with Quantum Brilliance, the USA with IonQ[2677], the UK with Orca and OQC or France with Pasqal. This is often related to the hybrid quantum-classical centers already mentioned.
- Foster **global partnerships** that are different in nature, between research laboratories within countries (as in the UK hubs), between particular labs across various countries, and between public and private research within the same country (CEA and Atos) or between different countries (Intel with Qutech). The raison d'être of all these partnerships can be identified: quantum computing is a complex scientific subject that cannot be mastered by a single laboratory or company. Collaboration is necessary to bring together talent from different specialties, between condensed matter physics, sensor and control technologies, optronics, cryogenics, semiconductor production, algorithmics and software development.
- Launch bilateral **countries partnerships** like the USA with Nordic countries, Switzerland, the UK and Australia, or France with The Netherlands and Singapore with Finland.

I tried here to consolidate a more global view with public and industry investments per country or region. This is based on some guestimates for large industry vendors in the USA (IBM, Microsoft, Google, Intel) but the public investment data is rather safe. What this shows is counter-intuitive: the first region in public investment is the European Union! It's investing more than the USA and even China. Still, the USA leads the international pack thanks to their industry investments, both from large IT vendors and from VCs in startups.

Europe's Achille's heel is not having these large IT vendors on one hand and investing less in startups in proportion to GDP. The result is some pressure put on European startups who have to find ways to get bigger fundings in Series B, C and beyond with investment sources outside the EU like the USA, Asia or even the Middle East oil countries.

I did this chart after seeing so many analysts providing wrong or outdated numbers on countries and region public investments in quantum technologies. The last one comes from a **BCG** report which tried in 2022 to compare of investments between the EU, the USA and China.

[2677] See IonQ Secures Contract to Provide Quantum Solutions to United States Air Force Research Lab, IonQ, September 2022.

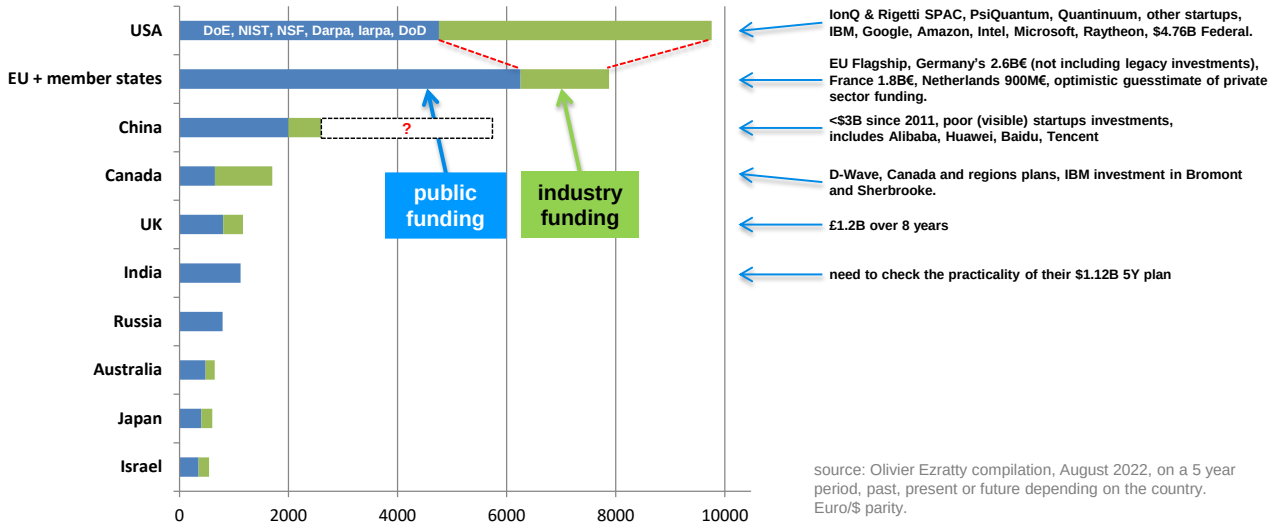


Figure 843: a consolidation of quantum technologies public and private investments with some raw estimated for large IT vendors. It creates a very different picture than what is commonly thought about the place of China and Europe. (cc) Olivier Ezratty, 2022.

Their data are wrong. Like many, in page 14, they overestimate China's investment (at $10B when it's probably way under $4B) and underestimate USA's which is about $4.7B as of August 2022 for 5 years instead of the mentioned $2.9B[2678]. They also showcase a $700M plan from France in 2019 that never existed. This is puzzling. But they showcase the harsh reality of a much smaller investment in startups in the EU compared with the USA, Canada and the UK. A similar report from the **World Economic Forum** contains the same wrong data on the USA, China, and also Japan[2679].

An evaluation of scientific publications in quantum computing done by **Insead students** in 2018 did show with no surprise to discover that the USA, Canada and China are the first countries to publish[2680].

A more detailed analysis was produced by **Michel Kurek** in September 2020 (sources of the illustrations in Figure 844) which did help relativize the influence of Chinese publications[2681]. Indeed, the Citations Per Publications is very low in China and also India, compared all Western countries.

The significant investments made by developed countries in quantum technologies raise fears that computing power could end up being concentrated in the hands of a few or even a single country or company. I don't believe this, at least not in the initial phase of development of these technologies. Knowledge on the subject is highly distributed, as are enabling technologies and strategic materials. I would rather situate the risk of concentration in a second phase of the maturation of this market, one that will see a market that was initially fragmented with many players concentrating through consolidation. It will probably do so for reasons that are more macro-economic than scientific or technological, through economies of scale and the platforming of offers. This explains why it is necessary to simultaneously keep an eye on the hardware, development tools and software applications of quantum computing.

Once the main scientific and technological uncertainties are lifted, the success of each company and country will depend on the classic key success factors of technology ecosystems: execution speed, team quality, funding levels, communication, marketing, sales, the ability to promote technology platforms to a maximum number of players and on a global scale.

[2678] See Can Europe Catch Up with the US (and China) in Quantum Computing? by François Candelon, Jean-François Bobier, Maxime Courtaux, and Gabriel Nahas, BCG, August 2022 (45 pages). You find the same China investment overstating in The Quantum Computing Arms Race is not Just About Breaking Encryption Keys by Adm. Mike Rogers and Nir Minerbi, Classiq, June 2022.

[2679] See State of Quantum Computing: Building a Quantum Economy, September 2022 (48 pages).

[2680] See VC investment analysis Quantum Computing, April 2018 (18 slides).

[2681] See Quantum Technologies : Patents, Publications & Investissements Landscape by Michel Kurek, September 2020 (52 pages).

This is where sovereigntist approaches combining protectionism of key players while ensuring maximum trade openness to the world to enable them to achieve economies of scale will have to be carefully adopted.

	COUNTRY	TP	%TP	TC	%TC	CPP	RCI	%ICPEI
1	USA	4,295	26.4%	108,128	44.8%	25.2	1.7	70%
2	China	3,706	22.8%	38,611	16.0%	10.4	0.7	44%
3	UK	1,428	8.8%	32,435	13.4%	22.7	1.5	120%
4	Germany	1,400	8.6%	38,339	15.9%	27.4	1.9	123%
5	Japan	1,106	6.8%	20,996	8.7%	19.0	1.3	99%
6	Canada	1,056	6.5%	23,104	9.6%	21.9	1.5	124%
7	India	991	6.1%	5,847	2.4%	5.9	0.4	33%
8	Australia	777	4.8%	20,777	8.6%	26.7	1.8	130%
9	France	699	4.3%	14,016	5.8%	20.1	1.4	117%
10	Italy	635	3.9%	10,522	4.4%	16.6	1.1	116%
	Total 10 countries	16,093	98.9%	312,775	129,5%	19.4	1.3	83.1%
	Total world	16,279		241,536		14.8		

*TP= Total Publication ; TC = Total Citation ; CPP = Citation par Publication = TC/TP ;
RCI = Relative Citation Index ; ICPEI = International Collaboration Publication Extended Index

Figure 844: publications and patents on quantum tech per country. Source: Quantum Technologies : Patents, Publications & Investissements Landscape by Michel Kurek, September 2020 (52 pages).

We'll go through the details, country by country, continent by continent. With one exception, Africa, which is little invested in the subject, at least as a producer of quantum technologies, maybe besides South Africa which seems to have started to get involved in the academic side[2682].

This summary shows which country best masters quantum computing technology per qubit type. All in all, we have a good balance between the USA and the European Union, although the USA have the benefit from having large IT vendors invested in the field in superconducting (Google, IBM), silicon (Intel), trapped ions (Honeywell, IonQ) and topological qubits (Microsoft).

What are the key success indicators of success for countries investing in the quantum race?

We'll probably have some analyst shops create their own quantum sort-of Shanghai ranking using composite metrics: public funding, scientific publications, patents and the likes, entrepreneurship spirit, number of startups, startups funding, large companies' investments, corporate adoption, skilled workforce and else. Guess what? US and China will probably rank first there. And smaller countries behind in some variable order. But what if Europe was consolidated?

[2682] See Will Africa miss the next computational revolution? by Amira Abbas, April 2020.

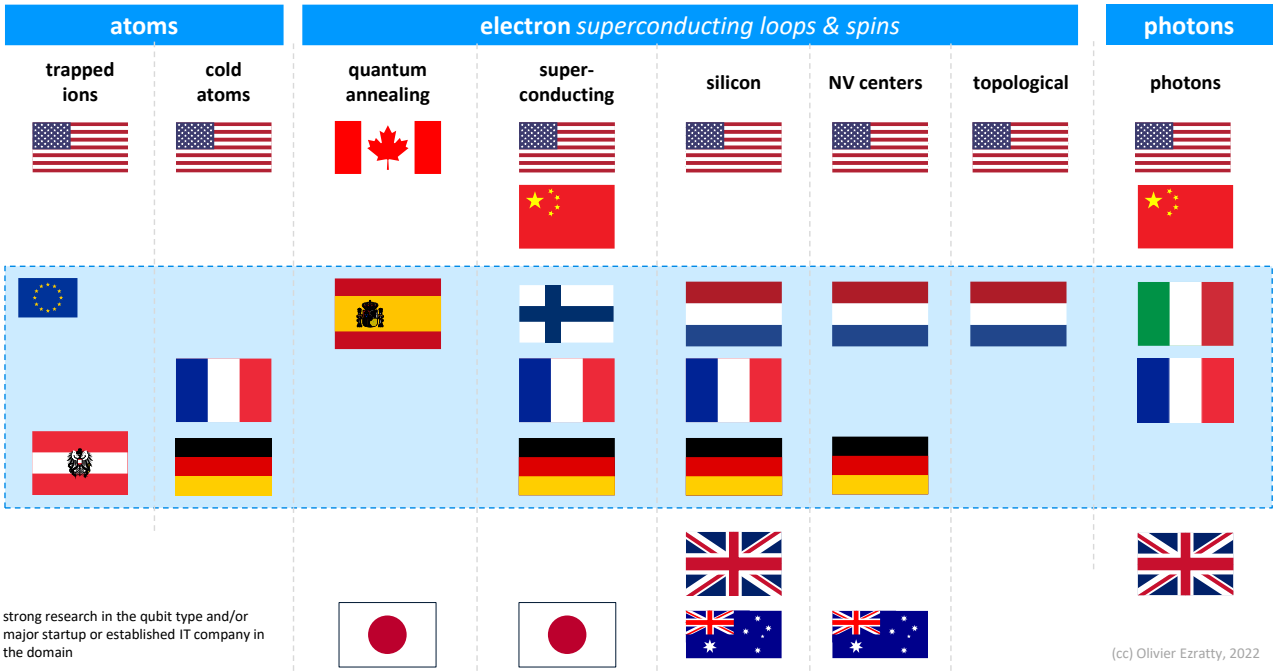


Figure 845: key quantum computing technologies per qubit type and country of origin.

North America

USA

Whatever the metric you use, the USA is leading the world in quantum technologies. They mix three components no other country or region has: a powerful Federal government investing significant amounts in fundamental research, large IT companies investing a lot as well in research and industrialization and a healthy well-funded dense startup ecosystem.

The coordination of research in the different branches of quantum physics started in October 2014, the White House produced two reports[2683]. It was not a plan but rather an inventory of what existed. Like almost all countries, quantum technologies were segmented in four quantum communication, sensing, computing and simulation. In 2017, lobbying from the industry and research started to push the federal government to launch a national quantum plan. It started with U.S. House of Representatives organizing a hearing in October 2017 (video). For three hours, elected officials questioned a panel of scientists including James Kurose of the NSF and John Stephen Binkley of the Department of Energy, who explained the basics of qubits and the associated sovereignty issues.

The Democrats were concerned about the Trump administration's proposed cuts in funding for civilian research in favor of defense budget increases and tax cuts. But the US Congress increased federal research budgets for fiscal year 2018 and beyond[2684], knowing that these budgets are then traditionally channeled mainly to American universities research laboratories. This is one of the few cases where the Republican-controlled Congress opposed the Trump administration.

[2683] The report Advancing Quantum Information Science: National Challenges and Opportunities, July 2016 (23 pages) was followed by a working meeting in October 2016.

[2684] See Trump, Congress approve largest U.S. research spending increase in a decade, Science, March 2018.

This happened consistently throughout all fiscal years of the Trump administration and will probably happen again with the Biden administration.

National Quantum Initiative Act

Then came the National Quantum Initiative Act that was first proposed on June 26, 2018 by the House of Representatives Science Committee (H.R. 6227, 25 pages). An equivalent proposal was done by the Senate on the same day. This project was the result of a proposal, the National Quantum Initiative-Action Plan, prepared by public and private research stakeholders (IBM, Google, Rigetti).

An intense lobbying campaign was carried out by several professional associations[2685], with the **National Photonics Initiative**, a professional association bringing together photonics physicists and industrialists in the sector, accompanied by the lobbying firm **BGR Group**.

This association, which wanted to make photonics a priority, was launched in 2012. It is sponsored by other entities: The Optical Society (OSA), SPIE (The International Society for Optics and Photonics), American Physical Society, IEEE Photonics Society, ALIA Laser Institute of America and a lot of other professional associations. The lobbying was also pushed by **Jonathan Dowling** (1955-2020, American), professor of physics at Louisiana State University and specialist in photonics[2686] .

The **Quantum Industry Coalition** brings together more generalist manufacturers such as Microsoft, Intel and Lockheed Martin as well as startups[2687]. This coalition is helped by the lobbying firm KL Gates. It is the 41st largest law firm in the world making $1B annually. The director of the Quantum Industry Coalition is Paul Stimers, a partner of KL Gate[2688]. To this should be added the **Quantum Alliance Initiative** launched in 2018 by the Hudson Institute, a conservative think tank, which creates proposed standards for QKD and QRNG and of course advocates for the development of this industrial sector in the USA.

NIST had also created with **SRI International** the **Quantum Economic Development Consortium** (QED-C) to develop the American quantum industry in the fields of communication and sensing[2689]. It is chaired by Joseph Broz, who is also vice-president of SRI, and by Celia Merzbacher, a semiconductor industry lobbyist who worked in the White House during the Bush 43 administration.

The Quantum National Initiative Act proposed allocating $1,275B over five years to fund civil quantum R&D, divided among the Department of Energy ($625M), NSF ($250M) and NIST which is focused on cryptography issues ($400M).

The Act also proposed the creation of a National Quantum Coordination Office within the White House Office of Science and Technology Policy. It asked the President of the United States to create a 10-year quantum plan, the first step being a five-year plan to be delivered one year after the passage of the law.

[2685] See Quantum computing finds its lobbying voice by Aaron Gregg, Washington Post, June 2018.

[2686] See Schrödinger's Killer App - Race to Build the World's First Quantum Computer by Jonathan P. Dowling, 2013 (445 pages) where the author was sending a warning about the risk to see China lead the quantum technology race. If the USA were not investing more: "*The future of the quantum Internet is in photons and the short circuiting of the development of optical quantum information processors in the United States means that the future quantum Internet will have 'Made in China' stamped all over it.* ", page 173.

[2687] See their Quantum Industry Coalition website.

[2688] See The US National Quantum Initiative by Paul Stimers, K&L Gates, October 2019 (6 pages).

[2689] See NIST Launches Consortium to Support Development of Quantum Industry, September 2018. And more details in U.S. Consortium Pulls Ecosystem Into Quantum by Susan Rambo, August 2019. As of July 2020, the association has 130 members from the private sector - large corporations and startups - and about 40 laboratories from universities and the U.S. public sector.

This bill was pushed by elected officials fearing that China will take over the quantum, especially in computer security[2690]. The USA likes to scare itself, even if, in the field of quantum technologies, it has nothing to be ashamed of with a density of public and private research laboratories and the major players having a large-scale industrialization capacity that almost no country can compete with. And their domestic market remains the largest in the world for enterprise computing applications.

The quantum bill was voted by the House in September and then by the Senate in December 2018[2691]. In September 2018, the White House published the National Strategic Overview for Quantum Information Science that included the terms of the congressional proposal. They emphasized research, training of scientists and international collaboration. At last, Donald Trump signed this law on December 21, 2018 just before the shutdown, but with no fanfare nor any scientists in the Oval Office[2692].

In December 2019, the **Quantum Information Edge** alliance was created, bringing together Lawrence Berkeley National Laboratory and Sandia Labs of the Department of Energy, the University of Maryland, Duke University (North Carolina), the University of Colorado at Boulder, Harvard, Caltech, MIT and the University of New Mexico[2693]. For the most part, the usual suspects of basic research in quantum computing, thus creating their "virtual hub" for coordinating research in this field. With a focus on error reduction at the qubit level, techniques for interconnecting qubits and the development of new quantum algorithms. For its part, the NPI embarked on a new lobbying campaign at the end of 2019 and early 2020 to increase once again the federal funds allocated to research in quantum technologies[2694]. In 2022, the campaign was still going on with pushes for more Federal investments in quantum technologies procurement[2695].

In February 2020, the White House published a memo from the National Quantum Coordination Office recommending the development of quantum networks[2696].

And in March 2020, the US executive proposed a new increase in quantum research budgets for the years 2020/2021[2697]. It included $450M for the Department of Energy, $330M for the NSF and $80M for the NIST. This was matched by a $1B increase for artificial intelligence research programs[2698]. In August 2020, the White House announced a 30% increase in the quantum and AI budgets for fiscal year 2021.

[2690] See How suspicions of spying threaten cross-border science by Patrick Howell O'Neill, December 2019, which discusses the direct and indirect methods used by China to plunder European and American quantum research and exploit it both civil and military, such as quantum radars, quantum sonars and QKD. Here is the link to retrieve the Quantum Dragon Strider study mentioned in the article, November 2019 (22 pages). You can indicate a bogus email to get it, the download does not go through an email. It evokes various partnerships in research that help the Chinese to exploit Western research. It is based on a few examples including the very detailed one from the University of Heidelberg in Germany. On the same subject, see also China's top quantum scientist has ties to the country's defense companies, December 2019, Quantum USA Vs.Quantum China: The World's Most Important Technology Race by Moor Insights and Strategy, October 2019 and New Warnings Over China's Efforts in Quantum Computing by Sintia Radu, January 2020.

[2691] See SIA Welcomes House Passage of Quantum Computing Legislation, September 2018.

[2692] See President Trump has signed a $1.2 billon law to boost US quantum tech by Martin Giles in the MIT Technology Review, December 2018. See Jeremy Tsu's The Race to Develop the World's Best Quantum Tech in IEEE Spectrum, December 2018, which discusses the CNAS report Quantum Hegemony-China's Ambitions and the Challenge to U.S. Innovation Leadership published in September 2018, which describes China's quantum strategy (52 pages). See also US intelligence community says quantum computing and AI poses an 'emerging threat' to national security by Zack Whittaker, December 2018.

[2693] See US alliance for quantum computing by David Manners, 2019.

[2694] See NPI Brings Quantum Experts to Capitol Hill to Advocate for Additional NQI Funding by Jo Maney, March 2020.

[2695] See The US government needs a commercialization strategy for quantum by Laura E. Thomas, senior director of National Security Solutions at ColdQuanta, December 2021. Pushing for federal procurement of US quantum computers through DARPA and the NSF.

[2696] See A Strategic Vision for America's Quantum Networks, White House, February 2020 (4 pages).

[2697] See Why is Trump funding quantum computing research but cutting other science budgets? The national security implications of this technology may be exaggerated by John Lindsay, March 2020.

[2698] See White House reportedly aims to double AI research budget to $2B by Devin Coldewey in TechCrunch, February 2020.

In December 2021, a memo was published by the NQI team showing for the first time the total Federal budget spent in quantum technologies by year with the legacy spendings and the NQI related spendings. It did show that the 5-year trend was a $4B plan[2699].

The US NQI (National Quantum Initiative) is run by the **National Quantum Coordination Office** (NQCO), hosted by the White House Office of Science and Technology Policy (OSTP).

It has a web site since October 2020[2700]! Its director is Charles Tahan[2701]. And if you wonder about the bureaucracy in your own country, here you are also with several related committees: the **National Science and Technology Council** (NSTC) Subcommittee on Quantum Information Science (SCQIS) that coordinates Federal R&D in quantum technologies, the **National Science and Technology Council** (NSTC) Subcommittee on the Economic and Security Implications of Quantum Science (ESIX) that handles economic and security implications across federal agencies[2702] and the **National Quantum Initiative Advisory Committee** (NQIAC) that advises the President, the Secretary of Energy and the NSTC Subcommittee on QIS.

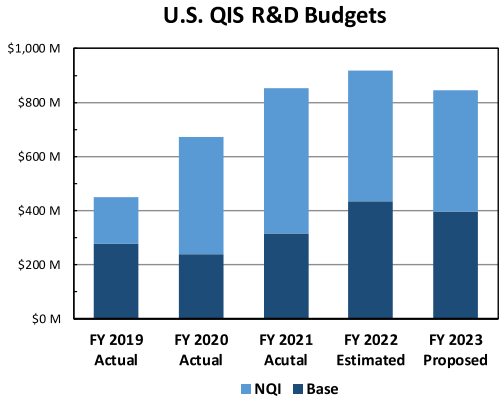


Figure 846: the most accurate Federal investment report on quantum technologies. Source: National Quantum Initiative supplement to the President's FY 2023 budget, January 2023 (47 pages).

In April 2021, the story went on with yet another Congress proposal, the **Quantum for Universal Advancement in Nationwide Technology Use and Modernization** (QUANTUM) for National Security Act of 2021[2703]. Two Senators introduced two bills to "*better position the United States to be globally competitive in quantum information science*". It's focused on developing Department of Defense quantum networking and telecommunications use cases and workforce developments.

This bill appears as a direct response to China's massive investments in quantum telecommunications infrastructures. It's kind of a military grade version of the National Quantum Initiative Act launched in 2018 that had mostly a civilian face despite the significant DoE funding it did incorporate[2704].

In February 2022, the NQI released a report on the development of quantum technologies workforce in the USA[2705]. It includes exposing the public to educational content about quantum technologies and to ensure quantum technologies are as inclusive as possible. The plan is mostly qualitative and doesn't provide means and objectives data.

[2699] See National Quantum Initiative supplement to the President's FY 2022 budget, December 2021 (46 pages).

[2700] The NQCO published the quick status report Quantum frontiers report on community input to the nation's strategy for quantum information science in October 2020 (32 pages).

[2701] Charles Tahan is a physicist specialized in condensed matter physics and quantum information science. He continues to publish some scientific papers from time to time, trying to not losing ground in his field.

[2702] In The role of international talent in quantum information science by National Science and Technology Council of the White House, October 2021 (20 pages), the NSTC worries about the quantum talent shortage in the USA and advocates a balanced approach between hiring international talent and protecting national security. The global hunt for talent is launched!

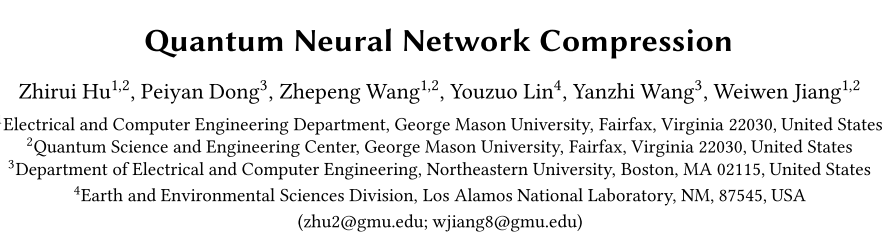
[2703] See Thune, Hassan Introduce Bills to Bolster the United States' Leadership in Quantum Information Science, April 2021.

[2704] And it's never enough! See for example America is Losing the Quantum Race with China by Theresa Payton, a former White House CIO, May 2022. Unfortunately, it contains only fainted documented anecdotal evidence and no significant hard data to prove that China is indeed ahead of the USA for all respects. Maybe the only real case is about QKD deployments but it's not even mentioned here.

[2705] See Quantum Information Science and Technology workforce development national strategic plan, February 2022 (34 pages.

The USA is concerned about managing its talent pool efficiently with, simultaneously caring about its national security. It is a concern fueled by a simple fact: a significant share of the quantum research talent pool in the USA are first generation immigrants.

Let's take this paper published by a research team from a University in Virginia and the DoE Los Alamos lab. All the names are Chinese! Are these Americans, first generation immigrants, or PhD students or post-docs who'll soon return to China?



Quantum Neural Network Compression

Zhirui Hu[1,2], Peiyan Dong[3], Zhepeng Wang[1,2], Youzuo Lin[4], Yanzhi Wang[3], Weiwen Jiang[1,2]
[1]Electrical and Computer Engineering Department, George Mason University, Fairfax, Virginia 22030, United States
[2]Quantum Science and Engineering Center, George Mason University, Fairfax, Virginia 22030, United States
[3]Department of Electrical and Computer Engineering, Northeastern University, Boston, MA 02115, United States
[4]Earth and Environmental Sciences Division, Los Alamos National Laboratory, NM, 87545, USA
(zhu2@gmu.edu; wjiang8@gmu.edu)

Figure 847: an example of a paper published in the USA with authors all having a Chinese name. See Quantum Neural Network Compression by Zhirui Hu et al, July 2022 (11 pages).

In May 2022, President Biden signed two Presidential directives[2706]. The first was an Executive order enhancing the governance of the NQI with the creation of an Advisory Committee. The second was a National Security Memorandum describing how the Federal government will prepare for the adoption of PQC cybersecurity to protect it from future quantum computing cryptology threats, in line with the first 4 NIST approved PQC standards announced in July 2022. The NIST is tasked with running a PQC migration project for the Federal government at the National Cybersecurity Center of Excellence and for the industry. The NSM also mandates new protections against IP theft and abuse.

In August 2022, the CHIPS Act was signed by POTUS with additional Federal funding of $152M per year for quantum technologies for the 2023-2027 period, going to NIST, the DoE and the NSF as usual. As a consequence, it adds about $760M to the 5-year $4B run-rate of quantum federal research expenditures[2707].

Military and intelligence federal agencies

Public laboratories investing in quantum computing cut across much of the federal military-industrial complex with internal research or external research funded through calls for proposals or joint laboratories with universities:

IARPA (Intelligence Advanced Research Projects Agency) funds third-party projects on quantum computing and quantum algorithms. They run several quantum programs that happen to involve Universities outside the USA. The only that seems still in place is **LogiQ**. Its goal is to improve the quality of qubits. It involves TU Delft (Netherlands), the University of Innsbruck, Duke University and IBM. IARPA also funds programs conducted by third parties. It is a small agency that employs fewer than a hundred people.

NSA is investing heavily in quantum technologies, both in the race to implement Shor's algorithm for breaking RSA-based public-key protected communications and for protecting sensitive communications with quantum keys and cryptography. This work is obviously not public. The NSA subcontracts some of its research to private companies such as Lockheed-Martin. It is also part of a joint laboratory with NIST and the University of Maryland, QuICS, which was launched in 2014.

[2706] See Fact sheet: President Biden Announces Two Presidential Directives Advancing Quantum Technologies, White House, May 2022.

[2707] See Quantum in the CHIPS and Science Act of 2022, QuantumGov, August 2022.

DARPA funds three programs in quantum technologies: long-distance quantum communications, quantum metrology applied to imaging, and neurological trauma diagnosis and PTSD. Funding goes to projects led by universities, startups and established companies[2708]. In 2020, they launched a NISQ computation challenge which led to the selection of 7 research teams as part of the ONISQ program[2709] and QAFS, a program on quantum annealing involving among others the Lincoln Lab from the MIT. In 2020, DARPA awarded ColdQuanta with a $7.5M project to build a neutral atom based quantum computer.

Army Research Office also has its own quantum research program covering the entire spectrum from sensing to quantum computing, cryptography and quantum communications.

US Air Force and its Air Force Research Laboratory's Quantum Communications lab is focused on quantum cryptography (QKD) and also quantum computing. The AFRL announced in December 2020 that it planned to work with the Office of Naval Research to test quantum technologies with the "Five Eyes" countries (USA, Canada, Australia, New Zealand and UK) for a Naval exercise. Another lab, the Quantum Information and Sciences Laboratory, does applied research in superconducting qubits, photonic qubits, trapped ions qubits, quantum algorithms and quantum sensing. They even deployed their own superconducting qubits system prototype, created with the MIT. They also awarded PsiQuantum with a $22.5M project to build a photonic quantum computer.

Office of Naval Research (ONR) is working on the use cases of QKDs for the Navy and on using of quantum algorithms related to the Navy operational needs.

Federal civil agencies

In quantum science and technologies, the key Federal civil agencies are the Department of Energy, the NIST, the NSF and NASA.

Department of Energy (DoE) has many research laboratories that are big consumers of supercomputing capacities like in Oak Ridge and Argonne. It also operates the Los Alamos National Laboratory (LANL) and its Quantum Institute (QI) launched in 2002 that also invests in quantum computing and cryptography. In particular, they fund research at UNSW in Australia as well as in Maryland. The DoE also runs the Sandia National Laboratories**,** which also conducts applied research in all areas of quantum physics.

The DoE launched a call for proposals to award 158 grants totaling $32M to 118 SMEs through the SBIR program. The grants are delivered in two phases, a first phase of $200K followed by a second phase of $1.1M for the best projects, spread over a period of two and a half years.

The DoE also announced in August 2020 the funding of five research centers in quantum technologies, all led by DoE laboratories, with $300M coming from the DoE and the rest from relevant institutions and the industry (IBM, Microsoft, Intel, Lockheed Martin)[2710]. These new research centers are **Q-NEXT** (Next Generation Quantum Science and Engineering Center, David Awschalom) led by Argonne National Laboratory which focuses on the industrialization of quantum hardware, **C²QA** (Co-design Center for Quantum Advantage, Steve Girvin) led by the DoE Brookhaven National Laboratory which will focus on ways to achieve quantum advantage in scientific applications, the **SQMS** (Superconducting Quantum Materials and Systems Center, Anna Grassellino) led by the Fermi National Accelerator Laboratory which will focus on superconducting qubits, the **QSA** (Quantum

---

[2708] See The DARPA Model for Transformative Technologies, 2019 (511 pages) which tells the story of how the agency works. It has about one hundred program managers in total with a total budget of about $3.5B. It explains how it connects fundamental research to difficult technology challenges.

[2709] See DARPA Challenge May Boost Quantum Value of NISQ Devices by Matt Swayne, June 2020. One of the selected teams includes a certain Davide Venturelli who studied at the University of Grenoble.

[2710] See National Quantum Information Science Research Centers by Ceren Susut, December 2020 (17 slides). Unstable link.

Systems Accelerator Center, Irfan Siddiqi[2711]) led by the Lawrence Berkeley National Laboratory which works on quantum computing hardware and software and the **QSC** (Quantum Science Center, David Dean) led by the Oak Ridge National Laboratory which will focus on quantum computing scalability issues.

The DoE then launched a $30M program in March 2021 on nanoscale matter and their use case in energy applications. It will fund the five existing DoE Nanoscale Science Research Centers and their research partners over 3 years. The awards size is between $1M and $2.5M[2712]. It also launched a $25M program in April 2021 on Quantum Internet including quantum repeaters, quantum memory and quantum communication protocols, opened to the 17 DoE labs.

NSF funds various research projects[2713]. In 2019, it launched a call for **Quantum Leap Challenge Institutes**, to fund research institutes conducting interdisciplinary research projects advancing the state of the art in quantum technologies[2714].

Their format is reminiscent of the UK quantum program hubs. Three hubs were selected in July 2020 for a total of $75M spread over five years: a first dedicated to quantum sensing led by the University of Colorado, a second dedicated to quantum computing led by the University of Illinois - Urbana-Champaign and a third also on quantum computing and rather software side led by the University of Berkeley[2715]. These three hubs bring together 16 academic institutions, 8 national laboratories and 22 industrial partners. On top of that, the NSF is also funding the consolidation of other initiatives like the one around Purdue University in Indiana[2716]. The NSF also launched a **Quantum Algorithm Challenge** in March 2020[2717].

NIST is a federal research institute with the Department of Commerce. Its historical role is sensing and the definition of weights and measures. Its work on atomic clocks naturally led it to look after quantum technologies. It has an annual budget of $1.2B and employs 3,400 people on two campuses, one in Boulder, Colorado and another one in Maryland, next door to the University of Maryland and north of Washington DC. Several of its research groups are dedicated to quantum technologies with the Quantum Processing Group for quantum computing, another for spintronics, one for quantum sensing and another for superconducting electronics. On top of this, the Computer Security Division of the Information Technology Laboratory (ITL) manages the call for tenders on the standardization of PQC (Post-Quantum Cryptography) that we have already covered in a dedicated chapter after page 837[2718]. NIST's PQC standardization strategy has wide implications. It will sediment the market around a dozen standards that will be royalty-free. This may favor large cybersecurity vendors instead of enabling new players to disrupt the market.

[2711] The QSA was awarded a funding of $115M for 5 years in August 2020. See New $115 Million Quantum Systems Accelerator to Pioneer Quantum Technologies for Discovery Science by Dan Krotz, August 2020.

[2712] See DOE Announces $30 Million for Quantum Information Science to Tackle Emerging 21st Century Challenges, March 2021.

[2713] See for example NSF Awards $2M For Research on Quantum Machine Learning With Photonics, September 2019 for the University of Maryland.

[2714] See Quantum Leap Challenge Institutes (QLCI), NSF, 2019.

[2715] See NSF establishes 3 new institutes to address critical challenges in quantum information science, NSF, June 2021.

[2716] Purdue University launched in July 2021 a new Center for Quantum Technologies funded by the NSF with an established team of 50 quantum scientists and engineers coming from various research institutions in Indiana working on many quantum fields (atomic and molecular optics, solid state quantum systems, quantum nanophotonics, quantum information and communication).

[2717] See Dear Colleague Letter: Quantum Algorithm Challenge, Anne Kinney and Margaret Martonosi, NSF, March 2020.

[2718] See this overview of NIST's scientific activities: Quantum Information Science & NIST - Advancing QIS Technologies for Economic Impact, 2019 (39 slides).

NIST is also a stakeholder in and a co-founder of three joint laboratories with two major universities, each located near its own campuses in the states of Colorado and Maryland, the JQI, QuICS with the NSA and JILA with the University of Colorado.

Figure 848: the JV labs from NIST.

The University of Maryland's **Joint Quantum Institute** (JQI)**,** established in 2006 is a fundamental quantum physics laboratory. It is the home of David Wineland, a long-time specialist in ion control by laser cooling, who won the Nobel Prize in Physics in 2012 along with Serge Haroche. It is in this laboratory that the IonQ startup by Christopher Monroe was launched in 2015. Many alumni from this lab also joined Honeywell's quantum team in Denver, Colorado. This laboratory employs 35 permanent researchers, 55 post-docs and 85 PhD students with an annual budget of $6M supplemented by various external funding.

The **Joint Center for Quantum Information and Computer Science** (QuICS) at the University of Maryland (UMD) launched in 2014 in partnership with NSA's research directorate that focuses on quantum computing architectures, algorithms and complexity theories to complement the JQI.

The **JILA** at the University of Colorado at Boulder which is dedicated to sensing technologies[2719]. It is home to two Nobel Prize winners: Eric Cornell (in 2001, for his work on Bose-Einstein condensates) and John Hall (in 2005, for his work on laser frequency combs).

NIST employs a fourth Nobel Prize winner in physics, William D. Phillips for his work on atoms laser cooling using the Zeeman effect in 1997, shared with Claude Cohen-Tannoudji from France.

NASA created in 2013 the Quantum Artificial Intelligence Laboratory (QuAIL) jointly with Google, located at the Ames Research Center near the Google's headquarters in Mountain Views to explore the field of quantum algorithms, in particular on a D-Wave quantum annealer they acquired and installed there.

USA local quantum ecosystems

The main geographical quantum hubs in the USA combine a mix of national labs like those from the DoE, Universities and commercial companies. So here we are:

- **California** with the Silicon Valley and in the Los Angeles area, with Stanford, UCLA[2720], Caltech[2721], UCSB, plus the labs from Google, Microsoft and Amazon, and also Rigetti. The Los Angeles area seems on part with, if not stronger than the Silicon Valley.
- **Massachusetts** with the MIT, Harvard and UMass Amherst.
- **Colorado** at Boulder, with Quantinuum, NIST and the University of Boulder Colorado[2722].
- **New Haven** with its very influential Yale University, particularly in the superconducting qubit domain, and Qci which is a spin-out startup from Yale.

[2719] JILA was created in 1962 as the Joint Institute for Laboratory Astrophysics but they now use only the acronym without this meaning given its extended activities beyond astrophysics.

[2720] UCLA got a $5M grant from Boeing to support the Center for Quantum Science and Engineering, as announced in May 2022.

[2721] In January 2022 was announced the creation of the "Dr. Allen and Charlotte Ginsburg Center for Quantum Precision Measurement" thanks to a donation from the couple.

[2722] The University of Boulder created the Qubit Quantum Initiative to foster interdisciplinary quantum research in a 4-floor building.

- **Illinois/Chicago** with two DoE labs (Fermi and Argonne), several universities and the Chicago Quantum Exchange ecosystem which regroups these labs, the University of Chicago, the University of Illinois, the University of Wisconsin and Northwestern University[2723]. The University of Chicago Polsky Center and the Chicago Quantum Exchange launched the first national quantum startups accelerator program in April 2021. In September 2022, the NRF (National Research Foundation of South Korea) awarded $1M (over 5 years) to David Awschalom and Liang Jiang from the University of Chicago to create a joint lab, "The Center for Quantum Error Correction".
- **New York State** with Princeton, the Flatiron Institute, IBM, GlobalFoundries and SeeQC.
- **Maryland** with the University of Maryland, IonQ, NIST, NSA and the Quantum Catalyzer quantum startups accelerator (Q-CAT) launched by Ronald Walsworth that creates quantum startups from scratch.
- **Tennessee** and **New Mexico** host three DoE labs and their quantum research centers.
- **Washington State** with the University of Washington and the Pacific NorthWestern DoE lab, given Microsoft and Amazon HQ are there but their quantum team mostly sits in part in Santa Barbara, California.
- Lesser developed ecosystems in **Indiana** (Purdue University, Midwest Quantum Collaboratory, a joint lab between Purdue University, Michigan State University and University of Michigan), **Virginia** (Virginia Tech), **Georgia** (GeorgiaTech) and **Florida** (Florida State University).

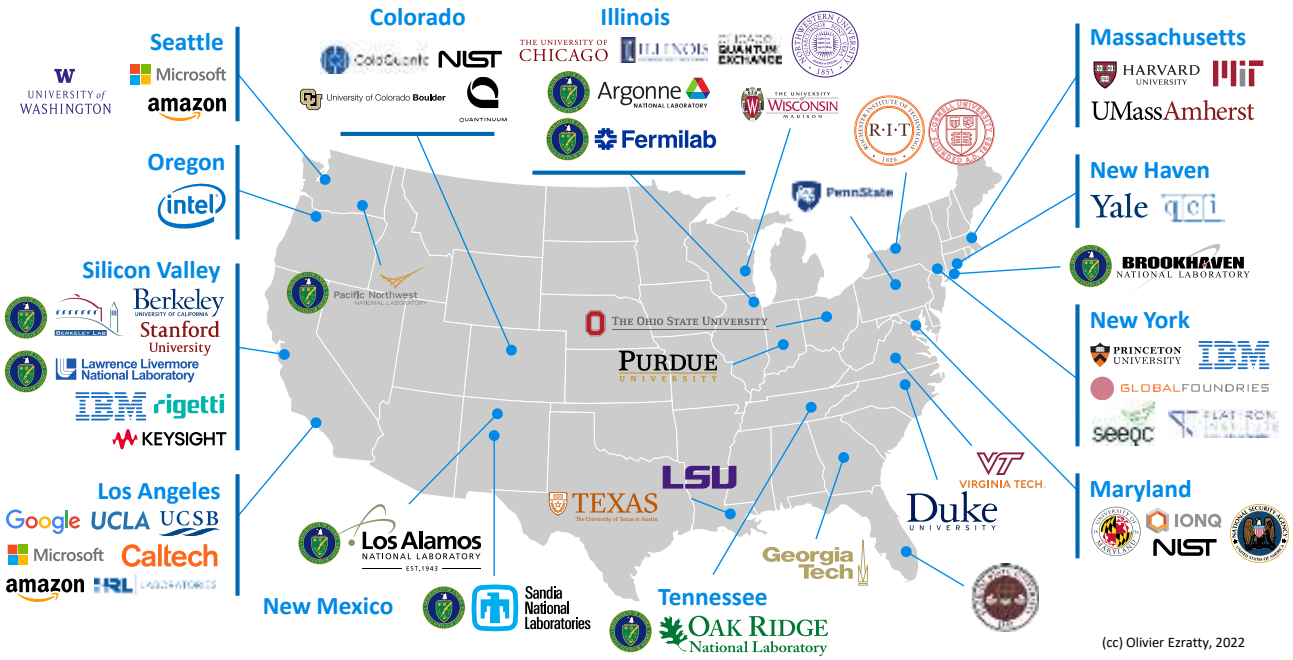


Figure 849: another map! You want to know where Argonne and Sandia Labs are? Here it is with the DoE labs, large Universities and vendors. (cc) Olivier Ezratty, 2022.

The above map in Figure 849 showcases this geographical distribution of USA's quantum technology R&D areas. The distribution is more even than in classical digital technologies, which are more concentrated on the country's West Coast and particularly in the Silicon Valley.

[2723] See Chicago Quantum Exchange welcomes new partners focused on manufacturing, computing, and the Chicago region, March 2022, and University of Chicago forges new bonds with European partners through Quantum and Sustainability conference in Paris, May 2022. It established a UChicago Center in Paris to foster collaboration between the Chicago and European quantum ecosystems.

Finally, let us recall a market reality that echoes economist **Maria Mazzucato**'s thesis on the public origin of technological innovations: the major American players are sourcing at different levels and throughout the USA and the world to advance their quantum technologies. Figure 850 is a good illustration of this phenomenon, showing how large IT players like IBM, Google, Intel, Microsoft, Amazon, Honeywell and even IonQ, surf on the work of publicly funded research labs not only in the USA but throughout the world. The last example being the creation of a Google AI lab in Australia in partnership with UNSW, the University of Sidney, Macquarie University and UTS, for the development of quantum applications.

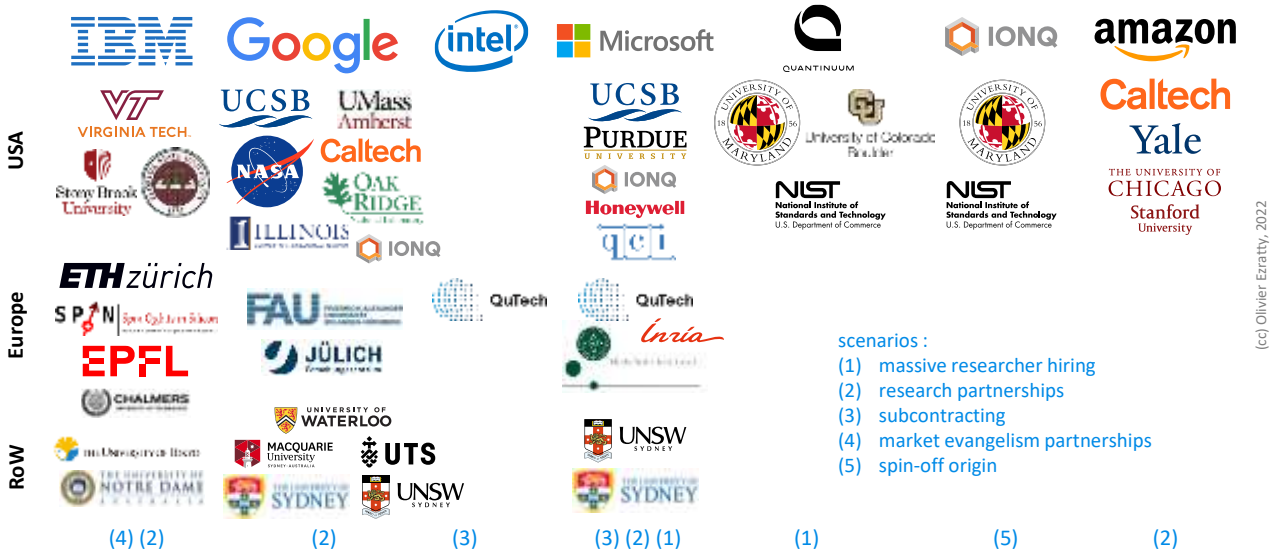


Figure 850: large IT vendors are reusing a lot of research and talent from universities both in the USA and in the rest of the world. Here's a map of who works with whom. (cc) Olivier Ezratty, 2022.

Canada

In Canada, a parallel can be drawn between artificial intelligence and quantum technologies. In both cases, the country's influence is far greater than its economic weight, at the basic research level, with a healthy startup ecosystem and best-in-class investment per capita.

This is due in particular to a constant and early-stage investments in research by government and universities and to a certain entrepreneurial dynamism.

Canada has two great quantum stars in research with **Gilles Brassard of the** University of Montreal who is with **Charles Bennett of** IBM Research the co-inventor of QKD's BB84 protocol.

Research

Canada is distinguished by a strong investment in basic research in quantum computing, including more than $1B of public investment over a decade, mainly in three institutions[2724]. Let's look at the Canadian ecosystem from East to West.

[2724] See Quantum Canada by Ben Sussman, Paul Corkum, Alexandre Blais, David Cory and Andrea Damascelli, February 2019 (6 pages) for an overview on Canada's quantum investments.

In **Québec**, the University of Sherbrooke Quantum Institute**,** near Montreal, is home to Alexandre Blais, a recognized specialist in superconducting qubits. Their **QSciTech** training program organized with industry partners and the Q2 initiative encourage student entrepreneurship. Several startups came out of it such as SBTech (metrology), Nord Quantique (quantum computing) and Quantic (sensing). In February 2022, the Québec Region announced an impressive plan of public/private investment of CAN $435M (US $350M) in the Sherbrooke region. It includes CAN $131M to create "Sherbrooke Quantique" coming from the region and the rest from industry investors including IBM. The setup of an IBM quantum computer in Bromont near Sherbrooke corresponds to a region investment of CAN $68M and CAN $62M from IBM.

The rest of the region investments (about $62M) covers various research funding and real-estate investments, including the innovation platform PINQ^2 (that is not just related to quantum technologies). 1QBit, Pasqal and Eidos-Sherbrooke announced they would install an office in Sherbrooke, representing a forecasted investment of CAN $205M over 5 years. Eidos-Sherbrooke is a video games studio that is planning to use quantum computing. The plan also contains a region funding of CAN $3,6M out of a total of CAN $8,1M for setting up a collaborative platform on quantum software design with CMC Microsystems who also manufactures some electronic components (CMOS down to 22 nm density, III-V, Si Photonics, superconducting).

Figure 851: a new map for Canada's quantum ecosystem from East to West where you see a startup concentration in Ontario. (cc) Olivier Ezratty, 2022.

In **Ontario**, the quantum ecosystem is centered around Toronto and Waterloo. The University of Waterloo Institute for Quantum Computing, near Toronto obtained $120M in 2017 to fund its various quantum research institutes, complemented by $53M in Australian funding from UNSW, the operator Telstra and the Commonwealth Bank of Australia. The IQC does both research and teaching. They offer short courses of one to two weeks in the summer on quantum cryptography and quantum computing. The IQC is directed by Raymond Laflamme, one of the fathers of QEC. They cover all aspects of quantum technologies with about thirty teams of theorists and experimentalists, about fifty post-docs and 125 PhD students. A dozen startups were created since 2002. The IQC is leading the Transformative Quantum Technologies (TQT), a seven-year research commercialization program funded by the Canadian government and its First Research Excellence Funds to the tune of $76M.

In January 2020, TQT launched the Quantum Alliance, an umbrella for IQC and TQT to link them to their Canadian and international ecosystem, including the fabric of quantum startups. The University of Waterloo also runs its Quantum-Nano Fabrication and Characterization Facility (QNFCF) with cleanrooms located in the Lazaridis Quantum-Nano Centre. The Waterloo quantum ecosystem also hosts the Research Accelerator Center of Quantum Technologies.

In **Alberta**, the University of Calgary is working on quantum communications and has deployed an experimental QKD network of a few tens of kilometers. The University of Alberta in Edmonton, north of Calgary, is also involved in this work[2725]. In 2020, the government of Alberta dedicated $11.8M to the creation of an international hub for quantum computing, $3M of which will fund quantum research.

In **British Columbia**, the UBC (University of British Columbia) Quantum Matter Institute (QMI), located primarily in Vancouver.

Government funding

As in most countries, the government is funding quantum research and the industry.

The Canadian government says it invested over CAN $1B in quantum research and education between 2009 and 2020. In April 2021, it announced its national quantum initiative with a CAN $360M (US $300M) plan spread over 7 years. Just before, in March, it announced a public funding of $40M for D-Wave[2726]. All this is packaged in highly optimistic business forecasts. The National Research Council of Canada (NRC) estimated that quantum technologies would generate CAN $139B turnaround and create 209,000 employments in Canada by 2045[2727]. It's quite optimistic given it's even larger than the most bullish worldwide forecasts! The forecast in 2022 was of 1,100 jobs creation by 2024.

Quantum industry

In the industry side, you can't escape **D-Wave** and the quantum software specialist **1QBit**. With over 36 quantum startups and SMEs, they are the second largest ecosystem in the world in this respect after the USA and UK.

Private funding includes donations from Michael Lazaridis, one of the RIM BlackBerry co-founders, with $75M to the **Institute for Quantum Computing** at the University of Waterloo and $128M in 1999 to the **Perimeter Institute for Theoretical Physics** also located in Waterloo. Together with Doug Fregin, also co-founder of RIM, they also created the **Quantum Valley Investment Fund** with a total of $100M in funding and the **Quantum Valley Ideas Lab**.

Let us also note the existence of the **Creative Destruction Lab**, a deep techs startup acceleration structure with a specialty on quantum technologies. They are located in Canada (Toronto, Montreal, Vancouver, Calgary, Halifax), in the USA (Atlanta) as well as in Oxford and Paris.

In 2020, of group of industry vendors created **Quantum Industry Canada** (QIC), an association promoting the Canadian quantum industry. It includes D-Wave, 1Qbit, Xanadu, Zapata Computing Computing and ISARA.

[2725] See Quantum Communication Network Activities Across Canada by Barry Sanders and Daniel Oblak, June 2019 (10 slides).

[2726] See Government of Canada contribution strengthens Canada's position as a global leader in quantum computing, March 2021. This funding looks curious considering the company was created back in 1999. But it's probably not yet break even and has a strong need for cash to maintain its activity and leadership in a yet unmatured market.

[2727] Source: Economic impact of quantum technologies.

Figure 852: the Canadian startup ecosystem by category. (cc) Olivier Ezratty, 2022.

Europe

Just making things clear, we're dealing here with geographical Europe, including European Union member states, the UK and Switzerland!

United Kingdom

As with many continental European countries, the United Kingdom has contributed to many advances in quantum physics since the 18th century with precursors and founders, followed by a new generation of scientists in the second half of the 20th century.

Let's mention **Thomas Young** (1773-1829), **Ernest Rutherford** (1871-1937), **Joseph John Thomson** (1856-1940), **James Chadwick** (1891-1974), **Paul Dirac** (1902-1984), **Brian Josephson** (1940), **David Deutsch** (1953), **Andrew Steane** (1965) and even more recently the creators of the QML language, **Thorsten Altenkirch** and **Jonathan Grattage**.

Research

In the UK, the main quantum research laboratories are located in the Universities throughout the country. All of these have one or several quantum physics laboratories. Their main specialties are found later in the UK quantum plan rollout with a lot of advanced photonics (Bristol, Oxford), electron spin (UCL), telecommunication and cryptography (nearly all of them), sensing (same) and the likes. See the list of UK Universities in the UK map in a forthcoming page.

Government funding

At the instigation of the physicist Sir **Peter Knight** (1947), **UK** was the first large country to launch a quantum technology structured plan, the **UK National Quantum Technologies Programme**, announced in November 2013. It had an initial funding of £270M over five years[2728].

[2728] See The UK National Quantum Technologies Programme Current and Future Opportunities by Derek Gillespie, November 2014 (29 slides) and Delivering the National Strategy for Quantum Technologies (5 pages).

This represented a much larger amount of funding than for previous initiatives in innovative materials or robotics. The plan did not start from scratch. It was built on an existing ecosystem of university research laboratories in quantum physics.

The plan was and remains coordinated by the **EPSRC** (Engineering and Physical Sciences Research Council), a non-governmental organization funded and supervised by the government. The plan involves **Innovate UK** (basic research funding), the **Department for Business, Energy and Industrial Strategy**, the **NPL (**National Physical laboratory, where Peter Knight had been Chief Science Advisor, it is UK's metrology lab), the **CGHQ (**their NSA) and **dstl** (army research).

Figure 853: the key public stakeholders of the UK quantum plan. (cc) Olivier Ezratty, 2021.

In a fairly conventional way, the UK plan targeted all the usual quantum fields: computing, security, and sensing with a strong focus on medical imaging. Funding was based on thematic hubs bringing together universities and selected by call for projects (£124M), training, technology transfer and industrialization[2729].

From the outset, the plan showed a strong commitment to creating business and attracting private capital. The original plan was to move research into startups as quickly as possible.

Four quantum hubs cover the major fields of quantum technologies and bring together teams spread over the territory in some thirty universities. All the hubs managers are scientists, supplemented by a business development director and a board of 8 people including industry vendors CTOs.

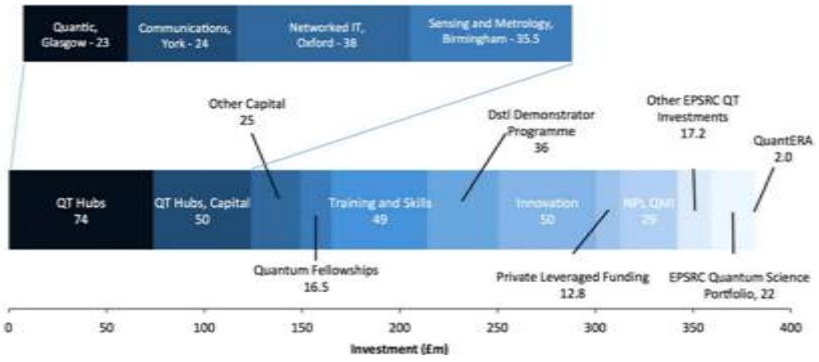


Figure 854: UK's investments in quantum technologies in the first phase of their plan from 2014 to 2019.

UK National Quantum Technologies Hub in Sensors and Metrology

The **UK Quantum Technology Hub Sensors and Timing** covers sensing, including time measurement and involves the universities of Birmingham, Glasgow, Nottingham, Southampton, Strathclyde and Sussex.

QUANTIC

The **Quantic** hub brings together the Universities of Glasgow, Bristol, Edinburgh, Heriot-Watt, Oxford and Strathclyde and focuses on quantum imaging. This gives us two hubs in the field of quantum sensing.

[2729] Diagram source: UK national quantum technology programme by Peter Knight and Ian Walmsley, October 2019 (10 pages).

The **Quantum Computing & Simulation Hub** brings together 17 universities and is led by Oxford University. It took over from the NQIT (Networked Quantum Information Technologies) hub in 2019. It focuses on computing and security issues[2730]. They are working on creating a network of trapped ions quantum computers.

The **Quantum Communications Hub** consolidates a dozen universities: Bristol, Cambridge, Glasgow, Heriot Watt, Kent, Oxford, Queen's Belfast, Sheffield, Strathclyde under the leadership of York University, companies such as Airbus, Toshiba, ID Quantique, Kets, and public agencies.

They are developing a quantum communication network between Bristol, Cambridge and Ipswich via the **UK National Dark Fibre Infrastructure Service** launched by the EPSRC (also linking Southampton and UCL in London)[2731].

This did not prevent the state security agency from expressing skepticism about the suitability of QKD in a four-page white paper published in April 2020[2732].

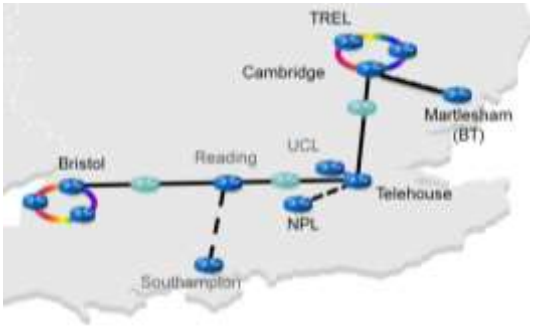


Figure 855: the UK National Dark Fibre Infrastructure Service.

These hubs are finally very multipolar, bringing together universities that are involved in several different hubs, according to the map on the next page[2733]. The United Kingdom has had a lot of ideas in managing this plan over the long-term.

In August 2022, as part of the NQTP, the EPSRC launched a new "Materials for Quantum Network" program led by Peter Haynes (Imperial College London) and Richard Curry (University of Manchester) to focus on quantum matter research. It seems that this topic will soon complement the usual computing/sensing/communications trio of all national quantum plans.

A progress report was published in 2015 by the EPSRC and Innovate UK followed by another interim report, the Quantum Age-Blackett review in 2016 investment launched in 2014 and extending the effort to the algorithmic and software part, in particular in liaison with the **Alan Turing Institute** and the **Heilbronn Institute for Mathematical Research** to propose case studies of computational problems to be solved[2734].

This was followed by a parliamentary report published in November 2018 which supported the continuation of the plan, the launch of a second phase of £350M over the period 2019-2024 and some fine tuning on the coordination between the different stakeholders (hubs, innovation centers, companies) [2735].

[2730] This includes the QuOpaL (Quantum Optimization and Machine Learning) initiative funded by Nokia and Lockheed Martin.

[2731] Diagram source: The Quantum Communications Hub, 2016 (11 slides).

[2732] See Quantum Security Technologies, NCSC, March 2020 (4 pages).

[2733] Map source: UK National Quantum Technologies Plan Strategic Intent, 2020 (38 pages). I added some of the large universities logos. See also UK national quantum technology programme by Peter Knight and Ian Walmsley, October 2019 (10 pages).

[2734] See The Quantum Age Technological Opportunities, 2016 (64 pages) and A roadmap for quantum technologies in the UK, 2015 (28 pages).

[2735] See Quantum technologies, House of Commons Science and Technology Committee, November 2018 (75 pages).

This led to the official announcement of Phase 2 in June 2019, following the recommendations of the House of Commons[2736]. With the expected private sector investments, the total of the two phases of the UK Quantum Plan was estimated at $1,227B.

Phase 2 funding renewed funding for hubs (£94M over 5 years), industrialization projects (£153M from the Industrial Strategy Challenge Fund, over 6 years[2737]), training (£25M over 5 years[2738]). It added the launch of the **NQCC (**National Quantum Computing Centre**)** for the development of quantum computing solutions, with £93M over 5 years[2739].

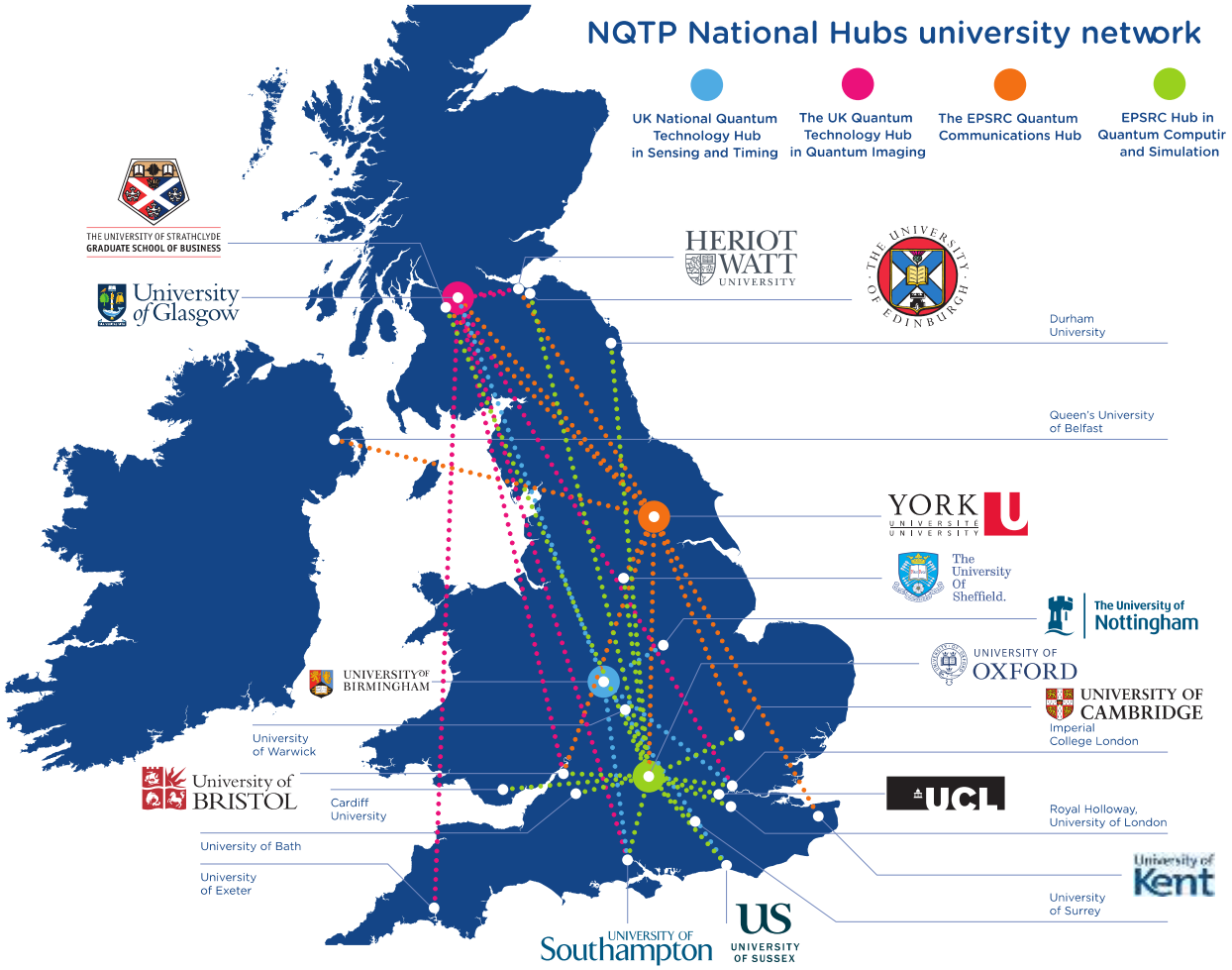


Figure 856: the UK universities map. Source: UKRI and logos added by Olivier Ezratty, 2021.

The first "UK" quantum computer was to be built by Rigetti (US). How can this be? It's linked to Rigetti having acquired a local startup, QxBranch and to its various connections with the local ecosystem and universities. But Oxford Quantum Circuits announced the launch of its cloud based superconducting qubits based computer in July 2021. All in all, the UK government has invested £100M per year in quantum technologies since 2014.

[2736] See UK government invests $194M to commercialize quantum computing by Frederic Lardinois.

[2737] The Industrial Strategy Challenge Fund (ISCF) was a multi-domains initiative of £2.6B backed by £3B of private investments, created to invest in challenges having a strong economical and societal impact. A dedicated Commercialising Quantum Technologies Challenge was then launched in two stages, first in 2018 with £20M and second with £153M completed by £205M from the private sector, in July 2019. To date, in 2021, over 40 such projects were funded. As of late 2020, over £200M were invested in UK startups.

[2738] Doctoral training in quantum technologies is not managed in the hubs but in doctoral centers such as the Quantum Engineering Centre for Doctoral Training in Bristol.

[2739] See Establishing the National Quantum Computing Centre (NQCC), August 2019 (64 slides). The construction started in September 2021.

The bulk of Phase 2 is the NQCC, which is led by **UKRI**, the **EPSRC** and the **STFC** (Science and Technologies Facilities Council), a government agency that conducts research in physics and astronomy and manages the country's major scientific instruments (particle accelerators, lasers, space engineering, etc.) [2740]. This center will produce NISQ and then LSQ computing demonstrators, develop quantum algorithms and software and their uses, and build a community of users around them. The center should open by the summer of 2021 and become fully operational in 2022. It will set up a NISQ machine that should be operational by 2025. In 2020, the preferred technologies were superconducting and ion-trapped qubits.

In May 2022, NQCC launched its SparQ Applications Discovery Programme and a collaboration with OQC. SparQ is a sort of directory aimed at UK-based companies and researchers who are looking for case studies of quantum computing[2741].

Figure 857: NQCC positioning. Source: NQCC. 2021.

The UK had recovered approximately 14% of the budgets for the first wave of European Quantum Flagship projects by October 2018. Despite the Brexit, the country will continue to benefit from it, as the collaboration with Europe on research survives the Brexit. For example, John Morton's UCL laboratory is part of the flagship project QLSI on silicon qubits driven by CEA-Leti and awarded in March 2020.

In November 2021, the UK signed a partnership agreement with the USA[2742], the first of a long list of USA bilateral partnerships later signed with Australia, all Nordic countries and Switzerland.

Quantum industry

On the entrepreneurial side, around 40 quantum technologies startups were launched in the UK with a good balance by category. It is the third country in the world in terms of the number of startups, behind the USA and Canada. In October 2022 was created **UKQuantum**, a quantum industry association with Kets, Orca Computing, Arqit, Nu Quantum, Riverlane and Oxford Instruments among its funding members.

The intellectual property management company **IpGroup,** launched in August 2020 a £12M fund to fund startups, these being selected by the independent agency **UKRI**. Projects funding range from £125K to £2M. Let's also mention the **Quantum Technology Enterprise Centre** from the University of Bristol which was a sort of startups incubator and training program for quantum startup founders. The QTEC incubation program offered a 12-months salaried fellowship to quantum scientists during the build-up of their startup and business skills training.

[2740] UKRI (UK Research and Innovation) is an autonomous non-governmental organization created in April 2018 with an annual budget of £7B and consolidates seven former research councils including the EPSRC and STFC, Innovate UK and Research England.

[2741] See Industry engagement prepares UK for quantum transformation, PhysicsWorld, November 2021 and Early adopters position themselves for quantum advantage, June 2022.

[2742] See Cooperation in Quantum Information Sciences and Technologies Joint Statement, November 2021.

Since 2016, QTEC helped the creation of 31 startups including KETS, QLM, Nu Quantum, Quantum Dice and Vector Photonics. The program funding ended in 2021 and QTEC is looking for funding to launch a new "cohort" of quantum entrepreneurs.

Figure 858: the UK startup scene is the most active in Europe (the old Europe, with them, before Brexit...). (cc) Olivier Ezratty, 2022.

Notable players are **Oxford Instruments** (cryogenics), **Oxford Quantum Circuits (**superconducting qubits[2743]), **Quantum Motion Technologies (**silicon qubits), **Cambridge Quantum Computing (**operating system, software, services, which merged with Honeywell Quantum Systems in 2021), **TundraSystems (**photonic qubits), **Orca Computing (**photon qubits) and **River Lane Research** (software). On the other hand, no major company in the country seems to be particularly invested in quantum computing, except perhaps in telecommunications.

Germany

Germany is a land of dense basic research in quantum technologies. It builds on a strong history of the many German founders of quantum physics with **Max Planck**, **Albert Einstein**, **Werner Heisenberg** and many others[2744]. It also has a strong ecosystem of industry vendors, particularly in quantum enabling technologies.

Research

The main research organizations and laboratories involved in quantum technologies are:

Max Planck Institute for Quantum Optics (MPQ), based in Munich, is one of the 84 MPIs and their 24,000 employees. It was the home of Klaus von Klitzing who discovered the quantum Hall effect in 1980 and got the Nobel prize in physics in 1985.

[2743] Oxford Quantum Circuit obtained funding from Innovate UK in April 2020 in a consortium of four companies and two universities. See Oxford Quantum Circuits-led consortium wins Grant to Boost Quantum Technologies in the UK by Quantum Analyst, April 2020.

[2744] See The Innovation Potential of Second-generation Quantum Technologies by the National Academy of Science and Technology, July 2020 (96 pages) which contains a list of key people in German quantum research at the beginning.

They specialize in cold atom-based qubits in particular. This MPI is associated with the International Max Planck Research School also based in Munich. Two other MPIs are dedicated to information technology, but do not seem to be invested in quantum.

Munich Center for Quantum Science and Technology (MCQST) in Munich was launched in 2019 and brings together Munich's quantum research centers: the MPQ, the Walther-Meißner-Institute for Low Temperature Research (WMI) and the city's two leading scientific universities: Ludwig-Maximilians-Universität München and Technical University of Munich (TUM). It covers all quantum technologies (simulation, computing, communication, sensors). The whole with a budget of 31M€ over five years and about 55 permanent researchers. In February 2022, the Bavaria region announced an additional funding of 300M€ for the Munich quantum valley supplemented by 80M€ of federal funding. Among other things, the funding will help build the upcoming Center for Quantum Computing and Quantum Technologies (ZQQ), a center that will provide access to superconducting, ionic and atomic qubits quantum computers. Meanwhile, in January a D-Wave Advantage was installed at Julich in JUNIQ (Jülich UNified Infrastructure for Quantum computing) that was created in 2019.

Fraunhofer Institutes for Applied and Partnership Research with its 72 institutes and 26,600 people. They comprise several institutes specialized in quantum physics: the **IAF** (Institute for Applied Solid State Physics) in Freiburg, the **IOF** (Institute for Applied Optics and Precision Engineering) in Jena, the **ILT** (Institut for Laser Technology) in Aachen, **FOKUS** (Open Communication Systems) in Berlin, **SCAI** and **IAIS** (quantum machine learning) in Sankt Augustin and **ITWM** (quantum HPC) in Kaiserslautern. On top of that must be accounted cleanrooms from **IPM** in Freiburg and **IPMS** near Dresden. In March 2022 was launched EIN Quantum NRW, a competence network for photonics-based quantum technologies in the North Rhine-Westphalia (NRW) lander, involving the Fraunhofer Institutes **FHR** (High Frequency Physics and Radar) and **IAIS** (Intelligent Analysis & Information).

Helmholtz Association groups 18 Research Centers that conduct basic research in response to major societal challenges, with a total of 40,000 people. It includes the Quantum Laboratory of the **Jülich Forschungszentrum** (*aka* Jülich FZ or Jülich Research Center) located between Aachen and Cologne and headed by Kristel Michielsen[2745], where Tommaso Calarco, who coordinates the European Quantum Flagship, also works. He is associated with the University of Aachen in the **JARA Institute Quantum Information** (IQI). The Helmholtz Network also includes the **Institute of Photonics and Quantum Electronics at the** Karlsruhe Institute of Technology (KIT).

Leibniz Association with its community of 96 centers conducting basic research includes the Institute for Solid State and Materials Research (IFW) in Dresden, Germany, which focuses on superconductivity and magnetism, the Institute of Photonic Technology (IPHT) in Jena, Germany, the Max-Born-Institute for Nonlinear Optics and Short Pulse Spectroscopy (MBI) in Berlin, Germany, and the Paul Drude Institute for Solid State Electronics (PDI) in Berlin, Germany.

Institute for Complex Quantum Systems at the University of Ulm between Stuttgart and Munich.

PTB is the federal office of sensing, which is obviously investing on quantum sensing like the NIST.

BSI is the federal office for information technology security[2746].

At last, let's mention here the **Quantum Alliance** which regroups the German clusters of excellence and research centers working in quantum science and technology.

[2745] Jülich Forschungszentrum started in 1956 in nuclear research. It also houses a number of supercomputers, such as the CEA's DAM at Bruyères-le-Châtel in France or the various US DoE research centers across the USA.

[2746] In Germany, the federal agency that protects information systems, which is the counterpart of the French ANSSI, published in May 2018 the report Entwicklungsstand Quantencomputer (*State of the art of quantum computing),* which provided an update on quantum computing, focusing in particular on cybersecurity issues (231 pages, in English). This was a very good overview of global quantum computing research. It provided a surprisingly accurate inventory of efforts in the field, particularly in US public research. But things have changed a bit since 2018.

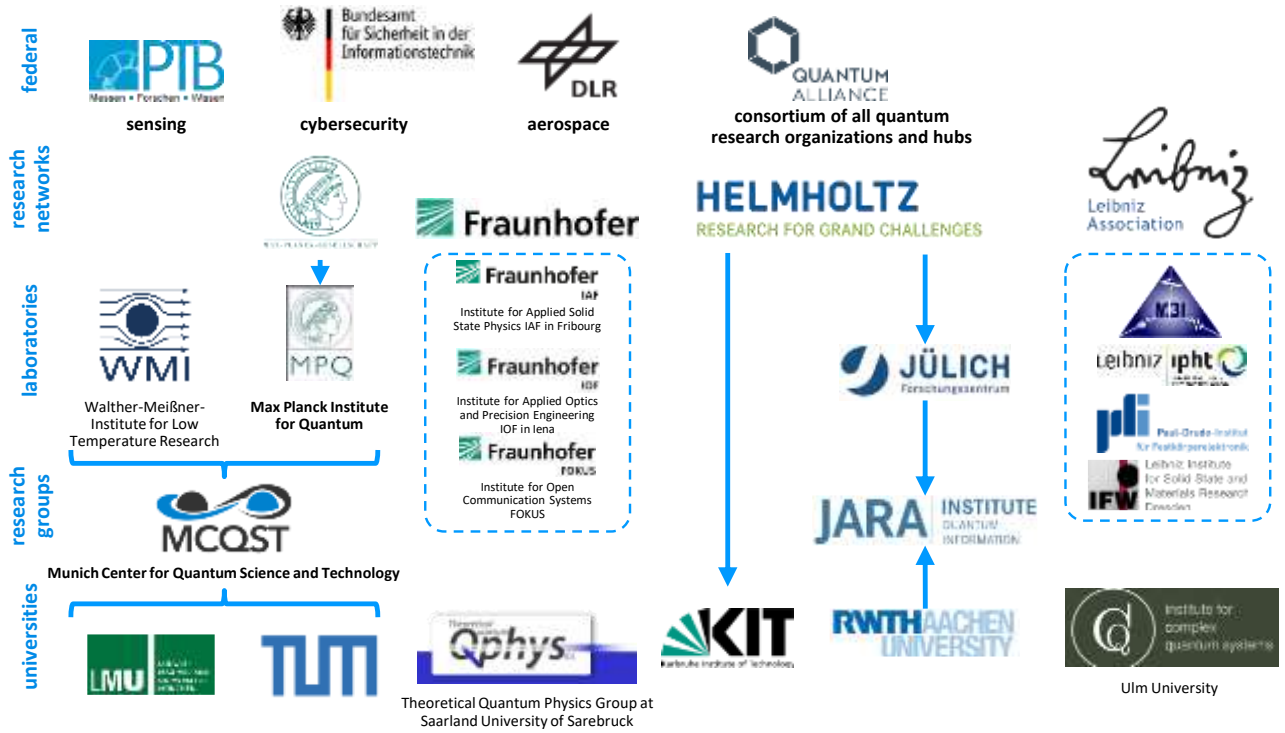


Figure 859: understanding the research ecosystem in Germany. (cc) Olivier Ezratty, 2022.

Government funding

In September 2018, the German Federal Research Ministry announced €650M in funding for quantum technologies over four years (2018 to 2022)[2747]. Like all such plans, it funds projects in quantum computing, quantum communication and quantum metrology. In September 2019, IBM announced that it would join this plan and install a quantum computer in Germany addressing researchers and cloud usages. It is not certain that this is the best approach to develop a German and European quantum industry, at least on the hardware side. The computer was actually launched early in 2021 in the Stuttgart region in an IBM facility[2748].

In June 2020, the German government more than doubled its efforts by announcing a seemingly incremental €2B in funding for its quantum plan, including investment in two quantum computers[2749]. The $2B included the initial 650M€ of the 2018 plan. The German government put in place a scientific and industry experts board of 16 members to propose a roadmap and funding allocation with a Joint presidency of a scientist (Stefan Filipp from TU Munich) and an industry member (Peter Leibinger from Trumpf). It made some proposals in December 2020 including creating an independent coordination body, Deutschen Quantengemeinschaft (DQG). In January 2021, the BMWi disagreed with some of these proposals, estimating that too much funding was directed to fundamental research at the expense of startups.

In May 2021, the plan was split in two parts with 1,1B€ managed by the Federal Ministry of Education and Research (BMBF) and 878M€ by the Federal Ministry of Economic Affairs and Energy (BMWi), focused on applications developments.

[2747] See German Government Allocates €650M for quantum technologies, the German government's announcement (in German) and the plan itself (51 pages).

[2748] It lead to misleading information regarding a supposed investment of the German government in IBM of $717M corresponding to these €650M in German government to invest $717M in IBM quantum computing efforts, WRAL Techwire, September 2019. At best, only a small share of these 650M€ were dedicated to cofund the IBM initiative in Germany. Looking at what was done in 2022 in Canada, you can guess that the German government participation was around 40-60M€.

[2749] See Germany: 2 Billion euros for quantum technology, June 2020.

One key showcased goal for this plan is to build two national quantum computers with 24, then 100 and later 500 functional (physical) qubits. DLR (Germany's Aerospace Center) was to receive the bulk of this funding (740M€) to work with small, mid-sized and large companies and create two related consortia. In 2022, DLR awarded QuiX a 14M€ contract to build a photonic quantum computer and Universal Quantum (UK) a 67M€ contract to build two trapped ions-based quantum computers to be installed in Hamburg. Their investment in trapped-ions caps 208M€ and also involves EleQtron (Germany).

The Federal government is not the only public body funding quantum research. Landers added about 500M€ including the 300M€ from the Bavarian region (probably with half of it coming from the Lander and the rest from the industry). How is that possible? German Landers (regions) have a very large budget independent from the Federal government (in a 42%/58% ratio). Bavaria being a large Lander, they have the means to invest significantly on research[2750].

For example, the lander cofounded two quantum research projects, NeQuS (quantum networks between quantum computers) and IQ-Sense (quantum sensing) for a total of 3.5M€ in August 2022.

Like with each country, the German quantum plan covers quantum computing, communications and sensing. The 2B€ effort is planning many projects, particularly in quantum computing research. Let's list some identified projects.

GeQCoS (German Quantum Computer based on Superconducting Qubits) with 14,3M€ BMBF funding, involving Fraunhofer Fribourg and Infineon). It was launched in February 2021 and will seemingly use German originated quantum technologies. The ambition is modest with a goal of 50 qubits.

QSolid is another superconducting qubit computer that would be tied to a HPC at the Jülich Supercomputing Centre, including optimized firmware and software. It will start with a 10-qubit system. The project budget is 76.3M€ with 89.8% being funded by the BMBF over five years starting in January 2022. On top of Julich, it involves Fraunhofer IPMS and Fraunhofer IZM-ASSID, Karlsruhe Institute of Technology (KIT), Leibniz IPHT in Jena and the PTB.

DAQC is a project launched in February 2021 which got 12.4M€ from BMBF. It is coordinated by IQM Germany and involves Jülich, Infineon and ParityQC from Austria as well as the Leibniz Computing Center and Free University of Berlin. It will create a digital-analog superconducting qubits system using IQM's architecture. This project is related to the Quantum Flagship OpenSuperQ project.

MANIQU is a project running from 2021 to 2023 related to the usage of NISQ hardware to undertake quantum simulations to simulate new materials. The participants are HQS, Bosch, BASF, the Friedrich-Alexander University in Erlangen, and the Heinrich-Heine University in Düsseldorf.

Q-Exa is yet another superconducting qubits project announced in November 2021, involving IQM. Their systems will be integrated with HPCs. The project funding is of 45.3M€. It seems to be a follow-up project to DAQC.

PhotonQ is a photonic quantum computer project launched with a funding of 16M€ and led by the University of Stuttgart with participations from the Universities of Würzburg, Mainz and Ulm, TUM Munich, the Institute of Microelectronics Stuttgart and Vanguard Automation GmbH. The four-year project first goal is to create a demonstrator of 8 qubits using MBQC and deterministic photon sources, silicon photonics circuits and new single-photon detectors.

[2750] A false number on German public investment circulated with a hefty 4,456M€ from Interference Advisors. This report is amazingly entirely wrong, making double bookings of the 2018 and 2020 announcements, using unsafe press reference ($717M allocated to IBM's effort...) and double-accounting subsequent quantum projects which are already part of the 2B€ 2020 announcement.

PhoQuant is another photonic quantum computer project, led by Q.ANT, a subsidiary of Trumpf, with the notable participation of Christine Silberhorn's Paderborn University lab and many others (Universities of Münster, Jena, Ulm, Humboldt Berlin, Fraunhofer IOF and IPM, HQS, Swabian Instruments, TEM Messtechnik, ficonTEC Service and MenloSystems).

ATIQ is a trapped ions computing project. The German government is funding 81,1% of the 44,5M€ project that will last from 2021 to 2026. Participants include Toptica (lasers). The project is coordinated by the Leibniz University Hannover with participations from Johannes Gutenberg University Mainz, University of Siegen, TU Braunschweig, RWTH Aachen, Physikalisch-Technische Bundesanstalt, Fraunhofer-Gesellschaft, AMO, AKKA Industry Consulting, Black Semiconductor, eleQtron, FiberBridge Photonics, Infineon, JoS QUANTUM, LPKF Laser & Electronics, ParityQC, QUARTIQ, Qubig, AQT, Boehringer Ingelheim, Covestro, DLR-SI, Volkswagen and QUDORA Technologies.

QUASAR is a semiconductor-based project using shuttling electrons with a QuBus, a quantum bus to transport electrons and their quantum information over distances of 10 µm. The partners are Infineon, HQS, Fraunhofer (IAF, IPMS), Leibnitz Association (IHP, IKZ) and the Universities of Regensburg and Konstanz. The project will run until 2025 to create 25 coupled qubits.

The resulting computer is to be deployed at JUNIQ. Jülich is also participating to the European Flagship QLSI project driven by CEA-Leti in France. QUASAR got a 7.5M€ funding from BMBF[2751].

QuaST is an enabling technologies project (Quantum-enabling Services and Tools for Industrial Applications) that will develop high-level libraries automatically decomposing and optimizes a solution into classical and quantum parts. The project is run by the Fraunhofer Institute for Cognitive Systems IKS with other Fraunhofer Institutes (AISEC, IIS, IISB), the Leibniz Supercomputing Center, and the TUM, plus DATEV, Infineon, IQM and ParityQC. The project sponsor is German Aerospace Center (DLR). The project will last 4 years and got a funding if 7.7M€.

QLindA is a quantum machine learning project led by Siemens with participations from Fraunhofer IIS, IQM and others.

We also have three enabling technologies projects: **QuMIC** (Qubits Control by Microwave Integrated Circuits, 6,3M€, 2021-2024), **qBriqs** (2M€, 2021-2024, compact cryogenic connectors, qubit readouts TWPA and HEMT amplifiers, filters and attenuators, DACs and ADCs and DC flux current generators) and **HIQuP** (2021-2024, 2,2M€, superconducting and cryogenic qubit control electronic circuits).

Germany also launched the creation of two QKD-based telecommunications networks, both funded by BMBF:

QuNET (165M€) which uses a standard QKD associated with terrestrial and satellite links. The project involves several Fraunhofer Institutes including the Heinrich Hertz Institute (HHI), the Max-Planck Institute for the Physics of Light and the German Aerospace Center (DLR)[2752]. The project launched in November 2019 was scheduled to last seven years and aims to create a communications protection infrastructure for the German government. This should lead to the creation of a secure European network. The private sector is also involved with Deutsche Telekom, ADVA Optical Networking and Tesat-Spacecom. Test sites will be implanted in Bavaria, Saxony and Thuringia.

Q.Link.X (14.8M€) for the creation of a terrestrial network in optical fiber and QKD based on quantum repeaters, managed by the Fraunhofer HHI[2753].

[2751] See Quanten-Shuttle zum Quantenprozessor "Made in Germany" gestartet, Jülich, February 2021.

[2752] See Germany's QuNET Receives €165 Million To Establish Quantum Communications Infrastructure, 2019, German ministry and research sector join forces to launch major quantum communications initiative, May 2019 and German Aerospace Center In QuNET Working On Satellite-Based Quantum Communication, November 2019.

[2753] See Germany splashes further €15m in quantum networks R&D project, October 2018.

Germany leads or participates to various European Flagship programs: **MetaboliQs** (NV center based medical imaging), **UNIQORN** (photon qubits chipsets), **S2QUIP** (hybrid photonic chipsets), **QRANGE** (QRNGs).

At last, the German national plan is funding three other initiatives associating research labs and industry vendors: **BrainQSens** (medical imaging with NV centers, 2,8M€), **Opticlock** (compact optical clock to synchronize communication networks, 6M€) and **QUBE** (space QKD with Cube-Sat, 3,12M€).

Quantum industry

On the private sector side, Germany has a various set of quantum startups including **Avanetix** (hybrid algorithms), **InfiniQuant** (CV-QKD cryptography), **PicoQuant (**photon counters), **Kiutra** (magnetic cryogenics), **HQS Quantum Simulations (**algorithms), **JoS Quantum** (software in finance), **QuantiCor Security, QuBalt (**both in post-quantum cryptography) and **QuTools** (sensing).

Figure 860: the German quantum industry. (cc) Olivier Ezratty, 2022.

Only a few quantum computing hardware startups have been created and recently like **It'sQ** (photonics) and **Planq** (cold atoms).

Many of the country's major industrial companies are also interested in quantum applications, particularly in chemistry (**BASF**), health (**Merck),** telecommunications (**Deutsche Telekom)**, components and automotive (**Bosch**, **Daimler**).

PlanQK (Platform and Ecosystem for Quantum-Assisted Artificial Intelligence) is a project to build a marketplace of quantum assisted artificial intelligence components, at first, quantum inspired algorithms. It gathers scientists from various universities (Stuttgart, Berlin, Munich) on top of Accenture, HQS, Deutsche Bundesbahn, Deutsche Telekom and other industries. It is supported by BMWi with a total funding of €19M.

In June 2021, ten German companies created **QUTAC** (Quantum Technology and Application Consortium) to develop quantum computing usable industrial applications in the technology, chemical and pharmaceutical, insurance and automotive industries.

The consortium was launched by BASF, BMW Group, Boehringer Ingelheim, Bosch, Infineon, Merck, Munich Re, SAP, Siemens, and Volkswagen. One of its goals is to create a cross-industry application portfolio.

There is another thing in Germany called **QuCUN** (Quantum Computing User Network) which also comprises SAP and BASF as partners. It is supported by the German Federal Ministry of Education and Research (BMBF).

The QuCUN platform launched in 2022 is "*designed to give potential quantum computing users – from SMEs to industrial giants – a central point of entry*". Does it mean that QUTAC is peripheral?

Let's also mention **PushQuantum**, a student initiative born in Munich that organizes lectures, workshops and entrepreneurship labs for wannabee quantum entrepreneurs.

Austria

Austria**'s** investment in quantum computing is concentrated in the **IQOQI**, the Institute for Quantenoptik und Quanteninformation in Innsbruck and Vienna. It focuses in particular on the design of trapped ions qubits. This led to the start-up **Alpine Quantum Technologies**, founded by Rainer Blatt and Thomas Monz of the IQOQI.

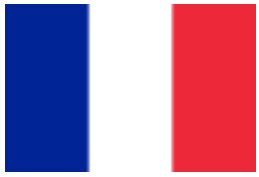
It has received €12.3M in public funding and competes with the **IonQ** (USA), which is positioned in the same niche of ion-trapped qubits, as well as **Quantinuum**. One other notable Austrian startup is **ParityQC** which develops ParityOS and a related architecture to codevelop quantum hardware and software platforms.

The Vienna Center for Quantum Science and Technology (**VQC)** is a partnership between the University of Vienna, Vienna University of Technology and the Austrian Academy of Sciences. It brings together a critical mass of about 20 quantum physics research laboratories.

Austria is also invested in quantum cryptography and is associated with China, with whom it has conducted experiments in sending quantum keys via the Micius satellite to set up secure video communication. **IQOQI** is collaborating with the **Grenoble University Space Center** (CSUG) in the development of a CubeSat-type quantum key relay satellite, similar to the one in Singapore, in the **Nanobob** project (presentation, 13 slides).

The Austrian government announced a formal quantum plan in June 2021 with 107M€ over 2022-2026 covering research and quantum technology developments. Quantum Austria is part of the Austrian 10 years Research Technology and Innovation strategy 2030 launched in 2020, in a country that spends overs 3.18% of its GDP in R&D. Part of the funding comes from the European Resilience and Recovery Facility (NextGenerationEU). The plan is managed with RFPs from the Austrian Research Promotion Agency (FFG) and the Austrian Science Fund (FWF).

France



France has a good breadth of research and industry activities in quantum technologies. Let's first mention its greatest scientists with **Henri Poincaré** (1854-1912), **Louis de Broglie** (1892-1987, Nobel prize in physics in 1929), **Alfred Kastler** (1902-1984, Nobel prize in physics in 1966), and **Claude Cohen-Tannoudji** (1934, Nobel prize in physics in 1997).

Serge Haroche (1944, Nobel Prize in Physics in 2012) is a pioneer in cavity quantum electrodynamics and on the interaction between photons in a superconducting cavity and Rydberg atoms passing through the cavity).

Of course, we can add **Alain Aspect** (1946), who invalidated Bell's inequalities in 1982 and verified the principle of non-locality of entangled photons, a cornerstone of the second quantum revolution, and was awarded the Nobel prize in physics in 2022. Other domains worth mentioning are in quantum photonics with **Pascale Senellart**, neutral atoms physics with **Jean Dalibard** and **Antoine Browaeys**, silicon spin qubits with **Maud Vinet**, **Tristan Meunier** and **Silvano de Franceschi**, quantum cryptography and telecommunications with **Philippe Grangier**, **Frédéric Grosshans** and **Eleni Diamanti** and PQC with various cryptographers like **Damien Stehlé**.

Research

Public research is organized around three national research organizations: **CNRS**, **CEA** and **Inria**. The first is involved in fundamental research in physics, mathematics, and algorithms. The second also does fundamental research in physics, particularly on superconducting qubits, and applied research on electron spins qubits as well as on photonics. At last, Inria is doing research in computer science, and for quantum technologies, on quantum error correction, cryptography, and quantum algorithms. Many laboratories are joint research units ("Unités Mixtes de Recherche" in French) between Universities, these national organizations and sometimes industry vendors like Thales.

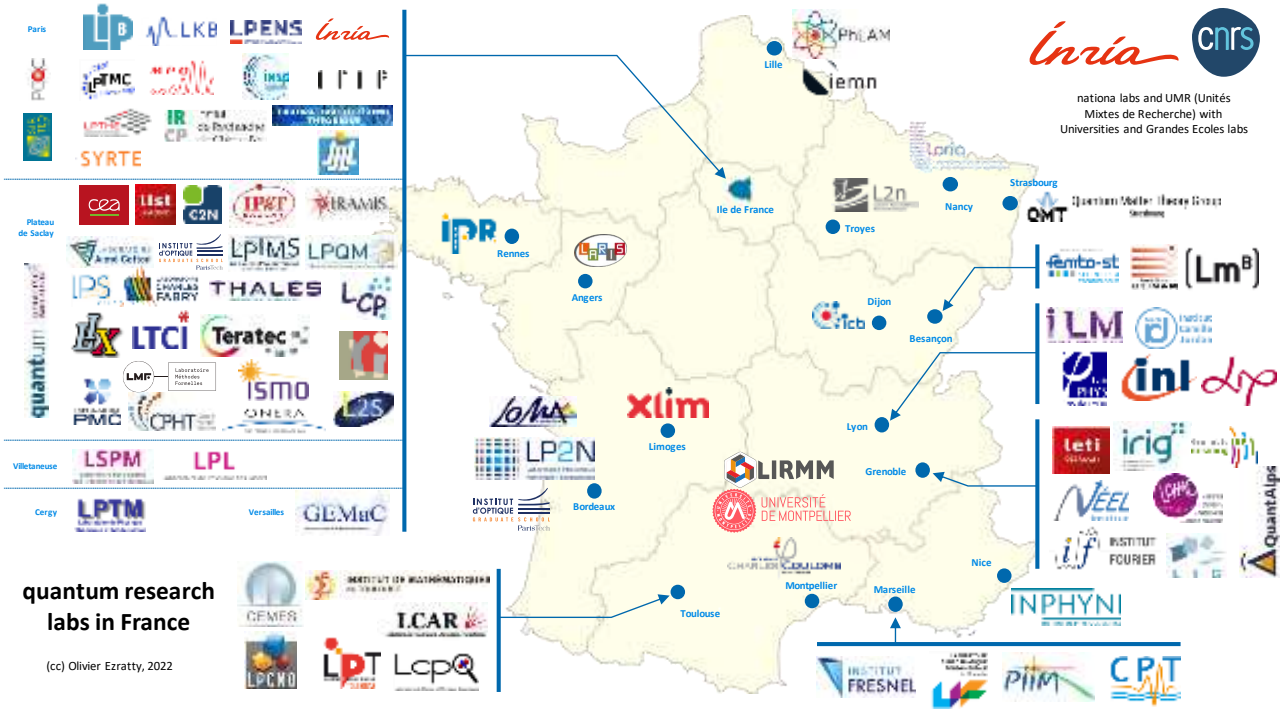


Figure 861: a beautiful map of France's research labs. (cc) Olivier Ezratty, 2022.

These research laboratories are mainly located in Ile de France and in Grenoble, but other regional locations are active such as Toulouse, Montpellier, Marseille, Lyon, Bordeaux, Besançon and Lille[2754]. Like many large countries, French laboratories are exploring many qubit tracks: superconducting, cold atoms, electron spins, photons and topological matter.

[2754] For this purpose, I consulted the websites of these laboratories and the fields of research they present, plus, when they were easy to find, the scientific publications of the researchers of these laboratories.

Public sector researchers get projects funding by answering various country and European RFPs[2755]. Of the more than 20 quantum startups in France 2021, 7 are from CNRS, two from Inria, two from ENS and one from CEA.

Ile de France

Ile de France is home to a good half of the country's research laboratories devoted to quantum technologies. Let's start with the laboratories that are located within Paris.

Inria's efforts in the Paris region are concentrated in the Quantic (Quantum Information Circuits) team of Pierre Rouchon, Mazyar Mirrahimi, Zaki Leghtas and Alain Sarlette, which is a joint venture between the CNRS, ENS and the Ecole des Mines de Paris.

They work on mathematical models of superconducting qubits, on quantum error correction (including cat-qubits), on proof of superiority of quantum algorithms and on cryptographic issues[2756]. The Cosmiq team led by Anne Canteaut, works on cryptographic algorithms, and David Pointcheval's Cascade team, works in cryptography and PQC. Inria also jointly runs many other teams with various labs from CNRS.

Other Inria teams are dedicated to quantum science and technology: IQA (LTCI, Saclay) is working on networking aspects in quantum computing, cryptography and photonics and quantum machine learning, QI with LIP6, MOCQUA with LORIA, CAPP (LIG, Grenoble) on contextuality and quantum combinatorial games, AlgoComp with IRIF, MC2 with LIP Lyon and PACAP with IRISA and Inria Rennes working on mapping quantum circuits to particular architectures and the new QUACS team on quantum algorithms in Saclay.

LIP6 (Laboratoire d'Informatique de la Sorbonne) hosts several recognized specialists in cryptography and quantum telecommunications (QKD): Eleni Diamanti was awarded a European Synergy Grand ERC for her work in the QUSCO (Quantum Superiority with Coherent State) project. Elham Kashefi is co-founder of the VeriQloud startup. She is also working on verified quantum computing, secure multiparty quantum computing, and features to achieve quantum advantages.

The **LPENS** (Laboratoire de Physique de l'Ecole Normale Supérieure) is the result of the merger in early 2019 of several physics research laboratories at ENS Paris, including the **LPA** (Laboratoire Pierre Aigrain), which specializes in nanotechnology and photonics.

They are working on numerous nanotechnologies used for the creation of qubits and the transport of quantum information: superconducting thin films, superconducting and microwave circuits for their control, two-dimensional electron gases with very high mobility, semiconductor quantum boxes, qubits based on carbon nanotubes.

Taki Kontos and Audrey Cottet's teams are at the origin of the creation of carbon nanotubes used as electron traps potentially usable in electron spin qubits, which led to the creation of the **C12** startup, already mentioned. The lab is also a participant on the work on cat-qubits related to the startup Alice&Bob.

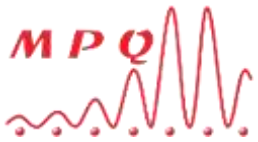
[2755] Some obtain ERC Grants (European Research Council): Synergy Grants for a few handfuls of teams (up to €14M over 6 years), and more often Starting (young researchers, up to €1.5M), Consolidators (experienced researchers, up to €2M) and Advanced (emeritus researchers, up to €2.5M spread over 5 years). Then European FET funding, funding via the European Quantum Flagship, or finally through various calls for projects at the national level (ANR).

[2756] This is specified in Inria strategic scientific plan 2018-2022, 2018 (93 pages), pages 47 and 48.

The **LKB** (Laboratoire Kastler Brossel) from ENS Paris focuses on quantum information and photonics, interactions between light and matter (Nicolas Treps and Valentina Parigi), quantum simulation and precision sensing with cold atoms (Christophe Salomon).

Thibault Jacqmin is working on microwave photon generation with NEMS (nano MEMS).

The IRIF (Institut de Recherche en Informatique Fondamentale) from CNRS and the University Paris Diderot is led by Frédéric Magniez who also teaches at Collège de France and hosts Iordanis Kerenidis, Sophie Laplante and two Inria teams. It works in quantum computing, cryptography and communications.



The **MPQ** laboratory (Materials and Quantum Physics) of the University Paris Diderot is particularly interested in the technique of ions trapped in the Quantum Physics and Devices (QUAD) and QITE (Quantum Information and Technologies) groups. But also, to the generation of entangled photon pairs (Sara Ducci).

The **LPTHE** (Laboratoire de Physique Théorique et Hautes Energies) of the University Paris Sorbonne works in condensed matter and statistical physics with applications in superconducting qubits.

The **INSP** (Institut des Nanosciences de Paris) of Paris-Sorbonne University is a generalist laboratory on nanosciences. They work in particular in different branches of photonics, on NV centers, on color centers qubits in silicon carbide, on spin and magnetism and on photonics components in III-V materials.

The **IRCP** (Institut de Recherche de Chimie Paris) associated with the Ecole Nationale Supérieure de Chimie ParisTech conducts research in innovative materials.

Philippe Goldner is working on the creation of qubits based on nanocrystals doped with rare earth ions such as europium or erbium, and is involved in the SQUARE project of the European Quantum Flagship, coordinated by the Karlsruhe Institute of Technology and also involving Thales. The laboratory is also involved in the European Quantum Flagship **ASTERIQS** project which is working on NV-based qubits in diamonds.

The **LPEM** (Laboratory of Physics and Study of Materials) of the ESPCI and the UMPC works in particular in superconductivity as well as on the fermions of Majorana.

The **LPTMC** (Laboratoire de Physique Théorique de la Matière Condensée) of the University Paris-Sorbonne has among other things several teams working on condensed matter physics like Jean-Noël Fuchs and Julien Vidal on topological insulators and Majorana fermions and Rémy Mosseri working on quantum information with topological qubits.

SYRTE (Laboratoire Systèmes de Référence Temps-Espace) located at Paris Observatory works in quantum sensing, in particular gravimetry, quantum gyroscopes and on time measurement with atomic and optical clocks. They are partnering with NIST. The quantum gravimeter and interferometry team is led by Franck Pereira dos Santos. SYRTE is led by Arnaud Landragin.

The **Laboratoire Jacques Louis Lions** (LJLL) is specialized in applied mathematics. It focuses on the analysis, modeling and high-performance scientific computation of phenomena represented by partial differential equations. Mario Sigalotti and Ugo Boscain, who specialize in the control of quantum systems and are also members of Inria, are among others.

The **Laboratory of Theoretical Chemistry** at Sorbonne University is directed by Jean-Philippe Piquemal (co-founder of Qubit Pharma) and is interested in computational chemistry, including quantum.

In September 2020, the **Quantum Innovation Center Sorbonne** (QICS) was inaugurated, a collaborative research structure associating LIP6, the LKB of the ENS and Inria.

The **Saclay plateau** has an even higher density of laboratories, located south-west of the Paris region. Most of these entities are consolidated in **Université Paris Saclay**.

At the **CEA**, Daniel Esteve's Quantronics team at the Iramis laboratory in Saclay has been working on superconducting qubits for nearly 20 years. Daniel Esteve's laboratory includes about fifteen people and is now managed by Hugues Pothier.

IphT (Institut de Physique Théorique de Saclay) associates CEA and CNRS. They work on the physics of condensed matter, including high-temperature superconductors, and on Majorana fermions. But their main focus seems to be mainly astrophysics.

The **LAC** (Laboratoire Aimé Cotton) is located at the ENS Saclay. It also works on cold atoms and interactions between atoms and light. In particular, they create qubits by combining an optically active erbium ion and a nuclear spin of yttrium.

The **C2N** (Centre des Nanosciences et des Nanotechnologies) of CNRS and Université Paris Saclay is a key quantum photonics laboratory. It is the home to Pascale Senellart and Jaqueline Bloch's labs. They work in particular on light-matter coupling in semiconductors. It also host quantum electronics teams (Frédéric Pierre).

The **LPS** (Laboratoire de Physique des Solides) works on magnetism, Josephson junction superconductors, thermodynamics, superconducting spintronics and quantum dynamics. They also develop codes for quantum and semi-classical dynamics and quantum control with applications in quantum information.

The **LPTMS** (Laboratoire de Physique Théorique et de Modèles Statistiques) has several strings to its bow in quantum physics without the link with quantum computing being immediately detectable.

The **LCP** (Laboratoire de Chimie Parisud) works on superconductors and on the dynamics and control of ions trapped by laser pulses. They develop hybrid computational models of quantum chemistry (quantum+traditional) using MCTDH (Multi-configuration time-dependent Hartree) which allows to solve the Schrödinger equation for the simulation of interactions between atoms in molecules.

On the program: condensed matter physics, modeling of classical and quantum systems via statistical physics, quantum chaos, number theory and quantum chaos, theoretical aspects of quantum information; cold atoms, quantum integrable systems, quantum groups, etc.

TelecomParistech's **LTCI** (Laboratoire Traitement et Communication de l'Information) is an industry laboratory operating with partnerships with the private sector and via chairs. Its "Quantum Information and Applications" (QIA) team specializes in the theoretical and experimental aspects of quantum communications.

They develop hybrid CV-QKD-based quantum cryptography protocols compatible with telecom operators' fiber networks and QKD repeaters. They are contributor, founding member and reporter to the ETSI QKD-ISG on the QKD standardization processor. The team is led by Isabelle Zaquine and includes Romain Alléaume.

ISMO (Institut des Sciences Moléculaires d'Orsay) works on quantum dynamics, interactions between heavy particles and electrons at low temperature, light/matter coupling and on software for the simulation of quantum physics.

The **CPht** (Centre de Physique Théorique de Polytechnique) is specialized among other things in the physics of condensed matter. But not to the point of creating superconducting qubits! We find there Karyn Le Hur's group, who is specialized in condensed matter physics.

The **Charles Fabry Laboratory** of the Institute of Optics Graduate school (IOGS) is specialized in lasers and quantum optics. It is home to Alain Aspect, Philippe Grangier as well as Antoine Browaeys, co-founder of the startup Pasqal and its laser-controlled cold atom qubits.

The **LIX** (Laboratoire d'Informatique de l'Ecole Polytechnique) is particularly active in post-quantum cryptography algorithms.

The **PMC** (Laboratoire de Physique de la Matière Condensée) is another laboratory of the Ecole Polytechnique. They work in particular on spin dynamics in semiconductors and magnetic thin films.

The **L2S** (Signals and Systems Laboratory) of CentraleSupelec is active in quantum systems research. In particular, the L2S is staffed by Zeno Toffano, who is focused on quantum states measurement.

The **LPQM** (Laboratory of Quantum and Molecular Photonics) associates the ENS Paris Saclay and the CentraleSupelec school. Their domains are coherence and quantum correlations.

The **LRI** (Laboratoire de Recherche en Informatique) located at CentraleSupélec is managed by Benoît Valiron, who teaches and conducts research in quantum computing, a field that is still relatively under-taught in engineering schools.

The **LMF** (Formal Methods Laboratory) was created in 2021 as a joint research center of University Paris-Saclay, CNRS, ENS Paris-Saclay, Inria, and CentraleSupelec with a focus on formal methods, combining 100 members from the former Laboratoire Spécification et Vérification (LSV) and the VALS team of Laboratoire de Recherche en Informatique (LRI). They target computational paradigms ranging from classical to emerging ones such as biological and quantum computing.

Thales **RT** (Thales Research and Technology) carries out R&D to create industrialized quantum sensing solutions. In particular, they have developed expertise in diamond NV centers.

Onera studies quantum optics at its Palaiseau site. It is in this capacity that it coordinates the ASTERIQS project of the European Quantum Flagship, "Advancing Science and Technology through diamond Quantum Sensing".

They also have teams of researchers in photonics, in III-V semiconductor materials (gallium, ...) with a prototype manufacturing unit located in their premises in Palaiseau, in metrology (gravimeter, atomic clock, accelerometer) and in QKD.

Let's move on to other parts of the Ile de France: Cergy-Pontoise, Villetaneuse and Versailles.

The **LPTM** (Laboratoire de Physique Théorique et Modélisation) of the University of Cergy-Pontoise is interested in cold atoms, in liaison with the Institut Francilien de Recherche sur les Atomes Froids (IFRAF). They also study graphene, electronic quantum transport, topological phases and entanglement.

The **LSPM** (Laboratoire des Sciences des Procédés et des Matériaux) of the University of Paris 13 in Villetaneuse is working on the manufacturing processes of NV centers, carbon nanotubes and graphene centers and associated applications.

The **LPL** (Laboratoire de Physique des Lasers) of the University Paris 13 in Villetaneuse works in photonics and cold atoms, their traps and on quantum metrology. It is the laboratory of Hélène Perrin, already mentioned, who is its Deputy Director.

The **GEMaC** (Groupe d'Etude de la Matière Condensée) of Versailles also works in the field of diamonds and graphene, on spin electronics and magnetism. It also works on QKD and photonic quantum memory.

Launched in 2014, the **Paris Center for Quantum Computing** (PCQC) brings together several dozen researchers from various laboratories in the Paris region, including Philippe Grangier. The **CNRS** has informally grouped its efforts with the Quantum Computing working group which works more on the algorithmic dimension.

Finally, **QuanTiP** (Quantum Technologies in Paris Region) is a community that groups research laboratories in the Ile de France region that are focused on quantum communications technologies. According to them, there are 650 quantum researchers in the Ile-de-France region in all (physics, algorithms, telecommunications, cryptography) spread over 100 teams in 30 research laboratories. It followed-on SIRTEQ in 2022, that was created in 2017.

We can also mention the initiative of the high-performance computing cluster **Teratec** (based in Bruyères-le-Châtel, near the CEA's Military Affairs Department) around quantum physics[2757].

[2757] Teratec brings together several private and public HPC players including Atos, CEA, CERFACS (European Center for Advanced Research and Training in Scientific Computing), Dassault-Aviation, EDF, IFPEN, PCQC (Paris Centre for Quantum Computing), Total and the University of Reims.

It aims to develop quantum algorithms, hybrid development methods, use cases, and to inform, train and animate a community. They benefit from an Atos QLM simulator installed at the CRTT (Centre de Calcul, Recherche et Technologie) of the CEA in Bruyères-le-Châtel.

Grenoble

Grenoble's quantum ecosystem is dense, well-organized and very focused on the creation of qubits based on electron spins but also on superconductors, all with good skills in photonics. It is probably the place where coordination between research teams works best, particularly by integrating the key stages of industrialization.

Quantum research in Grenoble is led by different branches of the CEA (Leti in nanoelectronics and IRIG in fundamental physics), the CNRS with Institut Néel, LPMMC and two joint CNRS and CEA teams: NPSC (NanoPhysics and Semiconductors) focused on quantum sensing, quantum photonics, quantum thermodynamics and the quantum foundations, and Quanteca, created in 2019, which deals with all kinds of solid states qubits (electron spins, superconductors).

CEA-Leti (Electronics and Information Technology Laboratory) in Grenoble is the CEA's micro and nanoelectronics laboratory. It is notably at the origin of the SOI wafer technology that led to the creation of SOITEC. Leti is focused on CMOS electron spin qubit engineering. The project was coordinated by Maud Vinet until November 2022 when she created Siquance and Jean-Charles Barbe since then. It federates the efforts of several CEA, CNRS and UGA laboratories.

CEA IRIG (Grenoble Institute for Interdisciplinary Research) is the counterpart of Institut Néel in fundamental research at CEA. It includes the Laboratory PHotonique ELectronique et Ingénierie QuantiqueS (PHELIQS), which works on the physics of condensed matter.

Institut Néel[2758], launched in 2007, is a CNRS laboratory specialized in condensed matter physics with a critical mass of researchers in quantum physics. Its researchers are exploring the possibilities of electron spin qubits (Tristan Meunier), superconducting qubits (Nicolas Roch), topological matter (Adolfo Grushin) and photonics. It also works on thermodynamics and the energetics of quantum computing (Alexia Auffèves), cryogenics (Sébastien Triqueneaux) and quantum foundations (Cyril Branciard).

The **LPMMC** (Physics of Condensed Matter) of the University Grenoble Alpes is a CNRS UMR focused on the theoretical physics of condensed matter and quantum physics, N-body quantum interactions, superconductivity and superfluidity, and on the temporal evolution of quantum systems under the effect of magnetic and electric fields.

[2758] The institute takes its name from Louis Néel (1904-2000, French), a physician of Lyon origin who was awarded the Nobel Prize in Physics in 1970 for his studies on magnetism and the discovery of antiferromagnetism. He is at the origin of the creation of the Polygone Scientifique de Grenoble, which brings together numerous research institutes and companies in the peninsula between the Isère and Drac rivers. The place hosted the first CEA site outside the Paris region in 1956, launched by Louis Néel. The CNRS established a foothold there in 1962, and in 1967 CEA-Leti was created. CEA-Leti is one of the world's largest civilian laboratories for applied research in nanoelectronics and nanotechnology. The Grenoble Science Park is also home to several international research organizations, the Institut Laue-Langevin, the European Synchrotron Radiation Facility and one of the branches of the European Molecular Biology Laboratory. In 2005 the CEA-Liten was created, a branch of the DRT specialized in new energies (photovoltaic solar, batteries, fuel cells, complete management of the carbon cycle, mixed energy management, innovative materials). In 2006, Minatec was launched, a nanotechnology commercial development center, later complemented by the Minalogic competitiveness cluster. In 2012, the Clinatec research center, founded by Alim-Louis Benabid, was launched, which is at the origin of the first complete exoskeleton for tetraplegics.

The **IJF** (Institut Joseph Fourier) of the University of Grenoble is working on quantum dynamics and in particular on issues of decoherence and thermal quantum noise.

The **LIG** (Laboratoire d'Informatique de Grenoble) is interested in quantum algorithms in general. One of its members is the researcher Mehdi Mhalla, who works on the quantum resolution of graph problems.

Research in quantum computing in Grenoble is currently structured around three initiatives: **QuEnG**, **QuantECA** and **QuCube,** which are not on the same level.

QuantAlps (formerly, between 2017 and 2021, QuEnG for Quantum Engineering Grenoble) is the Grenoble ecosystem ranging from philosopher to industrialist, a trans-laboratory, trans-disciplinary and trans-sectoral umbrella initiative.

The teams are working in physics on many other fields: in photonics, on superconducting qubits, electron spin qubits and qubits based on molecular magnets. Teams also make the link between quantum physics and philosophy. The initiative also includes training engineers in physics and quantum computing with various courses, including a project with Ensimag, Grenoble's leading computer science school. QuantAlps was launched by Alexia Auffèves and Anna Minguzzi. Anna is the Director of QuantAlps since Alexia Auffèves left Grenoble to work at Singapore's CNRS MajuLab in October 2022.

Lyon

Research in Lyon is well balanced between the physical part and the mathematical and software part of quantum.

The **Physics Laboratory of ENS Lyon** studies condensed matter. The Quantum Circuit Group of Benjamin Huard is working on superconducting qubits and their error correction codes. He was notably joined by Audrey Bienfait in 2019, who works on electron spin resonance and its applications in quantum sensing. It was also there that Théau Peronnin finalized his thesis in 2020 while creating the startup Alice&Bob with Raphaël Lescanne.

The **INL** (Lyon Nanotechnology Institute) is located at Centrale Lyon (Ecully). They work on semiconductors and photonics. They have a technological platform for component prototyping, particularly in photonics.

The **iLM** (Institut Lumière Matière) of Lyon is specialized as its name says in photonics.

The **Camille Jordan Institute** in Lyon is a research laboratory in mathematics that works in particular on quantum probabilities. It is distributed on several sites: Villeurbanne, Saint-Étienne and on the Centrale Lyon campus in Écully.

The **LIP** (Laboratoire de l'Informatique du Parallélisme) of ENS Lyon associates CNRS, Inria and Claude Bernard Lyon 1 University. Its MC2 team works on theoretical computer science and complexity theory. It includes Omar Fawzi, CNRS 2019 bronze medalist and specialist in quantum information theory. He leads his work in the MC2 team at LIP.

Occitanie

Quantum research in Toulouse is very focused on fundamental physics and quite far from quantum computing with the exception of **LPTT**. There are also two laboratories in Montpellier, one of which is associated with IBM. Let's mention the **QuantUM Hub** initiative launched by IBM Montpellier, the University of Montpellier, and the Occitanic Region.

The **Institute for Quantum Technologies in Occitanie** was created in January 2021 to consolidate all the Occitan research and industry organizations, including the research labs below from Toulouse and Montpellier.

The **CEMES** (Centre d'Élaboration de Matériaux et d'Etudes Structurales) in Toulouse is specialized in physics and optronics. It is interested in light-matter coupling at scale and the creation of sensors oriented more towards connected objects than quantum applications.

LCAR (Laboratoire Collisions-Agrégats-Réactivité) of the Paul Sabatier University of Toulouse works on Rydberg atoms. It is in the team of Juliette Billy and David Guéry-Odelin.

The **LPCNO** (Laboratory of Physics and Chemistry of Nano-objects) of INSA Toulouse is specialized in photonics and quantum electronics. They study electron and nucleus spins, quasi-particles and quantum dots. They aim at applications in quantum computing. Their research is looking at applications in the health sector.

The **ITM** (Institut de Mathématiques de Toulouse) of the University of Toulouse studies statistical and quantum physics. It is home to Clément Pellegrini who studies quantum information theory and quantum state measurement.

The **LPTT** (Laboratoire de Physique Théorique de Toulouse) works on superconductors and SQUID Josephson effect loops. They are involved in the Quantware project which has been co-funded among others by the NSA!

The **LCPQ** (Laboratory of Quantum Chemistry and Physics) of the Paul Sabatier University of Toulouse develops generalist quantum chemistry codes, contributing to molecular simulation efforts.

The **L2C** (Charles Coulomb Laboratory) of the University of Montpellier is working on quantum metrology, spin dynamics and graphene, with applications in magnetic microscopy.

The University of Montpellier is an IBM partner in the setting up of a joint laboratory on quantum which actually aims to evangelize customers on the general principles and tools of the IBM Quantum quantum platform.

The **LIRMM** (Montpellier Laboratory of Computer Science, Robotics and Microelectronics) focuses on the creation of quantum algorithms. It collaborates with IBM, Total and CERFACS.

Aida Todri-Sanial is one of their Research Director and works on quantum algorithms used for classical integrated circuits routing and on classical algorithms improving qubits gates mapping taking into account calibration data[2759].

[2759] See A Hardware-Aware Heuristic for the Qubit Mapping Problem in the NISQ Era by Siyuan Niu, Aida Todri-Sanial et al, October 2020 (14 pages).

Nouvelle Aquitaine

The Nouvelle Aquitaine ecosystem is specialized in sensing and enabling technologies like lasers, with its industry ecosystem comprising **Muquans**, **Azurlight Systems** and **ixBlue**. Since March 2021, this ecosystem is federated under the umbrella **Naquidis**, as part of the AlphaLRH cluster and with the support of the Region.

Besides the local branch of IOGS (Institut d'Optique Graduate School), here are two quantum research labs in the region.

The **LP2N** (Laboratoire Photonique, Numérique et Nanosciences) of the Institut d'Optique de Bordeaux does research in photonics and metrology based on cold atoms (microgravitometry). This is where the startup Muquans started.

The **LOMA** (Laboratoire Ondes et Matières) from CNRS works on quantum matter and is investigating, among other things, nanomechanical qubits based on carbon nanotubes.

The **XLIM** (Limoges) does among other things photonics. They are notably partners with Thales TRT. They are working on applications in polariton metrology, in particular SPR (Surface Plasmon Resonance).

Sud

There are also a few quantum physics laboratories in Marseille, three of which are directly related to the needs of quantum computing. And one laboratory in Nice.

The **Fresnel Institute of** Marseille is involved in photonics, so inevitably, it can contribute to advances in photon-based qubit management and QKD-based quantum cryptography.

The **CPT** of the Universities of Marseille and Toulon is working on quantum dynamics and wave diffusion in optical fibers and light guides. They are partners of various foreign universities: Aalborg University (Denmark), Pontificia Universidad Catolica de Chile, Karlsruhe Institute of Technology (Germany), Kyoto Institute of Technology and the Moscow Institute of Physics and Technology.

The **PIMM** (Physics of Ionic and Molecular Interactions) laboratory at the University of Marseille does research in plasmas, more related to the ITER nuclear fusion project than to quantum computing.

The **Laboratoire d'Informatique Fondamentale** de Marseille is particularly interested in quantum computing. Their Discrete Time Quantum Simulator project was launched in 2018. They are working on Quantum Walks and the Quantum Cellular Automata.

INPHYNI (Institut de Physique de Nice) of the Université Nice Côte d'Azur is interested in cold atoms, wave transport, interactions between light and atoms. It deploys a QKD test network between Nice in Sophia-Antipolis since 2019 in partnership with Orange. The quantum laboratory is directed by Sébastien Tanzilli.

Burgundy Franche-Comté

Besançon is home to three quantum laboratories and Dijon to a fourth.

The **LmB** (Laboratoire de Mathématiques de Besançon) of the Université Bourgogne Franche-Comté studies quantum groups and probabilities.

The **UTINAM** Institute of the University of Besançon studies quantum decoherence, control, diagnosis, processing and transport of quantum information in the field of quantum sensing.

Femto-St is a research institute in Besançon focused on nanosciences, optics and optoelectronics. They work in particular on optical telecommunications, nonlinear optics, optics-based Ising machines and quantum imaging.

Icb (Interdisciplinary Carnot of Burgundy) of the University of Burgundy, based in Dijon, includes a team studying quantum and nonlinear dynamics (DQNL).

Great East

The region includes three quantum laboratories located in Strasbourg, Nancy and Troyes.

The **Quantum Matter Theory Group** from the University of Strasbourg is involved in condensed matter physics and also works on the interactions between light and matter, with Rydberg atoms. Run by Shannon Whitlock, the lab is developing cold atom-based quantum systems.

The **L2n** (Lumière Nanomatériaux Nanotechnologies) of the Technology University of Troyes is specialized in optoelectronics and photon sources.

The **Loria** (Lorraine Laboratory for Research in Computer Science and its Applications) is based in Nancy. Two teacher-researchers are interested in quantum computing and algorithms: Simon Perdrix and Emmanuel Jeandel. The first is one of the main contributors of ZX-Calculus. Since 2021, Simon Perdrix is a PI at Inria Nancy.

Elsewhere in France

And finally, here are a few quantum physics laboratories located in other regions, in Rennes, Lille, Bordeaux and Limoges, but with no apparent direct link to quantum computing.

The **IPR** (Institut de Physique de Rennes) is attached to the University of Rennes. They are interested in quantum dynamics, the evolution of quantum states over time.

The **LARIS** (Laboratoire Angevin de Recherche en Ingénierie des Systèmes) based in Angers deals with various IT subjects. Within it, François Chapeau-Blondeau and Etienne Belin are interested in the impact of noise on quantum algorithms.

The **PhLAM** (Laboratoire de Physique des Lasers Atomes et Molécules) in Lille is interested in photonics and cold atoms.

The **IEMN** (Institute of Electronics, Microelectronics and Nanotechnology) is a laboratory located on four sites in Lille, Villeneuve d'Ascq and Valenciennes. They specialize in the design of quantum nanostructures.

International collaborations

International partnerships are very common in research. Many of the works of French researchers are carried out with researchers from other countries, including the USA, the UK, Austria, the Netherlands and Germany, Japan and Singapore (notably with joint international units of the CNRS IFLI and MajuLab).

CEA-Leti is a partner of **IMEC,** its counterpart in Belgium, based in Leuven, covering AI and quantum computing[2760]. Like CEA-Leti in Grenoble, they have a clean room for etching up to 28 nm on 30-cm wafers and another on 20-cm wafers for MEMS.

Since 2017, the **Grenoble University Space Center** has been collaborating with the Austrian **IQOQI** on sending quantum keys via satellite in the Nanobob project.

And there is another international collaboration on quantum involving France, the Netherlands (QuSoft) and Latvia.

Government funding

After Atos launched in 2015/2016 its venture in quantum computing emulation, the French government started to look at the opportunity to launch a quantum plan. Back then, it was involved in the European Quantum Flagship which was announced in October 2018.

Things really started with the creation of a parliamentary investigation commissioned by the Prime Minister in March/April 2019 and led by MP **Paula Forteza**, accompanied by **Iordanis Kerenidis** (CNRS researcher specialized in quantum machine learning) and **Jean-Paul Herteman** (former CEO of Safran). The parliamentary mission submitted its report on January 9, 2020, titled "Quantum: the technology disruption that France will not miss". The report made fifty proposals, 37 of which were made public. The government then created a national quantum strategy that included some but not all of the parliamentary mission's proposals. All this during the early stages of the covid pandemic. It was finally announced a bit late, in January 2021, but by President Emmanuel Macron, a premiere in the western world.

The ambitions of the strategy and its roadmap revolve around rather classical themes: NISQ quantum computing, Fault Tolerant Quantum Computing, algorithms and software, quantum telecommunications overall (including quantum cryptography and distributed quantum computing), quantum sensing, and at last, enabling technologies. This includes cryogenics, cabling, control electronics, vacuum control, lasers and photon sources.

The plan is spread over 5 years from 2021 to 2025 with 1B€ public funding and an additional 850M€ funding expected from European funds and the private sector (industry R&D and startups funding)[2761].

In 2021 and 2022, many components of the French quantum strategy were launched. There was an incremental 150M€ research program handled by CNRS, CEA and Inria announced in September 2021 and launched in 2022. Then, a hybrid classical/quantum platform announced in January 2022, which will be located at the TGCC supercomputing center handled by CEA. It will use the Joliot-Curie supercomputer in association with a QLM classical server from Atos for emulation and QPU drive, and a Pasqal quantum simulator. This HQI (Hybrid HPC Quantum Infrastructure) project is

[2760] See Partners Double-Team AI & Quantum Computing by Mathew Dirjish, November 2018.

[2761] See How France Is Becoming a Quantum Computing Power by Peter Suciu, The National Interest, January 2022 and What Europe can learn from France when it comes to quantum computing by Andersen Cheng, Sifted, November 2021.

partly funded by the EU HPC-QS program. An education program was launched with universities to expand training from license to PhDs. Other programs were launched for quantum startups accelerations, for enabling technologies and for the deployment of PQC cryptography systems.

Quantum industry

On the industry vendors scene, France has a handful ventures in quantum computing hardware front with **Alice&Bob** (cat-qubits), **C12** (carbon nanotubes electron spins qubits), **Pasqal** (cold atoms qubits), **Quandela (**single photon sources and photons qubits), **Siquance** (silicon quantum dots spin qubits) and **Crystal Quantum Computing** (using trapped ions in Rydberg states).

Figure 862: France's quantum industry ecosystem. (cc) Olivier Ezratty, 2022.

In the software side, we have **Qubit Pharmaceuticals** (healthcare), **QuantFi** (finance), **VeriQloud** (quantum telecommunications) and **Prevision.io** (quantum machine learning) plus a bunch of companies specialized in cryptography, mostly PQC with **CrytoNext**, **CryptoExperts**, **Ravel** and **Secure-IC**.

In quantum sensing, we can count on **Muquans** (microgravimeters, acquired by **iXblue** in 2021, becoming **Exail** in 2022), **Chipiron** (NV centers imaging), **Wainvam** (NV centers imaging), **Mag4Health** (imaging) and **Thales** (NV centers, SQUIDs and cold atoms sensing, lightweight cryogeny).

In addition to **Bpifrance** and the investment fund **Quantonation,** the **Deep Tech Founders** trains entrepreneurs/researchers in deep techs. It is an international program created by the Hello Tomorrow team. All these organizations are behind the creation of a structure to support the quantum ecosystem in partnership, the **Lab Quantique,** launched officially in April 2020. The Lab Quantique is a think tank for the development of talent, particularly at the crossroads between science and entrepreneurship. From a practical point of view, Lab Quantique organizes regular meetings that bring together mainly quantum technology entrepreneurs from France and abroad. These meetings took place in the form of videoconferences on Zoom during the covid-19 pandemic period in 2020 and 2021.Its objectives are to connect industry players, startups and researchers, to build bridges with the international community, to launch a program to accelerate quantum startups and to organize a major annual high-level conference bringing together all the stakeholders in the ecosystem, as well as an International Prize (attracting talent).

In the end, it will also take the form of a trade association mixing the quantum industry (large organizations, small businesses and startups) and its users (mainly, large companies like EDF, Airbus and the likes).

One France specificity in Europe is its large corporations directly invested in quantum technologies and quantum enabling technologies : **Atos** (software, emulators, quantum accelerators), **Thales** (sensors), **Air Liquide** (cryogenics), **Orano** (isotopes production like silicon 28), and small/medium businesses like **Radiall** (connectors, cabling, switches, attenuators, couplers, optical links), **ATEM** (cabling) and many in photonics (like **Exail, Azurlight Systems, Aurea Technology, Lumibird** and **Cailabs**) and even semiconductor manufacturing machines with **Plassys Bestek** and **Riber**.

The Netherlands

The Netherlands is one of the most active European countries in quantum technologies research and development, mainly around the University of Delft (**TU Delft**) and its **QuTech** branch.

It has long been a historical melting pot of quantum physics research in Europe. We have thus cited many great names at the beginning of this book: **Hendrik Antoon Lorentz** (1853-1928), **Heike Kamerlingh Onnes** (1853-1926), **George Uhlenbeck** (1900-1988), **Hendrick Casimir** (1909-2000) and **Samuel Goudsmit** (1902-1978).

In 2015, the government launched a 10-year, 135M€ plan to create a quantum computer[2762]. The investment was made in **QuTech**, TU Delft's quantum research center launched in 2014 with a 10-year budget of 145M€, half of which comes from TU Delft University and the other half from the NWO, the national funding agency[2763]. Qutech employs more than 180 people in all, of which only 37% are Dutch, with 25 permanent researchers.

The Netherlands government then announced a 7 years 615M€ plan in April 2021, complemented by an addition of 228M€ in 2022[2764]. This makes the country probably the greater investor in quantum technology in proportion of its GDP.

This public funding should drive private sector investments of 3.6B€, a very ambitious goal in comparison with the similar 565M€ expected in France. It is managed by the non-profit foundation **Quantum DELTA NL** that was created in 2020[2765]. The Netherlands plans to create 30.000 high-tech jobs and create a cumulative economic impact of at least 5B€ with quantum technologies. The country plan is organized around the creation of three technology demonstrators, four generic action lines and shared cleanroom facilities.

- **Quantum Inspire**, their cloud superconducting computer service that is already available and got a funding of 90M€.
- **Quantum Network** project on quantum telecommunications and cryptography, connected to the related European projects, with a funding of 62M€. They expect to quantumly connect three quantum computers by 2023 and five by 2026.

[2762] See the state of play of the Dutch National Quantum Plan in National Agenda for Quantum Technologies, Quantum Delta Netherlands, September 2019 (51 pages).

[2763] See QuTech's 2018 Activity Report (80 pages) as well as an independent valuation report published in 2019 and covering the period 2015-2018.

[2764] See Quantum Delta NL awarded 228 Million Euro for second phase of its programme to Accelerate Quantum Technology, April 2022.

[2765] See the plan details in Quantum Delta NL in a nutshell, 2021 (20 pages). Look also at the excellent Economic Impact of Quantum in the Netherlands, Quantum Delta NL, May 2020 (60 slides) which contains a lot of interesting market data. DELTA stands for Delft Eindhoven, Leiden, Twente and Amsterdam, completed by Nijmegen, Maastricht and Groningen.

- **LightSpeed** is a program connecting startups with investment funds. It's overselling a bit its value touting access to 13.6B€ in investment capital, representing the totality of the various funds managed by these investors. The 2022 funding extension added 15M€ for a startup seed fund.
- **House of Quantum** is a startup ecosystem facility to open in 2024 with a budget of 182M€. It would accelerate part of the 100 startups the country wants to consolidate by 2027. Within this house, the **Living Lab QT** that will focus on ethical, legal and societal aspects of quantum technology with research collaborations between universities, the public and private sector, with a funding of 20M€. They will open two related interdisciplinary university positions, create a desk and a toolkit for responsible innovation and entrepreneurship and create a covenant to be signed by private and public stakeholders promoting sustainable and safe use of quantum technologies.
- They also plan to invest 150M€ in the 5 cleanrooms from **NanoLabNL**, have a quantum sensors plan with 23M€ funding and a training program that should create 2000 PhDs and engineers by 2027 with a funding of 41M€.

QuTech is also associated with **Intel** and **Microsoft**. QuTech has received $50M in funding in 2015 from Intel as part of a partnership on their superconducting and electron spin qubits.

Microsoft has also been a partner of QuTech since 2010, which they have also depleted by hiring **Leo Kouwenhoven** in their Microsoft Research laboratory which is on site and working on topological quantum and fermion of Majorana in liaison with a team of QuTech dedicated to the same subject. The Netherlands looks like a brain reservoir for the American quantum industry.

Collaborative research approaches are making good progress, particularly with a view to recovering European funding. In October 2017, QuTech launched a partnership with the Institute of Photonic Sciences, the University of Innsbruck in Austria and the Paris Centre for Quantum Computer. QuTech is also a partner of the University of Aachen in the CMOS qubit. The University of Delft has also obtained for the European part of the QuNET project mentioned about Germany an ERC of 1,5M€ with a launch in November 2019 and an end planned for October 2024[2766].

Other initiatives with blurred contours have been launched such as **Quantum Helix,** funded under the European Quantum Flagship Program and Horizon 2020. The **Quantum Software Consortium** runs for 10 years from 2017 and has received €18.8M in public funding from the country's Gravitation Program. It brings together various Dutch laboratories: **TU Delft**, **QuTech** (part of the latter), **QuSoft** (a research laboratory dedicated to quantum software, launched by CWI, UvA and VU in 2015), **CWI** (Centrum Wiskunde & Informatica), the **University of Leiden, UvA (**University of Amsterdam) and **VU** (Free University of Amsterdam) to conduct research in quantum software and cryptography.

Other companies include **Delft Circuits** (superconducting cabling), **Leiden Cryogenics** (high-power dilution cryostats), **Qblox (**electronics for controlling superconducting qubits), **Single Quantum (**single photon detectors), **QuiX** (photonic processor, a subsidiary of Lionix, a foundry capable of producing photonics wafers in nitrates on SiO2), **Qu&Co** (quantum software), **QuSoft (**quantum software), **QPhoX** (quantum computer interconnection) and **ipCLock** (quantum clock).

In December 2020, the Dutch quantum industry created the **IMPAQT** consortium. The first members are Orange QS, Qblox, Delft Circuits, QuantWare BV (a new stealth spin-off from TU Delft creating superconducting QPUs) and Qu&Co. Their goal is to improve the coordination of how they are creating quantum computer enabling technologies.

At last, The Netherlands and France signed in September 2021 a Memorandum of Understanding to expand collaborations in quantum technologies, with Cédric O, the French Secretary of State for Digital and Electronic Communications and Mona Keijzer, the Dutch Secretary of State for Economic Affairs and Climate Policy. The bilateral collaboration includes research partnerships in silicon qubits

[2766] See A quantum network for distributed quantum computation, Cordis, 2019.

as part of the European flagship project QLSI, research-industry collaboration involving companies like Atos and Qu&Co, the creation of a joint portal listing job opportunities in France and the Netherlands (www.quantumjobs.fr and quantumjobs.nl) and collaboration to increase EU venture capital in the domain (involving Quantonation).

Belgium

Belgium is the host of the famous Solvay conferences created in the early 20th by Ernest Solvay. Their presence in the quantum science and technology scene is exemplified by **IMEC**, the international semiconductor and nanotechnologies research center based in Leuven, an equivalent to CEA-Leti in France, with 4000 employees.

IMEC's quantum technology activities are centered on producing superconducting and electron spin qubits on behalf of various laboratories and vendors as well as some cryoelectronics systems. Among other projects, they participate to the European Quantum Flagship QLSI project that is coordinated by CEA-Leti. They announced in August 2021 a partnership with **Xanadu**, for the development of fault-tolerant photonic qubits chipsets based on silicon-nitride.

Let's also mention the **Centre for Quantum Information and Communication** from the Free University of Brussels (Vrije Universiteit Brussel). It works on quantum measurement, quantum entanglement, quantum communication, quantum cryptography and quantum algorithms.

It has also worked on continuous-variable quantum cryptographic protocols, and developed quantum adiabatic algorithms.

In the vendor space, I have identified a company that was already mentioned, **QBee.eu**, a quantum accelerator and incubator created by Koen Bertels, who leads the Quantum Computer Architectures Lab in TU Delft and also works at Qutech.

Ireland

In Ireland, a first quantum computing initiative (QCoIr) was launched in 2020 with a funding of $11M. It included global companies like IBM and Mastercard, plus the Tyndall National Institute in Cork. It established a Quantum Center of Excellence.

Finland

Finland has a couple very interesting assets in quantum technology. In research you can count with Aalto University, the University of Helsinki, Tampere University and VTT Technical Research Centre of Finland. The Finnish Quantum Institute federates the efforts of Aalto University, the University of Helsinki and VTT.

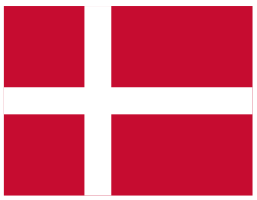
It is an organization fostering collaborative research (ResQ) and education particularly with public broad audiences (EduQ) and business adoption of quantum technologies within Finland (BusinessQ).

On the industry side, **Bluefors** is the worldwide leader in low temperature cryogeny used with quantum computers. **IQM** is by far the largest and best funded superconducting qubits quantum computing startup. Other Finish startups are **Algorithmiq**, **Ampliconyx**, **Kronus**, **Qplaylearn**, **Quanscient**, **Quantastica**, **SSH Communications Security**, **Unitary Zero Space** and **Vexlum**.

And you have the **CSC** computing center which hosts the LUMI supercomputer and will put in place an hybrid quantum/classical computing architecture with IQM as part of the EuroHPC HPCQS (High Performance Computer – Quantum Simulator hybrid) program.

In January 2022, Finland and VTT also launched **QuTI** with 10M€ to pool the expertise and resources of four research and eight industry partners over a three year period. It is centered around enabling technologies for quantum computing (materials, cryogeny, electronics, software, systems architecture). The program industry partners are Afore, Bluefors, IQM, Quantastica, Saab, Vexlum, and for companies outside Finland, Picosun and Rockley Photonics. At last, in April 2022, Finland and the USA signed a Joint Statement on Cooperation in Quantum Information Science and Technology very similar to the ones signed with Australia, Sweden, Denmark, Switzerland, Australia, and the UK in 2021/2022. A similar partnership was launched with Singapore in September 2022.

Denmark



Quantum research in **Denmark** is organized around the Center for Quantum Devices (**QDev)** at the Niels Bohr Institute (NBI) at the University of Copenhagen[2767]. It is a quality laboratory focused in particular on topological qubits, with its director Charles M. Marcus who also worked for Microsoft Research in this field jointly with the MSR teams of Leo Kouwenhoven in the Netherlands (respectively until 2021 and 2022).

QDev is a laboratory of physicists focused on the study of condensed matter, i.e. the physical lower layers of qubits, as can be seen in their publications. The team seems to be only a dozen people. Unfortunately, they cannot then rely on Danish or European industry vendors to consider the transfer of their research into the production of quantum computers. DTU (Danish Technology University) also entertains its QuantumDTU Center for Quantum Technologies.

In April 2022, NATO announced the setup of a NATO Accelerator for Quantum Technologies in Denmark. This innovation accelerator is installed at NBI. This was completed in June 2022 by the announcement of a global quantum partnership with the USA.

The Danish government invested $12M on quantum research between 2017 and 2019. It was completed in September 2022 by the launch of a $200M initiative by **Novo Nordisk** to build a generic quantum computer in 2034, most of the funding going to the Niels Bohr Institute.

Sweden

On the **Swedish** side, there is mainly the WACQT (Wallenberg Centre for Quantum Technology) which is part of the **Chalmers University** of Gothenburg and is co-financed by the Wallenberg Foundation. The WACQT has been funded under a 12-year plan with over $100M.

As in all countries, the center targets all quantum technologies domains (computing, communications and sensing). They are invested in superconducting qubits as well as in continuous variable qubits. They plan to create a 100 qubits superconducting computer. WACQT is also working on cold atom qubits from Rydberg... named after a Swedish physicist! Finally, it has launched a "Women in WACQT" initiative to develop gender diversity in quantum science.

In March 2021, the Wallenberg budget nearly doubled to $9M per year, allowing the hiring of 40 more researchers. In April 2022, Sweden and the USA announced a partnership on quantum technology similar to the ones with the UK, Finland, Denmark, Australia and Switzerland.

[2767] See Quantum technology in Denmark by KPMG, November 2020 (34 slides). This report from a well-known consulting company is highly disappointing. It doesn't mention any research lab besides NBI, any scientist besides Niels Bohr or any startup from the Danish scene. It contains only generalities.

Norway

Norway feared in 2018-2019 to miss the second quantum revolution. In 2020, it created a Gemini-center on quantum computing with SINTEF, the University of Oslo, NTNU, and in 2021, Simula Research Laboratory, a fundamental research organization belonging to the Norwegian Ministry of Education and Research, where Shaukat Ali leads research in quantum software engineering (among other things)[2768].

The project was led by Franz Georg Fuchs from SINTEF, an independent research organization with the goal to make Norway "quantum ready".

Later in 2021, the Norwegian Quantum Computing Centre was created consolidating research from 13 scientists from three partner institutions (SINTEF, the Norwegian University of Science and Technology *aka* NTNU and the University of Oslo) including Jeroen Danon from the Center for Quantum Spintronics at NTNU[2769].

Italy

Italy has a very active research in place in various technologies in quantum computing. Photon qubits are explored by **Fabio Sciarrino** at Università La Sapienza in Rome. He is an European pioneer of boson sampling experiments and wants to make it programmable. And the **Università di Padova** launched its own Quantum Technologies Research Center that works on trapped ions computing.

Francesco Tafuri from the Università Federico II in Naples works on superconducting qubits. The Italian National Institute for Nuclear Physics (INFN) is also working with the US DoE on superconducting quantum materials at the FermiLab in Chicago, which happens to be run by Anna Grassellino, an Italian.

In the quantum communication realm, **Paolo Villoresi** from the Instituto Nazionale di Ricerca Metrologica in Turin pioneered photons polarization encoding with a satellite in 2015. Italy also deployed its **Italian Quantum Backbone** (IQB) with a total of 1,850 km fiber link based on commercial fibers. It connects INRIM's premises in Turin to Milan, Bologna, Firenze, Rome, Napoli, Pozzuoli and Matera. From Turin, a 150 km fiber reaches Modane in France, and connects to Grenoble, Lyon and Paris, then Europe.

The public supercomputing center **CINECA** entertains a quantum computing lab. It tests the capacities of various quantum computers, develops quantum algorithms and hybrid solution associating classical supercomputers and quantum accelerators.

The big shortcoming of Italy is its weak private sector with not many industry vendors and startups engaged in quantum technologies.

As part of its recovery plan announced in April 2021, the Italian government allocated a budget of 1.6B€ to fund 7 new research organizations, one of these being focused on quantum technologies[2770].

[2768] See QuSBT: Search-Based Testing of Quantum Programs by Xinyi Wang, Paolo Arcaini, Tao Yue and Shaukat Ali, April 2022 (5 pages).

[2769] See Protected Solid-State Qubits by Jeroen Danon et al, October 2021 (6 pages).

[2770] See Italy's quantum scientists jostle for a superposition by Francesco Suman, April 2021.

Spain

On the research side, most of Spain's efforts are concentrated in the **ICFO** (Instituto de ciencias fotónicas) of Barcelona, which is mainly specialized in photonics. Other research in quantum is carried out at the Quantum Information and Computation Laboratory (GIC-UB) of the **University of Barcelona** as well as the **Autonomous University of Barcelona**[2771].

The **IFAE QCT** is the Quantum Technology Group from the IFAE (Institut de Fisica d'Altes Energies) from the Autonomous University of Barcelona opened its new lab and fab in October 2020.

On the startup scene, they have a startup, **Qilimanjaro** already mentioned, which develops mainly a cloud-based quantum software platform and a superconducting quantum annealer. Their chipset is manufactured at the IFA. And they have **Entanglement Partners,** a service provider that is clearly succeeding in selling quantum-related cybersecurity services.

They also animate the country's ecosystem, do evangelization and organize events. In 2017, the open innovation platform **Open Trends** launched **The Carrot Cake** to encourage projects in the quantum field. This complements the **Barcelona QBIT** think tank launched in 2015 and the **Quantum World Association** launched in 2017, which brings together Switzerland, Canada, Australia and Catalonia with startups such as ID Quantique, evolutionQ, h-bar and Entanglement Partners. Spain is networking, having realized that it could not go very far on its own.

In February 2022, UMIQ aQuantum-UEx was created, a Joint Quantum Software Research Unit between the Spanish quantum software and engineering company aQuantum and the University of Extremadura (UEx) consolidating a partnership that started in March 2020. They are collaborating on software research projects including the "QHealth: Quantum Pharmacogenetics Applied to Aging" project.

Seven Spanish quantum companies (Amatech, BBVA, DAS Photonics, GMV, Multiverse Computing, Qilimanjaro Quantum Tech and Repsol), five research centers (BSC, CSIC, DIPC, ICFO and Tecnalia) and the Universitat Politècnica de València launched in 2022 the CUCO Project to foster quantum computing research and development in Spain, particularly in the industry.

But regionalism works well in Spain as well, as another similar initiative was launched in the Basque country by the Provincial Council of Bizkaia. The goal is to foster the adoption of quantum computing in the industry. Participating members are Technalia (again), IBM, Telefónica, Accenture, the Bilbao City Council, Gaia, Silicon Europe, the UPV/EHU (the University of the Basque Country), the University of Deusto in San Sebastien and Mondragon Unibertsitatea (east of Bilbao).

Portugal

Portugal's key investment in quantum technologies sits with **QuantaLab**, a collaborative research center launched by **International Iberian Nanotechnology Laboratory** (INL) and the **Universidade do Minho**, both in Braga, Portugal. It focuses on quantum materials and quantum technologies. Portugal is also participating to European quantum projects including the QCI (Quantum Communication Infrastructure).

[2771] See Quantum Technologies in Catalonia, July 2019 (43 slides) which describes very well the quantum ecosystem of this key region of Spain.

Poland

Poland launched its National Quantum Information Centre in Gdansk (KCIK) in 2007 with 9 research institutions. Other interesting labs are the Quantum Physics Research Center focused on quantum cryptography and the International Center of Theory of Quantum Technologies (ICTQT).

The University of Warsaw is also very involved in quantum research, particularly in photonics with the Center of Quantum Optical Technologies (QOT), led by Konrad Banaszek[2772].

The Polish National Science Centre also coordinates the international research network **QuantERA,** itself funded by the European Union's Europe 2020 budgets. It does this in coordination with the French ANR. The countries involved, in addition to those of the European Union, are Switzerland, Israel (Bar-Ilan University) and Turkey. About thirty research projects had been funded after a call for proposals in 2017, some of which were subsequently funded in the European Quantum Flagship, such as SQUARE. They are all quantum physics projects (photonics, cold atoms, ...).

Some other Polish quantum research groups worth mentioning are The Quantum Research Group from the Polish Academy of Sciences which works on quantum computing, qubit measurement, error mitigation and software engineering and the Quantum Resources Group from the Jagiellonian University in Kraków that was created in 2020 and works on quantum information science.

In the ecosystem, The Quantum AI Foundation was created in 2019 by Paweł Gora. It organizes meetings of the Warsaw Quantum Computing Group (WQCG) and hackathons.

Hungary

Hungary launched in 2018 its quantum plan with a funding of about $10M, consolidated in a new consortium named HunQuTech consolidating the countries quantum research groups from various institutions and industry vendors.

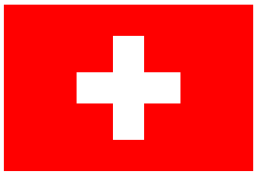
The participants are the Wigner Research Centre for Physics, the Institute of Physics the Faculty of Electrical Engineering and Informatics of the Budapest University of Technology and Economics, the Institute of Physics of the Eötvös Loránd University, completed by industry partners (Bonn Hungary Electronics, Ericsson Hungary, Nokia-Bell Labs, and Femtonics). The plan goals were to work on single photon sources for quantum telecommunications, pairs of entangled photons at telecom wavelength, free-space QKD systems, quantum memories, qubits and quantum gates and new quantum algorithms. Researchers also work on QRNG and PQC. In total, Hungarian researchers got 4 ERC from the EU in quantum physics and information science.

In 2022, the country launched the Quantum Information National Laboratory initiative that consolidates quantum research covering quantum computing and quantum telecommunications. Hungary also participates to the EuroQCI project since 2019. The country seems to have several intra-European partnerships like with Germany and the Netherlands.

In 2022, the Faculties of Science and of Informatics of the Eötvös Loránd University selected QuiX as a vendor for a photonic circuit to build their own research photonic quantum computer.

[2772] They however have not created the "first world's first quantum processor" as claimed in One-of-a-kind: Warsaw-based scientists build groundbreaking quantum processor by Jo Harper, The First News, February 2022. The related paper is Optical-domain spectral super-resolution via a quantum-memory-based time-frequency processor by Mateusz Mazelanik, Adam Leszczyński and Michał Parniak, Nature Communications, February 2022 (12 pages). It is about a (rather interesting) high-resolution spectrograph.

Switzerland



Switzerland is also mobilized on quantum technologies, particularly at **ETH Zurich**, which is collaborating with IBM and especially on quantum cryptography, notably with its startup **IDQ,** which is a leader in quantum random numbers generation used in quantum cryptography and elsewhere. And also with the Lausanne's **EPFL**.

The country has published a manifesto to promote its research and industrial efforts in quantum, Switzerland: At the Quantum Crossroads. The **Swiss Quantum Hub** brings together the Swiss quantum ecosystem.

The **Quantum Science and Technology Initiative** (QIST), a joint initiative of ETH Zurich and the University of Basel, which also involves the University of Geneva and EPFL Lausanne, has 34 faculty members and 300 students. It has been funded with $120M between 2010 and 2017.

It covers all the usual fields of quantum with, with a particular effort in quantum telecommunications. In August 2021, the EPFL launched though its own multidisciplinary Quantum Science and Engineering Center consolidating its research and academic efforts in all branches of quantum technologies.

The **Swiss Quantum Investor Club** was created in 2020 to link investors and quantum entrepreneurs and organize events in Geneva, Lausanne and Zurich, as well as the **Swiss Quantum Hub,** a think tank and accelerator for quantum startups, and the Quantum Computing Garage, a permanent hackathon.In November 2020, Martin Haefner, an alumn from ETH Zurich donated $44M to the ETH Foundation to have them build a quantum research facility. We could wish more wealthy people would make such long-term investments for their community! In another similar initiative, ETH Zurich and the Paul Scherrer Institute (PSI, which has its own proton accelerator and an electron synchrotron, the Swiss Light Source, that is equivalent to SOLEIL in France) created the Quantum Computing Hub in 2021, a joint quantum computing research center, focused on ion traps and superconducting qubits with the goal to host 30 researchers. ETH Zurich invested $36M there[2773].

In October 2022, Switzerland and the **USA** signed yet another bilateral quantum cooperation agreement[2774].

European Union

The **European Union** wants to consolidate its effort in quantum technologies. A "flagship project" germinated in 2016[2775] and was formally launched in October 2018 to fund collaborative research on all aspects of quantum information: sensing, communications, computing and simulation[2776].

[2773] See ETH Zurich and PSI found Quantum Computing Hub, May 2021.

[2774] See Joint Statement of the United States of America and Switzerland on Cooperation in Quantum Information Science and Technology, US State Department, October 2022.

[2775] It started with a Manifesto prepared by European quantum physics researchers. See Quantum hocus-pocus by Karl Svozil, 2016 (6 pages), a critic of the underlying scientific overpromises from the Quantum Manifesto published by European researchers, which led to the creation of the European Quantum Flagship program.

[2776] See the motivations behind the European Flagship: The Impact of quantum technologies on the EU's future policies: Part 1 Quantum Time, 2017 and Part 2.

It is theoretically endowed with 1B€ to be used for the development and diffusion programs of quantum technologies, spread over 10 years. In theory, because the budgets have not really been allocated at this level by the European Union. This Flagship is currently mainly focused on quantum computing fundamental physical. It has not yet looked at algorithms and software.

But the European Quantum Flagship is far from being the sole source of EU funding for quantum research and technologies. You also have to embed the ERC grants for individual researchers, other multi-partite projects (Europe Next, Qureca, H2020, Europe next) and startups funding via the EIC Accelerator.

This **Quantum Technologies Flagship** is one of the three European "flagships" that aim to place Europe at the forefront of major technological breakthroughs with strong community investment in research. The two other flagships are the "Human Brain Project" led by the Swiss Henri Markram and the Graphene project in nanotechnologies. The first phase of the Flagship included €132M spread onto 20 projects selected out of 140 applicants and for a period of three years. 130 additional projects will be later selected.

Launched by the European Commission on October 29, 2018 in Vienna (videos), the program covers the four usual quantum domains: computing, simulation, communication and sensing[2777].

Let's look at these projects. These projects involve an average of at least half a dozen countries, even partner countries like Switzerland and Israel.

Figure 863: the European Quantum flagship projects as of 2022. (cc) Olivier Ezratty, 2022.

It starts with three side projects related to quantum computing:

- **AQTION** (Austria, €9.57M) is trapped ions qubit computer project, planning to reach 50 qubits. Austria has a long history here and is quite legitimate. Atos is participating in this project.

[2777] See the Press Kit (28 pages), the complete list of projects and Europe Accelerating the Industrialization of Quantum Technologies, October 31, 2018, the title of which is somewhat misleading in that the majority of projects funded are research projects and not industrialization projects. And then there is The quantum technologies roadmap: a European community view, October 2017 (25 pages), which takes stock of the state of the art in Europe and around the world. See also The EU Quantum Technology Flagship by Elisabeth Giacobino, 2018 (41 slides and video).

- **MicroQC** (Bulgaria, €2.36M) plans to create another trapped ion computer.
- **OpenSuperQ** (Germany, €10.33M) is a superconducting qubit computer project led by Saarland University that also involves Spain, Sweden, Switzerland and Finland and a total of 10 research laboratories. The ambition is to create a 100-qubit system. IQM is the probable vendor who will provide the quantum system for this project.

Then we have four quantum simulator projects:

- **PASQuanS** (Germany, €9.25M) is a quantum simulator project based on cold atoms and trapped ions up to 1000 qubits. It also involves the UK, Atos and Pasqal.
- **PhoQuS** (France, 3M€) is a photonic based quantum simulator. It is led by a team of PSL researchers. It involves the use of polaritons.
- **Qombs** (Italy, €9.3M) is another photonics-based quantum simulator project.
- **SQUARE** (Germany, €2.99M) a quantum simulator project using trapped ions. It is led by the University of Karlsruhe and involves laboratories from Denmark, Sweden, Spain and France, including Thales. It seems that they are also seeking to create a quantum processor with universal gates.

Let's continue with projects in quantum communication and telecom security.

- **Quantum Internet Alliance** (Netherlands, €10M) (QIA) aims at deploying an Internet network protected by quantum key distribution (QKD) in mesh network mode and not just point-to-point. The quantum nodes or relays will be made up of systems using cold atoms. They will start with a three or four-node network. The project is led by TU Delft University. The CNRS participates in it, notably Eleni Diamanti, Elham Kashefi and Iordanis Kerenidis. The Sorbonne University also participates. Other participants include Swiss, Germans, Danes and Austrians (complete list).
- **QRANGE** (Switzerland, €3.87M) is a project to improve quantum random number generation techniques.
- **CiViQ** (Spain, €9.9M), or Continuous Variable Quantum Communications, is another QKD-based fiber telecommunications security project. The project involves 21 stakeholders covering the academic and industrial world, including CNRS, Institut Mines-Telecoms, Nokia Bell Labs France, Inria, Orange, as well as Mellanox.
- **Uniqorn** (Austria, €9.9M) is in the same niche and is working on a random number generator and a QKD system. It associates 17 organizations from 9 countries (Austria, Netherlands, Italy). The Israeli Mellanox is also involved there.
- **S2QUIP** (Netherlands, 3M€), Scalable Two-Dimensional Quantum Integrated Photonics, is another QKD-based secure communication project.
- **2D-SIPC** (Spain, €2.9M) is a project for the development of photoelectronic components made for networks secured by QKDs.
- **QMICS** (Germany, 3M€) or "Quantum Microwave Communication and Sensing" is about creating a microwaves-based links and networks between superconducting network nodes with applications in distributed quantum computing and also in quantum sensing.
- **NEASQC** (NExt ApplicationS of Quantum Computing) is a collaborative project launched in September 2020, to develop practical applications of NISQ (noisy quantum computers, an intermediate step before scalable quantum computers). It is an H2020 project that brings together European players including Atos, Total, EDF, the Loria laboratory from the University of Lorraine, Astrazeneca, HQS Quantum Simulations, HSBC and the University of Leiden (Netherlands).

- **QLSI** (France) is a new Quantum Flagship awarded in March 2020 to fund four years of fundamental research in silicon qubits. It is being driven by the Grenoble team under the responsibility of Maud Vinet at CEA-Leti. The project funding is 14M€ spread over 19 organizations: Atos, STMicroelectronics, SOITEC, CNRS Institut Néel, TU Delft, University of Twente and TNO in the Netherlands, IMEC in Belgium, UCL and Quantum Motion in the UK, Infineon, RWTH Aachen, University of Konstanz, Fraunhofer and IHP Frankfurt in Germany, University of Copenhagen and University of Basel.
- **QTEdu** (Italy) is about creating the quantum education ecosystem in the European Union. It's funded by H2020[2778].
- **QFLAG** (Germany, €3.48M) was the project managing the coordination for European Quantum Flagship projects. It was followed by the project **QUCATS** that covers the 2022 to 2025 period and is coordinated by Philippe Grangier (CNRS, France).

Then we have five quantum sensing projects already seen.

We note the strong predominance of projects piloted by German research laboratories (5), followed by France (4), the Netherlands (3), Spain (2), Austria (2), followed by Italy, the UK and Switzerland, all driving a single project. Large countries are present in many of these projects. As an example, France is involved in many of these projects. CNRS (France) alone is involved in 14 of the 20 projects[2779]. These projects do not yet include efforts in software, to create algorithms, development tools and business software solutions adapted to quantum computers. Such projects will probably be funded in subsequent phases[2780].

But other European quantum projects are funded with other vehicles than the Flagship.

QuantERA I (2014) and II (2021) is an alliance of research funders from member states created to reinforce transnational collaborations in inspiring multidisciplinary quantum research. The QuantERA II Consortium assembles 38 Research Funding Organizations from 30 countries, some being extra-EU. It complements the Quantum Flagship in early stages, serving as an incubator of new ideas which then can get integrated in Quantum Flagship projects but comes from participating countries (45M€ for QuantERA I and 40M€ for QuantERA II) and the EU (11.5M€ for QuantERA I and 15M€ for QuantERA II). There were two calls for projects in QuantERA I and one in QuantERA II with a selection done late 2021 and projects funding starting in 2022.

EQUIPE (Enable Quantum Information Processing in Europe) project aims to advance the industrialization of the creation of quantum computing and telecommunications solutions for industry[2781].

EuroHPC projects include quantum computing deployments in hybrid datacenters with first deployments of quantum simulators planned in Germany and France as part of the HPCQS project. In October 2022, six other EU HPC sites were selected for these deployments in Czechia, Germany, Spain, France, Italy and Poland with a total investment of 100M€.

[2778] See Expanding the European Competence Framework for Quantum Technologies, January 2022.

[2779] See New Strategic Research Agenda on Quantum technologies, February 2020 (114 pages) which details the state of play of the European Quantum Flagship projects.

[2780] See The Quantum Technologies Flagship: the story so far, and the quantum future ahead by Thomas Skordas and Jürgen Mlynek, October 2020 which looks at the flagship progress two years after the program started.

[2781] See Simulation on / of various types of quantum computers by Kristel Michielsen (40 slides).

European research is federated under the umbrella of **QCN** (Quantum Community Network). Its industry counterpart is the **QuIC** (Quantum Industry Consortium) announced in June 2020 and formally launched in April 2021[2782].

Founding members are companies that were involved in at least two European Quantum Flagship projects. They include Bosch, SAP, Atos, Thales, Muquans, Airbus and many others.

The consortium has an extensive work plan covering market needs assessment, analysis of the quantum technology value chain, development of standards and regulations, sharing of best practices in intellectual property protection and market evangelization, access to infrastructure, linking startups and investors, skills development issues and coordination with public authorities.

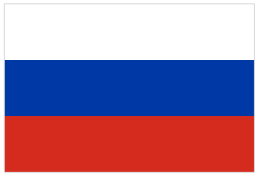
But there is another association, **|QBN⟩**, the Quantum Business Network, another European Quantum Community, which connects the industry, users, vendors and research.

LSQuanT is an initiative funded by the EU that was launched in 2021 and is dedicated to promoting "large-scale quantum transport methodologies", which deals with the physics of quantum transport digital simulation, to invent new quantum materials and devices[2783].

MATQu (Materials for Quantum Computing) is developing an European value chain to manufacture superconducting qubits. This H2020 project running from 2021 to 2024 with a total cost of 21M€ with EU funding of 6,5M€ is led by Fraunhofer Mikroelectronics, IAF and IPMS with the participation of CEA-Leti, IMEC, Soitec, BE Semiconductor Industries (semiconductor assembly equipment), IQM, VTT, Keysight, Siltronic (silicon wafers production), Kiutra, Atos, Mellanox, Beneq (atomic layer deposition equipment), Orange Quantum Systems and Technic France (engineering).

SPROUT (Scalable Platform for Quantum Technology) is a project launched in November 2021 by Delft Circuits and kiutra to provide a scalable cryogeny platform funded by the EU Eurostars program. They develop a demonstrator for a <1K cryogent platform based on cryogen-free magnetic cooling (the Kiutra specialty) and a multi-channel electrical cabling.

Russia



Russia is not very visible in the quantum scene, maybe because they have not built the same research and industry partnership that are seen in the western world. But like with AI, its government realized that quantum technologies were critical for sovereignty. In December 2019, Russia announced its own plan of attack on quantum technologies, which seemed very focused on military, intelligence and cryptanalysis applications[2784].

This plan got a five-year funding of $790M. In practice, it covers almost all fields of quantum technologies[2785]. In January 2022, Russia created it National Quantum Laboratory (NQL) run by Rosatom and with NRU HSE and MIPT, MISIS, P. N. Lebedev Physical Institute of RAS, Russian Quantum Center and the Skolkovo Foundation. The center will host a nano-fabrication center of 2,000 m^2 in Skolkovo. One might wonder how things will fare with exports restrictions to Russia after it started its war against Ukraine in February 2022. Many Western countries equipment vendors won't be in position to sell their hardware and Russia won't be able to count on China this time.

[2782] See Announcing the creation of the European Quantum Industry Consortium by Laure Le Bars (SAP), the first President of QuIC, April 2021.

[2783] See a related review paper: Linear scaling quantum transport methodologies by Zheyong Fan et al, December 2020 (61 pages).

[2784] See Russia joins race to make quantum dreams a reality by Quirin Schiermeier, December 2019.

[2785] Source: Quantum communication in Russia: status and perspective by Vladimir Egorov, 2019 (22 slides).

In January 2022, Rosatom announced a plan to build a trapped ions quantum computer that would be made available on the cloud by 2024. It is being developed by the Russian Quantum Center and the P.N. Lebedev Physics Institute of the Russian Academy of Sciences. They are starting with 4 qubits and, as such, are very late compared to state of the art quantum systems coming from AQT, IonQ and Quantinuum who have about 20 qubits in-store.

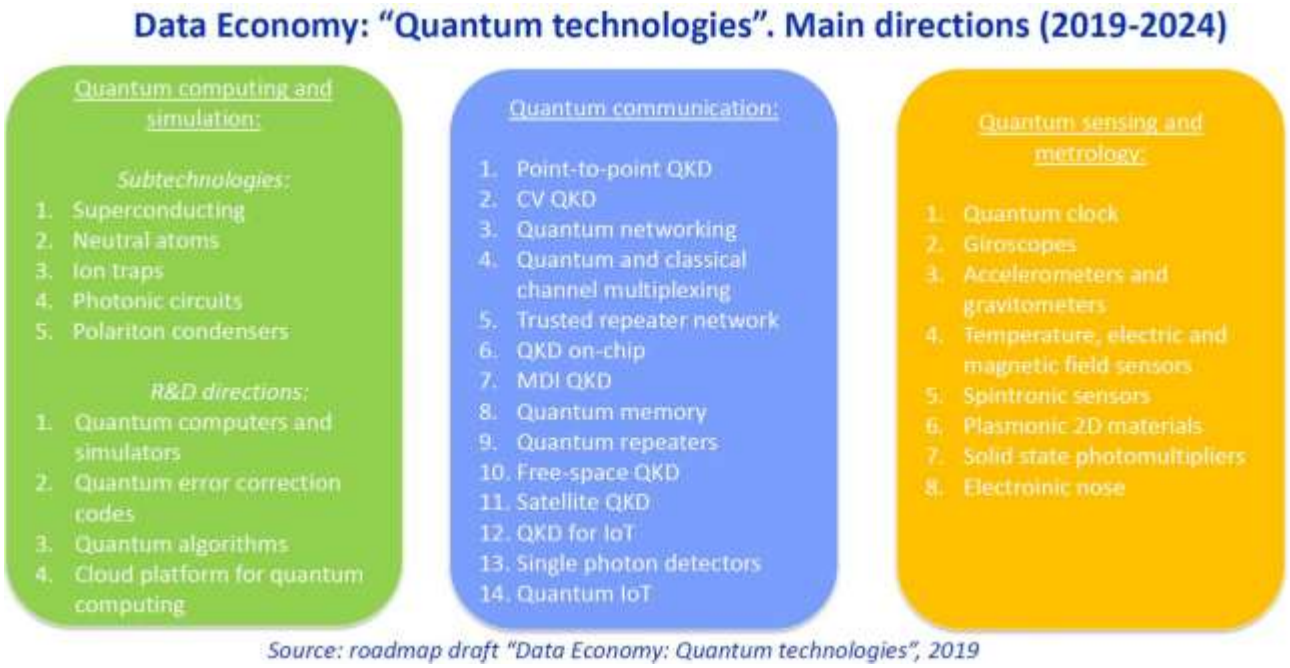


Figure 864: Russia's quantum plan priorities as of 2019. Source: Quantum communication in Russia: status and perspective by Vladimir Egorov, 2019 (22 slides).

Before all of that, the **Russian Quantum Center** was created in 2010, a private research center dedicated to the various application areas of quantum computing, including quantum cryptography. It employs over 200 researchers.

It covers many quantum computing branches: superconducting, trapped ions, photons and NV centers qubits, quantum sensing, QKD and a single photon detector. They collaborate with some international research organizations in the USA (MIT), Canada (University of Calgary), Germany (Max Planck Institute for Quantum Optics) and UK (University of Bath)[2786].

The St. Petersburg **ITMO University** has a QKD research laboratory as well as the **Kazan Quantum Center** which has deployed a QKD on a 160 km network in Kazan. The country also plans to launch a QKD quantum key communication satellite in 2023. A few other laboratories are invested in quantum technologies such as the **NTI Center for Quantum Communications** at MISiS University and the **NTI Technologies Centre** at Moscow University.

Industry wise, they are mostly in quantum cryptography with only one startup, **Qrate Quantum Communications,** the others being established companies, such as **Infotecs**, **Scontel** and **Smarts QuantTelecom**[2787].

[2786] This information comes from Evaluation Report of Russian Quantum Center, 2017 (7 pages). See also Quantum technologies in Russia, October 2019 (9 pages).

[2787] Here are some elements on this ecosystem: Quantum communication in Russia: status and perspective by Vladimir Egorov, 2019 (22 slides).

Africa, Near and Middle East

Israel

Israel was relatively quiet about quantum technologies until 2018 apart from Gil Kalai from the Hebrew University of Jerusalem who, since 2013, has shown a deep-rooted skepticism about the future of quantum computers. I was relatively surprised in 2018 to find out that the country was not very visible in the quantum research and entrepreneurship.

It was a stark contrast with other fields where this relatively small country has a significant impact worldwide: in software, artificial intelligence (where they have in excess of 400 startups), Internet, semiconductors, electronics, medtechs and biotechs to name a few.

Government funding

Then, things started to change[2788]. After a study carried out in 2017 by Uri Sivan from Technion to evaluate the country's quantum technologies efforts, a first initiative to better fund its research was launched in 2018 by the country's government and endowed with 75M€. It went mainly to Technion and the University of Haifa, which wants to design its own quantum computer and had also received a donation of $50M.

In December 2019, a panel of specialists commissioned by the government proposed a plan to invest $350M over 6 years in quantum technologies[2789]. In just a few months, the government approved this proposal which ended up with a funding of $400M, 60% of it supposed to fund academic research. The plan is fairly standard with an investment in human capital (faculty hiring and launching training courses), research and scholarships funding, attracting foreign researchers and the likes. The usual quantum technologies domains were picked with computing hardware and components, telecommunications, cryptography and sensing (with $40M), particularly with its military applications.

The Israel National Quantum Initiative (INQI) plan follows-up in naming the US plan announced in December 2018.

In March 2021, Israel announced it planned to create its own quantum computer, allocating a budget of $60M taken out of the national initiative. The goal is to create 30- to 40-qubit quantum systems. It was to take bids from both local players and international vendors, with a build or buy approach depending on the outcome. In July 2022, the government announced the creation of a quantum computing R&D center with a budget of $30M over a three-year. It selected their local star vendor, Quantum Machines to create the center that is supposed to work on superconducting qubits, cold atoms, trapped ions and quantum optics computers[2790]. The company will work with Classiq and Elbit Systems. Still, the ploy became a “buy” with Israel announcing the same month the procurement of an Orca Computing (UK) photonic quantum computer. They also work with ColdQuanta who already partners with Quantum Machines (like Pasqal in France) and Classiq[2791].

[2788] But not to the extent of this title; Israel has become a powerhouse in quantum technologies by David Kramer, Physics Today, December 2021 (4 pages).

[2789] See Israel joins the quantum club by Uri Berkovitz, December 2019 and Israel joins the race to become a quantum superpower by Anna Ahronheim and Maayan Hoffman, Jerusalem Post, December 2019.

[2790] See Quantum Machines to establish Israeli quantum computing center in $30 million deal by Meir Orbach, CTECH, July 2022.

[2791] See Inside ColdQuanta’s Role in the Israel National Quantum Initiative (INQI) by Brian Siegelwax, The Quantum Insider, August 2022.

Research

There are about 125 "principal investigators" in quantum technologies research in Israel spread in the following research institutions:

Ariel University with its Wireless Communication & Radars Lab, located in the Israeli settlement of Ariel in the middle of the Palestine West Bank. They work on millimeter wave and Terahertz sensors.

Bar Ilan University (Ramat Gan near Tel Aviv) with the Photonics and Optics group (Avi Peers, Eli Barkai and Dror Fixler) and the Institute of Nanotechnology and Advanced Materials which works on superconducting qubits (Michael Stern). These are integrated in QUEST (Quantum Entanglement in Science and Technology), a quantum research center launched in 2017.

Ben-Gurion University of the Negev (Beer Sheva) with the Sensing Technologies Lab (Asaf Gros), Quantum Magnetometry Group (Reuben Shuker) and the Atom Chip Group (Ron Folman). The startup AccuBeat (1993) which produces rubidium quantum atomic clocks, is a product of this university.

Hebrew University of Jerusalem with the Nano-Opto Group and Time Dissemination Group, and the Center for Nanoscience and Nanotechnology that works on superconducting qubits. The University also established its Quantum Information Science Center in 2013 to focus on secure quantum communication (QKD).

Technion (Haifa) with Quantum Information Processing lab (Tal Mor) which works on photonics, NMR and silicon qubits, the Russell Berrie Nanotechnology Institute created in 2005 (Gadi Eisenstein) and the Helen Diller Quantum Center which is working on photonics, quantum dots, superconducting qubits and cold atoms (Yosi Avron).

Tel Aviv University with its QuanTAU, their Quantum Science and Technology Center, working among other things on superconducting qubits.

Weizmann Institute of Science in Rehovot with the Center for Quantum Science and Technology (Adi Stern), the Quantum Circuits Group (Serge Rosenblum) working on superconducting qubits and the trapped ions group (Roee Ozeri) which created the first Israeli quantum computer in 2022 with 5 trapped ions qubits[2792].

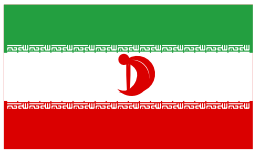
Quantum industry

The most visible startup in the field is **Quantum Machines** that sells qubit control hardware and software. Other Israeli startups and vendors in quantum technologies are Accubeat, ClassiQ (error control), Elta (sensing), Hub Security (PQC in HSMs), Mellanox Technologies (quantum communications, part of Nvidia), PhotoniQ (cold atoms interconnection), Qedma Quantum Computing (software), QuantLR (QKD) and Quantum Source Labs (photonic computing), Raicol Crystals (photonics), Tabor Electronics (RF electronics). Google's R&D lab in Tel Aviv also hosts researchers in quantum computing.

The **Quantum Technologies Consortium** created in 2019 assembles research institutions and industry vendors.

[2792] See A huge leap: Israeli researchers build country's first quantum computer by Ricky Ben David, Times of Israel, March 2022 and Trapped Ion Quantum Computer with Robust Entangling Gates and Quantum Coherent Feedback by Tom Manovitz, Yotam Shapira, Lior Gazit, Nitzan Akerman and Roee Ozeri, PRX Quantum, March 2022 (14 pages). These qubits use strontium. Their fidelity if 99.64% for a single qubit gate and 97.3% for two-qubit gates, which is not stellar.

Iran



Israel is not the only country in the Near and Middle East that seems to be invested in quantum research. **Iran** is also involved with at least two research laboratories, **Sharif University** which is working on quantum physics in partnership with Canada and the **Quantronics Lab** of the Iranian Technological University which is dedicated to quantum communication (QKD)[2793].

The country even organizes its conference on quantum computing, the **IICQI,** since 2007[2794].

United Arab Emirates

Each and every country wants « its » quantum computer. Even the emirate Abu-Dhabi got the quantum virus and decided to "build" its own quantum computer, even if "build" or "buy" are interchangeable in such a situation since it is a quantum annealing superconducting system coming from Qilimanjaro.

Still, it comes after the establishment of a Quantum Centre at the Technology Innovation Institute (TII) which hosts about 20 researchers coming from the Emirates and from various countries: Italy, Spain, Brazil, Greece, UK and Germany. This lab complements other labs in robotics, cybersecurity and energy. It even has some qubits manufacturing tooling.

Jose Ignacio Latorre is the chief scientist of this quantum research laboratory. He is a professor of theoretical physics at the University of Barcelona currently on leave, cofounder of Qilimanjaro and the director of the Singapore CQT since July 2020. Their key partners are Qilimanjaro, Universitat Catania in Sicilia and INFN, an Italian research network.

The QC-TII organized a webinar conference in June 2021, Atomtronics@Abudhabi with about 500 participants.

Intqlabs (2022, Dubai) is a contract research company created by Ankur Srivastava, from India, formerly an independent researcher, not affiliated with any lab. The company works on various fields: quantum computing, reversible classical computing, geo-magnetism and cybersecurity. They are talking about some form of "quantum and reverse computing" that would solve all current problems with quantum computing.

It's quite difficult to figure out whether it's some form of quantum computing or of classical reversible computing. All of this is patent pending, meaning that for at least a year and a half, you will have no idea what it's all about. Wait and see. They plan to license their technology to hardware manufacturers. They have otherwise created NGNSS (New Global Navigation Satellite System), an alternative to classical GPS solutions which as its name doesn't tell, is not requiring a satellite to function and uses magnetism detection and mapping.

Qatar

Qatar has also some ambitions in quantum technologies. In 2022, Hamad Bin Khalifa University (HBKU) announced the creation of the Qatar Center for Quantum Computing (QC2).

It received a $10M research grant from Barzan Holdings, a local defense industry vendor.

[2793] Source: Iranian research in quantum information and computation, June 2016.

[2794] See http://iicqi.sharif.edu/.

Let's also mention **QUANTUN**, the Quantum Tunisian Network launched in October 2021 to consolidate the work of quantum researchers in the country and **South Africa**'s Quantum Initiative (Sa QuTI) launched in September 2021.

Asia-Pacific

China

As in many technology sectors, **China** is loudly and clearly asserting its ambitions and power in quantum technologies[2795]. As in the UK, this investment was taken in hand early on by the executive and as early as 2013 with the involvement of Xi Jinping, the Chinese president, during a visit to the Anhui laboratory, focusing on quantum cryptography, combined with a training session.

Government funding

In 2015, Xi Jinping integrated quantum communication into the country's scientific priorities, in 13th plan covering 2016-2020. Maybe was it a benefit from having a government comprising a majority of politicians with some scientific background and also the result of Snowden's revelations on NSA's spying capabilities in 2013.

The amounts invested in quantum were respectively $160M in the 11th plan covering the period 2006-2010, $800M in the 12th plan covering 2011-2016 and $320M in the 13th plan starting in 2016, supplemented by $640M in funding from the regions[2796]. Later on, the Chinese government communicated an amount of $34B corresponding to several scientific priorities including quantum. This represented probably less than $1B between 2016 and 2020 and a total of $1.76B over 10 years. Other estimates are lower, in the $1.5B range for the 2006-2020 period[2797].

Figure 865: China's quantum investments from 2006 to 2021 did not exceed $1.8B. This number is very different from the $10B to $15B investment showcased in various analyst publications. These >$10B numbers are false and based on fuzzy propaganda coming from China and amplified by various US interests. Source: Chinese QC Funding by Xiaobo Zhu, 2017 (35 slides). And... 1 CNY ≈ 0.14 US $.

So, all the impressive $10B, $13B or $15B figures related to China's quantum technologies investments are probably completely off the mark. In 2021, China announced its new five year research plan, with a 11% global funding increase but with no details regarding quantum investments. At most, it would bring their 2006-2027 total quantum investments to about $3B, but definitively not $10B to $15B.

[2795] See Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership, CNAS, 2018 (52 pages) and Quantum information technology development in China by Yuao Chen, June 2019 (25 slides).

[2796] The 2016 quantum roadmap is available in "Quantum Leap: The Strategic Implications of Quantum Technologies by Elsa Kania" and John Costello (part 1 and part 2). See also Chinese QC Funding by Xiaobo Zhu, 2017 (35 slides).

[2797] See FactBasedInsight's Quantum Landscape 2020: China, March 2020.

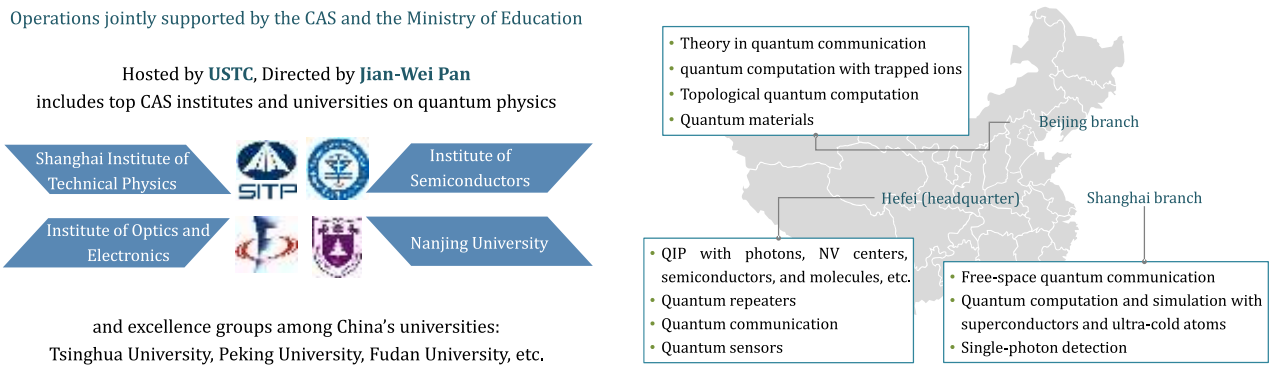


Figure 866: China's quantum ecosystem. Source: Chinese QC Funding by Xiaobo Zhu, 2017 (35 slides).

These investments are mainly spread over Beijing, Shanghai, and Hefei (500 km west of Shanghai). They specialize respectively in quantum communications, trapped ion computing, topological qubit computing and quantum materials for Beijing, silicon qubit computing, NV centers and photons, quantum communications and metrology in Hefei, and communication, superconducting and cold atom qubit computing and photon detection in Shanghai.

The Chinese plan is coordinated by the **USTC** (University of Science and Technology of China) of the Chinese Academy of Sciences (CAS) and under the leadership of Jian-Wei Pan[2798]. The most ambitious project is the "$10B" research center that partially opened in 2020, the **NLQIS (**National Laboratory for Quantum Information Sciences) of Hefei. This laboratory is focused on quantum computing and metrology for military and civilian applications.

Figure 867: Hefei's quantum lab.

It will employ 1800 research people, including 560 full-time researchers spread across two labs, three universities and a fab[2799]. But it seems this research center is also dedicated to research in artificial intelligence, semiconductors and other domains, including the installation of a (costly) light synchrotron. So, again, the related investment amounts are certainly not entirely dedicated to quantum technologies.

In November 2021, the USA decided to restrict exportation of quantum technology goods to China related. The US Commerce Department added three entities in China: the Hefei National Laboratory for Physical Sciences at Microscale, QuantumCTek to the Entity List for acquiring and attempting to acquire US made items in support of military applications. The goal is to prevent China from developing counter-stealth technology like advanced radars and counter-submarine sensors. It also blocks US technology for breaking encryption (quantum computing) or develop unbreakable encryption (PQC)[2800]. Indirectly, this will impact exports from other countries related to the US, mainly from NATO.

[2798] See The man turning China into a quantum superpower by Martin Giles in MIT Technology Review, December 2018.

[2799] See Hefei's plan to create a national laboratory for quantum information science has been reported to the state council, EEworld, May 2018.

[2800] See Addition of Entities and Revision of Entries on the Entity List; and Addition of Entity to the Military End-User (MEU) List, November 2021.

Research

On the quantum computing side, Chinese laboratories are testing all imaginable qubit technologies and regularly announce technological progresses. They seem to be rather ahead in photon qubits as we have seen about their boson sampling experiments but not really with other qubit types.

In 2017, the Hefei laboratory announced the realization of a test system of 10 superconducting qubits in aluminum and sapphire[2801]. The two qubit gates error rate of 0.9% was not best in class.

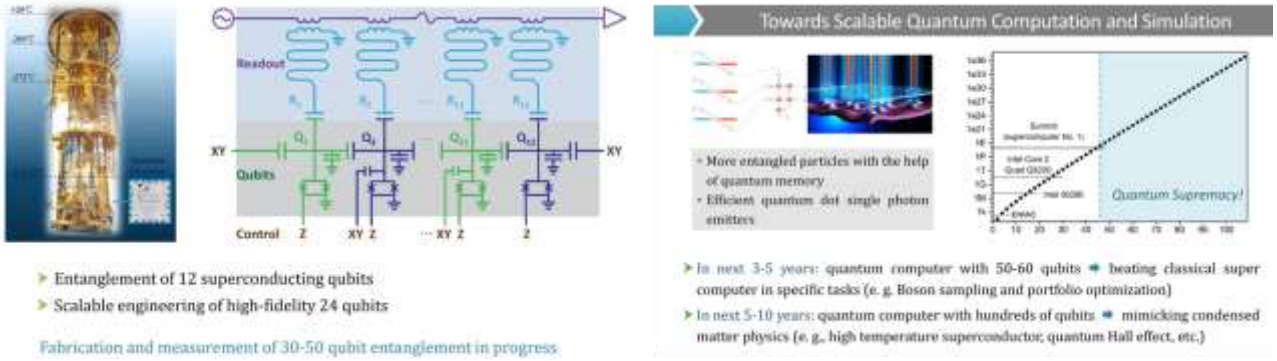


Figure 868: Source: 10-qubit entanglement and parallel logic operations with a superconducting circuit by Chao Song et al, 2017 (16 pages).

They were at 24 superconducting qubits in 2019. Their fidelity is 99.9% on single-qubit gates and 99.5% on two-qubit CZ gates, is much better[2802].

Their T1 duration, which defines the coherence time of the qubits is 40 µs, equivalent to what IBM obtains with its Q System One at 20 qubits. The Jian-Wei Pan team planned to reach 50 superconducting qubits by 2023.

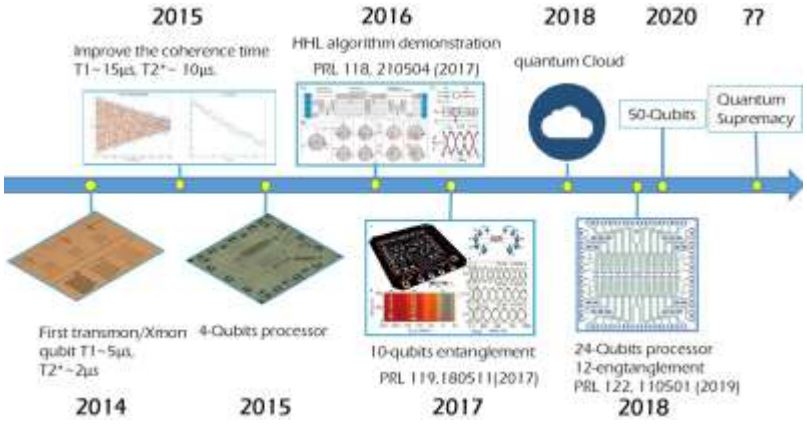


Figure 869: Source: Superconducting Quantum Computing by Xiaobo Zhu, June 2019 (53 slides).

It delivered on this promise in May 2021 with 62 superconducting qubits, implementing quantum walks, which makes comparisons difficult, for example with IBM's 65 superconducting qubits system launched online in September 2020[2803]. They followed with the announcement of a 66 superconducting qubits system quantum advantage, being seemingly a copycat of Google's Sycamore processor architecture and benchmarking.

The Chinese scientific level is good but not yet stellar. They mostly improve technologies developed in Western countries and do not generate many new ideas. On the other hand, they create experiments like boson sampling or QKD deployments at a large scale.

[2801] See 10-qubit entanglement and parallel logic operations with a superconducting circuit by Chao Song et al, 2017 (16 pages).

[2802] Source: Superconducting Quantum Computing by Xiaobo Zhu, June 2019 (53 slides).

[2803] See Quantum walks on a programmable two-dimensional 62-qubit superconducting processor by Ming Gong, Science, May 2021 (34 pages).

China does not seem to have a significant influence in the academic world on quantum algorithms and programming tools. We must never forget the strategic role of software and platforms in the digital economic battles! It looks like History is repeating itself in China for this respect.

Quantum industry

Public-private partnerships have been put in place, such as with **Alibaba,** who invested in the USTC to launch in 2015 the Shanghai Alibaba Quantum Computing Laboratory. It focuses on quantum cryptography and quantum computing. Quantum cryptography could be used to secure e-commerce transactions and data centers connections. In January 2018, Alibaba even launched a cloud-based 11 qubits system developed by USTC.

Figure 870: Alibaba's 11 qubit processor.

Alibaba is a serious contender in the superconducting qubit space with its fluxonium qubits variation.

Baidu launched in 2018 its **Institute for Quantum Computing,** which is being deployed in their Technology Park in Beijing with around ten people as of September 2019. It is led by Runyao Duan, a specialist in quantum information theory, with Artur Ekert as board member. They are mainly developing quantum software stacks in their QIAN full stack quantum software and hardware platform. They developed a quantum emulation solution in their cloud resources named Quantum Leaf[2804] and a bunch of other tools: Paddle Quantum (quantum machine learning), Quanlse (quantum pulse control for superconducting qubits), Qulearn (a quantum knowledge base), plus quantum error processing, measurement and control[2805], network architecture and quantum electronic design automation. They are also working also on a quantum Internet. In August 2022, they announced their first superconducting qubits quantum computer with 10 qubits named Qian Shi to be expanded later to 36 qubits.

Tencent also launched a Quantum Lab in 2018, led by Shengyu Zhang and based in Shenzhen. They plan to offer quantum computing resources in the cloud. The lab publishes work in quantum simulation and machine learning algorithms. It is developing QuAPE, a quantum control microarchitecture for superconducting qubits supporting multi-core QPUs parallelism that was prototyped with a FPGA circuit.

We can also mention the involvement of **ZTE** and many telecom operators and manufacturers in the deployment of secure fiber networks by QKD (**China Telecom, China Cable, China Comservice, China Unicom**) as well as various banks that use them.

Chinese startups are not very numerous at this stage, one of the reasons being that public research laboratories are well funded and have less incentive to create companies. One exception is **Origin Quantum Computing** which raised a record $163.4M to develop a full-stack superconducting qubits offering). Most other Chinese startups are in the quantum communication field, like **QuantumCTek** and **Qasky Science,** and have joined with ID Quantique and Battelle to form the **Quantum-Safe Security Working Group,** which federates the quantum cryptography industry.

Japan

Let's move to the rest of Asia, starting with **Japan**. The country stands out for its very active and long-term oriented fundamental research initiation of two key technological waves in quantum computing.

[2804] See Introduction to Baidu Quantum Program by Shuming Cheng, June 2019 (9 slides). They notably propose the Paddle Quantum library, released on GitHub, which supports neural network QML, quantum chemistry and optimization tools. All this in quantum emulation on classical data centers.

[2805] See for example Efficient characterization of quantum nondemolition qubit readout by He Wang and Ya Cao, August 2022 (11 pages).

It started with the creation of the principle of quantum annealing by **Hidetoshi Nishimori** in 1998[2806]. Then, there was the creation of the first superconducting qubits in 1999 by **Yasunobu Nakamura**, **Jaw Shen Tsai** (both then at NEC) in liaison with **Yuri Pashkin** (Lancaster University, UK). Unfortunately, this was not turned into some industry lead.

Research

Japan's public research is conducted by several independent agencies attached to various ministries that fund public laboratories, university laboratories and research partnerships with companies[2807]:

- **JST** (Japan Science and Technology Agency) funded by the Ministry of Research and which funds deep techs research projects and also promotes science to the general public and international scientific collaboration. In 2016, JST launched a project by Yasunobu Nakamura of "Macroscopic Quantum Machines" to assemble 100 superconducting qubits.
- **RIKEN** (Institute of Physical and Chemical Research) also funded by the Ministry of Research (MEXT), with a total of about 3000 researchers. It includes a laboratory in theoretical quantum physics, headed by Franco Nori, and another in photonics, headed by Katsumi Midorikawa. They work in particular on silicon qubits. It collaborates with Fujitsu since 2020 to build a supercomputing qubits computer.
- **NICT** (National Institute of Information and Communication Technologies) includes the Quantum ICT Advanced Development Center, which specializes in quantum cryptography. In July 2017, the institute carried out a demonstration of quantum telecommunications using a microsatellite, reminiscent of the Chinese experiment with the Micius satellite carried out the same year.
- **NII** (National Institute of Informatics) includes a hundred or so researchers and focuses on research in theoretical quantum computing but also works on superconducting and silicon qubits.

  The Japanese-French Laboratory for Informatics (JFLI) created in 2009 is based in Tokyo and hosted at both the NII and the University of Tokyo. It brings together researchers from the Universities of Tokyo, Keio, NII, CNRS, Sorbonne University (LIP6), Inria and Université Paris-Sud. This multidisciplinary team ranges from fundamental physics to algorithms and studies the feasibility of large-scale quantum computing as well as quantum cryptography. The laboratory is co-directed by **Kae Nemoto**, from the NII, one of the few women in this whole panorama. Damian Markham from CNRS LIP6 has been working there since the beginning of 2020.

- **NEDO** (New Energy and Industrial Technology Development Organization) which is attached to the Ministry of Economy and Industry, METI. It is particularly invested in quantum annealing with a project running from 2018 to 2022 with $4.5M per year.
- **AIST** (National Institute of Advanced Industrial Science and Technology) also funded by METI. It employs about 2300 researchers in all. Several laboratories appear to be dedicated to nanomaterial sciences. There is also a research group on precision measurement.

[2806] See Quantum annealing in the transverse Ising model by Tadashi Kadowaki and Hidetoshi Nishimori, 1998 (9 pages).

[2807] The most active quantum laboratories are located at the universities of Tokyo, Kyoto, Tohoku, Osaka, Nagoya, Keio, Tsukuka and Hokkaido. See Activities on Quantum Information Technology in Japan by Akihisa Tomita, June 2019 (19 slides).

- **QST (**National Institutes for Quantum and Radiological Science and Technology**)** was launched in April 2016 with an annual budget of $487M. This impressive amount is not exclusively allocated to quantum technologies. It mainly covers the vast field of quantum sensing and in particular medical imaging.

The Japanese government had launched various quantum initiatives such as **PRESTO** (since 2016) or the **CREST** cross-cutting program (also since 2016) as well as the **ERATO** projects in 1981 (Exploratory Research for Advanced Technology).

The country's quantum initiatives are currently part of its Fifth Science and Technology Plan, running from 2016 to 2022. In a typical Japanese way, this plan is linked to a societal goal "Society 5.0" to bring cyberspace and physical space closer together to solve society's social problems and create a human-centered society. All this with AI, quantum sensors and cybersecurity.

Figure 871: Japan's classical societal angle to sell some new technology wave.

Here are a few leading researchers in Japan in addition to those mentioned above[2808]:

Akira Furusawa of the University of Tokyo has the ambition to create a large-scale quantum computing solution with photon-based qubits. He's teaming up with NTT (see below) and plans to create a scalable computer by 2030[2809].

Yoshihisa Yamamoto (1950), a Stanford alumni and director of the NTT Physics and Computer Science Laboratory, who worked in photonics, QKD and quantum dots. He is very influential in Japan on the country's technological choices[2810]. He is the pilot of the Quantum Information Project (QIP), one of the national research program projects from FIRST selected in 2009 and which covered all branches of quantum applications[2811].

Kohei Itoh of Keio University has been managing the Q-LEAP project since 2018, which focuses on assembling different silicon isotopes into CMOS components and on NV center based quantum magnetometry (video). He is also a partner of IBM's Q Lab in Tokyo.

Yasuhiko Arakawa (1952) of the University of Tokyo specializes in semiconductor physics and optoelectronics, at the origin of new processes for the exploitation of quantum dots in sensing.

Yasunobu Nakamura (1968) who specializes in superconducting qubits and serves at the RCAST (Research Center for Advanced Science and Technology) of the University of Tokyo and at the CEMS (Center for Emergent Matter Science) of RIKEN[2812].

François Le Gall (1959) is a French researcher based at Kyoto University who specializes in quantum computing theory, mathematics, quantum algorithms and cryptography. He is also interested in distributed quantum computing (video). He has been living in Japan for more than 20 years.

[2808] Source: Q2B 2019 - International Government Panel, December 2019.

[2809] See Quantum computing: Japan takes step toward light-based technology - NTT, University of Tokyo and Riken aim for full-fledged system by 2030, Nikkei Asia, December 2021. The paper mentions a Japan $1.75B quantum plan. It is probably a mistake. See more reliable numbers in Concept of Quantum Technology Innovation hubs, 2021 (6 slides, broken link).

[2810] He is notably the co-author of the briefing note Quantum information science and technology in Japan, February 2019 (8 pages).

[2811] See First program overview.

[2812] See his presentation of the state of the art of quantum computing Development of quantum hardware towards fault fault-tolerant quantum computing by Yasunobu Nakamura (19 slides).

Masahito Hayashi of Nagoya University was originally a mathematician who then became a specialist in theoretical quantum computing. He coordinated the ERATO project on theoretical quantum computing.

Masahiro Kitagawa of Osaka University specializes in atomic nucleus spin-based quantum sensing in nuclear magnetic resonance with notable applications in medical imaging.

Mio Murao who created and manages the Quantum Information Group at the University of Tokyo that bears his name (Murao Group). This group specializes in distributed quantum computing, quantum systems simulation algorithms, quantum telecommunication protocols and quantum algorithms. She is very fluent in English, which has enabled her to serve as a connecting point between Japan and research teams in the USA (video).

Nobuyuki Imoto of Osaka University is leading research in quantum cryptography and telecommunications.

Masahide Sasaki of NICT leads much of Japan's quantum cryptography efforts. In particular, he has contributed to the SOTA project for quantum key communication using satellites[2813].

Government funding

The *flagship* project **Q-LEAP** launched late 2019 by the Ministry of Research (MEXT) seems the most ambitious and aims to catch up with both China and the USA, even if an alliance with the USA also seems to be on the agenda[2814].

The roadmap extends to 2039 with $200M spread over 10 years. The program targets quantum computing, quantum sensing and next-generation lasers. Most qubits technologies are funded: superconducting, cold atoms, trapped ions and electron spin. This "Flagship" will run until 2027.

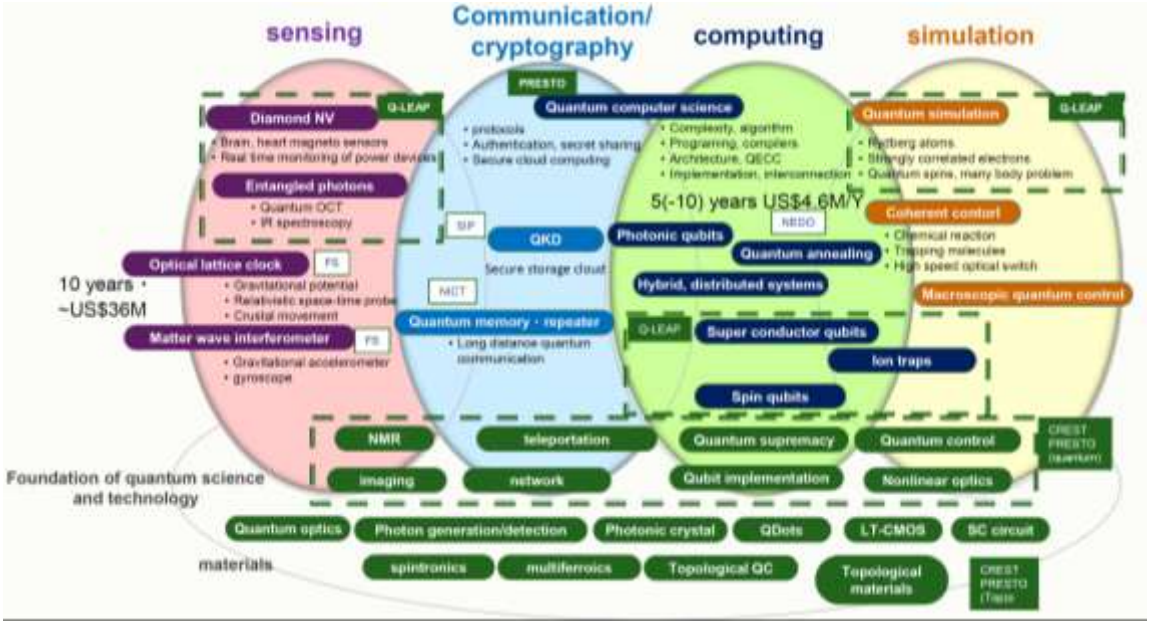


Figure 872: Japan's quantum ecosystem and plans. Source: Activities on Quantum Information Technology in Japan by Akihisa Tomita, June 2019 (19 slides)

[2813] See QKD from a microsatellite: the SOTA experience, October 2018 (10 pages).

[2814] See Japan plots 20-year race to quantum computers, chasing US and China by Noriaki Koshikawa, November 2019 and Land of the Rising Qubit: Japan's Quantum Computing Landscape by James Dargan, December 2019.

Quantum industry

Japanese startups are rather specialized in software and in particular for quantum annealing computing running either on D-Wave quantum annealers or on Fujitsu digital annealers. We have **A*Quantum** (2018, QA software), **D Slit Technologies** (2018, software), **Groovenauts (**2012, QA software), **Jij (2018,** QA software framework), **MDR** (2008, chemical simulation), **QunaSys (2018,** healthcare), **Sigma-I (**2019, QA software) and **Tokyo Quantum Computing** (2017, QA software).

Softbank's investment fund abounded with Saud family's money up to $100B was also planning to invest in quantum technologies[2815].

However, four years after its announcement, the fund does not seem to have a single stake in quantum technologies.

Figure 873: Japan's quantum industry vendors. (cc) Olivier Ezratty, 2022.

In the private sector, Japan's major industry groups are mainly focused on quantum telecommunications and cryptography, as well as on quantum and non-quantum annealing-based computing.

Hitachi also has a research laboratory located at the University of Cambridge (UK) that works on quantum key distribution, quantum computing and the creation of SQUID components for superconducting qubits. They are also working on silicon spin qubits quantum computing.

Toshiba Corporation has been involved in quantum cryptography since 2003. They are working on it with the Quantum Information Group (QIG) at the University of Cambridge, UK. They performed a first demonstration of quantum communication in 2014, sending 878 Gbits/s of secure data over a 45 km fiber between two areas in the Tokyo area over a cumulative period of 34 days, at a rate of 300 kbits/s. They were continuing the experiments in 2019 and beyond and with British Telecom in the UK[2816].

NTT maintains four applied quantum research laboratories, focused on quantum telecommunications and quantum cryptography, all with about 40 researchers[2817].

In 2017, telecom operator **NTT** launched a prototype photonics-based Quantum Neural Network (QNN) in collaboration with the **National Institute of Informatics** and the **University of Tokyo**. It was available on the cloud at qnncloud.com (video) but the service was discontinued in March 2019[2818]. This was done with Toshiba, NEC and the NICT in Tokyo with three nodes and 45 km apart[2819].They also work in the CMOS quantum dots qubits. NTT also developed LASOLV, a photonic based coherent Ising system with 2000 nodes[2820].

[2815] See SoftBank's Vision Fund Eyes Investment in Quantum Computing by Jeremy Kahn, Bloomberg, June 2017.

[2816] See Performance Limits for Quantum Key Distribution Networks by Andrew Shields, June 2019 (16 slides).

[2817] This leads to raising wages inflation for the most talented people, a bit like in Silicon Valley. See NTT offers researchers $1 million salaries in bid to lure top talent in cryptography, quantum computing, November 2019.

[2818] See Japan launches its first quantum computer by Walter Sim, November 2017.

[2819] See Tokyo QKD Network and its application to distributed storage network by Masahiro Takeoka, June 2019 (22 slides).

[2820] See LASOLV Computing System: Hybrid Platform for Efficient Combinatorial Optimization by Junya Arai et al, 2020 (6 pages).

Finally, several non-quantum annealing optimization computation projects on CMOS components have been launched. There is the **Fujitsu** offering, and also the NEDO project led by Masanao Yamaoka and Masato Hayashi at **Hitachi** in partnership with the AIST, RIKEN and NEDO (New Energy and Industrial Technology Development Organization, the equivalent of the energy branch of the CEA) laboratories[2821].

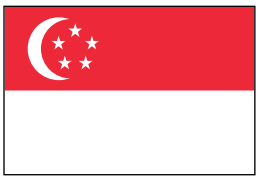
And then the **NEC** project in quantum annealing led by **Yuichi Nakamura** in liaison with Waseda University, those of Yokohama and Kyoto, AIST and Titech (Tokyo Institute of Technology). They are optimizing the classical part of annealing processing with NEC vector processors. The quantum part seems to be managed on D-Wave machines. NEC is also versed in quantum keys (QKD).

IBM announced at the end of 2019 the opening of a Q Lab in Tokyo in partnership with the University of Tokyo. IBM's investment in Japan follows a model already inaugurated in France in Montpellier in 2018, in Germany in September 2019 and in Canada with the Institut Quantique in June 2020: a partnership with a university, investments in training and above all, a technical and marketing investment to evangelize quantum among major customers[2822].

Finally, **Recruit Communications Ltd** (1960), a large $16B CDN company specializing in HR, communications and marketing, distinguished itself by launching a partnership with D-Wave in 2017 to develop quantum annealing-based solutions for the operational optimization of marketing, communications and advertising. In particular, they have developed the PyQUBO open source library, which simplifies the development of quantum annealing software applications[2823].

In September 2021 was launched Q-STAR (Quantum Strategic Industry Alliance for Revolution), an industry alliance to promote the usage of quantum technologies and particularly quantum computing and cryptography in various industries with the participation from Toshiba, Toyota, NEC, NTT, Hitachi, Fujitsu, Mitsubishi Chemical and Sumitomo among others.

Singapore



The small state of **Singapore** is known for its economic and entrepreneurial dynamism. Within the **National University of Singapore** (NUS), quantum research was consolidated in 2007 in the **Center for Quantum Technologies** (CQT) with an annual funding of about $15M. It was created thanks to some real political leadership, coming from the then Defense Minister of Singapore[2824].

[2821] See CMOS Annealing Machine - developed through multi-disciplinary cooperation, November 2018, Overview of CMOS Annealing Machines by Masanao Yamaoka, Hitachi, (4 pages) and A 2 x 30k-Spin Multi-Chip Scalable CMOS Annealing Processor Based on a Processing- In-Memory Approach for Solving Large-Scale Combinatorial Optimization Problems, November 2019.

[2822] See IBM Takes Its Quantum Computer to Japan to Launch Country-Wide Quantum Initiative by Anthony Annunziata, December 2019. In partnership with the University of Tokyo and IBM and the University of Tokyo Launch Quantum Computing Initiative for Japan by IBM, 2019. In August 2020, IBM embellished this partnership by announcing the creation of a consortium for the adoption of quantum technologies in Japan. See IBM Launches Global Consortium for Quantum Innovation by Chris Duckett, August 2020, which refers to an announcement that is really only about Japan: IBM and the University of Tokyo Unveil the Quantum Innovation Initiative Consortium to Accelerate Japan's Quantum Research and Development Leadership by IBM, August 2020.

[2823] See Recruit Communications and D-Wave Collaborate to Apply Quantum Computing to Marketing, Advertising, and Communications Optimization, May 2017.

[2824] Artur Ekert says he was persuaded to join Singapore in 2000 by Tony Tan, who was then the country's defense minister. He had met him at a conference where his visionary speech, for a politician, had impressed him. In 2005, Tony Tan took charge of the sovereign wealth fund Singapore Investment Corporation and then Singapore's National Research Foundation. He was at the origin of the strategy of targeted investment in cutting-edge research fields, which today we call deep tech. This Tony Tan then became the President of Singapore between 2011 and 2017. The CQT was launched in 2006. The story is told in the book 50 years of science in Singapore pages 362 to 387, February 2017. His personal credo: to be successful, you need to attract the right people, original ideas and then funding. Too often, this happens through funding.

It is vested in both quantum computing (cold atoms in Berge Englert's group, photons and superconductors in Dimitris Angelakis' group, trapped ions in Dzmitry Matsukevich's group), quantum cryptography (Kwek Leong Chuan's group) and quantum metrology (notably atomic clocks in Murray Barrett's group).

The CQT was led from its inception until July 2020 by Artur Ekert. Since then, it's run by José Ignacio Latorre. It brings together about twenty teams representing 22 permanent researchers, 60 research fellows and 60 PhD students, covering the four usual fields of quantum technologies. This represents a total of 300 people in all. Of the 22 research supervisors, about a quarter are Singaporeans who have usually done a thesis abroad. Singapore is doing well to attract talented foreigners and to ensure that they settle permanently in this country of five million people.

Six startups emerged from CQT with **Entropica Labs** (quantum algorithms), **Horizon Quantum Computing (**software), **Innovatus Q (**hybrid algorithms), **S-Fifteen Instruments (**quantum cryptography) and **SpeQtral** (satellite QKD).

Quantum communication is one specialty from Singapore. Since 2016, CQT has been associated with the telecom company **Singtel** and the NUS for the deployment of QKD on optical fibers with repeaters. At the end of 2019, a team from **Nanyang Technological University** (NTU) developed a 3 mm-sided chipset capable of integrating a CV-QKD, a continuous variable quantum key-based encryption system[2825].

In 2015, Singapore launched its Galassia-2U nanosatellite, created by CQT and used to experiment encrypted QKD based quantum communications. Galassia is integrated in a two-unit CubeSat format (two cubes on top of each other, see *opposite*). It weighs only 3.4 Kg in total. It was sent to space with 5 other satellites including the telecommunications satellite TeLEOS-1 (400 kg) at the end of 2015 by an Indian launcher.

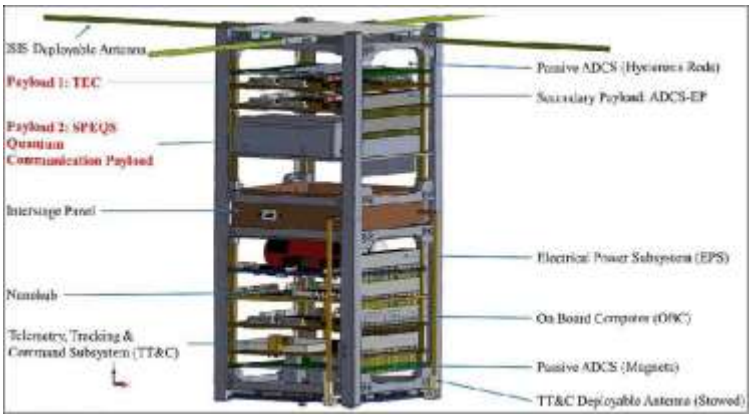


Figure 874: Source: https://directory.eoportal.org/web/eoportal/satellite-missions/g/galassia

In May 2022, as part of its Quantum Engineering Programme (QEP) started in 2018, Singapore launched three national platforms with a total funding of $23.5M for 3,5 years with a pooling of the resources and skills from CQT at NUS and NTU Singapore, A*STAR's Institute of High Performance Computing (IHPC) and the National Supercomputing Centre (NSCC).

- The **National Quantum Computing Hub** which will develop quantum computing capabilities and use cases for the industry.
- The **National Quantum-Safe Network** which will conduct trials of quantum-safe communication technologies for critical infrastructure.
- The **National Quantum Fabless Foundry** which will support microfabrication techniques for quantum devices and enabling technologies. Hosted at A*STAR's Institute of Materials Research and Engineering (IMRE), it will manage the micro and nanofabrication of quantum devices and related enabling technologies. This complements the Quantum Science and Engineering Centre (QSec) launched in December 2021 by NTU to design and manufacture various quantum chipsets using classical semiconductor manufacturing technologies.

[2825] See Quantum chip 1,000 times smaller than current setups, November 2019.

The lifetime of this type of satellite is six months[2826]. These experiments led to the creation of the S-Fifteen Space Systems. However, solutions have yet to be found to ensure that these satellites last longer in their low orbit and do not contribute even more to low orbit pollution.

Several partnerships and linking the French and Singaporean quantum ecosystems. The CQT welcomes several researchers from France, including **Steven Touzard**, **Miklos Santha** (CNRS) and **Christian Miniatura.** Christian is leading **MajuLab**, the joint CNRS-NTU research laboratory on quantum science. He is joined in October 2022 by **Alexia Auffèves** who was already partnering with a CQT research group in charge of studying noise and error correction codes led by **Hui Khoon Ng**. NUS is also partnering with the **Thales TRT** research lab based in Singapore, in security and sensing[2827]. **Sondra Lab** is another Franco-Singapore lab with CentraleSupelec, ONERA, NUS and DSO which is working in the fields of electromagnetism and signal processing applied to radar.

South Korea

In South Korea, the telecom operator **SK Telecom is** investing in quantum telecommunications[2828]. They are partners with Florida Atlantic University. They have also invested in 2016 in the Swiss startup ID Quantique. SK Telecom is also partner since 2017 with Nokia in the QKD field as well as with Deutsche Telekom with whom they have established a "Quantum Alliance" to create secure telecommunications.

SK Telecom has deployed a QKD network in the backbone of its 4K network in the city of Sejong on two links of 38 and 50 km respectively[2829].

Samsung is also investing in QKD and cryptography. They integrated a quantum random number generator in a dedicated version of a Galaxy smartphone for the Korean market in April 2020, with a component from ID Quantique, the Swiss startup acquired by SK Telecom in 2018. A new version was launched in April 2021.

Taiwan

Taiwan is very advanced in semiconductors with TSMC, the leader in CMOS fab and the only one with Samsung that is able to go down to an integration level of 5 nm, soon 3 nm and with plans to reach 1 nm. It is also still very present in the PC components market. This is particularly the case with motherboards (MSI, Asus, Gigabyte) and PC manufacturing (Quanta, ...).

It was logical in these conditions that the country becomes interested in quantum computing.

We can identify initiatives in students training and with a conference organized in September 2019[2830]. **Quantum Design** provides measuring instruments but does not seem to exploit technologies of the second quantum revolution[2831]. Finally, IBM has established a foothold in the country to help it adopt quantum technologies.

[2826] See Quantum Tech demos on CubeSat nanosatellites (41 slides).

[2827] See Singapore's NUS and Thales developing quantum technologies for commercial applications by Jamilah Lim, October 2021.

[2828] See SK Telecom Continues to Protect its 5G Network with Quantum Cryptography Technologies, March 2019.

[2829] See Quantum Safe Communication - Preparing for the Next Era by Dong-Hi Sim, June 2019 (21 slides).

[2830] See Quantum Computer: Envision the New Era of Computing, a conference in September 2019 and Quantum tech summer program in Taiwan a success, Taiwan News, July 2019.

[2831] See Quantum Design Taiwan.

In December 2020, Taiwan launched a $282M quantum plan over 5 years. It will consolidate its investments in the Southern Campus of Academia Sinica, the national academy of Taiwan, in Tainan. They plan to create a Quantum Technology R&D center between 2022 and 2024. On top of that, Hon Hai (FoxConn) created a Quantum Computing Research Center in January 2021.

In April 2022, the Taiwanese government announced as part of this plan the selection of 17 research teams in universities and the hiring of 72 project directors and 24 IT companies. They are looking at ways to improve quantum hardware and software and to leverage, if possible, their semiconductor industry.

Australia

The Australian National Innovation and Science Agenda announced in 2015 included 24 initiatives and $820M in funding over 4 years, of which $19M were allocated to the Center for Quantum Computation and Communication Technology (CQCCT) over 5 years in quantum computing.

The country is prolific in public-private partnership projects associating Australia with other countries[2832].

In 2017, the University of New Wales (UNSW), the Commonwealth Bank of Australia and telecom operator Telstra provided $52M in funding for the creation of a silicon quantum bit processor. One could hope that Orange will do the same in France with the CEA and/or a startup!

An investment fund of the Ministry of Defence, the **Australian Next Generation Technologies Fund** allocated $730M to 9 areas including one on quantum technologies over 10 years[2833].

Assuming that these funds were distributed evenly among the 9 initiatives, this gives us $8M of additional funds per year on quantum technologies for military uses, including sensing.

In February 2019, **CQC2T** (Centre of Excellence in Quantum Computation and Communication Technology) was created at UNSW, headed by Michelle Simmons. The goal was to create an electron spin quantum computer. With federal funding of $33.7M, it brings together a community of 200 researchers[2834].

Australia also has **EQUS** (Arc Center of Excellence for Engineered Quantum Systems), a national quantum sensing research center. It partners with Microsoft, Moglabs and Lockheed Martin, among others.

On the entrepreneurial side, there are three startups in the field of quantum technologies with **QuintessenceLabs (**QKD optical keys), **QxBranch** (software and consulting, an American startup with an office in Australia, acquired by Rigetti in July 2019), **Silicon Quantum Computing (**silicon qubits), **Quantum Brilliance** (2019) on top of which should be added **Archer** and their carbon electron spins qubits.

[2832] See Charting the Australian quantum landscape, February 2019 (5 pages).

[2833] See Next Generation Technologies Fund, 2016.

[2834] In early 2019, UNSW's CQC secured an additional $33M in funding at its official launch. See Federal govt funnels $33.7 million towards UNSW's quantum research by Matt Johnston, February 2019.

In May 2020, Australia put its quantum strategy in order with the publication of a plan by CSIRO[2835]. Their (fairly optimistic) ambition is to turn it into a $4B industry creating 16,000 jobs by 2040 out of a projected global total revenue of $86B. The projected breakdown is $2.5B and 10,000 jobs for computing, $900M and 3000 jobs for sensing and $800M and 3000 jobs for telecommunications. The goals? To define a coordinated strategy, to finance research and business creation, to train talents and to create a coherent industrial value chain.

A relatively new point in such a plan, is to explore the ethical, social and environmental issues that could be raised by quantum technologies. The subject has been growing in importance since 2020. They also address the question of the supply chain of key components and materials for quantum technologies.

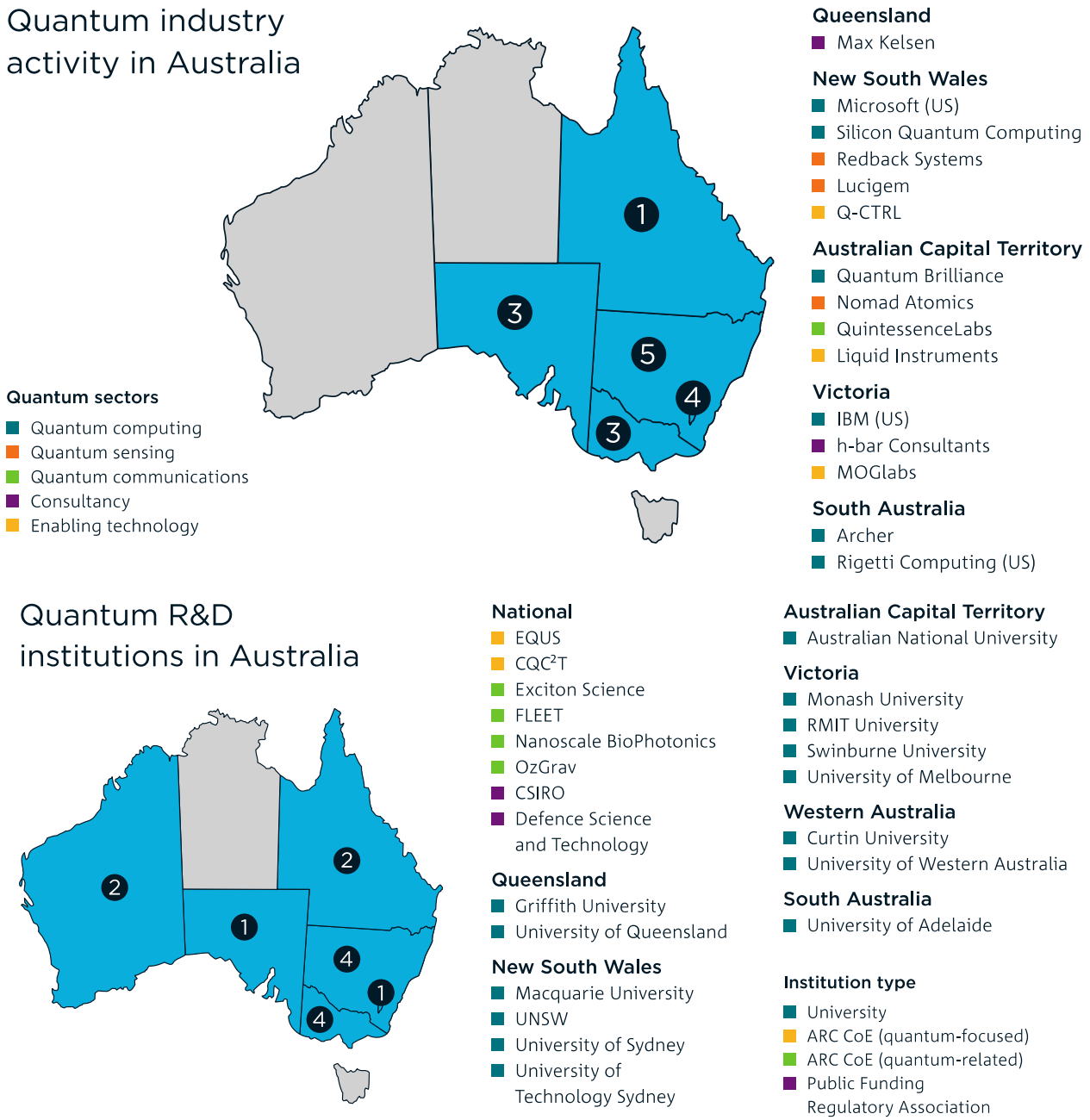


Figure 875: Australia's ecosystem. Source: Growing Australia's Quantum Technology Industry by CSIRO, May 2020 (56 pages).

[2835] See Growing Australia's Quantum Technology Industry by CSIRO, May 2020 (56 pages) and Australia could lose its quantum computing lead, CSIRO warns by John Davidson, May 2020.

As for companies and startups, they have some of them shown in this map. They highlight Microsoft and IBM. So be it. Rigetti because they have acquired the local startup QxBranch. And a few other startups, some of which are specialized around diamonds. In September 2022, the Tech Council formed the **Australian Quantum Alliance** to consolidate its quantum tech industry.

In terms of international partnerships, the country is associated with the University of Singapore for the creation of quantum telecommunication satellites.

In December 2020, Australia launched the **Sydney Quantum Academy,** a joint effort from Macquarie University, UNSW Sydney, the University of Sydney and UTS. It consolidates training offerings implemented by the partner Universities for undergraduates, PhDs plus some fellowships programs.

In November 2021, the Australian government allocated an additional US $80M to its quantum efforts, particularly for supporting the commercialization, adoption and use of quantum technologies and create new jobs.

It includes US $51M for the creation of a “quantum commercialization hub” with the task to build strategic partnerships with "like-minded countries" to sell Australia's quantum technologies, starting with the usual Commonwealth country partners and the USA. As a follow-up from the famous nuclear submarine deal with the USA (at the expense of an existing classical submarine deal with France) announced in September 2021, Australia cemented a global quantum partnership with the USA in November 2021, covering in a fuzzy way the exchange of quantum knowledge and skills. The University of Sydney is already part of an international consortium integrated in the US IARPA **LogiQ** program.

The Australian quantum ecosystem benefits from the country having Cathy Foley as its chief scientist given she led the development of a Quantum Technology Roadmap at CSIRO in 2020.

At last, in July 2022, Google announced new partnerships with Australian universities including UNSW and the University of Sydney. It extends what they already do with US universities, mostly for the development of quantum algorithms on Sycamore QPUs.

India

At the beginning of 2020, India launched an investment plan in quantum technologies, the **NMQTA** (National Mission on Quantum Technologies & Applications). This plan is well funded as a proportion of the country's GDP, with $1.12B over 5 years, at the same level as the American Quantum Initiative Act of 2018 or the European Flagship launched the same year[2836].

The plan covers the usual suspects: quantum computing, quantum telecommunications and quantum sensing. Ironically, the CEOs of IBM, Google and Microsoft who are strong investors in quantum computing are all of Indian origins (Arvind Krishna, Sundar Pichai and Satya Nadella)!

The Indian plan has an eye on China and wants to turn the country into a quantum leader, particularly in computing, telecommunications and cryptography.

In August 2021, **MeitY** (their Ministry of Electronics and Information Technology) launched the Quantum Computer Simulator (QSim) toolkit that was created by IISC Bangalore, IIT Roorkee and C-DAC. This software emulator of gate-based quantum code must not be confused with Qsim from Qsimulate and Google.

In January 2022, the **Indian Army** launched its Quantum Research Laboratory. So be it.

[2836] See India finally commits to quantum computing, promises $1.12B investment by Ivan Mehta, February 2020.

In February 2022, **Avasant** (an US consulting firm with a branch in India) and **NASSCOM** (the Indian software and IT service trade association) published a report on the opportunities of quantum technologies for India[2837]. It contained several nuggets like a quantum tech potential providing between $152B and $310B cumulative value to the Indian economy by 2030 with a maturity inflection point positioned in 2027.

They expect that 10K logical qubits will be available by 2030 (100 would be so nice…). But they expect a moderate workforce impact of 25K to 30K people in 2030. Also, India plans to develop a quantum computer with about 50 qubits by 2026. Also, they position the quantum Internet to be related to FTQC in their roadmap for 2027 and beyond. It does not really explain the connection between these two technologies. The document also shows the key role of the large Indian IT services companies in the adoption of quantum computing. As an example, in September 2021, Infosys Cobalt was partnering with AWS Braket to explore the business potential of quantum computing.

Among other things, the Indian plan has also accelerated the creation of startups in India, some being king in overselling their technology advances. This is the case of **QPI** and their projects of a one million silicon qubits and hybrid processor. Many of their new startups are multi-domains, such as:

- **QRLAB** (2020, India) who is a contract research, education and consulting company focused on quantum computing. They develop quantum inspired software, QML and also work on quantum Internet and cryptography.
- **Qulabs.ai** (2017, India) which builds quantum networks and has some expertise in QML in finance and for new drug discovery. That's quite broad in scope! Their QuAcademy facilitates students training.
- **Fractal Analytics** (2000, India, $685M) is an AI/data analytics company and a unicorn. It is creating an in-house quantum computing lab.

[2837] See The quantum revolution in India: betting big on quantum supremacy, Avasant, February 2022 (48 pages).

Quantum technologies around the world key takeaways

- The quantum startup scene has seen its peak company creation in 2018. A small number of startups like D-Wave, IonQ, Rigetti, PsiQuantum and Xanadu collected about 70% of the worldwide quantum startups funding. The investors FOMO (fear of missing out) and the "winner takes all" syndrome explain this situation.
- Most developed countries now have their "national quantum plans" and want to lead that space, particularly with quantum computing. The first ones were Singapore in 2007 and the UK in 2013. Investment comparisons are not obvious since these plans accounting are not the same from country to country (incremental funding vs legacy+incremental, private sector included or not, European Union investments included or not). All these plans invest a lot in fundamental research and on developing a startup and industry ecosystem.
- China's quantum investments have been overestimated for a while, both because of the ambiguity of China's communication and since various lobbies in the USA were pushing for increased federal investments to counter China's perceived threat. This worked particularly well during the Trump administration and seems to persist with the Biden administration.
- Europe and the USA are the greatest investors in quantum science so far. The European Union as a whole is the largest region for public investments in quantum research. The USA has a larger industry investment than Europe due to its large IT vendors investments (IBM, Google, Microsoft, Honeywell) and a traditional lead in startups funding, and, certainly, with its domestic market size and dynamics.
- Many countries did put quantum technologies in the critical field of "digital sovereignty" like if it was some sort of nuclear weapon equivalent.
- Each country has its own strengths and specialty although most of them invest in all the fields of quantum technologies (computing, telecoms/cryptography and sensing).
- Some analysts are wondering whether we'll get soon into a quantum winter, like the ones that affected artificial intelligence in the 1970s and the 1990s. One way to avoid it is to limit overpromises.

Corporate adoption

This book is intended for a wide audience interested in quantum technologies. It includes companies that may wonder what to do when facing such a deluge of hype, information, complexity and uncertainty. And this comes in addition to other technological waves to assimilate such as artificial intelligence, cryptos and other Blockchain, NFTs, the metaverse and 5G, not to mention cloud deployments and the classical business applications backlog.

The wave of quantum technologies is unique in that it is even more unpredictable and difficult to grasp than the other digital technologies waves. And yet, it is worth the attention, particularly in certain key verticals such as finance, healthcare, utilities and transportations. We are clearly in a technology push situation, meaning, here it is and it's up to us to imagine what to do with it. And quantum technologies, particularly computing, are not replacing legacy systems, but complementing them.

It's still a fairly green field and not only because scalable quantum computers are not yet available. It's also linked to having only a few people understanding how quantum computers are used and benchmarked. Innovation is still well ahead of us. And quantum technologies are not just about computing. It also deals with telecommunications, cryptography and sensing. This last domain might be under evaluated and could be strategic for many industries.

Large customers and their IT, digital transformation, innovation and R&D departments are exposed to a continuous stream of industry analyst and vendors pitches creating a sense of urgency for the adoption of quantum computing. It comes for example from **Capgemini**[2838], **McKinsey**[2839], **Deloitte**[2840], **Harvard Business Review**[2841], **Arthur D. Little**[2842], from **Pathstone**, a financial advisor company[2843]. It can take the form of a survey commissioned by a vendor, like **Zapata Computing**[2844]. Some even are completely off-the-mark on the role of quantum computing, such as in cybersecurity[2845].

I propose here a relatively simple and, all in all, fairly classic approach for corporations, which is laid out in a dozen points, some of which come from the experience of major large companies.

[2838] See Capgemini: Organizations need to get moving on quantum by Dan O'Shea, Fierce Electronics, April 2022.

[2839] See Quantum computing use cases are getting real—what you need to know, McKinsey, December 2021.

[2840] See Quantum computing in 2022: Newsful, but how useful? by Duncan Stewart et al, Deloitte, December 2021. Their assessment is the most honest of all, with cautious tales like: "*Many of the tasks that they currently do can be replicated on a standard laptop computer at a fraction of the cost. The problem with QCs' usefulness is not a lack of use cases, money, effort, or even progress. It's that current QCs are not yet powerful enough to tackle problems that can't be performed by traditional computers*".

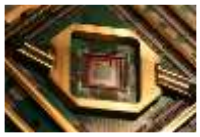
[2841] See Quantum Computing for Business Leaders by Jonathan Ruane, Andrew McAfee, and William D. Oliver, HBR, January–February 2022. With an interesting statement: "*Quantum computing will enable businesses to better optimize investment strategies, **improve encryption**...*". How can you trust this sort of report with such misunderstanding of how quantum computers will impact cryptography (it potentially endangers it and you won't be saved by a quantum computer)?

[2842] See Quantum Computing - The state of play and what it means for business by Albert Meige, Rick Eagar, Lucas Könnecke and Olivier Ezratty. I indeed participated (pro-bono) to the fact-checking of this work.

[2843] See "Quantum Impact" - The Potential for Quantum Computing to Transform Everything by Pathstone, December 2021 (35 pages).

[2844] In Report: 74% of Executives Warn Either Adopt Quantum Soon, or Risk Falling Behind Forever by Matt Swayne, The Quantum Daily, January 2022, reporting on the first annual report on enterprise quantum computing adoption commissioned by Zapata Computing: The First Annual Report on Enterprise Quantum Computing Adoption, Zapata, January 2022 (42 pages).

[2845] See Quantum Computing: 5 Potential Applications, January 2022 where this nugget can be found: "*Quantum computing could also help in the development of new encryption techniques, known as quantum cryptography*". Somebody should tell them that quantum cryptography does not run on a quantum computer!



technology screening

- understand quantum technologies
- concepts and wording
- decipher vendor's messages and hype
- understand the news
- what can quantum algorithms do?
- case studies applicability and range

education and training

- some developers, IT architects and line of businesses R&D scientists.
- study the link between quantum computing and R&D unsolved problems.
- online training
- initial training

needs analysis

- existing unsolved problems or problems that are too lengthy or costly to solve?
- create an internal communauty
- involved security specialists
- security protocols mapping

resources

- «Understanding Quantum Technologies» ebook (free, >1120 pages).
- ecosystem events (Q2B, QCB, Lab Quantique, …)
- vendors quantum offerings (IBM, Amazon, Microsoft, D-Wave, Pasqal, Quantinuum, IonQ, …)
- independant software vendors offerings (QC-Ware, Multiverse, …).

evaluation

- test some quantum algorithms at small scale
- on universal gates qubits as well as on quantum annealing or quantum simulators

Figure 876: a simple method to adopt quantum technologies. (cc) Olivier Ezratty, 2022.

Technology screening

Of course, you don't adopt any new technology after reading a news clip. But your management may push you to look at the trend and understand it. This top-bottom approach is amplified by the strategy consultants and analysts who are ringing the alarm bell in the direction of "business decision makers", up to, if they can, to CEO and executive boards.

The task is hardened with quantum computing because we are still in an intermediate exploratory phase where quantum computers are not yet really functional.

- Of course, you start with looking at the various **use cases** of quantum technologies in a "top-bottom" approach and what added value it could potentially bring to a business. This ebook can help you with its inventory of business applications, starting page 701. They are sorted by vertical market. If your market is not there, it doesn't necessarily mean that you shouldn't care. If you have a developer and/or mathematical background, you can have a look at what can be done at a lower level with quantum algorithms by looking at the algorithms part of this book, starting page 579.
- Then, you still need to understand the **technology dimensions** of quantum computing and related telecommunications and cryptographic matters. One thing is to understand what is the state of the art, how its changing over time, what are the scientific and technology challenges. This technology screening has to be done on a continuous basis. Things are changing fast in this domain.
- Don't miss the potential of **quantum sensing**. It may be enormous in various industries where precision is mandated. Quantum sensing helps measure with greater precision nearly any physical dimension: time, gravity/acceleration, magnetism, electro-magnetic waves and the likes.
- Learn how to **decode** analysts, research labs and vendors lingua, particularly in the field of over-promises. I provide a few examples in this book, about the fact that quantum computing is not a miracle solution that can speed up all computer processing. Learn some tricks to assess the real technology readiness level (TRL) of advertised quantum innovations. Also, understand that quantum computing is not adapted for big data applications. One important aspect here is the timing of innovations given the analysis timeframe is quite large, sometimes accounted in decades.

- Attend **ecosystem events** such as the QC Ware Q2B conference, Lab Quantique meet-ups, or quantum business conferences that are now organized all around the world. And real-life events are back after the long covid lockout period of 2020/2021.

Needs analysis

Many vendors will push you to look at your needs even before describing what is really possible to do today. This is one reasonable approach but it should not be implemented independently from a real technology assessment.

- Identify **intractable problems** in the company's applications and business needs portfolio. This is a question that developers and data scientists can sometimes answer. For example, these are complex optimization problems involving the orchestration of many resources. You have also to look at your current existing or potential usage of high-performance classical computing. What if scenarios can also be built on the power quantum computing can bring. For example, what if you could solve such or such complex business problem that was never addressed, particularly related to some optimization process?
- Then, back to technology, look at the related case studies, existing algorithms that are supposed to solve these problems. Understand the **scope of existing case studies**: are they small scale pilot projects or deployable applications? Most of the time, they are in the first category. They interrogate vendors and independent specialists on the size and characteristics of the quantum computers and/or hybrid systems associating a quantum computer and classical computers that would solve the business problem.
- Create an **internal community** of engineers and business specialists interested by quantum technologies, as Goldman Sachs, Morgan Stanley, BMW, Volkswagen, Airbus, EDF and Total have done, for example. It can be fed with presentations from research labs and vendors and also sharing the understanding engineers have about quantum technologies, identify key questions to ask, brainstorm about business needs where quantum technologies could help.
- Launch a mapping of **security protocols** threatened by quantum computers and the infamous Shor integer factoring algorithm. What data in the present that could be intercepted now could have some value in the future for an attacker? If present data has some value more than 5 to 10 years from now, you may need to start worrying and looking at QKD and PQC solutions or even revisit the way you implement applications in the cloud.
- Look at what your **peer companies** and those from your own ecosystem are doing with quantum technologies. Some may be vocal, like in the financial sector, some less. But there’s now no lack of industry events where this topic is discussed.

Training

Training a core team of people will be necessary to launch the two previous steps.

- Train a **few developers** in quantum programming. This can be done by letting people interested in the matter spend time on it on their own. The information and tools are available online with IBM, Microsoft, Atos, D-Wave and many other places. Open-source cloud-based tools are already there. The youngest and most curious developers will probably be the ones who will best adapt to quantum computing programming paradigms, which are difficult to assimilate when being trained for classical programming. These must also have a stronger mathematical background than the average developer. Analog electronics engineers can also be interested with quantum programming giving the analog nature of the underlying processes like interferences between qubits.

- Understand the links between **quantum computing and artificial intelligence**. Quantum machine learning is a new sub-discipline of quantum algorithms that deserves to be explored and understood.
- The small hidden advertising in this book is here: I propose a **one or two days customized training** for corporate engineers, IT people, R&D and innovation specialists who are curious to discover the whereabouts of quantum computing and other quantum technologies.

Evaluation

- Talk to the many quantum computing **independent software vendors**, particularly with those who are specialized in your vertical.
- Test **some algorithms** in the cloud with universal quantum computers (IBM, Amazon and Microsoft cloud, Xanadu, etc) or quantum annealer (D-Wave) or with emulators (Atos, IBM, Microsoft, Amazon, Google). The available case studies are discussed in this book in the section on algorithms and applications by market, starting page 707.
- Do not hesitate to test algorithms on D-Wave **quantum annealers** despite their relatively poor image among universal quantum computer purists. Quantum algorithms for these computers are suitable for solving complex optimization problems and represent a large part of what quantum computing can bring, whether in biology or finance, to take just two examples.
- Also keep an eye on **quantum simulations** which are useful for solving two main classes of problems: materials and chemical simulations, and complexity problems. Pasqal (France) and ColdQuanta (USA) are not far from delivering very interesting hardware here. The first Pasqal system with 100 cold atoms qubits is available in the cloud since mid-2022.
- Avoid the **do nothing approach**. Since quantum technologies adoption takes a while, you would be left behind against your competition. This may look contradictory with the need to avoid falling into the current quantum hype. Well no. Sort the hype and find what is useful! You'll find stuff!

Congratulations, you have saved yourself an overpriced McKinsey or BCG study!

Quantum technologies and society

We will leave quantum physics, hardware, mathematics and algorithms to focus on the links between quantum technologies and society. We are still at the very beginning of this technology revolution. What will follow is a mixture of observations and interpolations. Like with any digital technology wave, the quantum wave will affect society and industries at several levels, some of which can be anticipated, others less easily.

I am interested in connecting the potential impact of quantum computing with regards to mankind ambitions, the role of science fiction in the buildup of quantum imaginary, the philosophy of quantum physics, the way in which religions and spiritual movements may embed quantum whatever in their thinking, quantum technologies ethics, education and training in quantum computing, the role of gender balance in the sector and, at last, quantum vendors marketing side effects.

Human ambition

Quantum computing is easily presented to the general public, or understood, as bringing a computational power defying imagination, going beyond anything that has been done so far. Quantum computing would thus be a way to circumvent the current sluggishness of Moore's law. It would make it possible to maintain some sort of eternal technology growth exponentiality. This may give the impression that, with quantum computing, mankind will have a tool providing him with infinite power and total control of information, in the line of many myths built around artificial intelligence and its ultimate mythical destiny, Artificial General Intelligence (AGI). In 2018, the futuristic American physicist and author **Michio Kaku** predicted that quantum computers will be the ultimate computers capable of surpassing human intelligence[2846]. Here we go again with the Singularity!

Artificial intelligence and quantum computing seem to have no boundaries. They illustrate mankind's desire for power and omniscience, to shape matter if not minds, and to have the capacity to predict the future, making it almost deterministic. So much that it would be the abandonment of free will[2847]. Of course, not!

Figure 877: no, quantum computers won't end free will!

Quantum physics has generated its share of questions about the nature of the world. The indeterminism of quantum state measurement has become that of life. Quantum entanglement has given rise to pseudo-scientific explanations of telekinesis and the transmission of thought. We will see in the following section how quantum medicine mixes nano and macro worlds in a fancy way.

[2846] See The World's Most Disruptive Technology (That No One Is Talking About), Part II by Ian Connett, 2018.

[2847] As suggested by this article in The Atlantic of June 2018, the title of which has little to do with the content!

The mechanical nature or not of consciousness is at stake. For **epiphenomenalism** (definition), our consciousness is the result of physical phenomena in our body and brain but without direct external physical effects. Behavior is the result of the brain's action on the muscles.

For **mysterianism**, the understanding of consciousness is beyond the reach of Man. As consciousness depends at a low-level on quantum phenomena which govern a-minima the relations between atoms of the molecules of our brain, some people deduce a little quickly that quantum computing would allow AI to become general as in this debate! But these are at this stage fancy elucubrations.

Ambitious projects such as the European **Human Brain Project** led by Henri Markram aim to simulate the brain's behavior in a computer and thus to understand how it functions from start to finish, even if it is not possible to do so on even a molecular scale. In another fashion, the ability of quantum computers to simulate quantum phenomena has also sustained the idea that we are objects of a great simulation. An idea that ignores the constraints of dimensionality.

An exploration of the mysteries of quantum computing and complexity theories allows us to put our feet back on the ground. Complexity theories describe various limits to the nature of problems that can be solved with quantum computing. Computational omnipotence does not exist. We will always be obliged to use various forms of reductionism to simulate the world, i.e. we will only be able to do it correctly at "macro" scales and not at "micro" or "nano" scales for matters related to computational magnitude[2848]. A bit like predicting the weather thanks to the finite element method applicable to large portions of sky and not at the level of each water molecule.

The limits of the possible will be constantly pushed back, but they will remain. Just like those of understanding the world which are confronted with the temporal and spatial limits of the Universe. We will probably not be able to know what was happening before the big bang nor to evaluate the existence of multiverse. Being unverifiable, these interpretations of the world can only remain speculations and not become real science. In the same way, our physical means will probably never make it possible to simulate our world in-extenso.

Quantum physics also introduces a lot of chaos and randomness into biology that no computer will ever be able to fully simulate and control.

Finally, this quote from Scott Aaronson sums up the quest for quantum computing. This would be justified by the desire to counter those who say it is impossible. The rest is the icing on the cake[2849]. This is obviously some humor, not to be taken at face value!

Figure 878: Source: A tale of quantum computers by Alexandru Gheorghiu (131 slides).

Science fiction

Science fiction and particularly movies and TV series have been great sources of inspiration and also of delirium about the potential of quantum technologies.

[2848] See Three principles of quantum computing by Yuri I. Ozhigov, Moscow State University of M.V. Lomonosov, June 2022 (10 pages) which tries to address this topic.

[2849] The quote comes from A tale of quantum computers by Alexandru Gheorghiu (131 slides, slide 31). The Combination Problem for Panpsychism by David Chalmers (37 pages) and Why Philosophers Should Care About Computational Complexity by Scott Aaronson (59 pages) ?

They have created an imaginary world made of teleportation (**Star Trek)**, supraluminal speed transportation (**Star Trek**, **Star Wars)**, various entanglements and miniaturization (as in **Ant Man**[2850]), states superposition (**Coherence)**, parallel or multiverse worlds (**Fringe**, **Spiderman**, **Counterpart**, **Dark**, **Doctor Strange in the Multiverse of Madness**) or time travel (**Interstellar**, **Umbrella Academy**).

Figure 879: quantum in science fiction movie and TV series.

In some cases, the quantum term is used without any scientific connection to quantum physics, as in the 2013 James Bond **Quantum of Solace,** which means approximately "an ounce of consolation".

Or it plays the role of the "MacGuffin", popularized by **Alfred Hitchcock,** the gizmo that the protagonists will look after from the beginning to the end of a movie without us really understanding what's inside or all about. This is the case of the **Ronin** movie. We find another one in the movie **Hard Kill** with Bruce Willis released in February 2020. Bad guys are trying to get the "code" that will activate a "quantum AI", but its contours are quite blurred. All we know is that it could eventually do some "good" things just like hacking an airliner to crash it. In short, it's a banal "dual" civil-military solution. The bullets will rain down until the bad guy is dead without us really knowing what it's all about.

However, a small 11-page guide tries to explain quantum physics to screenwriters[2851]! It contains some language basics that can be used to create scripts. The usual scriptwriters do not hesitate to twist things, like **Christopher Nolan** with his elastic vision of time arrows in Interstellar or Tenet.

In March 2020, the eight-episode TV mini-series **Devs** was the first to be built around the prowess of a quantum computer capable of reconstructing the past up to Christ's crucifixion and predicting the future anywhere on Earth. With a video! Of course, this doesn't make any sense with today's technologies, but also with those of tomorrow[2852].

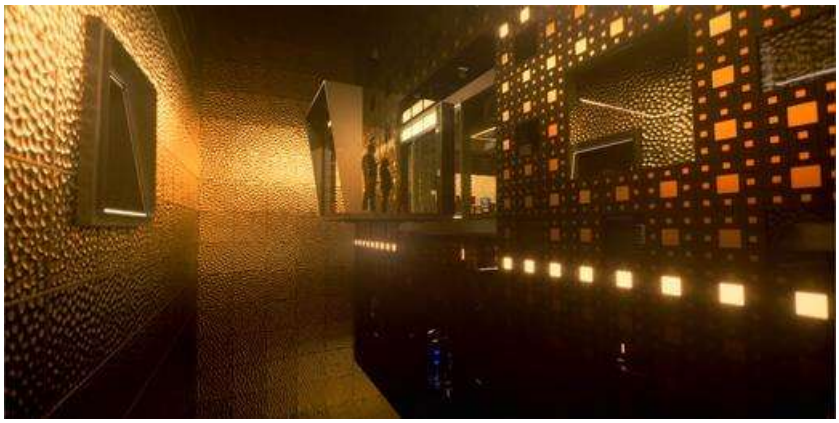


Figure 880: Dev's series quantum computer is sitting in a suspended huge cage.

[2850] See 'Ant-Man' science adviser explains the real-life physics behind the film by Denise Chow, July 2018, which explains the links between quantum physics and the scenario of the last Ant Man. Well, knowing that there is none to enlarge or miniaturize a character.

[2851] See The Sci-Fi Writer's Guide to Quantum Physics by Radha Pyari Sandhir, 2019 (11 pages).

[2852] The stylized quantum computer features an elongated candlestick that resembles those of IBM and Google quantum computers. It is not connected to anything at all from the top, but that's okay! The whole thing is enclosed in a huge cube that is suspended and magnetically isolated. See this beautiful analysis of the series: "Devs" by Alex Garland: a quantum thriller in Silicon Valley by Romane Mugnier in Usbek&Rica, May 2020.

It's a level of complexity problem and also about getting the training data. Even assuming that the Universe is totally deterministic, it is impossible to capture the precise position of all particles in space to determine their past and future. And this comes up against one of the key principles of quantum physics, Heisenberg's indeterminacy.

Figure 881: Dev's quantum computer is not well isolated…!

Its derivative states that one cannot accurately capture the position and velocity of an elementary particle. From this point on, everything falls into place to model and simulate the world with precision!

In 2015, episode 11 of season 2 of **Scorpions** featured a quantum computer made of lasers and a large plexiglass cube capable of injecting ransomware into the US Federal Bank with just 4 qubits! Quite a feat! The heroes hack the computer dressed as cosmonauts and by redirecting the beam of one of the lasers towards the luminous cube. We are far off from any realistic quantum computer here!

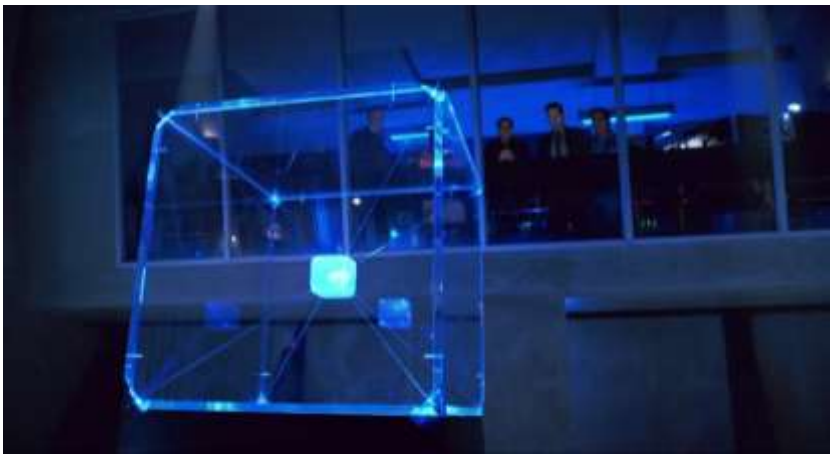


Figure 882: Scorpion's quantum computer could endanger banks with… 4 qubits!

Science-fiction is fine when it stays in the science-fiction realm. The problem starts when pseudo-researchers present science-fiction as if it was actual science instead of classifying it in a rough "hard science-fiction" category that is looking for some form of scientific credibility although being most of the time heavily farfetched. So, when some singularists tell you science and quantum physics could help resuscitate the dead using some fancy Dyson sphere and the likes, just forget it or just have some fun[2853].

These science-fiction dreams are far removed from the science of today and probably tomorrow. Their benefit is to create vocations. Dreaming drives innovation. Even when a young person discovers that science does not allow them to realize the scenarios of these fictions, they can discover the infinite field of applications of quantum physics and still be creative. If real-world quantum technologies are less impressive than Star Trek magic, it still can do wonders and bring new generation of researchers and innovators.

[2853] See A Dyson Sphere Could Bring Humans Back From the Dead, Researchers Say by Stav Dimitropoulos in Popular Mechanics, March 2021. Which refers to Classification of Approaches to Technological Resurrection by Alexey Turchin (Digital Immortality Now, Foundation Science for Life Extension) and Maxim Chernyakov (Russian Transhumanist Movement), not dated (39 pages). It suggests a Dyson sphere, some quantum algorithm based on a QRNG and some weird magic with an Everetian parallel universe could help resuscitate the dead. The science-fiction, not science at all. It also suggests quantum physics could help read data from the past, a bit a la Devs.

The use of quantum physics in Hollywood movies can also be used to convey other messages. As is often the case, they can agitate the potential of an external threat against which the USA should respond with strength. It would not be surprising to see fictions emerge in which the quantum threat comes from China. These movies often illustrate the myth of the hero who can get through adversity, also illustrating an alternative to the centralized powers of governments[2854].

In novels, fiction can also have pedagogical virtues. This is to some extent the case of **The Key of Solomon,** a novel by Portuguese author José Rodrigues Dos Santos published in 2015. In an affair mixing espionage and quantum computing, the hero spends his time teaching quantum physics to the other protagonists of the story. This gets the message across in a didactic way and without overly taxing science.

Quantum foundations

Philosophy is a process of critical reflection and questioning about the world, knowledge and human existence. It creates a connection between all these dimensions. The discovery of quantum physics at the beginning of the 20th century created a real philosophical shock wave through the upheavals it brought to our understanding of the world at the microscopic level[2855]. It called into question key notions such as the links between reality and observations, or between ontology and epistemology. And the debates are still raging about it. If you meet a group of quantum physicists and want to have some fun, ask them the simple question: “what is a quantum state” or “what does the wavefunction mean?”! They may not agree on a (simple) answer.

Quantum physics and its missing ontology

Science has always been closely linked to philosophy. It is not by chance that a doctorate is a "PhD", or Doctor of Philosophy, whether in humanities or in so-called hard or exact sciences.

The great physicists and mathematicians of the 19th and early 20th centuries were also philosophers, which is less common now, due to a process of accelerating specialization.

The creators of quantum physics were constantly questioning the impact and meaning of their discoveries. **Niels Bohr** was also both a physicist and a philosopher, influenced in particular by **Søren Kierkegaard** (1813-1855, Danish). **Erwin Schrödinger** was even more of a philosopher than a physicist. He had studied Western and Indian philosophy before creating the famous wave function that bears his name[2856]. An assistant to Niels Bohr, **Werner Heisenberg** had also invested a lot of his time in philosophy and it related well with his work around the mathematical modeling of quantum physics and the famous indeterminacy principle.

[2854] See Quantum Computing, Hollywood and geopolitics by Jean-Michel Valentin, March 2019. The author is a French specialist in strategic studies, sociology of defense and American strategy. The article relies heavily on the film Mortal Engines (2018), whose scenario only indirectly emphasizes quantum, with a past quantum war that ravaged the planet.

[2855] In practice, these upheavals occur mainly at the nanoscopic scale, that of atoms and their constituents, the nuclei and electrons. However, quantum effects can also be observed at the scale of large groups of particles that can be microscopic, as is the case with large molecules and their wave-particle duality, in Bose-Einstein condensates or superconducting currents. Knowing in all this that the frontier between quantum physics and classical physics has regularly evolved over the last century.

[2856] Michel Bitbol indicates that in the epilogue of "What is life? Mind and matter", Erwin Schrödinger wondered whether consciousness was singular or plural. If consciousness is only experienced in the singular, its extension to a global consciousness such as that of the Universe is only a risky extrapolation and difficult to prove experimentally. The thesis of a consciousness of the Universe is defended by some scientists. See for example Is the universe conscious? It seems impossible until you do the math by Michael Brooks, April 2020, which refers to the work of German mathematicians who try to define mathematically the notion of consciousness, allowing them to apply it then to the universe as a whole. Details are in The mathematical structure of integrated information theory by Johannes Kleiner and Sean Tull, 2020 (22 pages). It's cold and abstract!

The debates that agitated the physicists of quantum mechanics often took as much the form of philosophical jousting as of physical or mathematical debates, all the more so since the founders of quantum physics were not experimenters and were rather theoreticians[2857]. History has, moreover, forgot the names of the experimentalists[2858].

Quantum physics has generated endless debates since its beginnings because its formalism is difficult to associate with the principles of reality usually applicable in classical physics. Intuitive classical physics understanding has historically been associated with an ontology. In Newtonian physics, the notion of state with position and motion of an object and the laws of evolution of these properties allow the prediction of phenomena such as the motion of planets. These evolutions are perfectly observable and deterministic.

Figure 883: some books on quantum physics and philosophy.

Quantum physics was founded without such an ontology although it served to explain some known physical phenomenon like the blackbody radiation, the photoelectric effect or hydrogen's absorption and emission spectrum[2859].

It was created as a set mathematical postulates that could help predict experimental results. You have mainly the Schrödinger wavefunction for non-relativist massive particles and others like Dirac and Klein-Gordon equations for relativist particles. In quantum physics, the prediction instrument is a probabilistic wave function that is difficult to apprehend. It is coupled with a whole host of new notions that have no equivalent in the macroscopic and classical world: energy quantification, wave-particle duality which applies to matter (electrons, atoms) and photons (all have a momentum p related to a wavevector k using Planck's constant $\hbar$, as $p = \hbar k$), the influence of measurement on the quantities to be measured[2860], measurement indeterminacy and the notion of chance.

[2857] The book Fantaisies quantiques - dans les coulisses des grandes découvertes du xx^{e} siècle by Catherine d'Oultremont and Marina Solvay, 464 pages (2020) tells the story of the famous 1927 Solvay conference. It is a very beautiful history of quantum physics that tells touching stories of its various protagonists in the first half of the 20th century. It seems the book is not yet available in English.

[2858] We mentioned many of them at the beginning of this book, such as Johann Balmer, Theodore Lyman, Friedrich Paschen, James Chadwick, Arthur Holly Compton, George Paget Thomson, Clinton Davisson and Lester Germer. The names of these experimental physicists generally do not ring a bell to the general public and scientists, whereas the general public has heard much more about Max Planck (with his constant more than for the black body radiation explanation), Albert Einstein (for the theory of relativity more than for the photoelectric effect explanation), Niels Bohr (for his model of the atom), Erwin Schrödinger (more for his cat analogy than for his wave equation) and Werner Heisenberg (for his indeterminacy principle, commonly called uncertainty, but not much for this huge work on quantum physics mathematical foundations). Among the founding fathers, Paul Dirac, Wolfgang Pauli and John Von Neumann were geniuses but are way behind in notoriety.

[2859] An ontology deals with what is, types and structures of objects, properties, events, processes and relationships in all areas of reality. It is usually opposed to epistemology, which covers how to obtain valid knowledge.

[2860] This is not valid only in quantum physics and the infinitely small. It works regularly at the macro scale, as in any survey with biased questions for example.

Quantum physics is a predictive, not descriptive theory. It doesn't describe physically the electrons and other particles when they behave quantumly. It doesn't physically explain entanglement nor wave-particle duality.

Einstein's position was that quantum physics was an incomplete theory when creating his famous EPR paradox in 1935. Werner Heisenberg asserted in 1927 that quantum physics established the final failure of causality! The knowledge of the present no longer made it possible to predict the future from the application of the laws of physics, all the more so as the knowledge of the present with precision is also impossible[2861].

Some like Niels Bohr concluded that it was useless and even counterproductive to create some quantum physics ontology. Many attempts were contradicting each other or weren't even realist per se. Some like Hugh Everett believed that reality was a universal $|\Psi\rangle$ function, David Bohm devised some pilot waves explanations, Christopher Fuchs et al are focused on the role of agents actions and experiences in quantum Bayesianism and its derivative QBism, CSM's ontology argues that states pertain to systems and contexts, and so on. We end up having competing postulated ontologies frequently enabling the same predictions. These are hard to sort out.

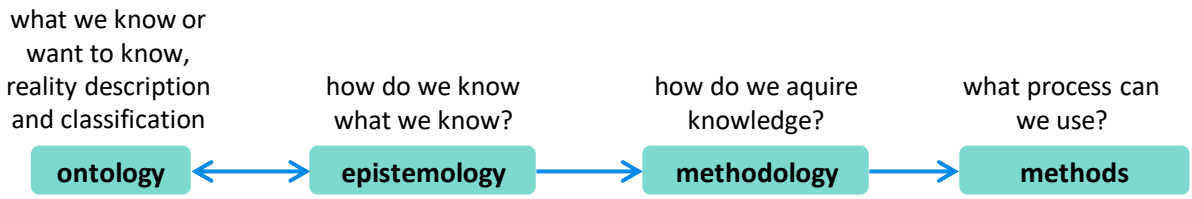


Figure 884: ontology, epistemology, methodology and methods defined.

The relationship between measured values, measurement and the observer is also debated. Would a true measurement be one that does not alter the quantity to be measured at all, a feat hard to attain in the infinitely small? In fact, quantum mechanics is contextual, the measurement depends on its context, which does not detract from its objectivity[2862].

The mathematical formalism of quantum physics from 1900 to 1935 was not at all disconnected from the observable physical world. It made it possible to explain experimentally studied phenomena such as black body radiation, interference from Young's slits with light and matter waves, or spectral excitation lines of atoms under a wide range of conditions. We have seen how important they are in photonics, with trapped ions, cold atoms or NV centers. Electron spin explained the hyperfine energy levels of atoms observed in 1922 in the Stern-Gerlach experiment[2863].

Relativistic quantum chemistry derived from Paul Dirac's equations explained spectral shifts of transitions involving low layer electrons of heavy atoms moving at relativistic velocities. The list is long.

If quantum physics explained experimental measurements, linking the observed reality and the theory, it was however insufficient to produce an unanimously accepted representation of reality. It is part of a history of science that described matter step by step, with nested Russian dolls. Atoms were initially abstract, theoretical entities before being embodied and accurately described and then directly observed as we do now with electron microscopes or cryogenic microscopy (Cryo-EM).

[2861] "*In the strong formulation of the causal law, 'If we know the present with exactitude, we can predict the future,' it is not the conclusion, but rather the premise that is false. We cannot know, as a matter of principle, the present in all its details.* " vu dans One Thing Is Certain: Heisenberg's Uncertainty Principle Is Not Dead by Ava Furuta in Scientific American, 2012.

[2862] This approach is challenged by the Bayesian quantum interpretation (QBism for Quantum Bayesianism) promoted from 2002 onwards by Carlton Caves, Christopher Fuchs, Rüdiger Schack and then David Mermin. See in particular QBism The Future of Quantum Physics by Hans Christian von Baeyer, 2016 (268 pages).

[2863] This one made a beam of heated silver atoms pass through a non-homogeneous magnetic field, which generated two distinct spots on a screen.

The very existence of atoms was debated at the end of the 19th century between Ludwig Boltzmann who believed in them and Wilhelm Ostwald and Ernst Mach who opposed them.

Protons and neutrons were then discovered. These were split into quarks and gluons with particle accelerators, turning the physical world into a maybe endless fractal. Obstacles to understanding it could simply be related to the enormous amount of energy that needs to be injected into particle accelerators, which is increasing the more elementary the particles are.

Quantum Physics interpretations

Quantum physics philosophy belongs to the broad field of **quantum foundations**. It focuses essentially on the multiple possible interpretations of the same theory and their mathematical formalism. They all ask related questions such as: does reality exist independently of the observer? What is the physical meaning of the wave in the wave-particle duality? Is it a real wave of an indeterminate nature or is it a simple statistical and probabilistic mathematical model incomplete in its ability to describe physical reality[2864]? Other quantum foundation fields include work on the measurement problem and its indeterminism, the associated notions of causality, local realism and the completeness of quantum mechanics[2865].

Many of these theories deal with the complicated notion of **contextuality** in quantum physics according to which quantum measurements is not revealing pre-existing values but depends on the measurement context like the angle of a spin measurement in the famous Stern-Gerlach experiment or of a photon polarization angle[2866]. Contextuality is dealt with in the **Kochen-Specker** theorem *aka* the Bell–Kochen–Specker theorem demonstrated by John S. Bell in 1966 and by Simon B. Kochen and Ernst Specker in 1967. It's a "no go theorem" that creates constraints on the types of putative hidden-variable theories trying to explain the predictions of quantum mechanics in a context-independent way.

Several interpretations of quantum physics have thus emerged to try to provide answers to these many questions.

[2864] These different interpretations can be evaluated according to the criteria of scientificity of Karl Popper (1902-1994, Austrian/English), according to which a theory is scientific if it can be refuted by crucial experiments giving precise results. The theory cannot be shown to be irrefutable. A proven scientific theory is therefore always between two waters, in the state of a theory corroborated by facts, until proven otherwise. The history of physics has shown, however, that the "serious" theories of the past were mainly challenged by the broadening of their perspective and context: with large masses and high velocities (for relativity) and in the microscopic (for quantum physics). In their initial contexts, they remained perfectly valid. I like the very current example of the search for dark matter, which would represent 85% of that of the Universe. Its existence is not yet experimentally demonstrated but is assumed by the application of the laws of gravity and relativity applied to the cohesion of galaxies. It can be refuted or partially verified at present in at least three ways: by discovering elementary particles associated with dark matter (quantum detectors are built in this sense, and have so far given nothing), by modifying the laws of general relativity as the Israeli Morchedai Milgrom is trying to do, or by discovering hidden matter such as the dust of galaxies that could explain all or part of their cohesion without using dark matter. Belief in God and many areas of metaphysics are not part of science because they are neither demonstrable nor refutable. See on this subject the interesting debate between André Comte-Sponville and Jean Staune in André Comte-Sponville - Jean Staune: Will science refute atheism?, June 2007, where some allusions are made to quantum physics.

[2865] See Argument for the incompleteness of quantum mechanics based on macroscopic and contextual realism: EPR and GHZ paradoxes with cat states by Jesse Fulton et al, August 2022 (20 pages). The hidden-variables debate is not closed yet!

[2866] Works on contextuality frequently deal with discrete variable quantum systems. It can be extended to continuous variable systems. See The Interplay between Quantum Contextuality and Wigner Negativity by Pierre-Emmanuel Emeriau, April 2022 (221 pages), a thesis under the direction of Elham Kashefi and Shane Mansfield and the related Continuous-variable nonlocality and contextuality by Rui Soares Barbosa, Tom Douce, Pierre-Emmanuel Emeriau, Elham Kashefi and Shane Mansfield, May 2019 - April 2022 (44 pages).

Copenhagen interpretation is the canonical version of quantum foundations[2867]. It is essentially probabilistic. Quantum physics postulates and the wave function describe all that we can know about reality but not reality itself, which is neither accessible nor meaningful. It adopts the positivist approach according to which one sticks to observations, laws and phenomena, without seeking to know their intrinsic nature. It was the "Bohrian" side of the historical debate between **Niels Bohr** and Albert Einstein, mainly between 1927 (in the famous Solvay Conference in Brussels) and 1935 (the EPR paradox paper and subsequent discussions). Adopted by Werner Heisenberg, Max Born, Wolfgang Pauli, Paul Dirac, it is the classical and dominant interpretation of quantum physics that is still mostly taught like in the Cohen-Tannoudji/Laloe/Diu bible of quantum physics. It is satisfied with an essentially mathematical and probabilistic model that does not seek to physically describe the entire real world. There are, moreover, sub-branches in the Copenhagen interpretation, notably around the open and closed theories that had opposed Heisenberg and Dirac from 1929 onwards.

Bohm interpretation came from **David Bohm** (1917-1992, American then Brazilian and British). He proposed in 1952 a so-called deterministic version of quantum mechanics, called "De Broglie-Bohm theory". It was inspired by ideas initially promoted - but partly abandoned - by the French physicist and took up the idea of the existence of hidden variables, insinuated by Albert Einstein in the 1930s, and by Louis de Broglie, in the form of pilot waves[2868]. The existence of local hidden variables was disproved in 1982 with Alain Aspect's famous experiment. But the promoters of the therefore explicitly nonlocal Bohmian theory are still very active, including in France[2869].

Many worlds interpretation and its Universe wave function was proposed in 1957 by **Hugh Everett** (1930-1982, American) and after being almost forgotten, revived by **Bryce DeWitt** in 1970. It then became the multiple worlds or multiverse interpretation in an article published in Physics Today[2870]. It is said to be realistic in the sense that the Universe is a huge wave function with a (immensely) large number of parameters. It never collapses and the world is deterministic, but split in parallel branches. DeWitt's interpretation transforms quantum probabilities within this universal wave function into parallel worlds that exist simultaneously. Since it is impossible to verify that parallel worlds exist, the theory is not refutable. It's the case with all interpretations based on the same formalism. We are therefore far from an experimentally supportable interpretation[2871]. This theory has also been promoted by David Deutsch, also known for his quantum algorithms.

[2867] The "Copenhague interpretation" naming was created by Werner Heisenberg in 1955. It consolidated Heisenberg's and others contemporary views on the realism of quantum physics and concepts that were not promoted by Niels Bohr in the 1920s like the wave packet collapse and the views on the subjective observer in quantum measurement. It's a post-mortem consolidation on the quantum physics foundations. See Who Invented the "Copenhagen Interpretation"? A Study in Mythology by Don Howard, Department of Philosophy of University of Notre Dame, Indiana, 2004 (15 pages).

[2868] The Bohmian approach is well popularized in Quantum Physics Without Quantum Philosophy by Detlef Dürr, Sheldon Goldstein and Nino Zanghì, 2013 (304 pages). It is completed by Quantum solitodynamics: Non-linear wave mechanics and pilot-wave theory by Aurélien Drezet, July 2022 (29 pages).

[2869] With Aurélien Drezet from Institut Néel, Grenoble.

[2870] See Quantum mechanics and reality by Bryce S. DeWitt, 1970 (6 pages) as well as The Many-Worlds Interpretation of Quantum Mechanics by Bryce DeWitt and Neill Graham, 1973 (146 pages) which contains "The theory of the universal wave function" by Hugh Everett, 1957. DeWitt's interpretation is also called EWG for Everett-Wheeler-Graham. John Wheeler was supervisor of High Everett's thesis and Neill Graham, a student of DeWitt. Seen in Everett's pure wave mechanics and the notion of worlds by Jeffrey A. Barrett, 2011 (27 pages).

[2871] See Making Sense of the Many Worlds Interpretation by Stephen Boughn, 2018 (36 pages) which dismantles a bit the model of parallel universes, especially in terms of dimensioning. By calculating the number of bifurcations of the Universe since its birth, and taking Planck's time as a basis, we end up with a number of parallel worlds that is beyond comprehension and all imaginable analogies. As for Schrödinger's cat, the dead cat and the living cat cohabit in two parallel worlds and the matter is settled!

It feeds a many science fiction drams and mad mysticism, everything being linked to everything and vice versa, especially souls and consciences. Howard Wiseman extended this theory with embedding interactions between these many worlds[2872].

	Copenhagen	Bohm	Everett / DeWitt
world entities	macroscopic quantum objects	wave function and particles position	wave function with quasi-classical world
determinism	indeterminism	determinist	deterministic
probabilities interpretation	objective	epistemic	objective
theories predictions goal	measurement results	particles position	agents bet
locality	non-locality	non-locality	locale
theory mathematical formalism	Schrödinger equation, projections, probabilities	Schrödinger equation and pilot waves	Schrödinger equation

Figure 885: the top three interpretations of quantum physics. Source: the excellent thesis The plurality of interpretations of a scientific theory: the case of quantum mechanics by Thomas Boyer-Kassem, 2011 (289 pages).

GRW theory published in 1986 by the Ghirardi-Rimini-Weber trio proposes a different formulation of Schrödinger's equation with a spontaneous reduction of the wave function that is not simply related to the notion of measurement. This is a rare formalism that could experimentally validated.

QBism is a derivative from quantum Bayesianism, starting with some ideas by **Edwin Jaynes** (1922-1998, American, yes, the Jaynes from the Jaynes-Cummings Hamiltonian) and pushed by **Christopher Fuchs**, **David Mermin** et al, based on **Frank Ramsey**'s anti-realist interpretation of probability (1903-1930, British philosopher) and **Ludwig Wittgenstein**'s work (1889-1951, Austrian philosopher)[2873]. It interprets quantum physics through the eye of the observer agent actions and experiences.

Relational Quantum Mechanics (RQM) was crafted by **Carlo Rovelli** in 1994. This relational ontology considers that a quantum state is defined by the relation between any pairs of systems. One of them can be an observer. It is inspired by special relativity principles and its observer reference model.

CSM ontology was proposed in 2015 by **Alexia Auffèves** and **Philippe Grangier** in order to reconcile the Copenhagen interpretation with realistic models[2874]. CSM is a minimalist ontology designed to pacify somewhat these old debates.

[2872] See Quantum Phenomena Modeled by Interactions between Many Classical Worlds by Michael J. W. Hall, Dirk-André Deckert and Howard M. Wiseman, PRX, 2014 (17 pages).

[2873] See Quantum Wittgenstein - Metaphysical debates in quantum physics don't get at 'truth' – they're nothing but a form of ritual, activity and culture by Timothy Andersen, Aeon, May 2022.

[2874] CSM results from the creation with Nayla Farouki of the CEA of a group dedicated to the foundations of quantum mechanics in Grenoble. In 2013, they form a group with Philippe Grangier, who has long defended contextual objectivity. CSM is documented in several papers: Contexts, Systems and Modalities: a new ontology for quantum mechanics, January 2015 (9 pages) lays out the key principles of CSM ontology, tying physical properties to the system, and to the context in which it is embedded. Violation of Bell's inequalities in a quantum realistic framework, International Journal of Quantum Information, February 2016 (5 pages) reuses a lot of content from the first paper, commenting on observed "loophole free" violation of Bell's inequalities. Recovering the quantum formalism from physically realist axioms, Nature, December 2016 (8 pages) derives Born's probabilistic rule and unitary transforms from CSM. Then What is quantum in quantum randomness?, Philosophical Transactions of the Royal Society A, April 2018 (9 pages), Extracontextuality and Extravalence in Quantum Mechanics, Philosophical Transactions of the Royal Society A, May 2018 (7 pages), A generic model for quantum measurements, July 2019 (8 pages) and Deriving Born's rule from an Inference to the Best Explanation, October 2019 (6 pages). See one critic of CSM in Comments on New Ontology of Quantum Mechanics called CSM by Marian Kupczynski, 2016 (8 pages). And the more recent Contextual objectivity : a realistic interpretation of quantum mechanics by Philippe Grangier, 2001 (5 pages).

In this model, the properties that are measured, called **modalities,** are attributed to a **system** (studied system, as isolated as possible) within a **context** (completely specified measurement device like a photon polarizer or Stern-Gerlach experiment) Modalities are jointly associated to the system and its context, not just the system, building a contextual objectivity[2875]. In CSM, randomness doesn't just come from Heisenberg's indeterminacy principle but is a direct consequence of the quantization postulate and the contextual nature of reality.

CSM can also help explain the origin of probabilities, non-locality and quantum-classical boundary. Non-locality, aka the EPR paradox, has nothing to do with an action at a distance, but appears because a modality belongs to both a system and a context. It also solves the Wigner's friend thought experiment paradox based on a recursive observer of a measurement agent[2876].

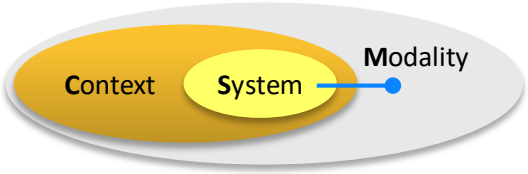


Figure 886: CSM's simple view.

There are many more interpretations of quantum physics than qubit types around! Like **superdeterminism** (which deterministically the observed violations of Bell's inequalities in entanglement experiments with some yet unknown hidden variable[2877]), **consistent histories** (which avoid the use of a wavefunction collapse to describe physical processes and tries to get rid of the measurement theory[2878]), **modal interpretation** (class of interpretations created starting in 1972 by Bas van Fraassen which introduced a distinction between a dynamical state over time and a value state at a given time[2879]), **quantum darwinism** (which explains how the classical world emerges from the quantum world [2880]), **dynamic histories** (which reinterprets quantum mechanics as deterministically evolving dynamical world lines in a 5D universe not far from a many-worlds interpretation[2881]), **Quantum Coherentism** from Claudio Calosi and Matteo Morganti, **Foundationalism** (there must be a source of being), the **Geometrodynamic Model of Reality** from Shlomo Barak and the **Quantum Conceptual Turn** from Diederik Aerts and Massimiliano Sassoli de Bianchi[2882] and the **category theory** of Gennaro Auletta, a sort of generic unifying meta-logic theory applicable to quantum physics[2883].

[2875] Within the usual quantum formalism, a modality is a pure quantum state and a context is a complete set of commuting observables (CSCO). For a given context, CSM defines N distinguishable modalities that are mutually exclusive. If one modality is "true", or "realized", the others are "wrong" (or "false"), or "not realized". The value of N, called the dimension, is a characteristic property of a given quantum system, and is the same regardless of the context.

[2876] The Wigner's friend paradox is driving hot debates among physicists in quantum foundations. See for example A general framework for consistent logical reasoning in Wigner's friend scenarios: subjective perspectives of agents within a single quantum circuit by V. Vilasini and Misha P. Woods, ETH Zurich, September 2022 (47 pages).

[2877] See Rethinking Superdeterminism by Sabine Hossenfelder and Tim Palmer, May 2020 (13 pages) and What does it take to solve the measurement problem? by Jonte R. Hance and Sabine Hossenfelder, June 2022 (11 pages).

[2878] See Consistent histories and the interpretation of quantum mechanics by Robert B. Griffiths, Journal of Statistical Physics, 1984 (55 pages).

[2879] See The scientific image by Bas Van Fraassen, 1980 (248 pages) and Modal Interpretations of Quantum Mechanics, Stanford Encyclopedia of Philosophy.

[2880] Also see Quantum Darwinism, Decoherence, and the Randomness of Quantum Jumps by Wojciech Zurek, 2014 (8 pages).

[2881] See A Dynamic Histories Interpretation of Quantum Theory by Timothy D. Andersen, August 2020 (13 pages).

[2882] See Diederik Aerts and Massimiliano Sassoli de Bianchi - The quantum conceptual turn, May 2021 (48 mn) from the International Workshop on Quantum Mechanics and Quantum Information, Quantum Ontology and Metaphysics, April 2021. See also Are Words the Quanta of Human Language? Extending the Domain of Quantum Cognition by Diederik Aerts and Lester Beltran, December 2021 (27 pages) which makes a symbolic projection from quantum physics phenomena to the way human language works.

[2883] The category theory is described at the end of The Quantum Mechanics Conundrum by Gennaro Auletta, 2019 (879 pages) which contains a good primer on quantum physics in its first 150 pages.

Other ontologies abound like **Structuralism**, **Perspectival Objectivity**[2884], **Pluralism** (atomism), **Monism** and **Infinitism**, but their scope goes beyond quantum physics.

Where are the schools of quantum foundations? In Europe, there is a quantum foundations epicenter in Italy but you find contributors in most countries. There are also two foundations who provide research grants on quantum foundations: the **Templeton Foundation** and **FQXi** (Foundational Questions Institute) which covers quantum foundations and cosmology and was created in 2005 by cosmologists Max Tegmark and Anthony Aguirre.

Other interpretations

Among the physicists who have contributed to the field of quantum physics philosophy. **Pascual Jordan** (1902-1980, German) built a theory of free will according to which one is not freer by acting randomly or in a determined way, breaking the idea that quantum non-determinism would be a proof of human free will. **Henri Stapp** (1928, American) worked on consciousness and believes that it governs the world and reality and that it can only be explained by quantum physics[2885].

Roger Penrose (1931, English) considers that consciousness results from the reduction of the wave packet and **Elizabeth Rauscher** (1931-2019, American) was a physicist who first became interested in philosophy and then moved on to parapsychology[2886].

On the other hand, **Steven Weinberg** (1933-2021, American), Nobel Prize in Physics in 1979 for his work on the unification of the weak and electromagnetic forces, thought that philosophy is of little use in quantum physics other than to protect us against the errors of other philosophers[2887]. This view was shared by **Stephen Hawking** (1942-2018, English).

In France, in addition to the CSM ontology creators, **Michel Bitbol**, a biophysicist and philosopher of science, is interested in particular in the question of consciousness, **Etienne Klein,** originally an engineer and physicist, is specialized in the philosophy of science at the CEA, as well as **Alexei Grinbaum** and **Vincent Bontemps** who are both part of Etienne Klein's LARSIM laboratory.

Quantum physics raises other physico-philosophical questions such as does a total vacuum exist? Indeed, quantum physics describes the energy of the vacuum, which would always be crossed by various real and virtual particles. From a practical point of view, it is therefore difficult to create an empty space that is not crossed at all by electromagnetic waves or particles of all kinds. If therefore nothing exists, what was there before the big bang? And let's not talk about the nature of time, which is still a matter of debate.

[2884] See Perspectival Objectivity or: How I Learned to Stop Worrying and Love Observer-Dependent Reality by Peter W. Evans, University of Queensland, 2020 (16 pages).

[2885] See Mind, Matter and Quantum Mechanics by Henry P. Stapp, 2009 (303 pages). This is the kind of book that makes non-testable hypotheses that then become gospel for the quantum medicine quacks we are talking about in the dense section dedicated to quantum fumbling. And yet, the basic idea is nothing extraordinary: brain chemistry, like all chemistry, is based on many facets of quantum physics. This becomes complicated when the hypothesis is put forward of an implementation of entanglement in consciousness. Quantum medicine goes out of the scientific game when it claims that these mechanisms can be controlled from the simple will, without counting the action on the other organs (preferably sick ones) of the human body.

[2886] Elizabeth Rauscher was the cofounder of the Fundamental Fysiks Group in 1975 with George Weissmann to work on quantum foundations. She is co-author with Richard Amoroso of The Holographic Anthropic Universe, 2009 (510 pages). They discuss a model for creating a scalable quantum computer called "Universal Quantum Computing" that is difficult to grasp between real science and crackpot science and is based on a theory called "Unified Field Mechanics" that is difficult to evaluate. The subject is detailed in Brief Primer on the Fundaments of Quantum Computing by Richard L Amoroso, 2017 (140 pages). Richard Amoroso is Director of the Noetic Advanced Studies Institute in Oakland, California. Noetics is interested in the links between quantum states and consciousness. And this goes well beyond the realm of science with Pragmatic Proof of God (Part I & Part II, 2017 by Richard L. Amoroso (34 and 13 pages).

[2887] See the chapter "Against Philosophy" in "Dreams of a Final Theory", 1994, Steven Weinberg, which is contradicted in Physics Needs Philosophy / Philosophy Needs Physics by Carlo Rovelli, 2018. Carlo asserts that saying that science does not need philosophy is to be doing some sort of philosophy of science! See also The Trouble with Quantum Mechanics, 2016.

Beyond Quantum Foundations

The current philosophical approach to quantum physics baffled me a bit. Most of the writings in this discipline are full of mathematics and physics. They must break records in this respect compared to any other subject covered by the field of philosophy. Above all, they do not deal much with human sciences per se.

What are the human consequences of these different interpretations of quantum physics? Are there philosophical questions other than these related to the interpretation of realism at low-level? There is much to be done in this area. The notions of uncertainty and indeterminism inevitably lead to the notion of free will and destiny (as seen by Pascual Jordan). The quantum philosophical focus on the microscopic and nanoscopic scale of physics could also be a form of reductionism preventing a wide-angle view of its societal impact.

Also, is the extension of the scientific field infinite? What are the limits of human knowledge that seeks to explain and interpret everything about the way the Universe works? What do we miss and why? What links can be made with our humility? What are the structural limits to our insatiable curiosity? I am only reformulating the very notion of Kantian metaphysics, the "*science of the limits of human reason*".

The philosophical question thus concerns the notion of the feasible and the unfeasible and its evolution over time, a perspective provided by the history and philosophy of science. What are the limits of human ingenuity? What is superhuman? Will we be able to create ultra-reliable and *scalable* quantum computers? The theories and classes of complexity, discussed in this book, should also serve as tools for this kind of thinking.

How to extend the interpretation of quantum physics to the metaphor of quantum computation: highly rich and complex inside but simple after measurement is done? Could it be used to simulate the living and create it in silico? This will then raise questions about man's power over nature and the associated responsibilities. We will also see the resurgence of debates on scientism, the "*science-led society*", as well as on technology solutionism, a concept promoted by **Evgeny Morozov**, which could provide answers to all problems, especially environmental and health problems, which cannot be treated properly with the required urgency.

These questions arise more and more at a time when precaution prevails over everything, when there are fears of technological blunders in almost every field (nuclear, GMOs, fertilizers, vaccines, artificial intelligence and 5G), when the very notion of scientific progress is no longer accepted and when cognitive relativism no longer allows us to distinguish between the serious and the farfetched, leading to a collective mistrust in science. In the following section, we will precisely study a question that belongs to the field of philosophy, the question of the ethics of quantum computing.

Are these questions really specific to physics and quantum computing? Aren't they recurrent as soon as a major new technology shows up? Perhaps, but these questions deserve to be asked, like those raised by the commoditization of artificial intelligence since 2012.

The interpretations of quantum physics are in any case there to remind us that in all matters, we must multiply the angles of view of problems to better analyze them. This is obviously full of lessons from a metaphorical point of view.

I wonder about all these questions by observing that, if they are not dealt with, they tend to become the field of esotericism and charlatanism as we will see in a following section dedicated to quantum fake sciences. It is a bit as if the philosophy of quantum physics had remained at the stage of fundamental research without moving on to the stage of applied research. In a way, it is in line with the level of market maturity of the technologies of the second quantum revolution. Let's bet that as quantum technologies will mature, the more this applied philosophy will develop and allow us to write a new chapter in this exciting history of science.

Responsible quantum innovation

We'll cover here the broad topic of responsible innovation and ethics pertaining to quantum technologies. We'll drive some lessons from the current quantum hype and also from what happened with artificial intelligence. We'll look at the various initiatives around the world.

Quantum hype side effects

The "quantum hype" has been perceived as being problematic for a while, mostly by many scientists who fell that the field was oversold, particularly by industry vendors of all sizes[2888]. It's hard to position the peak oil of the quantum hype ("Quipe" for some authors[2889]) but at least, with following the money invested in startups, 2021-2022 were defining years with the large funding rounds of startups like PsiQuantum and the initial public offerings (IPOs) through SPACs (special purpose acquisition companies) of IonQ, Arqit, Rigetti and D-Wave. Governments have been fueling this hype with their large national(istic) quantum initiatives and their aspirations for some technology sovereignty.

While technology hypes have always existed and contribute to drive emulation, innovations and a field attractiveness, it works well when scientists and vendors deliver progress and innovation on a continuous basis after a so-called peak of expectations. It fails with exaggerated overpromises and underdeliveries that last too long. In that case, it could cut short research and innovation funding, creating some sort of quantum winter[2890].

In the "Mitigating the quantum hype" paper published in January 2022[2891], I drove some lessons from past technology hypes and investigated the current quantum hype and its specifics. I laid out the structural changes happening like the vendors hype profound and disruptive impact on the organization of fundamental research. I then made some proposals to mitigate the potential negative effects of the current quantum hype including recommendations on scientific communication to strengthen the trust in quantum science, vendor behavior improvements, benchmarking methodologies, public education and putting in place a responsible research and innovation approach.

Learnings from AI

Artificial intelligence ethical concerns became a real political issue in 2018. This was very apparent in France in the **Villani Mission Report on Artificial Intelligence published in** March 2018 as well as in a **Report of the House of Lords** published the same month and on the same subject in the UK[2892].

It highlighted the need to ensure, at least morally, but, if possible, practically, that AI-based solutions respect society and avoid generating or perpetuating training data-originated discriminations. Hence two salient topics such as the explicability of algorithms and the limits of the manipulation of our emotions, particularly via more or less humanoid robots and voice agents.

[2888] See Quantum computer researcher warns that the industry is full of ridiculous hype by John Christian, Futurism, March 2022, Quantum Computing Hype is Bad for Science by Victor Galitski, Maryland University, July 2021 and the quite exaggerated view from Nikita Gourianov from Oxford University, as described in Oxford scientist says greedy physicists have overhyped quantum computing by Tristan Greene, TheNextWeb, August 2022 and with a response in Separating quantum hype from quantum reality - Are the sceptics too sceptical? By Simon Benjamin, Financial Times, September 2022. See also Disentangling the Facts From the Hype of Quantum Computing by James Clarke, Intel, IEEE Spectrum, September 2022.

[2889] See Hope and Hype in Quantum Computing by Philip Nikolayev and Susmit Panda, Quantum Poet, June 2022.

[2890] See What if Quantum Computing Is a Bust? by Chris Jay Hoofnagle and Simson Garfinkel, January 2022.

[2891] See Mitigating the quantum hype by Olivier Ezratty, February 2022 (26 pages).

[2892] See AI in the UK: ready, willing and able?, March 2018 (183 pages).

The difficulty to explain how deep learning algorithms work has been exaggerated. If it is true that multilayer neural networks are somewhat abstract. But it is equally abstract for almost any software, with or without AI, that can affect our daily lives. But we've forgotten that a little. When a software from the Visa group rejects your credit card payment abroad, we almost never get an explanation of the whys and hows it was rejected and how to avoid it. Bayesian fraud and machine learning based detection techniques are not explained to consumers.

Ethical quantum

Quantum computation is likely to amplify this quest for explicability. It is even less obvious to satisfy with quantum algorithms, which follow a logic that few developers can grasp. Quantum algorithms are likely to be even more complicated and less understandable than those of today's AI. This is amplified since we cannot observe their inner working and intermediate quantum states. Only the "classical" result is measured at the end of the operations. Moreover, from about fifty qubits, it becomes impossible to emulate a quantum algorithm on a classical computer.

Their possible biases will not necessarily come from the data that feeds them because, for a certain period of time, quantum computers will probably not exploit large volumes of data. We can therefore speak literally of the term algorithm bias, whereas when we talk about AI, we are dealing more with training data bias rather than algorithms bias.

But this will be judged on a case-by-case basis. Depending on whether the applications of quantum computing optimize automobile traffic, manage energy distribution, optimize financial portfolios of the wealthy, create new molecules in chemistry or biology or help the NSA break the codes of private communications, the stakes will not be the same[2893].

Ethical questions related to quantum technologies will undoubtedly emerge. They will be associated with a whole range of applications of quantum computing: the simulation of the dynamics of organic molecules. It will probably be limited at the beginning to the simulation of relatively simple molecules. The simulation of complex proteins folding is a hypothesis that has not yet been validated. In a distant hypothetical future, we may be able to simulate larger biological ensembles.

When this is simulated and then altered, for example to create new therapies, the rejection of GMOs or vaccines will seem like distant memory. New fears will show up and scientists will have to get involved to prevent them from spreading. These irrational fears will emerge because of exaggerations about the capabilities of quantum computers. We already hear about "quantum robots", which means nothing, but can impress and drive wild thoughts.

The example below in Figure 887 is eloquent from this point of view with two titles in 2014 when quantum computing was nearly just about D-Wave and which, in practice, are only relaying a rather banal scientific publication, Quantum speedup for active learning agents (15 pages) describing quantum algorithms for the execution of agent networks used in robotics bringing a so-called "quadratic" performance gain, therefore... not exponential, therefore, not extraordinary[2894].

Each time, we will have to decode and take a step back. In 2022 emerged a proposal to quantumly link the brain with a quantum computer[2895].Not only is it really farfetch but it’s probably not a good idea to create trust with quantum computing to elaborate such crazy scenarios.

[2893] This is the point raised by Emma McKay in Should We Build Quantum Computers at All? A Q&A with Emma McKay, quantum physicist turned quantum skeptic by Sophia Chen, APS News, August 2022.

[2894] See Article 1 and Article 2.

[2895] See An approach to interfacing the brain with quantum computers: practical steps and caveats by Eduardo Reck Miranda, Enrique Solano et al, January 2022 (6 pages).

Figure 887: the fuss about quantum robotics… in 2014! When science fiction is mixed with science, things get confusing.

We have enough of it with Neuralink, the Elon Musk startup that works on neural implants that would supposedly be connected to some AI to augment the brain capacities, when it is more relevant for treating some neurodiseases like Parkinson's.

A good approach for the quantum scientific community would be to pre-empt these fears by analyzing them as early as possible and defusing them if possible, so as not to be in a situation that would block scientific progress and innovation useful to society because of these irrational fears[2896]. Also, good examples can be given with researchers who admit having published scientific erroneous papers[2897].

Various initiatives started to pop-up in 2021 around quantum ethics in Australia, the UK, the Netherlands, Canada and the USA. It's following a similar pattern than with artificial intelligence but earlier given the maturity of the sector. So far, contrarily to what's happening in the AI field, it has not yet been hijacked by large industry vendors or even regulators. Most initiatives were born out of the research community.

Still, there are already some similarities and overlaps between the AI and quantum ethics frameworks that are showing up.

On the AI side, many AI charters have been published since 2018. One of these comes from the **GPAI** (Global Partnership on AI[2898]) launched by 15 countries in June 2020 including France and Canada. Its goal is to foster the development of responsible and inclusive IAs based on human rights, favoring diversity, while driving innovation and economic growth. The GPAI did set up experts run working groups on responsible AI, data governance, the future of work and at last, on innovation.

OECD launched its **AI Policy Observatory** (OECD.AI) in February 2020, an online platform consolidating information to help states craft their public AI policies. OECD defined its own AI principles (OECD AI Principles) that were adopted by 42 countries in May 2019. Also in 2020, the **AI Rome Call for AI ethics** gathered the Vatican, Microsoft, IBM and others to whitewash about the same goals as GPAI.

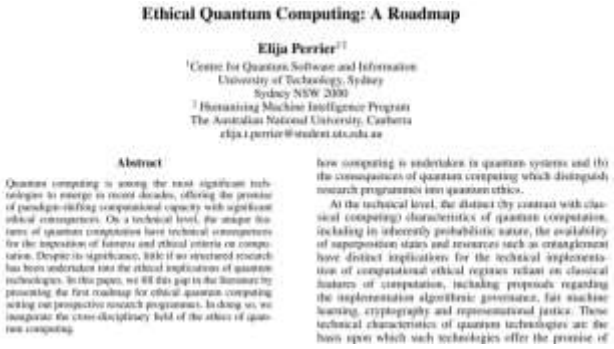
[2896] See Ethics education in the quantum information science classroom: Exploring attitudes, barriers, and opportunities by Josephine Meyer, Noah Finkelstein and Bethany Wilcox, University of Boulder, Colorado, February 2022 (15 pages) where the authors argue that quantum ethics and social responsibility should be incorporated in quantum information science education from the beginning.

[2897] See one good example with On a gap in the proof of the generalised quantum Stein's lemma and its consequences for the reversibility of quantum resources by Mario Berta, Fernando G. S. L. Brandão et al, May 2022 (22 pages) which shows that an initial proof from one of the authors was incorrect. An author who works at Amazon!

[2898] With Canada, Germany, Australia, South Korea, USA, Italy, India, Japan, Mexico, New-Zealand, UK, Singapore, Slovenia and the European Union.

And these are just a couple initiatives among many others, frequently driven by industry vendors who are lobbying for self-regulation instead of tight government-based regulations.

In the quantum space, **Australia** was the first country that launched a quantum ethics initiative. Early on, in 2019, **CSIRO**, the Australian scientific research agency, mentioned the need to explore and address any unknown ethical, social or environmental risks that may arise with the next generation of quantum technologies[2899]. It was followed in 2021 by a white paper published by Elija Perrier from the Centre for Quantum Software and Information at the Sydney University of Technology[2900].



Ethical Quantum Computing: A Roadmap

Elija Perrier[1]

[1]Centre for Quantum Software and Information
University of Technology, Sydney
Sydney NSW 2000
[2] Humanising Machine Intelligence Program
The Australian National University, Canberra
elija.t.perrier@student.uts.edu.au

Abstract

Quantum computing is among the most significant technologies to emerge in recent decades, offering the promise of paradigm-shifting computational capacity with significant ethical consequences. On a technical level, the unique features of quantum computation have technical consequences for the imposition of fairness and ethical criteria on computation. Despite its significance, little if no structured research has been undertaken into the ethical implications of quantum technologies. In this paper, we fill this gap in the literature by presenting the first roadmap for ethical quantum computing setting out prospective research programmes. In doing so, we inaugurate the cross-disciplinary field of the ethics of quantum computing.

how computing is undertaken in quantum systems and (b) the consequences of quantum computing which distinguish research programmes into quantum ethics.

At the technical level, the distinct (by contrast with classical computing) characteristics of quantum computation, including its inherently probabilistic nature, the availability of superposition states and resources such as entanglement have distinct implications for the technical implementation of computational ethical regimes reliant on classical features of computation, including proposals regarding the implementation algorithmic governance, fair machine learning, cryptography and representational justice. These technical characteristics of quantum technologies are the basis upon which such technologies offer the promise of

Figure 888: Source: Ethical Quantum Computing: A Roadmap by Elija Perrier, February 2021-April 2022 (40 pages).

It was spun out of the Association for the Advancement of Artificial Intelligence (www.aaai.org). The paper starts with defining the quantum physics postulates[2901], then cover ethical quantum computation and asks many ethical related questions that could be asked for any kind of classical computing. They mention the complicated question of quantum algorithms auditing. Quantum algorithms indeed may become black box similarly to deep learning, leading to some explainability issues. So, on top of the various XAI (explainable AI) initiatives like the one launched by DARPA in the USA, will we see emerging the field of XQC for Explainable Quantum Computing?

It also mentions the need for some Quantum Fair Machine Learning (QFML). It may not be such of a problem since QML may not be used to process huge volumes of personal data due to quantum computing limitations in data loading techniques, which may last for a long time. They even go as far as asking whether quantum interferences implemented in quantum algorithms are ethical in nature. They also cover privacy and cryptography matters. Is Shor going to kill our private life? How could some differential privacy be implemented with quantum computing[2902]? Other topics involve distributional ethics and fair distribution which are classical economical questions arising with any new technology. At last, they wonder about the impact of quantum simulations and whether it could be implemented to simulate people's personal behavior.

The paper seems highly influenced by the works on ethical AI and sometimes mixes science-fiction with real state of the art understanding of what can and will be done with quantum computing. But it asks good questions. Another Australian paper focused more recently on the need to involve all stakeholders, beyond the classical market awareness creation[2903].

In the **UK**, ethical quantum computing became a topic promoted by the media The Quantum Insider starting in December 2020. They released a short video documentary trying to explain what quantum computing is and the related ethical issues involved with researchers like John Martinis and

---

[2899] See Growing Australia's Quantum Technology Industry, CSIRO, 2019 and The 'second quantum revolution' is almost here. We need to make sure it benefits the many, not the few by Tara Robertson, June 2021.

[2900] See Ethical Quantum Computing: A Roadmap by Elija Perrier, Centre for Quantum Software and Information, Sydney University of Technology, February 2021-April 2022 (40 pages).

[2901] They define only the first 4 quantum physics postulates and not the whole 6, and their fourth postulate doesn't correspond to the canonical Born rule related principle.

[2902] See Quantum Differential Privacy: An Information Theory Perspective by Christoph Hirche et al, February 2022 (26 pages).

[2903] See Talking about responsible quantum: Awareness is the absolute minimum... that we need to do by Tara Roberson, December 2021-September 2022 (15 pages).

entrepreneurs like Ilana Wisby[2904]. They are highlighting the need for democratizing quantum technology skills, mention the risks on privacy and security and the need to address quantum AI bias. They also pinpoint the "Hype-Fear-Disappointment Cycle" and recommend to set realistic expectations to avoid triggering fears and biases. Researchers from Oxford University are also studying responsible innovation in quantum technologies[2905].

Other ethical issues to be addressed cover the potential harmful manipulation of the human genome fears, the (positive) quantum use cases to find environmental solutions and the energetic footprint of quantum computing.

In **The Netherlands**, the government 615M€ initiative launched in April 2021 includes a 20M€ plan on quantum ethics and societal impact research run out of the Living Lab Quantum and Society spun out of Quantum Delta NL, the foundation established to run the Netherlands quantum program. They also create ethical, legal and societal standards for quantum technologies and their applications.

The **World Economic Forum** launched its Quantum Computing Governance initiative in February 2021[2906]. It wants to standardize an ethical framework enabling the responsible design and adoption of quantum computing. They ask the ever-lasting question: will the public trust technologies which they cannot understand and whose results they cannot verify as if they could do it with existing digital technologies. They advocate the use of preemptive involvement in technology design to make sure ethical issues are addressed as early as possible. With that, they are assembling a "*global multistakeholder community of experts from across public sector, private sector, academia and civil society to formulate principles and create a broader ethical framework for responsible and purpose-driven design and adoption of quantum computing technologies to drive positive outcomes for society*". They will frame the conversation, drive quantum ethical issues awareness, study quantum related risks, design quantum computing ethics principles and framework and test it with some case studies.

In **Canada, Q4Climate** is an initiative for using quantum technologies in climate research, an initiative coming from the Institut Quantique, the University of Waterloo and Zapata Computing. It looks like a small think tank. It explains how some quantum chemistry algorithms could potentially solve some environmental problems[2907].

In the **USA**, some spare initiatives are launched by academics like Chris Hoofnagle from Berkeley, or a while ago, by Scott Aaronson[2908].

Interestingly, none of these initiatives mention the field of quantum sensing, which could also have some underlying ethical issues to be addressed, particularly when used in the military. Quantum radars, quantum imaging, precision gravity measurement and its impact on underground resources exploitations are a couple examples.

[2904] See Quantum Ethics documentary, December 2020 (13 mn) published by TheQuantumInsider as part of a series of "conversations". It was followed by several posts like Quantum Ethics Series: Understanding the Issues and Expanding the Conversation by Matt Swayne, 2021.

[2905] See Asleep at the wheel Responsible Innovation in quantum computing by Philip Inglesant, Carolyn Ten Holter, Marina Jirotka & Robin Williams, October 2021 (14 pages).

[2906] See Quantum Computing Governance Principles, Insight Report, January 2022 (35 pages).

[2907] See Quantum technologies for climate change: Preliminary assessment by Casey Berger, Agustin Di Paolo, Tracey Forrest, Stuart Hadfield, Nicolas Sawaya, Michał Stęchły and Karl Thibault, June 2021 (14 pages).

[2908] See Law & policy for the quantum age : a presentation by Chris Hoofnagle, February 2021 (58 mn), Law and policy in the quantum age, by Chris Jay Hoofnagle and Simson L. Garfinkel, January 2020, free download (602 pages), and Why Philosophers Should Care About Computational Complexity by Scott Aaronson, 2011 (53 pages).

Religions and mysticism

In recent millennia, the human race has developed the habit of devoting a cult to one or more higher divine powers of an imprecise nature, but explaining everything and everything else.

Mankind probably began to attribute this power to natural phenomena that he could not explain like the Sun or the stars. Mankind then went from multiple systems of gods to a single all-powerful God. In a way, the monotheistic religions realized before time the theory of unification so much sought after by physicists. This story is told with hindsight by **Yuval Harari** in Sapiens and with cynicism by **Richard Dawkins** in "The God Delusion".

For some scientists or believers in an afterlife, quantum physics renews the desire to explain the inner works of the Universe by some divine power. It gives the impression of providing an ultimate scientific explanation for everything, of God, and of his ability to control and supervise everything[2909]. The quantum function most often emphasized in these explanations is entanglement.

It makes it possible to envision a Supreme Being who, thanks to this physical phenomenon, can control all the particles of the Universe and at a distance. It would also explain strange synchronicity phenomena. The wave-particle duality also makes it possible to imagine or explain many magical scenarios such as remote healing, telekinesis or telepathy[2910].

Some of the protagonists of these theories are themselves quantum physics scientists. One of the best-known is **David Bohm** (1917-1992), already mentioned in the quantum foundations section, page 1001, who came closer to Indian spiritualism in the 1960s, simultaneously with the Beatles! He was convinced that the laws of the Universe were governed by some spirit[2911]. He is one of the initiators of the theories of **quantum cognition**, a field of cognitive theories based on the mathematical formalism of quantum mechanics, and relying on analogies.

The literature on quantum derived spiritualism is sometimes mind blowing, such as Google's Quantum Computer May Point People to God, from 2013. According to the (anonymous) author, a perfect quantum computer could attempt to simulate the appearance of life on Earth and demonstrate through absurdity that it would not be possible without divine intervention. But who says that the result would not be the opposite? Quantum computing could invalidate classical theories of evolution.

Figure 889: quantum computer won't point you to God either! Source: Google's Quantum Computer May Point People to God, 2013.

[2909] On this subject, see the Wikipedia fact sheet that briefly describes quantum mysticism.

[2910] A good inventory of these different debates can be found in The Quantum God An Investigation of the Image of God from Quantum Science, 2015 (81 pages) which evokes the notion of consciousness of the Universe. See also the almost parodic Nothing is solid "All is energy".

[2911] See Lifework of David Bohm - River of Truth by Will Keepin, 2016 (22 pages).

They do not specify the number of zillions of entangled qubits that would be required to support this. Of course, because they have no idea which algorithms to use. And who care about quantum error correction!

All of this is religion-science fiction and can generate heated debates with people who will never be on the same wavelength, some adopting a classical scientific approach and others a mystical and more emotional one.

Public education

Quantum computing will amplify a situation observed with artificial intelligence: a huge gap between those who understand it and those who use it, coupled with a shortage of skills. It is right now definitely a world of specialists, and it is even harder to grasp than most other digital-related disciplines. Today, this world is balanced between specialists in condensed matter physics and quantum algorithms and software[2912].

By extrapolating a little and drawing inspiration from the history of computer science, we can anticipate that software will gradually take over when quantum computing becomes commonplace, especially if it leads to applications in all sectors of industry.

In today's digital economy, there are many more software specialists than there are with semiconductors. The economies of scale are actually much greater with the latter between producers and users. Quantum will probably not escape this, even if initially the market for quantum computers will not be a volume market.

In the short term, there is a great need to popularize the field and also avoid its technical jargon. You must proceed step by step, broadening the audience in a progressive way from the techie to the non techie[2913]. In parallel, training decision-makers in the industry and institutions must also be done. It is becoming even more important as the quantum technologies hype is peaking with the flurry of vendors and research labs announcements that are regularly showing up[2914].

Many initiatives around the world are launched to train the public on quantum physics and technologies. Let's mention the **National Q-12 Education Partnership** launched as part of the National Quantum Initiative and targets middle-school and high-school students. Industry participants include IBM, Google, Microsoft, AWS, Rigetti, Intel, Lockheed Martin, Boeing, Zapata Computing, APS Physics, Optica, IEEE USA and QubitbyQubit (a training organization). They organize the event QuanTime in spring 2022 with hundreds of quantum activity classrooms for K-12.

Other initiatives are gamifying the learning process like with **Quantum Odyssey** from Quarks Interactive (2020, Romania, 230K€) that were launched in 2020. They replace Dirac's bra-ket notation and linear algebra used by scientists by a visual puzzle-building approach. It's proposed to discover and learn gate-based quantum algorithms. **Quantum Chess** from Quantum Realm Games (2019, USA). The game embeds quantum phenomenon in the game play with pawns able to make multiple moves simultaneously in sort of superposition.

[2912] See Eleven risks of marrying a quantum information scientist by Nicole Yunger Halpern, 2020. A second degree but realistic inventory of the life of a quantum scientist in the USA.

[2913] See for example The Quantum Prisoner, a free scientific and technological video game is now available online, CEA, October 2020.

[2914] In Democratization of Quantum Technologies by Zeki C. Seskir, Steven Umbrello, Christopher Coenen and Pieter E. Vermaas, August 2022 (22 pages), the authors define the various aspects of a democracy and include educational efforts, like IBM's continuous evangelization efforts that started in 2016. They also pinpoint the asymmetry between the quantum ecosystem stakeholders and the general public which "has to be educated" but do not participate to a democratic decision making process. It also describes the counter-narrative on the democratization of quantum technologies like cybersecurity threats, its geopolitical dimension, and the habit to position quantum physics as impossible to understand, abusively quoting Richard Feynman. The authors do not describe the process followed by governments when launching their quantum plans, which embedded some participatory process with quantum ecosystem stakeholders but had their share of discretionary decision making, sometimes even escaping the minds of top policy makers.

Likewise, the very serious CEA in France launched **The Quantum Prisoner** in English in 2020, a free online adventure game inspired by quantum logic and targeting kids over 12 (meaning, adults are welcomed…). It has 10-12 hours of gameplay with a journey across the globe to find out what happened to a physician who mysteriously disappeared in the 1960s. Playing as Zoe, a young woman, gamers must solve over 30 technology, science and engineering-based puzzles.

Many other quantum games were created for educational purpose, like **Alice Challenge**, **Hello Quantum** and **Hello Qiskit** by IBM and the University of Basel, **Particle in a Box**, **Psi and Delta**, **QPlayLearn** (covered later), **Quantum Cats**, **Quantum Flytrap**, the **Virtual Lab** by Quantum Flytrap, **ScienceAtHome**[2915].

Some educational tools are specialized in quantum optics such **Quantum Games with Photons** from the MIT which is an open source puzzle game with 34 levels and a sandbox, and **The Virtual Quantum Optics Laboratory**, an optical lab running in a browser which enables you to build quantum optics experiments with all sorts of optical devices (lasers, PBS, depolarizer, etc, in Figure 890 *on the right*).

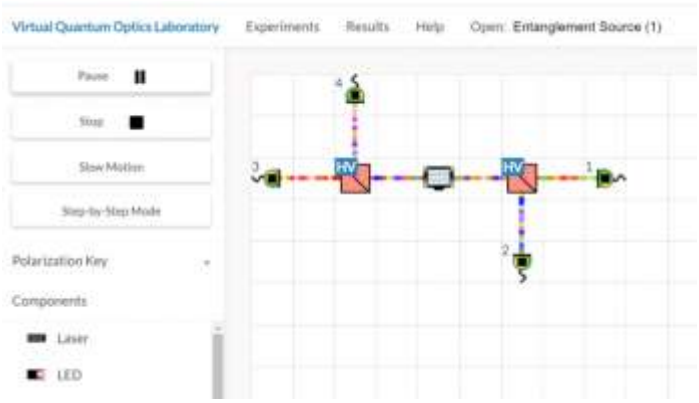


Figure 890: The Virtual Quantum Optics Laboratory.

CoSpaces is a similar simulation tool created in Italy and aimed at teaching quantum computing[2916].

Professional education

All these countries launching well-funded quantum plans create a significant challenge with professional education along the whole cycle from bachelor to doctorate. Before being an industry competition, quantum technologies are a talents one. We can expect that there will be more money to spend than talent to hire with it for a while.

Existing quantum professional training is significant in quantum physics. Most universities in the world have special programs from bachelors/licences and masters to PhDs. Some groups are organizing summer schools for PhD level students like the famous **Ecole de Physique des Houches** doctoral and summer school in the French alps with various sessions on quantum physics. Look for example at the 2019 summer school agenda's speakers!

There are a couple new disciplines where more and more people will need to build knowledge and skills on. Quantum systems engineering create real machines that work from start to finish. This requires decompartmentalizing disciplines and bringing together physicists and engineers. The technologies involved are varied and include photonics and lasers, analog and digital electronics, thermodynamics, fluid mechanics, various components manufacturing techniques, and the design of complete systems. Quantum engineering involves many complementary disciplines[2917]. With AI, it is a new challenge for higher education that is being prepared.

[2915] See an inventory of quantum games in Quantum Games and Interactive Tools for Quantum Technologies Outreach and Education by Zeki C. Seskir get al, July 2022 (48 pages).

[2916] See Quantum computing teaching with CoSpaces by Francesco Sisini, Igor Ciminelli and Fabio Antonio Bovino, September 2022 (8 pages).

[2917] The schematic comes from the Introduction to Quantum Computing presentation by William Oliver from MIT at Q2B in December 2019.

In the purely mathematical and software fields, very important disciplines come into play for creating end-to-end quantum solutions: algorithms design, software tools design and applications software development. Added to this is the field of post-quantum cryptography.

The creation of business applications also requires skills at the crossroads between the above and vertical markets, which are often themselves scientific as in life sciences (organic chemistry, protein folding, photosynthesis, ...), materials sciences (battery chemistry, superconducting materials) or other branches such as portfolio management and risk assessment in finance or optimization problems in logistics, transportation and marketing.

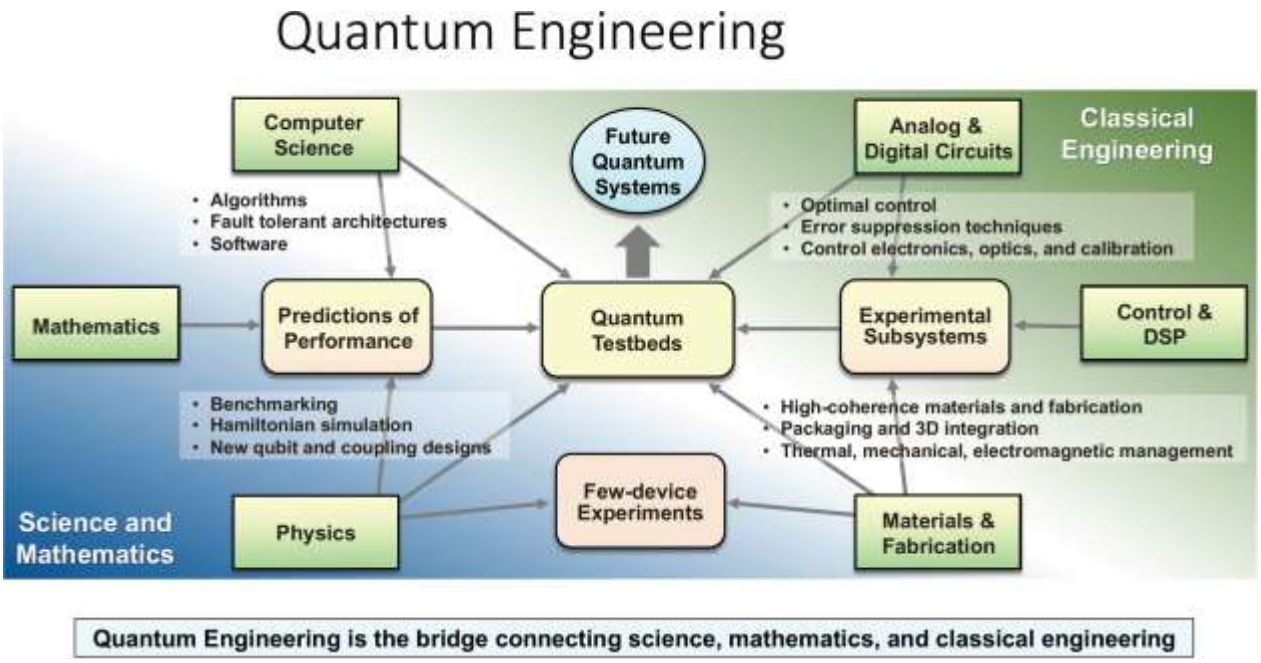


Figure 891: quantum engineering defined. Source: Introduction to Quantum Computing by William D. Oliver, MIT, December 2019.

Quantum technologies will be found with many different professions:

- **Fundamental physicists** (solid-state physics, condensed matter physics, light-matter interaction, quantum optics) who combine theoretical and experimental approaches to understand low-level phenomena.
- **Quantum technologies researchers** who turn fundamental discoveries into first proofs of concept in the laboratory. These research teams combine physics, technology and engineering researchers.
- **Design engineers** who create technical subsets of quantum computers to complete finished products. They essentially do the "D" of "R&D" by relying on the R of physicists.
- **Research engineers**, who participate in the development of new materials and new technologies in semiconductor fabs, or process engineers who design the manufacturing processes for these integrated circuit systems supporting qubits.
- **Technicians** for certain components manufacturing and/or for the deployment of technologies such as quantum cryptography in the telecom space. But only once this technology is deployed on an industrial scale, probably by generalist or specialized telecom operators.
- **Software tools developers** who must be associated with previous researchers and engineers. Indeed, for the time being, the design of these tools still has to take into account the physical characteristics of quantum calculators/accelerators.

- **Application developers**, whose numbers will increase as the computing power of quantum computers grows. Most of the time, they will need to have three key sets of technical skills: one is being able to program quantum computers, the second will be the ability to turn business problems into quantum programs (including the related mathematical/physics related know-how) and at last, they will have to know about classical programming since most quantum algorithms are hybrid.
- **Project managers** who manage projects and teams that combine these different professions.
- **Business strategists**. Brian Lenahan goes as far as defining the job of "quantum business strategist" which looks like an equivalent of the chief digital officer for quantum technologies related projects, creating the link between IT and business managers. This role is about crafting a quantum plan with mission, vision, goals, strategies, KPI's and tactics. In other words, it is an old-fashioned consultant[2918]!
- **Support activities** like in HR, marketing, business development (managing industry partners) and sales (to end-customers), communication, public relations, legal, finance, startup creation and acceleration.

As in many disciplines, researchers and engineers are increasingly required to be versatile. Teams must be structured around a strong interdisciplinarity and transversality. They need "technological polyglot" teams that link all these professions and skills. In particular, physicists will have to be increasingly interested in engineering and engineers in physics[2919].

Finally, when you turn to the business side with actual products that can be marketed and sold, you need the whole mix of skills usually found in technology marketing and sales: product marketing, operational marketing, business development and partnerships, creating ecosystems and, above all, pure and simple B2B sales for a starter. This is completed by the generic skills associated with deep techs startups creation (organization, business planning, recruitment, funding, etc.) and with intellectual property attorneys who must grasp the specificities of the quantum vocabulary.

Quantum sensing products are beginning to be marketed, and in a market that is currently niche.

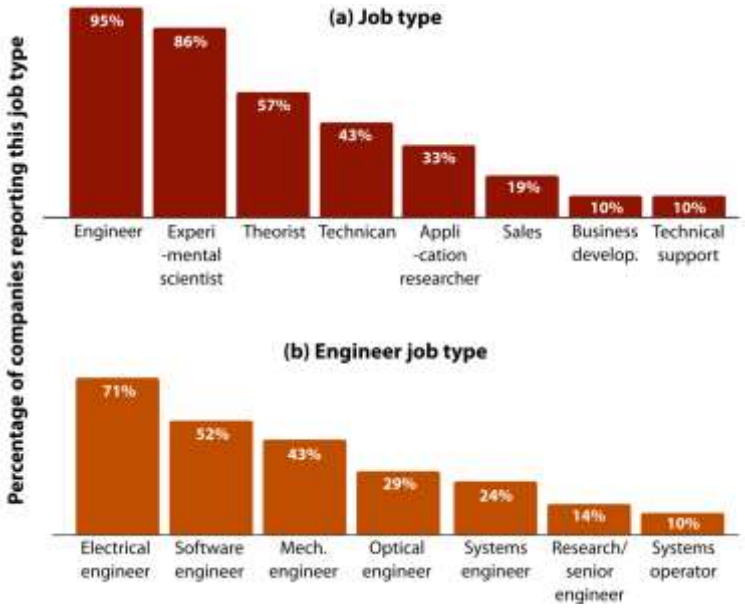


Figure 892: an American inventory of engineering jobs and skills in quantum technologies. Source: Preparing for the quantum revolution -- what is the role of higher education? by Michael F. J. Fox, Benjamin M. Zwickl et H. J. Lewandowski, 2020 (23 pages).

[2918] See What is a Quantum Business Strategist? by Brian Lenahan, April 2021 and his related book Quantum Boost: Using Quantum Computing to Supercharge Your Business by Brian Lenahan, May 2021. Brian Lenahan also created in September 2021 the Quantum Strategy Institute with various people from Spain, UK, France and the USA with the goal to bridge the gap between quantum science and businesses.

[2919] See Defining the quantum workforce landscape: a review of global quantum education initiatives by Maninder Kaur and Araceli Venegas-Gomez, Qureca, February 2022 (35 pages) which makes an inventory of the various quantum educational resources across the world and Building a Quantum Engineering Undergraduate Program by Abraham Asfaw, Alexandre Blais et al, 2021 (25 pages). See also the QTEdu, the European Quantum Flagship program on education which launched 11 pilot programs on education in quantum technologies and the associated report The Future Quantum Workforce: Competences, Requirements and Forecasts by Franziska Greinert et al, August 2022 (16 pages) which is based on a survey on quantum skills needs in Europe.

Quantum cryptography systems are in the experimental field phase and could be deployed on a larger scale in the coming decade.

Quantum communications with the objective of leading to quantum communications networks will develop in a second phase, combining fiber and satellite networks with quantum ground relays. This is a complementary field to the development of quantum computers.

Finally, quantum computing and simulation will progressively evolve and see their field of application widen as the qubits number and quality in quantum computers grows. It will be a process of continuous innovation.

As in the case of classical computing, the weight of software is bound to become dominant in skills requirements. This explains why many publications insist on the need for quantum application developers. This is what the major players such as IBM, Google and Microsoft, not to mention D-Wave, Rigetti and IonQ, are "evangelizing" about[2920].

Nevertheless, in parallel with the software market development, an intermediate phase will require a lot of skills in engineering and in the different branches of quantum technologies. In some cases, training can be shared between universities, particularly when teachers are scarce. That's what is implemented in the Université Paris-Saclay with the ARTEQ interdisciplinary year positioned before masters M1 and M2, to feed M2 masters in quantum physics and quantum information science.

Figure 893: ARTEQ training in Saclay.

Training in public higher education should introduce quantum science and technology as early as possible in the bachelor's and master's degree programs. It will also be necessary to create master's degrees in quantum engineering, bringing the world of research and engineering closer together.

The training offer will depend on several parameters: funding for teacher-researchers or teaching positions, the creation of vocations, the ability to attract teachers and students from wherever they come.

Continuing education may include both scientific and technological courses (quantum physics, quantum communications, quantum algorithms and software) and strategic courses (understanding of the issues, knowledge of the players, economics of the sector, good practices). This is probably the less well address market need, so far. It can or could be delivered by private organizations, by higher education organizations as well as via online courses offered by Coursera and the likes.

Self-training allows enthusiasts to discover these sciences and technologies by themselves, but it is not self-sufficient as it is sometimes the case in artificial intelligence.

[2920] Look at it this way: Quantum Computing Demands a Whole New Kind of Programmer by Edd Gent, May 2017 (slightly ahead of schedule), The Hitchhiking Cat's Guide to Getting a Job in Quantum Computing by Jay Gambetta, October 2019, Building Quantum Skills With Tools For Developers, Researchers and Educators, IBM Research, September 2019 and Some useful skills for quantum computing by Chris Granada, January 2020, which also emphasizes mathematical and software skills.

It must be complemented by quality pedagogical support, if only to do and correct exercises. As far as the software part is concerned, this will perhaps change the day when development tools will be possible with higher levels of abstraction than today.

Scientific events organized by quantum hubs, research laboratories and companies serve to facilitate transdisciplinarity among researchers and engineers. They can be interdisciplinary symposia, thematic conferences or workshops.

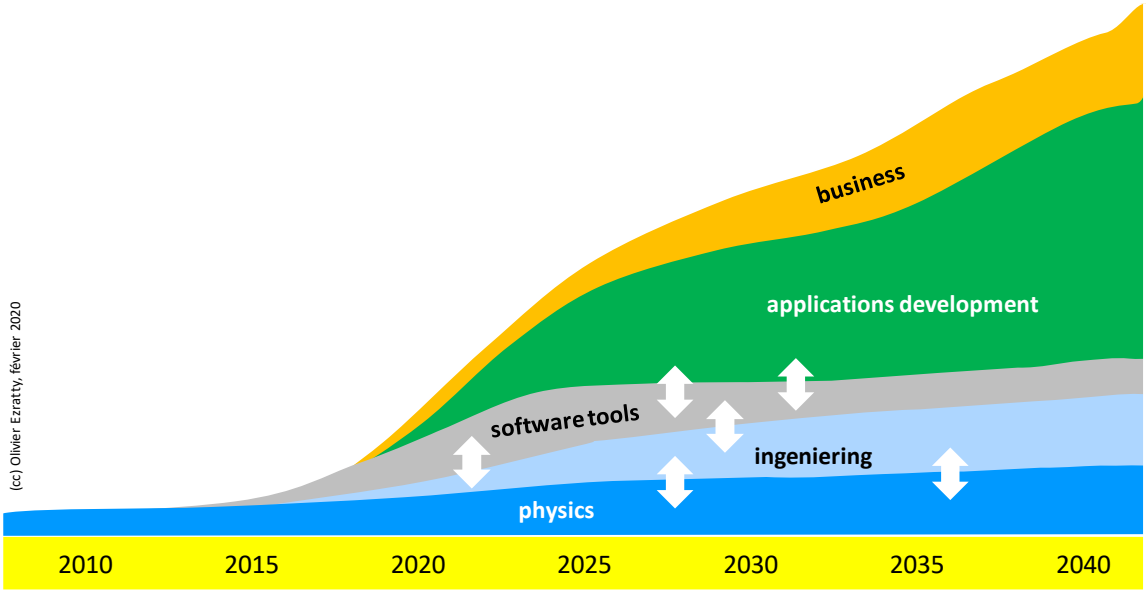


Figure 894: how quantum tech skills need will evolve over time. More engineering and then more software and more business skills. (cc) Olivier Ezratty, 2020.

It will also be necessary to attract as many women as men in these courses, otherwise there is a risk that a whole sector will develop, as in AI, which is far too masculine. Not to mention the increase in the diversity of students' social backgrounds, which remains a key means of republican promotion, despite its current decline.

Upstream of all these courses, the creation of vocations among young people is indispensable. Science fairs can also contribute to this. It is a long-term task, as is the creation of vocations in science in general and in the scientific and technical professions of the digital world in particular.

There are some pure players around in the quantum computing educational market, many of them offering open sourced eLearning contents:

Q-munity (2019) is a training organization and community connecting young individuals in quantum computing. With its 1000 members, it organizes summer camps (well, outside pandemics), conferences and workshops.

It was created by Anisha Musti, a quantum computer scientist who worked on Shor's algorithm, quantum teleportation and quantum machine learning.

QubitbyQubit (USA) is a quantum programming online learning initiative from The Coding School, created by a Brown University undergraduate in 2014. It was created by Kiera Peltz and is sponsored by IBM and Google.

Qplaylearn (2020, Finland) develops an online visual quantum programming training tool targeting a broad audience including high school students. They collaborate with various universities in Finland as well as with IBM.

Quantum Country (USA) is a tutorial web site on quantum programming created by Andy Matuschak and Michael Nielsen. It contains "mnemonic medium" that makes it easy to remember what you read. These are long reads including some good story telling and some exercising. It starts with the basics of quantum programming, then covers key algorithms like Grover search.

QuTech Academy is offering free online courseware on quantum technologies for engineers[2921].

CERN has a series of introductory conferences on quantum computing from **CERN** (7 x two hours tracks), broadcasted in November and December 2020, also targeting engineers[2922].

Qureca (2019, UK) sells online "Quantum for Everyone" courses for business people (at £400). These courses are delivered by Araceli Venegas-Gomez, the founder of Qureca, Bruno Fedrici, a French consultant and lecturer on quantum technologies and QuantFi, a French Startup specialized in Finance applications. The company also offers hiring services and other professional services for startups and businesses (community management, events organization, business development and strategy).

EFEQT (Empowering the Future Experts in Quantum Science and Technology for Europe) provides a learning experience between academic research and free interdisciplinary exploration for 25 students and young researchers. It takes the form a scientific hackathon, the first one was organized in October 2021 and ended with a graduation in September 2022. The best participants will receive a fast-track access to do a PhD or post-doc at EFEQT partner universities in Germany and Strasbourg in France. The program is supported by the Quantum Flagship's Quantum Technology Education Coordination and Support Action (QTEdu CSA).

Jobs impact

Finally, what about the future of quantum-related employment, a question that Sophia Chen asked herself in Wired in June 2018? It's difficult to assess because we're thinking over several decades and about use cases that are still uncertain. There will be, as with AI, those who know and those who don't, those who code and those who use stuff, those who create wealth and those whose jobs are threatened.


WIRED

SOPHIA CHEN SCIENCE 09.06.18 08:00 AM

QUANTUM COMPUTING WILL CREATE JOBS. BUT WHICH ONES?

Figure 895: who knows? There are so many uncertainties on the speed of how quantum tech will mature.

For the moment, quantum computing does not generate any specific jobs threats, because it will enable us to do things that mankind can't do today. There is no logic of replacement, at most optimization as for applications based on graph optimization like those of the traveling salesman.

[2921] See QuTech Academy Online Learning.

[2922] See Online introductory lectures on quantum computing from 6 November, 2020.

Gender balance

Gender unbalanced in all STEM jobs and particularly in computer science is a known fact and it has been so for a long time. You can look at all the statistics and they are not good. It started to go awry in computer science in the early 1980s when computing became mainstream. Many initiatives have been launched worldwide to rebalance gender in all these domains. They have mostly failed, or maybe did they just made things better than if nothing was done. Are quantum technologies different for gender balance?

Figure 896: some women role models around the world, from research to the industry. (cc) Olivier Ezratty, 2021-2022.

Problems

This domain is already highly male-dominated, in the lineage of computer science and artificial intelligence. The specialty is still too masculine as it stands. Quantum physics founder in History books are mostly men, particularly in the seven first quantum wave theoreticians narrow club with **Planck-Einstein-De Broglie-Schrödinger-Heisenberg-Dirac-Born**. You have to really dig into the History of science to recognize the role of **Emmy Noether** and **Chien-Shiung Wu**, the few female scientists of this era. Also, only three women were awarded a Nobel prize in physics with **Marie Curie** (1901), **Maria Goeppert** (1963, for her work on nuclear physics) and **Donna Strickland** (2018 for her work in pulse lasers). But besides Marie Curie, they don't yet have the recognition status of **Linda Lovelace**, **Grace Hopper** and **Margaret Hamilton** in computer science.

The statistics are depressing with only 20% women in STEM (in the USA) and it doesn't seem to be better in quantum science[2923]. Women's representations in culture, media and toys still play a leading role in crafting this unbalanced world. And this is just about gender balance. In the USA quantum scientific community, many groups are fighting against discriminations beyond gender balance issues.

[2923] See The Quantum Computer Revolution Must Include Women by Chandralekha Singh, Scientific American, January 2021 and The Upcoming Women In Quantum Summit III And Its Secret 70 Year-Old Legacy par Paul Smith-Goodson, December 2020. See also Women in Quantum Technologies - What are the challenges, February 2020.

Only a few countries are faring better, like in Asia. Is the condition of women in universities and research labs different than in business organizations? It probably depends on their values, leadership and culture. The scientific world seems as competitive and tough than the private sector even if its rules are different, based on h-indexes, conference talks and the likes. Still, in most places, research is a longer term activity which may create better conditions for women.

On top of that, the language used in quantum science is very masculine[2924]. It evokes the notions of superiority (supremacy) and auxiliaries (ancilla), the former echoing a higher authority, and the current "white supremacy" resulting from South African Apartheid and which is still stirring the US political scene. The second notion takes up the notion of "female servant" in Latin, slavery and racial segregation, whereas the technical term was coined in 1995. These are symbolic items but they deserve to be corrected. One solution is to talk about quantum advantage even if the meaning is slightly different from quantum supremacy (doing impossible things in classical computing vs doing things better). Some are advocating the usage of “useful advantage” in reference to use cases that provides some value with data inputs and outputs, but it doesn’t embed the distinction between supremacy and advantage. Another solution already mentioned consists in using the term **primacy**[2925].

A mix of other authors ask for creating a language void of competition connotations that should be comprehensible, specific and practical, open, accessible, responsible, culturally embedded and meaningful[2926].

Hope

There’s still hope. It seems easier to identify dozens of women who are real inspiring role models and play a key role in quantum science and technologies and anywhere in the world. Many of these were at the origin of key scientific advancements in quantum technologies. You may know the famous threshold theorem co-demonstrated by **Dorit Aharonov**! There are a few startups created by women like **Silicon Quantum Computing** (SQC, Australia), created by **Michelle Simmons, Oxford Quantum Circuits that is led by Ilana Wisby, Quandela, co-founded by Pascale Senellart,** VeriQloud co-founded by **Elham Kashefi** and Qureca, created by **Araceli Venegas-Gomez**. In the Corporate world, **Krysta Svore, Patty Lee** and **Anne Matsuura** play leading roles at respectively Microsoft, Quantinuum and Intel. In Europe, **Laure Le Bars** leads SAP’s quantum research efforts on top of being the first President of the QuIC industry consortium.

The Quantum Insider launched in 2021 a series of interviews of key women working in the quantum industry. It included for example **Mercedes Gimeno-Segovia**, Systems Architecture VP for PsiQuantum, **Olivia Lanes** North-America lead for Qiskit at IBM, **Helena Liebelt** from Deggendorf Institute of Technology, Intel and SheQuantum, **Christine Johnson**, CEO of Ingenii, **Lior Gazit** quantum software engineering team lead at Classiq, **Ying Lia Li**, CEO from Zero Point Motion (UK), **Katerine Londergan**, CMO at Zapata Computing Computing, **Anindita Banerjee** Security VP at QNU Labs, and **Rojalin Mishra** senior hardware verification engineer at Riverlane.

Also, quantum tech is still a green field and it’s not too late to attract young women in this emerging and promising discipline. There are already women playing leading technical and business roles in quantum startups on top of the cofounders mentioned above[2927].

[2924] As Karoline Wiesner of the University of Bristol points out very well in her succinct The careless use of language in quantum information, 2017 (2 pages).

[2925] See Quantum Computing 2022 by James D. Whitfield et al, January 2022 (13 pages).

[2926] See Quantum Technologies and Society: Towards a Different Spin by Christopher Coenen, Alexei Grinbaum, Armin Grunwald, Colin Milburn and Pieter Vermaas, November 2021 (8 pages).

[2927] See 52 Wonder Women Working In Industry As Quantum Scientists & Engineers by James Dargan, The Quantum Daily, August 2021.

Initiatives

Some initiatives have been launched around the world to promote and help women in quantum technologies. They are matching what has been done for a while in the computer science and information technology fields. Gender oriented actions are a mix of associations, events and media visibility initiatives. Too many of these are seasonal, and centered around the Woman's Rights day, on March 8th, each and every year.

Let's mention a few of these:

- **Women in Quantum** by **OneQuantum** is a think tank gathering quantum leaders worldwide in dedicated chapters, with the goal to influence government action, vendor relationships and the quantum ecosystem. It offers a resources, services and events platform for quantum startups to collaborate. Women in Quantum is one of the "chapters" of this organization, run by Denise Ruffner (also, Chief Business Officer of Atom Computing), organizing quarterly Women in Quantum events, the last one being held online in June 2021[2928].
- **Women in Quantum Development** is a professional network of quantum tech enthusiasts in the Netherlands, with events and mentoring programs. It belongs to a new trend, with national quantum plans containing specific initiatives around the ethics and social impact of quantum technologies. Netherlands is a good best practice for that respect. There's also a gender equality workgroup in the **EU Quantum Flagship**.
- The **University of Bristol** organized a two-day Women in a Quantum Engineering event in December 2019.
- Some research labs and organizations showcasing their women quantum scientists and engineers like at the **Lawrence Berkeley National Lab** from the DoE in the USA[2929], at the **Harvard** Center for Integrated Quantum Materials[2930], at **Yale University**[2931], with **IBM**[2932] and **Microsoft**[2933].
- **SheQuantum** (2020, India) is an eLearning provider offering quantum computing education content targeting women.
- In France, the association **Quelques Femmes du Numérique!** promotes women in tech, particularly engineers and scientists using quality photography portraits with over 750 women in various fields (artificial intelligence, Blockchain, cybersecurity, IT, etc) and over a dozen in quantum techs[2934]. It launched many initiatives including promoting quantum science to female teenagers.

Solutions

Like in any domain, particularly in social science, there's not yet a common agreement on what should be done to create a better gender balance in STEMs and in quantum science.

[2928] See the casting of the Fall 2020 edition.

[2929] See Women of Quantum Computing Go Tiny in Big Ways by Elizabeth Ball, June 2021.

[2930] See Ask a Scientist: Women in Quantum Science and Technology, November 2020.

[2931] See WIQI (Women in Quantum Information) Group.

[2932] See Encouraging more women in quantum: four insights from four women, IBM UK, March 2021.

[2933] See Women of Microsoft Quantum Part 1 and Part 2, March 2020.

[2934] Disclaimer: I'm the cofounder and photographer of this association. Whenever I can in media and events speaking opportunities, I propose to create a duo with one the quantum scientist women I know well.

Should we encourage some affirmative actions or not? Some are worth the effort like the European Union ERC Grant program which extends since 2010 the age limit by 18 months per child plus other anti-bias measures. Paternity leaves are also taken into account[2935].

In the way women scientists and entrepreneurs are promoted, I believe we should be more engaged but with subtlety. For example, it's more efficient to value scientists and entrepreneurs for their achievement and who happen to be women instead of doing this explicitly because they are women. An implicit communication is sometimes more efficient than an explicit one. Finding women talents should be a sort of backstage work. It requires some discipline. When organizing training and events, and with any media speaking opportunity, make sure gender balance is respected. It involves having some knowledge of the field ecosystem and of its female leaders. Don't say "there are only a few of them", but "where are they?" and look for them. Also, let them talk about their science.

We should also promote a broad range of role models in different fields and jobs to inspire young talents.

It's also about building inclusive and welcoming work environments in universities, research labs and commercial vendors.

Of course, in a broader scale, media and fiction play a key role. The geek in TV series and movies is too frequently an introverted male. We need more Felicity Smoak, the geek from the TV Series Arrow! At last, do that all year long and not just on March 8th.

Quantum technologies marketing

The last point to be mentioned here is the role of marketing and propaganda. Quantum technologies are the perfect spot to broadcast extraordinary and impressive claims that few specialists can fact-check. It's a world of superlatives and exaggerations. It started in 2019 with Google's supremacy claim.

We are going to be drowned in innovation propaganda that will blur things. Scientists in the field will no longer recognize their creations. Popular news related to quantum computing will continue to start explaining qubits with their superposed states 0 and 1 and... stop there!

Consulting firm will also strive in simplifications. This **BCG** set promoting quantum computing in the pharmaceutical industries is quite amazing although, hopefully a bit dated (see Figure 897). It mentioned the ability of a quantum computer to solve an "*infinite number of problems simultaneously*", confusing, infinity and exponentiality, and then also, superposition and problems. They did estimate the quantum computing market in the pharmaceutical industries in the USA to sit between $15B and $30B with no precise date. A market forecast from 2018 expected that global IT spending dedicated to drug discovery would have reached $5.3B by 2020[2936]! That is not really consistent.

Marketing and communication are all about making fancy claims and simplifying facts with wild exaggerations. One can wonder, how is the bullshit created in marketing when there's so much science behind most projects? It starts with the businessification of quantum technologies. The rules of the game for a staring looking for some VC funding is to talk about customer use cases and market size, creating an echo chamber to the crazy numbers published by industry analyst firms. You will therefore have plenty of quantum computing hardware and software companies web site presenting the same story about the beauties of quantum computing in pharma, financial services, transportation and the industry, if not to fix climate change, but nearly nothing on their actual technologies and products.

[2935] See ERC Gender Actions, 2021 (14 slides). It provides some data on the share of women applicants vs men who get ERCs and H2020 grants based on the discipline. Across the board, women have about 20% less chance to get a funding.

[2936] Source: Growth Insights Report: Global Pharmaceutical Drug Discovery IT Solutions Market 2017-2020 - Key Initiatives by Big Pharmaceutical Companies, January 2018.

Figure 897: an example of fact-checking on a BCG forecast related to the healthcare industry. Source: The Qubits are coming, BCG Henderson Institute, June 2018, extracted from the report The Coming Quantum Leap in Computing. Comments by Olivier Ezratty, September 2018, updated in 2021.

A key form of bs shows-up when quantum hardware startups are hiding simple information like the number of qubits of their QPU (a practice from Anyon Systems in Canada as of 2022 and OQC in the UK in 2021). It usually means that they are too shy to say that they have fewer than 5 operating qubits and therefore are not competitive against companies like IBM (127 qubits as of August 2022) and Rigetti (80 qubits as of the same date). How about qubit fidelities? They are usually hidden as well. Or like with Anyon, they are published without a number of qubits which tells a lot (it's hard to have good fidelities over a large number of qubits, and if their fidelities are bad with an undisclosed number of qubits that must be small, it smells fishy).

Another doubtful practice from quantum hardware vendors connects the dots between customer orientation and unmature hardware platforms is to say: we create application-specific quantum hardware. While it may make sense in some cases, it's an economic and technology non-sense. Successful hardware companies create economies of scale, like IBM in the 1960s with its family of IBM 360 mainframes. Hardware must be generic for a large range of applications. Like Nvidia GPGPUs that are used for both machine learning and scientific applications thanks to a broad software support. On top of that, if one hardware platform has so many limitations that it's bound to be used for only one category of application, you as a customer will be locked-in. Then, you can listen to the technical rationale behind custom-hardware platforms. But specialists will tell you it doesn't make much sense in general.

At last, some quantum hardware vendors will sell you fancy customer-oriented application benefits, without presenting any real quantum advantage whether in results precision, execution time, solution price or spent energy for the environmentally conscious as compared to best-in-class classical solutions.

And yet, I am the first to be convinced of the benefits of quantum computing in pharmaceutical applications, and in particular for simulating the behavior of organic molecules. These die-cut exaggerations are delirious and remind me of those that were made about the Internet of things a few years ago.

In the same vein, the **quantum transistors** evoked in this presentation by Movimento Group for the autonomous vehicles of 2030, stem from a lack of knowledge of the state of the art of quantum computing, its speed of progression and the physical nature of qubits[2937]. Bearing in mind that transistors have been using quantum phenomena since their creation!

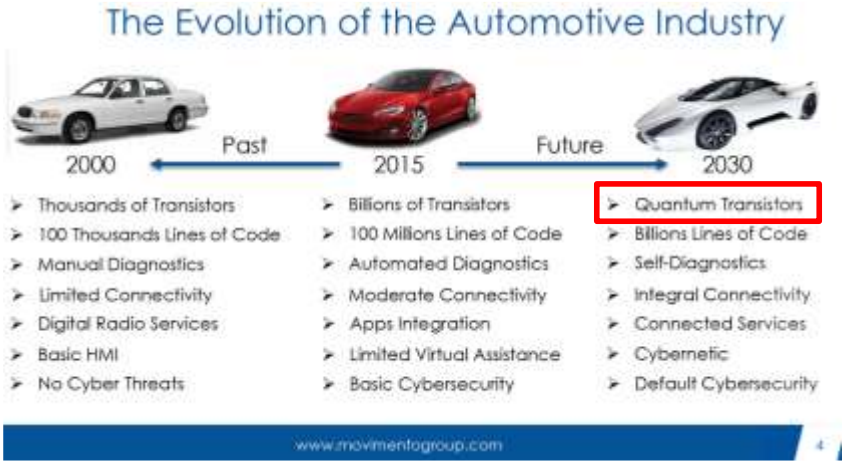


Figure 898: quantum transistors for the automotive industry? Well, maybe not!

Quantum technologies and society key takeaways

- Quantum technologies can become one of the artefacts of Mankind's technology ambitions, pushing the limits of what can be achieved in the line of some works done in artificial intelligence. It may give the impression that mankind's power has no limit. A sound scientific mind will however understand that quantum computing has its own limits. The world can't be simulated, the future can't be predicted, and apparent free will can persist.
- Science fiction has built an imaginary of what quantum technologies could achieve, with teleportation, supraluminal traveling speeds, various entanglement and miniaturization feats, parallel or multiverse worlds and time travel. While none of these things are possible given our current scientific knowledge, it can create scientific vocations and drive new generations to solve actual problems.
- Quantum foundations is the branch of science philosophy that aims to build some understanding of the real world. Quantum physics' formalism is difficult to associate with the principles of reality usually applicable in classical physics. While classical physics understanding has historically been associated with an ontology with objects position and motion enabling the prediction of phenomena such as the motion of planets. Quantum physics lacks such an ontology describing the physical world. Beyond the canonical Copenhagen interpretation (psi and the wave equation), many scientists tried to create such ontologies and the debate is still raging.
- The quantum scientific community is starting to investigate the ethics of quantum technologies. Like with artificial intelligence, it will be questioned on algorithms explainability and auditability, on what it will do to simulate if not tweak matter and life and on how to handle public education. Some related initiatives have already been launched by scientists in Australia, The Netherlands, Canada and the UK.
- The education challenge around quantum sciences and technologies is enormous, both for the general public and with specialists. There's a need for better pedagogy, accessible educational content and also for sound fact-checking information.
- Gender balance is already an issue in quantum technologies with a low share of women in the field, particularly with vendors. Hopefully, there are many top women scientists and entrepreneur role models around who can inspire a new generation of women teenagers. Many initiatives around the world have been launched for that respect.
- At last, quantum technologies vendors marketing must be watched carefully. It is and will be full of exaggerations and approximations. The worse will happen with vendors outside the quantum technology sphere.

[2937] See Protecting Autonomous Vehicles and Connected Services with Software Defined Perimeter, 2017 (21 slides).

Quantum fake sciences

One of the most fascinating topics in the mainstream impact of quantum physics is the way some people integrating it into alternative dubious scientific approaches. The vast framework of "quantum medicine" is a fairly coherent stream of thought and practice from this point of view. It has given rise to the proliferation of gurus of all kinds and to voluntary or involuntary scams based on miracle machines for detecting electromagnetic waves or vague energies, and restoring your body balance. It is at best a subset of the vast placebo effect industry!

Other fields took over quantum physics and long before quantum computing became a visible subject: management and marketing, not to mention politics[2938]. Quantum physics is essentially used there as a source of inspiration by analogy. But the “gurutisation” of these sectors is also quite common, linking together currents of thought that revolve a lot around magical thinking.

Quantum biology

The starting point of quantum medicine is, however, scientifically relevant and interesting. Some low-level biological phenomena can be well explained at a low-level by quantum physics. Of course, since everything is quantum at this scale!

To mention just a few examples, this is obviously the case of **photosynthesis** in plants, which uses the photoelectric effect transforming a photon into electron displacement, leading after the Calvin cycle to the production of glucose that is used to store energy. The same applies to **retina cones and rods** which capture light. **UV-B rays** participate in the synthesis of Vitamin D3 precursors in the skin again using the photoelectric effect but with a different wavelength[2939]. Quantum physics also explains the **capture of terrestrial magnetism** in the brains of many birds via a special protein called cryptochrome. This mechanism relies on the protein's ability to detect magnetic variations through some electron quantum entanglement[2940]. Quantum biology is a serious scientific domain and it deserves its proper attention[2941].

So far so good.

[2938] The concept of quantum politics is still in its infancy. Here is some literature from economic and social researchers on the subject. For example, Quantum like modelling of the non-separability of voters' preferences in the US political system by Polina Khrennikova, University of Leicester, 2014 (13 pages) seeks to model the choices of US voters and the entanglement or not of the choice of presidential candidate and congressional candidates showing that it can decouple under certain conditions. And Quantum Politics: New Methodological Perspective by Asghar Kazemi, 2011 (15 pages) creates a link with chaos theory and the butterfly effect. The paper was written just after the 2011 Arab revolutions. See also Schrodinger's Cat and World History: The Many Worlds Interpretation of Alternative Facts by Tom Banks, who uses Bryce DeWitt's Multiple Worlds Thesis to explain the election of Donald Trump in 2016 by a giant tunnel effect. That maaaayyyy be a little exaggerated! In 2022, some writer tried to explain the Russia invasion of Ukraine with quantum physics. See Quantizing the Invasion of Ukraine by Nicholas Harrington, 2022 (not precisely dated…) and another paper described a quantum parliament, in A two-party quantum parliament by Theodore Andronikos and Michael Stefanidakis, January 2022 (23 pages).

[2939] See The Relationship between Ultraviolet Radiation Exposure and Vitamin D Status by Ola Engelsen, 2010.

[2940] See Resonance effects indicate a radical-pair mechanism for avian magnetic compass by Thorsten Ritz et al, 2004 (4 pages), Cellular autofluorescence is magnetic field sensitive by Noboru Ikeya and Jonathan R. Woodward, January 2021 (6 pages) and Magnetic sensitivity of cryptochrome 4 from a migratory songbird by Jingjing Xu et al, June 2021.

[2941] See The Future of Biology is Quantum - A proposal for a new scientific research organization by Arye and Clarice D. Aiello, May 2022 which calls for the creation of a dedicated research lab on quantum biology, that would be directed by one of its authors.

Then, some renowned scientists want to explain the origin of consciousness with quantum physics. Several major schools of thought are related to each other like the **Orch-OR theory**, the **holographic** dimension of DNA and **biophotons**. And then there are all the works around **structure of water** and **water memory**.

None of these works obtained the agreement of a majority of scientists, but it still deserves a little review. If only to understand how they are quickly being misused by the quantum medicine charlatans over the world.

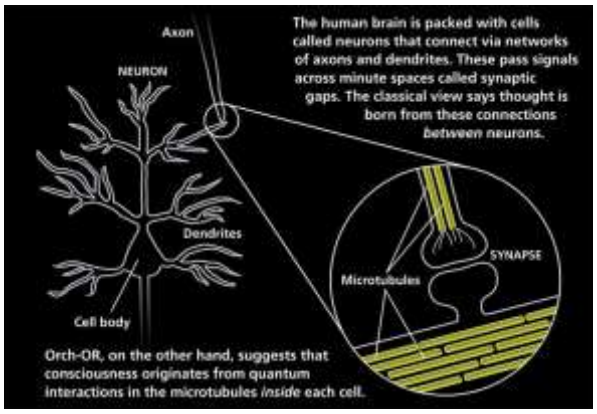


Figure 899: Orch-OR top-level view.

Orch-OR Theory

According to **Roger Penrose** (English, 1931[2942]) and **Stuart Hameroff** (American, 1947), consciousness is housed and managed by microtubules, the complex fibrous structures that, together with actin filaments and intermediate filaments, constitute the structure of neuron cells, called the cytoskeleton, and in the case of neurons, the dendrites, synapses and axons[2943].

In 1996, they proposed the Orch-OR (Orchestrated Objective Reduction) model according to which these microtubules were coherent quantum systems explaining consciousness.

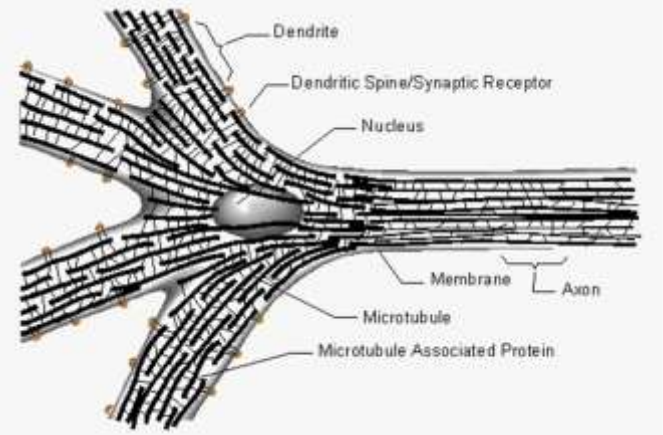


Figure 900: Orch-OR low level view with neurons and their microtubules.

For them, consciousness is managed in the neurons within these microtubules and not by their interconnections via dendrites/synapses pairs. In 2011, Roger Penrose and Stuart Hameroff even suggested that these microtubules would be quantum nanocomputers capable of managing qubits and associated calculations[2944]. If this were true, the power of this computer in number of qubits would be immeasurable because a single neuron comprises about 100 million tubules, the brain 86 billion neurons and more than 600 trillion connections between neurons! These theories obviously do not specify how the entanglement between these qubits would work on this scale.

[2942] He was awarded the Nobel prize in physics in 2020 for his seminal work on black holes.

[2943] Illustration source: Is our brain a quantum computer? by Laurent Sacco, April 2018.

[2944] Other theories think that quantum entanglement also works elsewhere in the brain, at the level of phosphorus atoms associated with calcium. This would allow the creation of quantum bonds between neurons. See Quantum Cognition: The possibility of processing with nuclear spins in the brain by Matthew Fisher, 2015 (8 pages). As the article indicates, this raises questions but does not provide answers! Therefore, any rather rapid interpretation of the "quantum brain" is to be taken with a grain of salt.

Ironically, the indirect impact of this gargantuan sizing would be to push back even further in time a possible singularity, the moment when a computer would reach the computing capacity of a human brain in raw computing power[2945]. We are dealing here with another current of thought, promoted in particular by **Ray Kurzweil**.

The Orch-OR theory was revived in 2014 with the discovery of quantum vibrations in microtubules by **Anirban Bandyopadhyay** from the National Institute for Materials Science in Japan[2946]. But that doesn't explain anything. Roger Penrose and Stuart Hameroff also asserted that this behavior is influenced by some type of gravity-related wavefunction collapse[2947]. Consciousness is a "macro" phenomenon. Trying to explain a "macro" phenomenon by a single "nanoscopic" process is meaningless because it completely gets rid of the entire biological hierarchy between the two and the other nanoscopic mechanisms at stake in the nervous system: neurons themselves, neurotransmitters, synapses and dendrites, neurons nucleus, brain regulatory glial cells, and on a larger scale, senses and brain macro-organization[2948].

For example, we can explain a good part of living things via the weak hydrogen-hydrogen bonds - (which are of quantum nature, of course) that are linking together the two DNA strands, or with the oxygen and phosphorus bonds, in DNA and RNA, which are strong and can thus explain the cohesion of these fundamental molecules of living things.

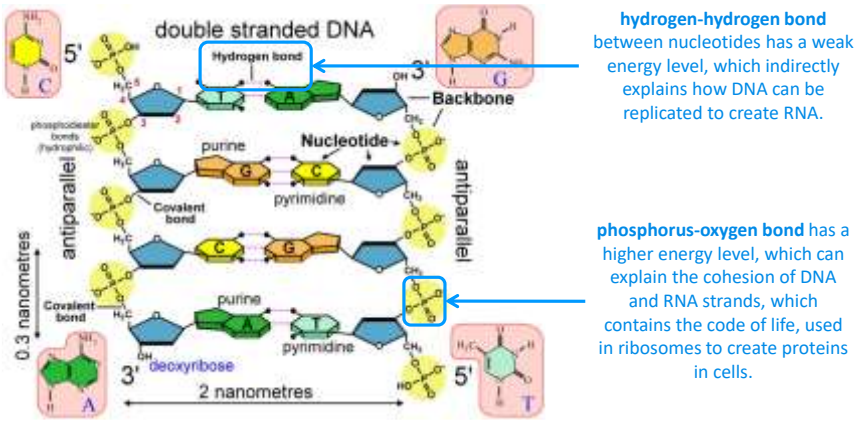


Figure 901: you can build a whole explanatory theory on life with just two chemical liaisons (hydrogen-hydrogen and oxygen-phosphorus). Source: http://universe-review.ca/F11-monocell08.htm.

However, this is obviously not enough to explain consciousness or how your heart, eyes and kidneys work. One could also easily build a bozo theory associating consciousness with electrons if not with quarks and gluons. Indeed, without electrons, there's no chemistry and no consciousness! It explains the chemical bonds between atoms.

[2945] See Consciousness in the Universe Neuroscience, Quantum Space-Time Geometry and Orch OR Theory by Roger Penrose, 2011, 50 pages). All this is documented in Orchestrated Objective Reduction of Quantum Coherence in Brain Microtubules: The "Orch OR" Model for Consciousness, 1996 (28 pages) as well as in Consciousness, Microtubules, & 'Orch OR' A 'Space-time Odyssey' by Stuart Hameroff, 2013 (28 pages), Are Microtubules the Brain of the Neuron by Jon Lieff, 2015 and popularized in The strange link between the human mind and quantum by Philipp Ball, 2017. Roger Penrose has collaborated with Stephen Hawking on gravitational singularities and radiation emission from black holes. Hawking had developed a cosmological theory combining the theory of relativity and quantum physics.

[2946] The discovery is disputed by Matti Pitkanen in New Results about Microtubules as Quantum Systems, 2014 (18 pages).

[2947] An physics experiment did invalidate most of this theory. See Quantum theory of consciousness put in doubt by underground experiment, PhysicsWorld, July 2022 referring to At the crossroad of the search for spontaneous radiation and the Orch OR consciousness theory by Maaneli Derakhshani et al, Science Direct, September 2022.

[2948] See this interesting discussions on Orch-OR in Why is Orch-OR ignored by the mainstream scientific community?, Quora, and also Falsifications of Hameroff-Penrose Orch OR Model of Consciousness and Novel Avenues for Development of Quantum Mind Theory by Danko Dimchev Georgiev, 2006 (32 pages) which debunks many of Stuart Hameroff and Roger Penrose assertions in the Orch-OR model with an in-depth neurobiology analysis.

Fortunately, nobody has yet ventured into this kind of explanation. In short, explaining consciousness by the possibly quantum nature of a particular structure of neurons is the most simplistic reductionism possible, ignoring all the other knowledge available... or yet unavailable[2949].

DNA would also have a quantum function. A curious paper of Russian, German and English origin describes quantum and non-localized phenomena in DNA, verified in a famous experiment based on laser light diffraction, in Figure 902[2950].

The bio-digital DNA wave (20 pages) explains that DNA is in fact a hologram, which interacts with its environment with laser radiation.

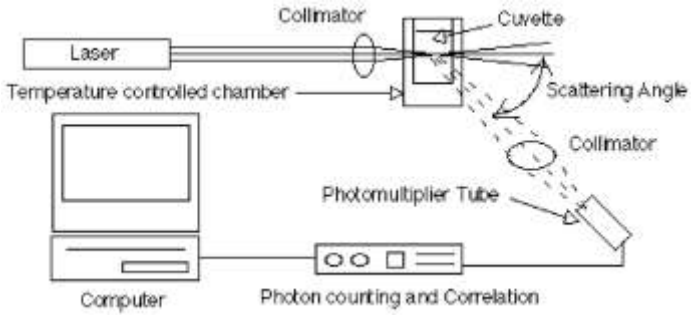


Figure 902: Source: DNA as Basis for Quantum Biocomputer, 2011 (22 pages),

Through quantum entanglement, the chromosomes of several cells would interact with each other via these radiations. The Russian of history and leader of this work is a certain **Peter Gariaev,** creator of the concept of BioHolograms within his **Wave Genetics Institute** in Moscow[2951].

Other attempts to explain consciousness by quantum physics have been created. **Matthew Fisher** from UCSB wanted to investigate the brain's potential for quantum computation, based on phosphorus ions spin entanglement[2952]. He launched his **Quantum Brain Project** (QuBrain) with a 1M€ funding in 2018 from the Heising-Simons foundation. Since then, the Project was discontinued. Others like **Johnjoe McFadden** from the University of Surrey in the UK try to explain consciousness with electromagnetic waves circulating in the brain[2953]. At last, some journalists invent some quantum influence where it doesn't exist[2954].

Biophotons

Another alternative school of thought is related to **biophotons**. These are the low light emissions in the visible generated by living beings. They were discovered in 1922 by the **Alexander Gurwitsch** (Russia). The theory of biophotons was perfected by the **Fritz Albert Popp** (Germany). It complements at a low-level the hologram DNA thesis.

It describes the emission of photons from molecules such as DNA, but also the emission of photons related to the energy metabolism of cells such as the transformation of ADP molecules into ATP in the mitochondria of cells.

[2949] A similar reductionism process shows up in Scientists think quantum tunneling in space led to life on Earth by Tristan Greene, TheNextWeb, March 2022, that refers to A pathway to peptides in space through the condensation of atomic carbon by S. A. Krasnokutski et al, Nature Astronomy, February 2022 (13 pages). They explain the appearance of life on Earth for some low-level chemical reaction that could happen on an asteroid. But this reaction is even more likely on Earth given the conditions on the planet!

[2950] See DNA as Basis for Quantum Biocomputer, 2011 (22 pages).

[2951] The history of the theme is explored in Quantum BioHolography A Review of the Field from 1973-2002 by Richard Alan Miller, Iona Miller and Burt Webb (23 pages), but these texts do not give any idea of its scientific validity.

[2952] See Quantum Cognition: The possibility of processing with nuclear spins in the brain by Matthew P. A. Fisher, 2015 (8 pages).

[2953] See Integrating information in the brain's EM field: the cemi field theory of consciousness by Johnjoe McFadden, September 2020 (13 pages) covered in New research claims that consciousness itself is an energy field - a professor says this could be the key to building conscious machines by Victor Tangermann, in Futurism, October 2020.

[2954] See Your brain might be a quantum computer that hallucinates math by Tristan Greene February 2022 referring to Neuronal codes for arithmetic rule processing in the human brain by Esther F. Kutter et al, Science Direct, March 2022 (15 pages).The words quantum and entanglement do not appear in the scientific paper. Ergo the first title is pure clickbait.

The biophotons are ultraviolet and visible light emissions, at levels that are much lower than the mid-infrared emission occurring at around 12 microns wavelength. Up to a few hundred photons per square centimeter of organ analyzed could be detected, often at the skin level.

These biophotons are also made of coherent light - photons with the same frequency. They would constitute a form of inter-cellular communication[2955].

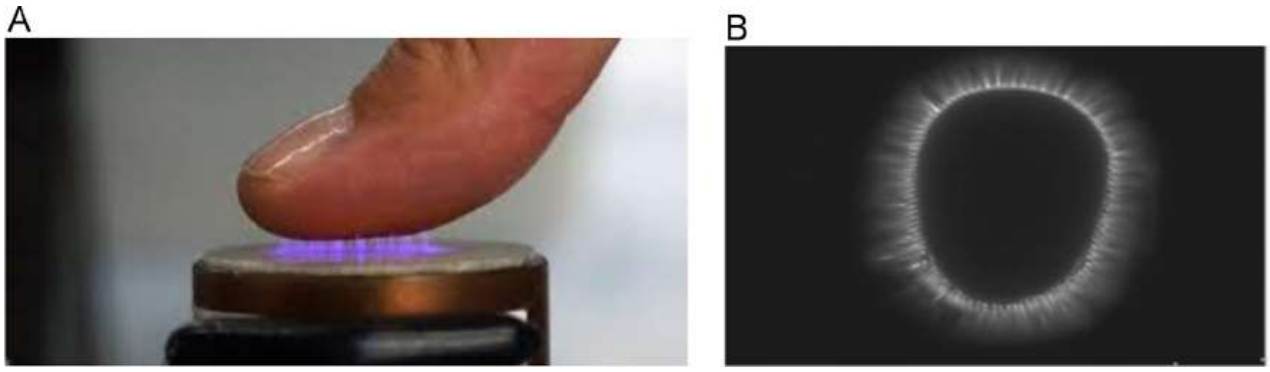


Figure 903: Biophotons. Source TBD.

I wonder how this communication works: at what range, due to the obvious attenuation of photons scattering, and with what precision targeting (direction, orientation).

According to Fritz Albert Popp, raw foods emit more biophotons than cooked foods, and organic raw plants emit five times more biophotons than traditionally grown plants. Conclusion: eat raw and organic! This is also a reason to have prehistoric men regret having discovered fire!

In any case, the detection of biophotons on the 10 fingers of the hand would make it possible to detect cardiac pathologies[2956]. The **ClearView** scanner used exploits a curious process: it sends a high-voltage pulse that creates an electromagnetic field around the finger that amplifies the biophotons that are emitted. This excites molecules in the air, creating a plasma between the sensor and the finger (*above left*) that ionizes the air, generating the emission of UV and visible light. This is the **Kirlian effect**, discovered by the Russian Semyon Kirlian in 1939.

The ionization that is captured by the camera (*above right*). The software analyzes the generated shape and compares it to a pathology database. I have a hard time figuring out the exact link between bioluminescence and this process! And what about the receptors of these biophotons?

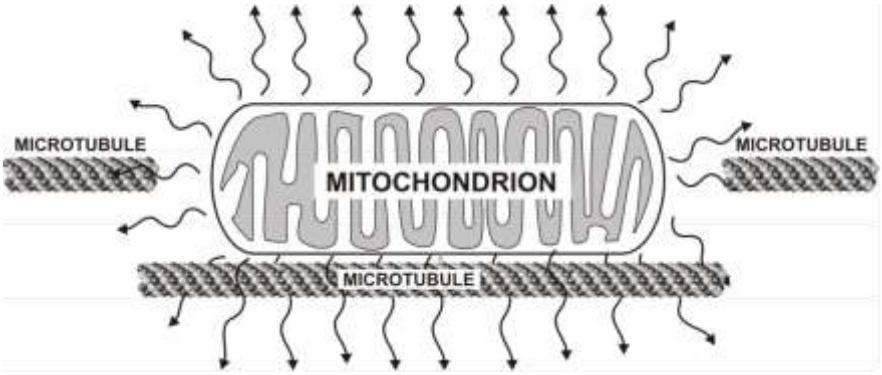


Figure 904: Source: Emission of Mitochondrial Biophotons and their Effect on Electrical Activity of Membrane via Microtubules, 2010 (22 pages).

[2955] As described in Photonic Communications and Information Encoding in Biological Systems by S.N. Mayburov, 2012 (10 pages) and popularized in Biophoton Communication: Can Cells Talk Using Light?, 2012 in the MIT Technology Review.

[2956] According to Detecting presence of cardiovascular disease through mitochondria respiration as depicted through biophotonic emission by Nancy Rizzo, 2015 (11 pages).

Well, it comes from the neuron microtubules, of course, closing the loop[2957]! According to Popp: "*matter would only be condensed light*"[2958]. By the way, biophotons would be a way to explain chi.

David Muehsam mentions many biological effects of biophotons, which would be involved in the regulation of neurotransmitters secretion (for rats) but without the distinction between correlation and causality being visibly made in the associated publications[2959].

If all that was just science and research! But hell no. It helps snake oil vendors to sell miracle healings through the control of the body by conscience. Practitioners of quantum medicine are very often psychosomaticians exploiting mysticism and autosuggestion to generate, in the best of cases, a good placebo effect that can work with certain mild pathologies. Even so, they justify their methods on the contested work of researchers such as Roger Penrose and Stuart Hameroff, already mentioned, but also Karl Pribram and Henry Stapp, who want to explain human consciousness by quantum phenomena intervening at a low-level in the brain that would also explain a so-called immortality.

Wikipedia's Quantum Mind fact sheet reports on the evolution of this branch and the associated criticisms. It underlines the fact that there is no way to apply possible quantum phenomena such as entanglement at the scale of macroscopic brain molecular or cellular structures.

Entanglement is even less justifiable to connect the brain at long distance to the "*holographic global consciousness of the Universe*" promoted by **Karl Pribram** and **Paola Zizzi**[2960]. In the same way, it does not necessarily make sense to link mind and matter as waves and particles and their famous duality. This leads otherwise to absurdities that explain psychic phenomena of synchronicity by the collapse of the wave function of consciousness, an explanation as absurd as Schrödinger's cat thought experiment. Even if the theories of Penrose and Hameroff were verified, the shortcut would be a little hasty, moving quite too fast from a nano-phenomenon to a macro-phenomenon!

The other commonly proposed method involves the use of various electromagnetic waves, including the famous and smokey **scalar waves**. The idea is to exploit them to restore the balance of unbalanced organs, exploiting the wave-particle duality and the ability to restore the basic energy level of... we don't know. Particularly given the proposed waves are not really targeted.

It is notable, however, that few scientific specialists in quantum medicine mention the capabilities of future quantum computers to simulate the operations of organic molecules and create new therapies. Maybe because known applications of quantum computing in health care are part of traditional allopathic medicine, that they usually avoid or at least complement.

However, I found a vague trace of with **Matti Pitkanen** (Finland) who, in the framework of his work on TGD (Topological Geometrodynamics), proposes a unified theory of physics, and puts forward the idea of creating DNA-based quantum computers[2961]. He believes that DNA communicates "with the Universe". It is also based on Luc Montagnier's experiments on DNA. Matti Pitkanen provides the basis for highly speculative theories on the supposed consciousness of the Universe[2962]. His theories of the unification of physics are so complex that they are impossible to understand, and eventually to validate by experience or to refute.

[2957] This is what comes out of Emission of Mitochondrial Biophotons and their Effect on Electrical Activity of Membrane via Microtubules, 2010 (22 pages).

[2958] See Introduction of Consciousness in Matter from Quantum Physics to Biology (18 pages) by Jacqueline Bousquet, a former CNRS researcher who died in 2013.

[2959] See The Energy That Heals Part II: Biophoton Emissions and The Body of Light by David Muehsam, April 2018.

[2960] See Consciousness and Logic in a Quantum-Computing Universe, 2006 (25 pages).

[2961] See Quantum Mind, Magnetic Body, and Biological Body by Matti Pitkanen, August 2018 (186 pages).

[2962] See TGD Universe as a conscious hologram, February 2018 (612 pages).

In the field of light-based therapy, one puzzling solution being sold comes from **Bioptron AG** (1988, Switzerland), part of **Zepter Group** (1986, Switzerland), since 1996. Its "Bioptron Quantum Hyperlight" uses "hyperpolarized light" generated with fullerene (C_{60}), a molecule also used by Archer for trap its electron spin qubits. Among other benefits, it treats injuries pain, avoiding pain killer drugs. So far, so good. The system generates some vertically linearly polarized light which passes through a filter containing these fullerene molecules which happen to rotate at a $1.8x10^{10}$ frequency per second. It creates "*perfectly ordered hyperpolarized light*" that is supposed to have some quantum properties similar to those of the biomolecules inside our bodies. Practically, this light is made of both vertically and horizontally polarized photons that "*without exaggeration, [...] reestablish the balance and harmony of energetic processes in biostructures and to harmonize cells, bringing them to back to their initial state of natural equilibrium*". Contrarily to many of the pseudo-quantum scams we'll cover later in this section, this offer is fairly well documented, even scientifically[2963]. You're flooded by tons of scientific information, historical references, links to Nobel prize inventions and scientific publications. But many indices generate serious doubts[2964]. Among others, it mentions these dubious Emoto's research on water structure and the way it can be changed with music and good mood.

Water memory

The last area on the fine line between science and charlatanism is that of water. It features a model of thought close to Roger Penrose's **Orch-OR** theory, which consists in explaining everything about life based on a few isolated physical phenomena at the microscopic level. The phenomenon of the **memory of water**, its explanation by **electromagnetism**, and parallel theories on the **water structure** are all mixed together.

One of the starting points around the role of water is **Jacques Benveniste**'s work on water memory. This immunology and allergies specialist was a director of an Inserm research laboratory in Clamart, France. He conducted experiments that led to the conclusion that "*water could preserve a memory, a print, of substances that have passed through it*". With Israeli, Italian and Canadian researchers, he published a landmark article in Nature in 1988, which was soon contested[2965]. He described a series of experiments that showed the effectiveness of anti-IgE (anti-immunoglobin E) causing the loss of histamine-containing granules by a type of white blood cell, basophilic cells, even when this anti-IgE is repeatedly diluted to the point where no anti-IgE molecule can be found in solution. For this to work, solutions must be shaken vigorously after each dilution, using the "dynamization" principle!

[2963] See the Bioptron Quantum Hyperlight brochure (60 pages) and Hyperpolarized light 2018 (318 pages) by Djuro Koruga.

[2964] Some are well documented in an extensive analysis, although a bit dated, in Cancer and the magic lamp, February 2009. It shows that most scientific surveys were of small scale and non audited and with no control group trials. It was done only on wounds healing. But the vendor web site touts many medical indications that their device is supposed to treat, without any scientific evidence, beyond wounds healing: osteoarthritis, arthroses, lowered motivation and the inability to feel happy. All are good indications, in the best case, of some placebo effect. On top of that, the Zepter also sells blue and red LED light therapy devices, for 500€. The Bioptron is priced at about 1000€.

[2965] See Human basophil degranulation triggered by very dilute antiserum against IgE, Jacques Benveniste et al, June 1988 (3 pages) and Ma vérité sur la mémoire de l'eau by Jacques Benveniste, 2005 (122 pages). The book contains a preface by the Nobel Prize winner Brian Josephson. In this book, published after his death in 2004, Jacques Benveniste recounts his experiences, his tumultuous relations with the medical mandarins over several decades, the story of the publication of his famous article in Nature in 1988 and other experiments conducted during the 1990s and early 2000s.

In the article, Benveniste hypothesized that the phenomenon could be explained by the creation of structured networks in water or by persistent electric or magnetic fields. They would constitute some sort of "water memory" which would "record" the allergen characteristics and reproduce its effects on basophilic cells. This was supposed to explain high dilutions used in homeopathy!

Therefore we propose that none of the starting molecules is present in the dilutions beyond the Avogadro limit and that specific information must have been transmitted during the dilution/shaking process. Water could act as a 'template' for the molecule, for example by an infinite hydrogen-bonded network[12], or electric and magnetic fields[13,14]. At present we can only speculate on the nature of the specific activity present in the highly diluted solutions. We can affirm that (1) this activity was established under stringent experimental conditions, such as

Figure 905: water memory key description in Benveniste's Nature paper. Source: Human basophil degranulation triggered by very dilute antiserum against IgE, Jacques Benveniste et al, June 1988 (3 pages).

The promoters of this empirical medicine devised by **Samuel Hahnemann** around 1810 and explained in the book "The Organon " thought they had finally found their scientific support.

Testing and evaluation protocols were flawed in many ways. Solutions were not analyzed by spectrographic analysis to deduce their molecular composition[2966]. Only electrophoresis was used to detect the presence of ions[2967]. The presence of histamine resulting from the release of granules from the basophiles had not been assessed.

It was realized in other experiments that there was none! Moreover, the phenomenon presented a cyclic character of a period of 8 dilutions (in Figure 906), according to the successive dilutions, but being out of phase by four dilutions from one experiment to another. No explanation is given for this cyclic phenomenon[2968]. The electromagnetic theory that would explain the phenomenon is his other Achilles' heel.

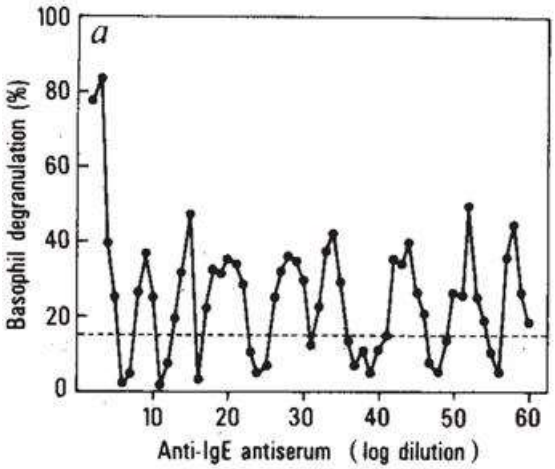


Figure 906: Source: Human basophil degranulation triggered by very dilute antiserum against IgE, Jacques Benveniste et al, June 1988 (3 pages).

It is weakly substantiated. These waves are not characterized, measured nor their source explained. The story of Jacques Benveniste is the story of a curious experimenter who lacks, however, the bases in adjacent disciplines around electromagnetism.

However, he did investigate long-range electromagnetic fields, inspired by the work of Italian physicists specialized in quantum electrodynamics, **Giuliano Preparata** (1942-2000) and **Emilio Del Giudice** (1940-2014). In 1990, he set up an experiment with the CNRS Central Laboratory of Magnetism in Meudon, France, which showed that the activity of the diluted solution is modified by prolonged exposure to a magnetic field. The experiment used animal hearts with an electrical apparatus invented by **Oskar Langendorff** (1853-1908). In another experiment carried out over several years, he also uses an amplifier using a sound card from a microcomputer to transmit the properties of a solution to another neutral liquid. This leads to the concept of "digital biology"[2969].

[2966] Raman spectrometry will be used in other experiments, much later from 2007, on various homeopathic strains.

[2967] At high dilutions, electrophoresis showed that there was no anti-IgG molecule left in the active ingredient.

[2968] Ironically, the process used does not prevent allergic reactions as is expected in homeopathy, which wants to treat evil with evil, but in low doses. Here the anti-IgE causes the production of histamine and does not prevent it. Some debunking came with "Memory of Water" Experiments Explained with No Role Assigned to Water: Pattern Expectation after Classical Conditioning of the Experimenter by Francis Beauvais, 2018 (20 pages).

[2969] This story is well told in L'âme des molécules, une histoire de la mémoire de l'eau by Francis Beauvais, 2007 (626 pages). The author was one of Jacques Benveniste's experimenters.

After the death of Jacques Benveniste in 2004, his work was taken over by **Luc Montagnier** (1932-2022, French), who created the first AIDS treatment and got the Nobel Prize in medicine in 2008. He described low frequency waves (7 Hz) that would be emitted by DNA strands. He set up an experiment in which the waves of DNA molecules are transmitted through a coil fed at 7 Hz to pure water in another test tube. A PCR is then used to regenerate the DNA in this test tube (DNA multiplication process, "polymerase chain reaction").

And gel electrophoresis is used to decode the replicated DNA! In the experiment, this DNA corresponds exactly to the original DNA. His code would have been transmitted by electromagnetic wave[2970]. But the documentation does not specify which DNA was used as a primer for PCR! Indeed, a PCR does not start from zero and a bunch of nucleotides, but uses DNA strands to replicate them[2971]. The work of Luc Montagnier is related to that of the Italian **Emilio Del Giudice**, again, on the structure of liquid water[2972]. It will not surprise you to learn that this kind of discovery is rather controversial among specialists[2973].

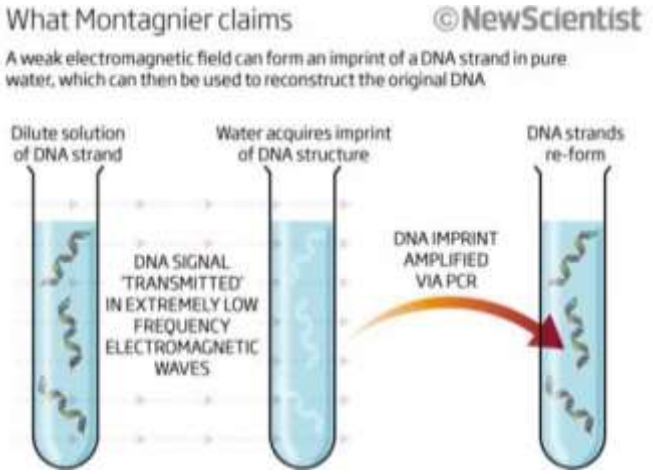


Figure 907: Montagnier claimed DNA could be created in water containing just... water molecules. How did carbon, phosphorus and nitrogen atoms appear? Source: NewScientist.

And Luc Montagnier's publication was not made in a peer-reviewed journal. But he continues to publish, with international teams, on interesting research explaining by the quantum field theory how DNA polymerase works[2974]. The relationship between water and quantum physics is being emulated by others and drove the creation of many scams selling structured water and the likes[2975].

Konstantin Korotkov (Russia) did some experiments supposed to show that projecting negative emotions on water reduced its energy level and vice versa[2976]. This guy created IUMAB (International Union of Medical and Applied Bioelectrography), an organization that promotes the use of bioelectrography devices[2977]. He is promoting DGV Bio Well cameras, aura detection systems around patients that would materialize the chakras, via the analysis of the "gas discharge".

[2970] See explanations in Luc Montagnier's article DNA waves and water, January 2010 (10 pages). Montagnier and the quantum teleportation of DNA by Vincent Verschoore, January 2011, is the source of the illustration.

[2971] This PCR problem is noted in The Nobel disease meets DNA teleportation and homeopathy, January 2011.

[2972] See Mae-Wan Ho's Illuminating Water and Life, 2014 (18 pages) which describes the theories of Emilio Del Giudice, who died that same year.

[2973] See Luc Montagnier and the Nobel Disease by David Gorski, June 2012.

[2974] See Water Bridging Dynamics of Polymerase Chain Reaction in the Gauge Theory Paradigm of Quantum Fields by Luc Montagnier et al, 2018 (18 pages).

[2975] See Hypotheses quantum of mechanism of action of high homeopathic dilutions, is a doctoral thesis by Mathieu Palluel, 2017 (252 pages). Its first part is a fairly well-supplied history of homeopathy. It also covers the experiences of Jacques Benveniste and Luc Montagnier. The quantum part starts on page 181 and is quite weak. This PhD student was definitely not a physicist. He makes a countersense on Schrödinger's equation on page 189. He uses quantum field theory and quantum electrodynamics in a weird context, water at room temperature. On page 201, the paper states that water molecules have a diameter of approximately 3 nm while it is 0.27 nm. It also talks on page 221 about the Nobel Prize of "Serge Laroche" instead of Serge Haroche. In short, this thesis document was poorly reviewed by the people who validated it, and who were not at all up to date in quantum physics.

[2976] See The First Korotkov Intention Experiment by Konstantin Korotkov, January 2018 as well as The Intention Experiment on H2O, 2007 (18 pages) which reproduced his experiments in the USA.

[2977] He is also the author of The Emerging Science of Water: Water Science in the XXIst Century by Vladimir Voeikov and Konstantin Korotkov, 2018 (253 pages), a work or current of thought that certainly influenced Marc Henry's work, unless the opposite is true.

Figure 908: Bio-Well measure human energy using bio-electrography, inspired by Konstantin Korotkov. These are clearly scams.

We then have **Mazaru Emoto**'s MRA (Magnetic Resonance Analyzer) (1943-2014). He conducted experiments analyzing the impact of emotions on the structure of water. Experiments that were never reproduced independently[2978]. You probably guessed it!

OK, emotions can generate infrared waves and gases that can be exhaled, producing in turn a minute reaction on exposed water[2979]. This makes it possible to sell a concentrated structured water that can be used to prepare distilled water, **Indigo Water** (*opposite*, source). Here is the description: "*A geometrically perfect water with the "Message" your body is waiting to receive. Dr. Emoto's Indigo Water contains eight ounces of highly charged hexagonally structured concentrate. By mixing one ounce of concentrate with one gallon of distilled water, you are creating eight gallons of structured water from this 8 ounce Indigo water. This is about a one month supply of structured water*". For $35. By the way, it doesn't mention if it's drinking water or shower water!

The delirium continues with the structured water of **Rustum Roy** (American). Structured water is said to be an antibiotic: "*One molecule of structured water in 100 million molecules of drinking water can destroy all germs present in a wound. The American army has used this water in Iraq and Afghanistan. Obama uses structured water to wash his hands*". Verification made, the only example that can be found is the healing of a foot wound and it's water associated with money[2980]. And how can we restructure water, so to speak? Simple: by heating it, with vortexes, magnetic fields, music, the force of thought, "frequencies" or minerals!

The concept of wormholes comes from the astronomer **Nicolaï Kosyrev** (1905-1983) who discovered lunar volcanism and the biologist **Rupert Sheldrake** (1942), who became an expert in telepathy. This led to **Vodaflor**'s Voda vortexors which generate vortexes in water to structure it with models ranging from 936€ to 3300€ depending on the desired water structuring rate.

More recently, the discourse around the benefits of water in homeopathy was renewed with the integration of quantum electrodynamics as an explanatory feature. Why not, since almost nobody can understand anything about it, except the few physicists in this domain[2981]. Not to mention the lack of

---

[2978] This is well explained in The pseudoscience of creating beautiful (or ugly) water by William Reville, 2011. See also the site Structure-altered water nonsense which makes a good inventory of commercial offers of structure water in the USA. The 1995 style layout serves the site but the inventory of solutions is edifying. Masaru Emoto also certified an effect of exposing zam zam water that is produced at Mecca to Quran. The water is supposed to have similar miraculous effects, a bit like Lourdes' water in France.

[2979] See The experiments of Masaru Emoto with emotional imprinting of water, 2018 (11 pages).

[2980] In Ultradilute Ag-Aquasols with extraordinary bactericidal properties : the role of the system Ag-O-H2O, 2006 (13 pages). Rustum Roy is also the author of The Structure Of Liquid Water; Novel Insights From Materials Research; Potential Relevance To Homeopathy by Rustum Roy, 2009 (33 pages).

[2981] See Explaining Homeopathy With Quantum Electrodynamics by Antonio Manzalini and Bruno Galeazzi, 2018.

experimental protocols to verify anything. Again, we are confronting a fake science because it cannot be refuted[2982]!

The structured water business has evolved a little. Instead of selling structured water, some companies are now selling bottles that create this structured water with regular water. It is just a bottle, or sometimes contains a blender. Gullibles can buy it for about $60 on Amazon.

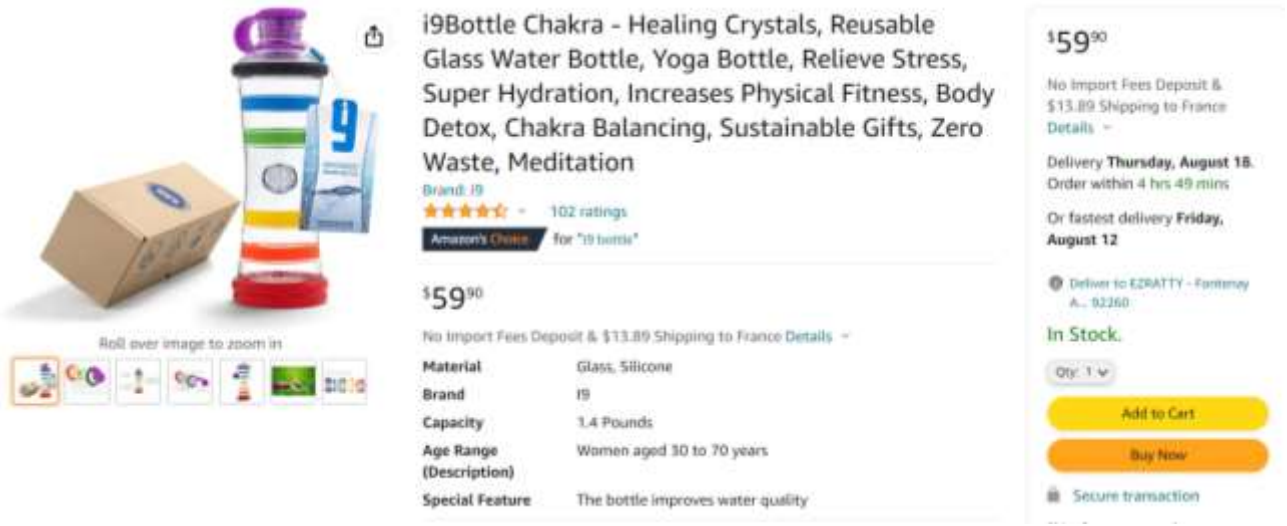


Figure 909: you can buy plastic bottles that will structure your drinking water. It's even not a thermos!

To conclude this part before moving on to the most beautiful scams of pseudo-quantum medicine, let us recall that there is a fine line between low-level science and its high-level interpretation, especially when it is then exploited by unscrupulous entrepreneurs.

And we're not done finding more of the same such as some weird quantum behavior of water in carbon nanotubes[2983], superconductivity in the brain[2984] or other elucubrations on quantum cognition[2985]. This will undoubtedly fuel new waves of quantum mysticism!

Quantum medicine

As Wikipedia's quantum healing page on quantum medicine points out, this discipline misuses the jargon of quantum physics to make people believe in magical cures for certain pathologies that traditional medicine, well or badly practiced, cannot treat properly[2986]. The phenomenon is already over a decade old.

Method for detecting false science

The methods used to promote false quantum science in health (and in general for that matter) are easily detectable to an educated person, or just with some common sense:

- It starts with some **scientific statement** associating very quickly humanities and biology and making approximate shortcuts on quantum physics.

[2982] Fortunately, some scientists address this nonsense, such as L'homéopathie confrontée à la physique by Alain Bonnier, 2014 (34 pages), which dismantles homeopathy in a very didactic way, relying in particular on Planck's constant.

[2983] See Evidence of a new quantum state of nano-confined water by G. F. Reiter et al, 2011 (5 pages).

[2984] See Possible superconductivity in brain by P. Mikheenko, 2018 (10 pages).

[2985] See What is quantum cognition? Physics theory could predict human behavior by Nicoletta Lanese, January 2020.

[2986] These methods are also well described in Richard Monvoisin's Quantox - Ideological Misuses of Quantum Mechanics, published in 2013 (in French).

- The solutions are being promoted with some **esoteric jargon** using unprecise terms like wave, matter, vibration, vortex and energy[2987].
- When they exist, **tests are performed with small samples** that are not statistically representative. The arguments are often based on non-verifiable anecdotes. The miraculous healings observed in Lourdes, France, are even better documented and, moreover, as probable as those occurring in the hospital environment[2988], i.e., between 1/350,000 and 1/100,000 cases.
- Many specialists sell various, rather expensive, **healing materials or devices**, not considered as medical devices, and whose effectiveness is clearly related to the placebo effect.
- These solution's marketing target **vulnerable people** (sick, elderly, etc.). It can be seen in the media used for advertising it.
- The **vague side of the pathologies covered**. Some are related to pain management or to what can be treated by placebo effect, such as psychonomy [2989]. Others target all the major pathologies of the moment: chronic diseases, cancers and in some cases even neurodegenerative diseases.
- **Extended resumes** with impressive diplomas and scientific guarantees to be taken with a grain of salt for many quantum medicine specialists. There are even "diploma mills" in the USA, where you can buy a doctorate in medicine or another junk discipline at a reasonable price. A bit like in the late Trump University.
- Rare **scientific publications** and when they exist, rarely published in peer-reviewed journals, knowing that this validation is already not enough to be a guarantee of seriousness. These therefore become "private" publications. Or it can't be falsified, like with this paper on quantum immortality that is based on a mathematical approach the many-worlds interpretation[2990].
- Some **conspiracy theories** about the pharmaceutical companies lobbying and other healthcare professionals who will do anything to prevent alternative solutions from emerging.

Nonetheless, there are positive comments from readers of these books that show that the market for gogos is a thriving one. It takes place in a context of loss of confidence in politics, media and science and the development of many conspiracy theories, fueled by the fluidity of the Internet and social networks.

Quantum medicine marketing

Let's review some of the reference books that promote this curious quantum medicine.

Quantum Healing by Deepak Chopra (1988) seems to be foundational. It comes from a former endocrinologist. He became an Ayurvedic practitioner, coming from traditional Indian medicine. According to him, quantum thinking explains some cases of psychosomatic healings that resemble self-healing. The author is a star in the field, especially in India and the USA, with a total book sales of over 10 million copies and a personal fortune estimated at over $80M[2991]. The content of his works

---

[2987] You find a marvelous example with the Quantum Field Medicine web site that consolidates all these fancy alternative quantum medicines, mostly all based on placebo effect. You have consciousness awareness techniques, acupuncture, homeopathy, electro-magnetic resonance, Timewaver (another electrical product scam), color and light therapy and sound/music therapy.

[2988] See Miracles de Lourdes, Charlatans.info, March 2022.

[2989] Which is yet another false science associating mind and body.

[2990] See Theoretical Quantum Immortality and its Mathematical Authority by Ce Han, February 2021 (8 pages).

[2991] See Alternative medicine is not medicine by Joel Gottsegen, Stanford Daily, October 2014.

is of course quite weak scientific speaking, especially when he deals with quantum physics, mostly in metaphorical terms[2992]. Of course, all of this is plain bullshit and has been debunked[2993].

Amit Goswami's **The Quantum Doctor** (2004) is along the lines of Deepak Chopra's theories. The author is an Indo-American physics teacher who practiced in Oregon between 1968 and 1997, but in nuclear physics. He defines himself as a quantum activist who even has his own Quantum University which seems to be to healthcare what Trump University was to business schools. According to him, quantum activism through consciousness can save civilization. He also demonstrates scientifically (!) the existence of God by building upon Deepak Chopra's consciousness of the Universe thesis. In his work, he explains the therapeutic effectiveness of "integral medicine" which combines allopathic medicine and more or less soft, alternative and traditional medicines, particularly Indian and Chinese. But god's existence can also be proven with some laser beams[2994]!

The scientific content of the book fits on a tiny postage stamp. It looks even like a giant quantum joke. The idea is the following: your organs are born in good health. A time passes, like a qubit would become after a Hadamard gate, it becomes superposed in good and bad health. Then, with the strength of your consciousness, you could provoke a quantum wave function collapse of your organs into the health version. That simple! It's a scam version of this poor Schrödinger's cat.

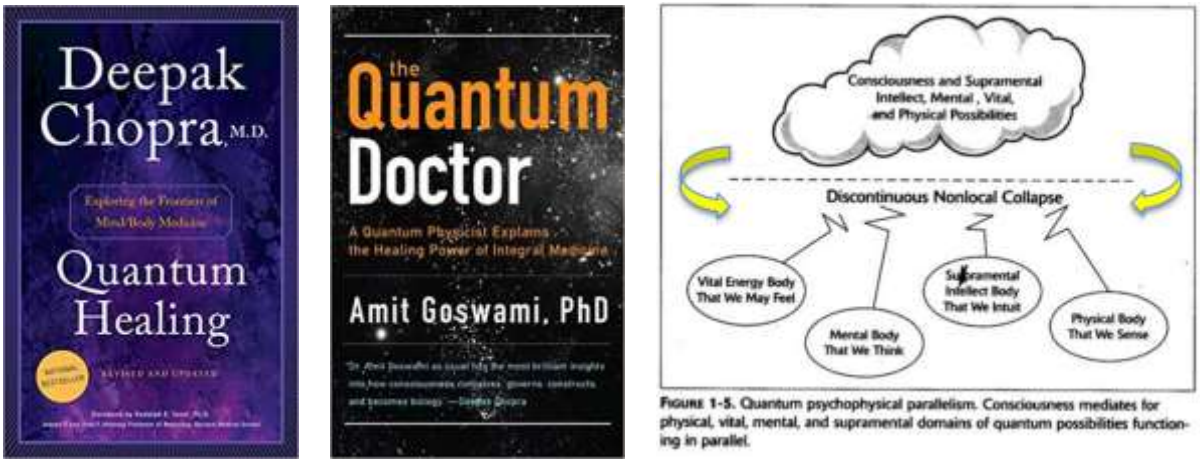


Figure 910: Deepak Chopra and Amit Goswami are promoting a quantum medicine with no scientific content. At best, it's placebo.

[2992] On this subject, I watched the enlightening debate between Deepak Chopra and Richard Dawkins (Mexico, 2013, 1h13) which highlights the difficulty of reconciling Chopra's emotional and symbolic approach with Dawkins' rationalist and scientific approach. At one point, the debate focuses on the supposed Universe intelligence that exists according to Chopra and at all levels, from elementary particles to the entire Universe. While this makes no sense to Dawkins beyond biological beings with brains, or computers imitating them. It is a homothetic debate with the link between consciousness and the pathologies that consciousness would or would not necessarily control. The other interesting part of this debate concerns the notion of quantum leap on the appearance of language or certain biological evolutions that are a view of the mind for Richard Dawkins. The latter even denounces Chopra's "deliberate obscurantism". For Richard Dawkins, consciousness is explained or will be explained by neuroscience and certainly not by Deepak Chopra's meta-consciousness galimatias.

[2993] Chopra's discourse has been thoroughly debunked in Problems of Deepak Chopra's discourse: a metalinguistic analysis of "Quantum Healing" by Caderno Brasileiro de Ensino de Física, December 2021 (29 pages). He was also awarded the "Ig Nobel prize" in 1998 "*for his unique interpretation of quantum physics as it applies to life, liberty, and the pursuit of economic happiness*".

[2994] See Interference of Two Independent Laser Beams – Scientific Evidence of God by Henok Tadesse, December 2021 (5 pages). Published on viXra!

The work also seeks to explain the effects and precepts of oriental medicines (chakras, reincarnation, ayurvedic medicine, acupuncture)[2995]. Here are a few selected excepts with the "*morphogenetic fields of the vital body*", "*when the mind creates the disease, sometimes healing is impossible to achieve on the mind level. One must then make a quantum leap to the supramental to heal*" or "*quantum collapse is also fundamentally non-local. Therefore, the non-locality of healing, as in healing through prayer, finds a clear explanation within the framework of quantum thinking*". With quantum entanglement, one can relate everything to everything and explain everything.

Amit Goswami mentions distant healings through prayer by referring to an experiment by physicist **Randolph Byrd** in 1988. The statistical representation was very weak with 6 healings out of 26 patients of not well specified cardiac pathologies. It may not surprise you to find out that it was demonstrated that prayers did not have any large-scale effects[2996].

He also quotes the telepathy experiment of **Jacobo Grinberg-Zylberbaum** (Mexico)[2997]. It involved measuring EEG waves on a participant to assess the impact on him of a flash of light arriving on one of the participants, both of whom were in Faraday cages. The experiment was repeated later between 2000 and 2004 using MRI[2998].

A small technical detail: there cannot be any radio waves transmission between the participants who are in Faraday cages, no photon either, nor particles with a common history in the brain of the participants.

Others have a slightly more scientific view of the quantum nature of consciousness, such as **Ervin Laszlo**, even if the latter relies a bit too much on quantum entanglement in his explanations[2999].

Other pseudo-scientists promote fancy theories related to the so-called quantum medicine.

James Oschman (USA) promotes a concept of life energy, based on electric currents and water related quantum phenomenon. He invented the concept of perineural brain cells, which are obviously only the glial cells that surround neurons, but with a different name and which generate energy that goes to the hands[3000].

Kiran Schmidt is a German who does "information medicine". He also promotes strange machines that are supposed to cure everything, especially under the brand **Inergetix CoRe**.

Nassim Haramein deals with the energy of creation and also water memory. He is selling fancy products through his Resonance Science Foundation. The starting point? Some work on his unified field theory, an old Holy Grail of fundamental physics[3001]. This scientist thinks he has discovered an infinite source of energy. Of course, none of the work of this "scientist" was validated by his peers.

[2995] Illustration source: Messengers and Messages-then, now, and yet to come (15 pages).

[2996] See Studies on intercessory prayer, Wikipedia.

[2997] Documented in The Einstein-Podolsky-Rosen Paradox in the Brain: The Transferred Potential, 1994 (7 pages).

[2998] See details and results.

[2999] In Why Your Brain Is A Quantum Computer, 2010. This thesis is partly deconstructed in The Myth of Quantum Consciousness, 2002 (19 pages), although it is an earlier work.

[3000] He is the author of Energy Medicine, James L. Oschman, 2000.

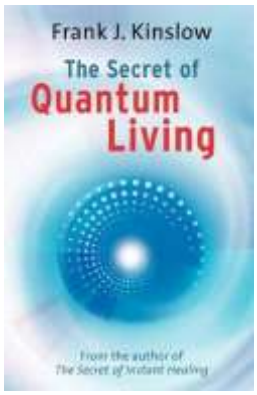
[3001] His list of scientific publications deals with neutrons and protons. A part of the articles have been published in the journal Neuro Quantology which is not considered as being serious and whose review committee does not include any scientist in quantum physics or neuroscience. This publication process is known and exists in other fields such as medicine.

This guru markets ARK crystals, which are magical crystals that heal or improve the performance of athletes. They even publish a study on how to improve athlete performances. It used a double-blind method with a placebo effect for half of the test subjects. Given the study involved only 10 athletes, 5 men and 5 women, with progress of about 10%, thus within the margin of error of the sample. The study was done by the Energy Medicine Research Institute laboratory, versed in studies of fancy products such as LifeWave placebos marketed in a Tupperware-style pyramidal model.

Figure 911: there's no science in ARK crystals, it's a scam.

These crystals would also help accelerate plant growth! Prices range from 277€ to 1850€. This is part of a trend in the sale of magic crystals that dates from a few years ago and where the offer is pletho-ric[3002].

Frank J. Kinslow's **The Secret of Quantum Healing** (2011) introduces the notion of "Quantum Training", a "*scientific, fast and effective* method that *reduces pain and promotes healing"*. In a few words, it is about having your consciousness send vibratory waves to your organs to heal them. By the play of interferences, they will cancel the evil.



Another Schrödinger's cat trick with the application of the quantum mechanics of the pico (elementary particles) to the macro (the organs). It is mainly aimed at physical and emotional pain. It is a variant of meditation. It should be avoided for the treatment of hypothyroidism or about anything else by the way!

This kind of work has the particularity of always being very vague on the notion of pathology treated, especially if a pseudo-medical apparatus is involved, as is the case here. Even if the "Quantum Training" is supposed to work remotely.

Quantum Intronic Medicine from Christian Daniel Assoun deals with quantum biology. It is a form of epigenetic treatise describing DNA memory by quantum mechanics. According to him, "*WATER is the first quantum liquid: its current state is liquid* whereas *its state should be gaseous".* This book describes the presence of a third DNA catenary in the form of physical plasma (hydrogen)[3003]. He states that his "*work is currently focused on the INTRONIC parts which represent 95% of our DNA and which are unfairly classified as silent or even useless".* Intronic is used in the sense of DNA "introns", the part of DNA genes that is transcribed into RNA when the genes are expressed.

[3002] See Dark crystals: the brutal reality behind a booming wellness craze by Tess McClure dans The Guardian, September 2019, A Cynic's Search for the Truth About Healing Crystals by Katherine Gillespie in Vice, September 2017 and The Sickening Business of Wellness by Yvette d'Entremont, December 2016. Those guys also promote the water memory theory. See Does Water Have Memory?, ArkCrystals, July 2021.

[3003] Ebook downloadable here. It is also documented in The 3rd Strand (or 3rd Catenary) of DNA by the same author and which dates from 2011/2012.

These are eliminated during splicing which generates mature RNA that will then be used in the ribosomes to make proteins. In fact, introns represent only 25% of human DNA. The rest, about 73%, corresponds to sequences that are effectively non-coding in the DNA of our chromosomes, but whose role in the regulation of genes is progressively revealed with research. Exons, the coding part of genes, represent 1.5% of human DNA (source).

Christian Daniel Assoun believes that DNA could be strengthened with "the *help of new tetravalent elements such as Germanium or Silicon (reverse optoquantic properties)*". Why germanium and silicon? Because they are in the same column of Mendeleev's table as carbon with four free electrons. This is a good idea for creating extraterrestrial life. So why didn't life on Earth use silicon, which is as abundant as carbon? One of the reasons is that silicon oxide (SiO_2) is inert and solid while carbon oxides (CO, CO_2) are gaseous and therefore more easily recombinable with other atoms and molecules. Also, carbon is more abundant than silicon on the surface of the Earth.

Christian Daniel Assoun is also the founder of the **Glycan Group**, in 1996, a company selling organic silicon for various uses and notably as a food supplement. Their subsidiary Glycan Pharma was struck off the commercial register in 2012. The company is in competition with Silicium Espana, a company linked to Loic Le Ribault, who died in 2007, who was also passionate about organic silicon. The two companies had a legal dispute in 2011 over the use of the G5 trademark.

At last, you also can count on the many books on Transurfing by **Vadim Zeland** who introduces himself as a physicist. This quantum model of personal development is based on the idea that "*When the parameters of mental energy change, the organism moves to another lifeline. When the parameters of mental energy change, the organism moves towards another life line*". So be it!

Scalar wave generators

The best of the quantum medicine scams are the **scalar wave generators**. These are electromagnetic waves associating a supposedly horizontally polarized electro-magnetic wave and another vertically polarized wave of the same frequency but 90° or a quarter wavelength out of phase.

Scalar waves were initially promoted by a certain **Thomas Bearden** in the USA as well as by the Russian **Sergei Koltsov** with his Functional State Correctors (CEF[3004]). Bearden explains this in a 1991 interview. He had also invented a **MEG** (Motionless Electromagnetic Generator) capable of extracting free energy from the vacuum and thus, of generating more energy than it consumed. A product that has of course never been commercialized.

Scalar waves were also promoted by a German scientist, **Konstantin Meyl**, with a paper that had to later be retracted[3005]. The general public propaganda on scalar waves is a big fantasy and always linked to alternative medicine literature. These waves would come from the Sun with neutrinos and have no energy loss over distance. The brain is supposed to produce and sense scalar waves with its own interferometer. It would explain telepathy and other paranormal effects. Well well.

[3004] Watch this video Functional State Correctors (FCS) - Koltsov Plates, 2014 (55 minutes) which is a good digest of any scientific theory.

[3005] See "Way out there" paper claiming to merge physics and biology retracted, RetractedWatch 2013 and Scalar Wave Transponder device by Konstantin Meyl, 2005 (70 pages).

Scalar waves would also make it possible to treat diabetes (I or II? Who cares...), kidney stones, Parkinson's disease, heart attacks, osteoarthritis, cancer and also aging. As for type I diabetes, which is linked to the autoimmune destruction of beta cells of the islets of Langherans in the pancreas, it is not clear how waves of any kind would bring dead cells back to life. The proposed solution?

Scalar wave generators such as the **INDEL** at 8820€. Given its price, it targets professionals in a kind of Ponzi model. This generator produces a scalar wave field with a voltage of 2V. It also includes a music modulation accessory for therapy practices and wellness centers. It is also available at **QuWave**.

Figure 912: scalar waves cost a lot and do nothing.

You can also (not safely) rely on the **ETHX-SCIO Biofeedback** from William Nelson, which combines global therapies and advanced quantum physics (in Figure 912). The device scans the body on 10,400 different frequencies to detect many pathologies. It then rebalances the body's energy with quantum biofeedback. The toy also runs 200 biofeedback therapies with the world's largest health software that integrates Western and Eastern philosophies[3006]. The EPFX-SCIO includes a wave diffuser box, connected to the patient with sensors attached to his ankles, wrists and skull. One could almost do both an EEG and an ECG with it! All this for getting some placebo!

Figure 913: SCIO Biofeedback is not better.

In the scam devices category, you also find the **Healy** and its bioresonance features using some electrodes and supposed to cure many illnesses[3007]. At best, it can be a temporary pain killer. Another device, the **TimeWaver**, is based on "quantum field theory" from a certain Burkhard Heim (1925 - 2001, German) on the 12-dimensional composition of the universe where "*the light quantum effect communicates mainly with the Global Information field (GIF) i.e. at a nonenergetic, non-phenomenal and therefore more causative level*". It looks like a biofeedback device similar to the one above. Burkhard Heim did try to unify all quantum theories but he was neither a Dirac or a Feynman[3008]! The TimeWaver site also mentions of **Kozyrev mirrors** using cylindrical aluminum sheets that were used for extrasensory perception experiments in Russia. But it doesn't seem to be involved in the TimeWaver device.

Other various Russian 'quantum' scientists, dead or alive, are frequently used in support of these scam devices like Nikolai Kozyrev, Vlail Kaznacheev or Alexander Trofimov. When you look at their biographies online, you quickly find that they were not at all mainstream quantum scientists. This is all full of esoterism, not science.

[3006] See How one man's invention is part of a growing worldwide scam that snares the desperate ill.

[3007] See A Skeptical Look at the Healy "Bioresonance" Device by Stephen Barrett, July 2020.

[3008] See TimeWaver System website. They hopefully have a: « *Disclaimer: Science and conventional medicine does not acknowledge the existence of information fields their medical and other important TimeWaver systems and their applications due to lack of scientific evidence. The said application is based on, treatment options, experiences and anecdotal reports from the practice*".

Quantum medallions

Quantum medallions for smartphones have become commonplace for several years and target another phobia, electromagnetic waves and 5G. This is the case of **Quantum Science**'s Quantum Shield medallions (on Amazon and Alibaba). One also finds some in the form of USB keys **5G BioShield** which contain a "*quantum holographic catalyst*".

Figure 914: quantum medallions and 5G quantum keys are fancy gadgets for the gullible. That's a huge market!

It is obviously a huge quantum bullshit of the first kind. It is accompanied by a scientific justification that is not worth a lot of money[3009]. The American FTC has flagged these products as vulgar scams[3010]. It was even later discovered that some of these medallions were radioactive due to their component metals. And worn on a long period of time, they could actually be dangerous[3011].

In the field of wacky quantum devices, let's finish with the **Quantum 5 Ozone Generator** using Neos Technology from the **Longevity Resources** (sources). It uses a quartz electrode. It's supposed to help purify indoor air. There is one major drawback: ozone can also be toxic to the human body and cause respiratory problems. It can also affect plants health. In short, quantum medicine may one day emerge in the wake of scientific discoveries, but the ones proposed today is for the time being full blown charlatanism.

Figure 915: a quantum ozone generator to purify indoor air. It may work but it is not quantum.

They have the advantage of generating at least a placebo effect for users and filling the wallets of their promoters. Except that this can be dangerous if the placebo effect is used instead of a traditional treatment that is essential to stay alive.

I will not, however, trash all the techniques and approaches mentioned here. Some may make sense, even though there is still a lack of both a scientific corpus and more solid evidence to support them. But most are fake sciences and are quite easily detectable.

Quantum skin care

I discovered the scam category of **quantum cosmetics products**, coming mainly from China that was mentioned in a 2022 Rand Corporation on China and the USA investments in quantum technologies. In it, Jian-Wei Pan is said to have criticized companies claiming to sell "quantum skin care" products in China[3012].

QUANTUM
FACIAL AESTHETICS

Let's make a roundup of these scams. We have for example a Quantum Health Super Lysine+ Cold-Stick sold on Amazon, Energecia Quantum Beauty sells quantacosmetics bullshit stuff, BioEqua sells energized nanospray skin care, probably with stirred magic water, Age Well Fundamentals sells Phyto5 quantum energy facial skin care that balances the energy vitals and is made in Switzerland

---

[3009] See "Aton" True Cell, Atom and Particle Concept by Ilija Lakicevic, 2019 (8 pages).

[3010] See Cell Phone Radiation Scams, 2011.

[3011] See Anti-5G "quantum pendants" are radioactive by Jennifer Ouellette, ArsTechnica, December 2021.

[3012] See An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology by Edward Parker, Rand Corporation, February 2022 (140 pages).

(but not at ETH Zurich), Quantum Botanika, Halcyon Skin Care, Ratzilla Cosme, Quantum Aestetics, Quantum Life and Igesto. In the same vein, Boiron is selling X-ray homeopathy products for curing skin rash. You read it well!

Quantum management

Quantum management is a new and fashionable practice that seeks to draw inspiration from the general principles of quantum mechanics. Its practitioners are frequently followers of more or less occult sciences who have converted to target corporate markets that are more financially attractive than consumer markets. The vulnerability of educated executives and managers to the most outlandish proposals is always amazing.

However, we can indeed identify many analogies between quantum physics and management in the broadest sense of the term. For this purpose, I have pushed the envelope and reused advanced quantum physics fundamentals and applied it to your usual business life. Any resemblance with a real-life situation would be totally fortuitous or entirely intentional, as you will guess[3013]. As a warning, I must precise that all of this is not serious at all. It is a way to make fun of many things, both the various gurus using quantum physics in scams and, also, life in the enterprise.

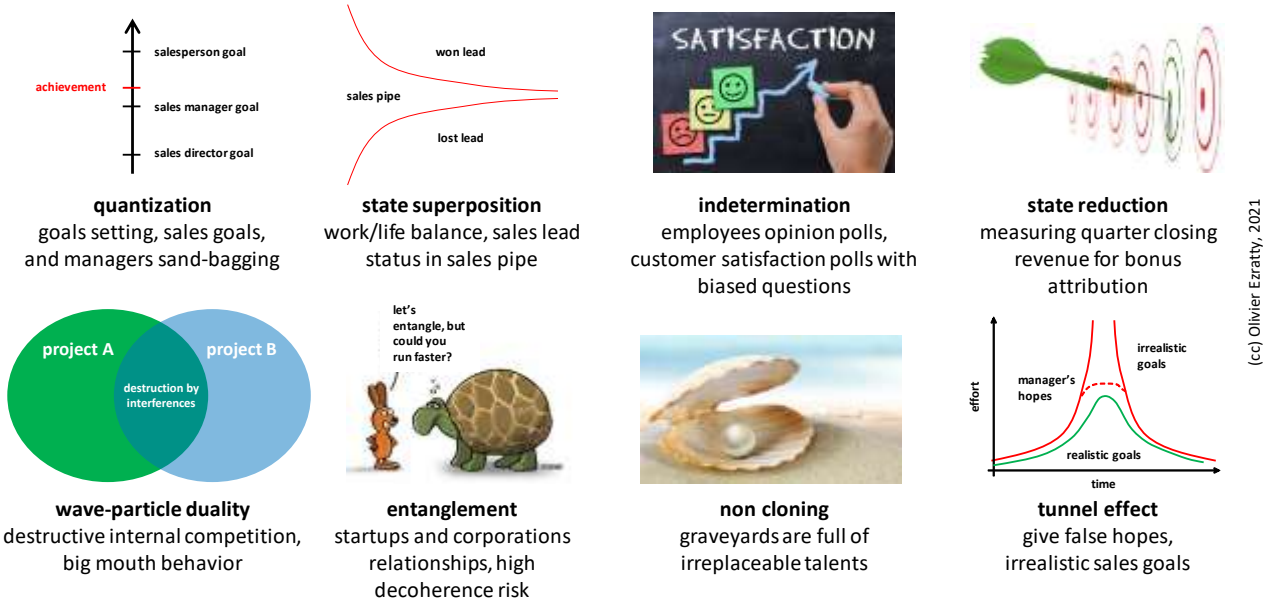


Figure 916: my useless framework for quantum management. (cc) Olivier Ezratty, 2022.

Quantization means that certain physical values can only be very precise, discontinuous and not arbitrary, like the energy levels of a hydrogen atom. After all, an employee is just a cell in a spreadsheet. He's there one day and gone the next. Workforce management is indeed quantum. A company's workforce at a given time is a discrete integer number.

But if we average it over a period of time, taking into account departures during the period, part-time employees, fixed-term contracts, apprenticeships, subcontractors and people whose real activity we are not sure of, it is no longer an integer but a number of FTEs (full time employees) or FTEs (full time equivalents) that is at least a sum of fractions. Fortunately, it is never a complex number and one escapes Hilbert's spaces to represent them.

[3013] I didn't rely on the proposal in Toward a Quantum Theory of Humor by Liane Gabora and Kirsty Kitto, January 2017 (10 pages) that is quite poor in its scientific and mathematical content.

Quantization also manifests itself with sand bagging, when a sales manager is distributing his own sales goals to his team by adding a quantum margin of safety. The last link in the chain, the unfortunate poor salesperson, will be assigned a goal that is greater than that of all the layers of management above. Only certain layers of sales management have this flexibility. The end result is that salespersons become Rydberg state atoms: they are excited with a very high level of energy and they sometimes burn out. This system is designed so that the base salesperson does not reach his or her objective and is penalized on the bonus side, unlike managers above him or her. Particularly if you want to fire him or her. Judgment about individuals is also subject to quantization. A person is often smart or nice, or a total moron. Personal judgments are rarely nuanced in grey. Yet, in a purist application of quantum physics, this kind of judgment should be a more vague and subtle wave function, until you measure it during a stressful experience.

The top of quantization? Those nasty Internet popups where the given choice is "OK" or "Later". For the quantum measurement guru, it's a real-life example of an exaggerated POVM (see Glossary).

Superposition is very common in business. For example, thanks to smartphones and other laptops, employees are kept both at work and in their personal lives all day long. It can also manifest itself in regulatory compliance, which is variable geometry in many companies. And then, of course, in the application of the company values defined in Powerpoint slides and rehashed by managers or the HR department. States superposition also manifests itself in the evaluation of leads that are closed or not in a sales pipeline. They are usually assigned a closing rate which is an amplitude and phase $|\psi\rangle$ until it is known whether the deal is lost or won, which is like the wave-packet collapse happening with quantum measurement, on a basis state $|0\rangle$ or $|1\rangle$. This collapse also occurs if an external event creates a lead quantum state decoherence. For example, a competitor who wins the deal under the nose of the salesman. This quantum analogy, however, will not help you improve your sales pipe closing rate.

Indeterminacy works with the measurement of employee satisfaction, where the measuring tool always influences the quantity to be measured. This is true as well in the questions asked in opinion polls, which are often oriented. More generally, the measurement of any parameter in a company by a consulting firm like McKinsey, particularly during an audit, will probably lead to changes in the measured quantities (e.g., downsizing, management change, reorganization and the likes). You just hope that your enterprise won't become a planar wave afterwards.

One variation of Heisenberg's principle of indeterminacy is that one cannot accurately measure both the position and velocity of a particle. The analogy in business would be the observation of a growing startup: by the time one understands where it is at a given moment, it has already changed its situation (headquarters, staff, CEO, turnover, M&A, company name, product, done a pivot). This is why it takes an infinite amount of energy to create an up-to-date startup base in one country or worldwide, even with only quantum technologies startups. So, thank you Crunchbase for the effort!

Measurement is in line with the history of quantization when measuring revenue at the end of a fiscal quarter. In this case, one is obliged to provide numbers and not to rely on some closing rates fuzzy logic. If only to determine the bonuses of sales representatives. Otherwise, Bill Gates said loud and clear in 1997 that "*bad news should travel fast in efficient companies*". But not too fast my dear, otherwise you'll get fired. That's what is called a non self-destructive measurement.

Wave-particle duality manifests itself with real people in companies who work on competing projects and happily annihilate each other. It is the phenomenon of interference linked to the waveform aspect of each and every projects! You also have the loudmouthed managers facing their teams (thus, in the state of a solid particles) who turn into wipes in front of their own management (thus, in the state of very low-energy waves).

This behavioral duality is also often observed with irascible managers who become docile sheep once at home, or who fail to properly educate their children. Can a trendy startup Chief Happiness Officer be quantum? In any case, this person must fight on a daily basis against a universal phenomenon: a good number of passions quickly fade with time, such as the amplitude of a Rabi oscillation, which is commonly observed in quantum physics and is related to superconducting qubit decoherence (Figure 917).

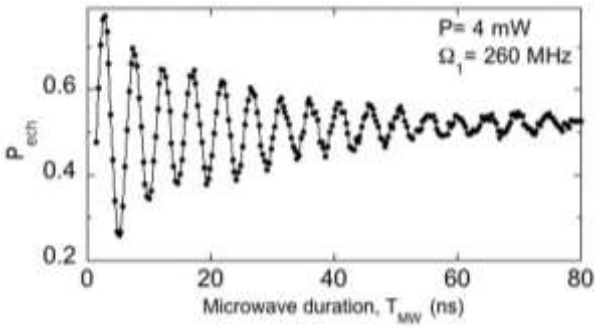


Figure 917: the Rabi oscillation of your motivation over time.

The Doppler effect also allows to indirectly put an end to a messed-up project with light, for example, via a well-managed leak in the media. Remember Theranos?

Entanglement applies to startups that are integrated into the open innovation programs of large companies. Everything goes well until the appearance of decoherence between the startup and the corporation! I create a product and you want a customized solution, I need speed and you're too slow, etc!

Entanglement also occurs with the teleportation of rumors faster than light. It is also known that the coherence time of qubits is linked to their good physical, magnetic and vacuum insulation, often at very low temperature, in order to avoid any external disturbance. This is the opposite of the open spaces in companies where employees are crammed together! It has long been claimed that open spaces improve teamwork, whereas their main purpose is to compress real estate costs!

No-Cloning Theorem says that it is impossible to identically clone the state of a qubit or quantum, has an application in business life with all those people who are believed to be irreplaceable until the day they leave or die. The theorem applies in particular when the departing manager is not replaced and whose role is then distributed among several existing managers, a bit like a quantum error correction with ancilla qubits and projective measurements. The theorem also works with successful entrepreneurs who find it difficult to replicate a success from one area to another.

Tunnel effect makes it possible to implement change management. It consists in presenting a wonderful future situation and making people forget the difficulties to get there. The principle could also be adopted by the Gartner Group with its famous innovation adoption cycle curves ("hype cycle"), as some technologies do not necessarily pass through the valley of death, as was the case for smartphones. It had benefited from the reality distortion field of a certain Steve Jobs, a great adept of quantum management principles. By the way, the trajectory Apple-Next-Apple was a great application of the tunnel effect, Next being a relative failure while both Apple were successes.

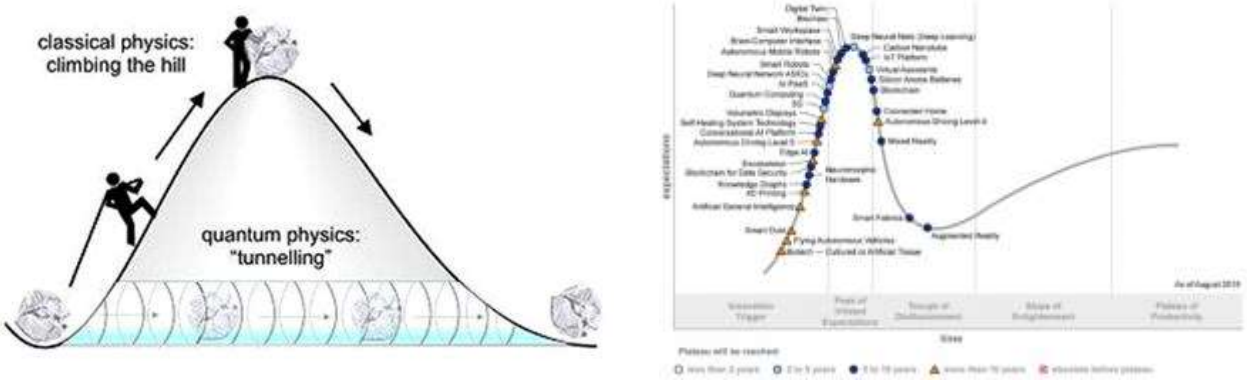


Figure 918: the quantum tunnel effect and hype effects. Sometimes, hype is so strong that it creates a pass-through from hype to success without a valley of death.

Superconductivity is linked to meeting rooms. Employees and managers are conditioned to be even-spin bozos, who can be assembled in meeting rooms or covid-zooms. Organizational superconductivity also avoids resistance to change. You freeze employees and their resistance to change disappears. Which is a bit paradoxical because once frozen, you are as solid as a rock, and defrosting is not obvious. If we take the principles of Deepak Chopra's quantum pseudo-medicine, a company is in a superposed state between a healthy leader and a declining star. The strength of leadership should theoretically allow the wave packet function of the company's quantum state to collapse in the healthy leader state. In real life, this collapse is tricky to achieve and companies simply collapse. The processes that lead the company to find itself in a declining situation are most often irreversible and linked to a slow decoherence with the environment, competitors and customers who have not waited to adapt. Corporate life is not a reversible quantum gate nor any sort of linear algebra. It's mostly nonlinear. Try, for example, to turn Nokia into the leader of Android smartphones!

Universal Gates Quantum Computing has a beautiful analogy in the life of companies with the management of calls for tenders such as those for communication agencies. The responses of candidate agencies are superposed states of a quantum register.

They undergo a simultaneous evaluation process, as in an oracle-based quantum algorithm. In the end, only one offer emerges: the winner. But during this process, there may be some quantum entanglement affecting the winner final proposal. Translation: the elements of certain answers will magically appear in the winner's answer. Again, perhaps via the enterprise quantum tunnel effect.

Finally, let us mention this other universal principle, the very famous **quantum teleportation** of human stupidity to large sections of the company or in the population. It uses superdense falsehoods encoding. And contrarily to actual teleportation, it travels faster than light. It is so fast that it is the only plausible explanation.

All of these analogies are amusing but not very useful for improving management. Even if its scientific dimension is more than questionable, parody is finally an interesting form of pedagogy!

Other exaggerations

There are many startups or ventures surfing on the quantum technology wave with various intentions. Some are just quantum startups with fluffy claims and others have only quantum in their name but nothing else.

One classical exaggeration comes with making cross-predictions between one digital trend and quantum computing. This one predicting that we'll have **quantum digital twins** is based on the usual wrong premise that quantum computing is made for compiling huge swaths of data[3014].

Dark Star Quantum Lab (2020, USA) introduces itself as a contract defense and space research company covering applied quantum physics and quantum information science (QIS). They develop tons of quantum stuff: quantum software and quantum emulation solutions, unspecified hardware, a 'Sentinel' mobile phone including a QRNG.

They also claim to have developed a Qloud high-frequency trading, a Qoin (quantum-secured cryptocurrency), a BloQchain (quantum-secured blockchain working with Qoin), a use-case of Nash embedding to create error-free qubits and, also, some Star Trek Tricorder fancy stuff.

[3014] See Why we need Quantum Digital Twins by Ian Gordon, Head of Data at Houses of Parliament Restoration & Renewal, January 2021.

This laundry list of things is not credible. And they don't seem to have any real defense customer. Looks like it's not really serious[3015].

Also quite weird is this **Quantum_AI Group Of Companies** with its 15 branches dealing with aerospace, artificial intelligence, naval, finance, energy, automotive, electronics and... quantum computing. They develop, take it or leave it: Nano-Flux, a range of flux-qubits superconducting computers, Q-optic, the most powerful optical qubits quantum computer, BEC, the fastest Bose-Einstein condensate based trapped ions computer (seems they mixed some things here) and also SSL, a solid-state quantum computer and Infinity-Q a high-performance heavy load quantum computer. Interestingly, these 4 ranges of systems have respectively 40, 200, a 1.6 and 128 billion qubits and they look the same in their 3D rendered pictures.

They are supposed to be based in Stanford, Boston, India, Abu Dhabi, Dublin and Tel Aviv. They still have a CEO, a certain Ranobijoy Bhattacharya. If it's not an April's fool, what is it? Some new form of mythomania?

Quantum physics abuse can be found in various other product categories. In China, for example, a so-called **quantum satellite camera** was used to produce high-resolution panoramas. The view presented was that of Shanghai with 195 billion pixels. Practically, the pictures were captured from the top of a skyscraper - there is no shortage of them in Shanghai - and not by any satellite. It used conventional high-resolution cameras that have nothing more quantum than the very classic photoelectric effect used in CMOS sensors to transform photons into electric current. The information is totally bogus and was only used to generate buzz.

Unfortunately, many media outlets around the world have taken the bait without any doubt [3016].

For its part, a French SME **What-Innove** from the East of France, specialized in renewable energies, claims it is creating an engine that captures energy from vacuum. How does it work? An unlikely mix combining a quantum field generator, the creation of photons from vacuum energy exploiting the Casimir effect, the combination of magnetodynamics and space-time, ambient temperature and pressure superconductors (which would win them a Nobel Prize if it worked), and negative entropy. They just need €2.7M of funding to move ahead!

You are also entitled to a beautiful **quantum cooler** from **Chillout Systems** that has only quantum in its name. It uses a compact classic compressor[3017].

Figure 919: the non-quantum cooler from Chillout.

Other cases extrapolate to the macro scale of quantum phenomena observed at a nano scale. This is the case of **time inversion** with quantum computing, a view of the mind that is linked to the reversible nature of quantum gates but does not mean that one can go back in time scale in macroscopic practice[3018].

[3015] See one scientific publication of their own, which is quite short: How many physical qubits are needed exactly for fault-tolerant quantum computing? by Faisal Shah Khan, Dark Star Quantum Lab, December 2021 (4 pages).

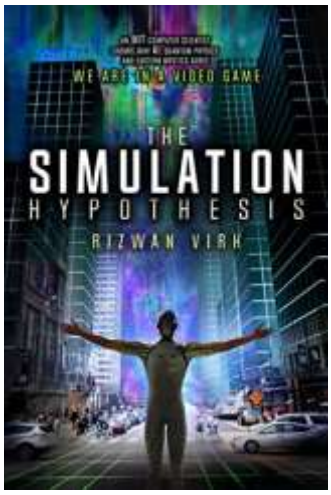
[3016] See 60 seconds over sinoland: quantum satellite camera used to do movable, panoramic photos of Shanghai, December 2018 (video) and Truth Behind Viral 24.9 Billion Pixel Image Taken By Chinese "Quantum Satellite" by Anmol Sachdeva, December 2018 and the Bigpixel website to view the view.

[3017] See Chillout Systems Quantum Cooler. It is sold for $2199.

[3018] See Arrow of time and its reversal on the IBM quantum computer by G. B. Lesovik et al, 2018 (14 pages) and Does the IBM quantum computer violate the second principle of thermodynamics?, 2019.

We also have equally wild theories willing to **predict the future** with quantum computing. If it is true that quantum computing allows us to evaluate all the solutions of a complex problem, it is reduced to simple problems in view of the complexity of macroscopic life, even if it could be deterministic[3019].

The next step is to consider that we are actually living in a **simulation**.



This is the theory presented in Rizwan Virh's The Simulation Hypothesis. The author presents himself as an MIT Computer Scientist, whereas he is more of an entrepreneur in video games, more accustomed to books on entrepreneurship than on science. This kind of simulation scenario is roughly equivalent to believing in a kind of omnipotent God who controls everything or who created the simulation tool. The question can moreover be recursively implemented: if this creator has developed a simulation tool, who created his universe and isn't this one also a simulation?

Another case that should inspire the utmost caution is that of this curious company **Precog Technologies**, which claims to offer solutions for teleportation, time travel and anti-gravity systems. Miracles one stop shopping!

The company was created to valorize the intellectual property of a certain Anisse Zerouta that is covered in a dubious scientific paper[3020].

Another guy, from **Quanta QB** (South Africa) thinks he has also found a qubit architecture that showcases a miraculous 0% error rate[3021]. Good luck with that!

We also saw the first quantum financial scam appear in 2018 with this fake article in the Guardian reporting a quantum computer project for Elon Musk's finance[3022]. The trained eye quickly detects that it is a montage, like this series of **QuantumAI quantum** computers that are nothing more than D-Waves annealers whose logo has just been photoshopped.

Second, the article is supposed to come from the Guardian, but not the url! It quotes a number of scientists from research laboratories around the world, all with Russian names. The article points to **QuantumAI**'s online service which would be able to go around robbing the rich and redistributing the money to the poor. And the site indicates that the startup has Jeff Bezos and Bill Gates as advisors and IBM, Microsoft and OpenAI as partners.

There is another, called **Quantum Code**. Obviously, run away! It is in fact a scam designed to rob users of their savings, but in an indirect way. The site offers to create an account by providing its coordinates. These are then resold to unscrupulous companies of shady financial products that exploit leads of prospects easy to fool.

[3019] See Interfering trajectories in experimental quantum-enhanced stochastic simulation by Farzad Ghafari et al, 2019 (7 pages).

[3020] See The Seed Theory: Unifying and replacing quantum physics and general relativity with "state physics" by Anisse Zerouta, 2017 (28 pages) which develops a theory of parallel worlds that does not seem to meet the criteria of a scientific publication worthy of the name. Anisse Zerouta is a company manager in Paris born in 1973, first with Elysee Communication (2008-2011) then with Avenir Optique, an optician (2011-*), companies with only one employee, its founder (source). Created in September 2018, Precogtec would have a CTO, a certain François Bissege, who has a PhD in sociology (source) and another employee, Julien Darivel, who has a DUT and worked at PSA. It's bizarre!

[3021] See I made the Quantum Breakthrough, June 2019.

[3022] See Elon Musk to Step Back From Tesla And SpaceX, Jumps on Quantum Computing Financial Tech (not dated).

Figure 920: do you spot the scam?

Other financial scams promising skyrocketing return on investment on mysterious quantum investments in the stock market are now current[3023].

We can also quote **Qubole** which launched its Quantum SQL server, which has nothing quantum[3024]. The **Samsung** Quantum 8K processor launched in 2018 was not particularly quantum either, except via its classical CMOS transistors.

Figure 921: QuantumAI and its financial scam.

In consumer products goods, we have this washing powder **Quantum Max** of the brand **Finish** from the Reckitt Benckiser group. And also **Quantum American** PQ rolls and Quantum red wine from **Beringer,** a brand from Napa Valley, California.

[3023] That one is a concentrated feat of bullshit: https://secure2.wealthdaily.com/o/web/362894 using the one line sentences tactic to strengthen its messaging. Each and every line would deserve some debunking.

[3024] See Qubole launches Quantum, its serverless database engine by Frederic Lardinois, June 2019.

Figure 922: anything can be quantum, your washing machine powder, your toilet paper and your wine or beer.

Otherwise, **Quantum Corp** (USA) does nothing quantum and just manages tape storage. The same goes for **Quantum Entanglement Entertainment** (Canada) which, as its name indicates, is in the content market. **Quantum Surgical** (France) makes surgery robots for liver cancer, which have nothing quantum. **QuantumScape** is a solid-state lithium battery manufacturer in the USA. **QuantumSi** created a silicon-based DNA advanced sequencing machine that doesn't seem to use any second-generation quantum technology, **Quantic** Executive MBA has only quantum in name. **Quantum Metric** is providing cloud based digital content design software tools. There is even a Chinese company created in 2016 named **Quantum Technologies** (officially "Guandong Technology") that sells some augmented reality product with nothing quantum at all. **Quantum Switch** is not a quantum switch from the physical standpoint. It states that it creates "*A New Era In Quantum Defined Data Centres*" but does just service classical colocation data centers.

Figure 923: all those companies chose to use quantum in their name, but they have nothing quantum.

At last, **QuantumLeaf** is a cannabis software company servicing the cannabis industry in the USA. **Quantum of the Seas** is a famous cruise ship covering all oceans. Even **McKinsey** got into this game, labelling its data-science consulting and service offering QuantumBlack! And don't be confused between **Quantum Health** which provides healthcare services to company's employees and **Quantum Health** which sells among other things an insect repellant. Hopefully, despite the company name, they don't claim the repellant use a specific quantum effect. It's just branding washing, not more. We're safe!

Quantum fake sciences key takeaways

- Quantum physics has been for a while integrated in highly dubious offerings, particularly in the healthcare and energy domains.
- There is a proliferation of gurus and scams-based miracle cures machines for detecting electromagnetic waves or vague energies, and restoring your body balance. It is at best a subset of the lucrative placebo effect industry targeting the gullible!
- The shift from some low-level physics studies on water and matter led some scientists to explain consciousness with quantum physics. This form of reductionism is unproven. It's the same with scalar-waves detectors or generators, miraculous healing crystals, structured water and other quantum medallions.
- This part proposes a simple methodology to detect these healthcare related scams, with using some common sense.
- We uncover some other scams in the free energy generation category. These systems are supposed to extract some energy from vacuum when their only actual effect is to pump money out of your wallet.
- Quantum physics is sometimes used in management and marketing. This book offers you a nice in-depth parody of these methodologies.
- At last, we showcase a few companies using quantum in their branding when they have nothing quantum at all to offer.

Conclusion

Quantum technologies perfectly symbolize the world of innovation and extreme entrepreneurship: it is full of uncertainties, risks and failures. There is "test & learn", the crossroads of many sciences, the need to invest well in advance of economic success, with a critical role for government investments, the only ones able to invest in the long term, more than 10 years ahead. Numerous parallel paths of exploration have been launched by researchers and entrepreneurs. Only a few will succeed. A new industry is emerging from all of this.

After reading part or the totality of this book, you may find out that its premise was misleading. “Understanding quantum technologies” is indeed a quest and a journey, but you never reach the destination. There’s always something you didn’t understand well and need to review again and again. For a starter, you may spend some time on the Bloch sphere trying to grasp what it represents and its various angles, then try to understand either how quantum algorithms work or how circuit quantum electrodynamics operate in a superconducting qubit, or, say, how quantum photonics really work up to the mysteries of MBQC.

To write this book over the course of the last four years, I downloaded and compiled more than 4500 documents freely available on the Internet, viewed dozens of hours of conferences and courses on YouTube, and met dozens of researchers and entrepreneurs.

Like in a thesis, I have here to thank many people and friends who helped me craft this book over my 5-year journey in quantum science and technologies. First of all, **Fanny Bouton**, with whom I started this quantum adventure in 2018 and who now runs quantum operations at OVHcloud.

Figure 924: the first quantum scientists we met in 2018, Alain Aspect, Cyril Allouche, Philippe Duluc, Daniel Esteve and Maud Vinet.

In chronological order, here are the first scientists and other people we met back in 2018: **Alain Aspect** (IOGS), **Daniel Esteve (**CEA Quantronics), **Christian Gamrat (**CEA LIST), **Maud Vinet (**CEA Leti in Grenoble, now at Siquance), **Tristan Meunier (**CNRS Grenoble), **Alexei Tchelnokov** (CEA Grenoble), **Laurent Fulbert (**CEA-Leti Grenoble), **Cyril Allouche** and **Philippe Duluc (**Atos), **Bernard Ourghanlian** and **David Rousset (**Microsoft), **Pat Gumann (**IBM), **Etienne Klein (**CEA), **Christophe Jurczak** and **Zoé Amblard (**Quantonation), **Nicolas Gaude** (Prevision.io) and **Françoise Gruson (**Société Générale).

Then, in 2019, with **Philippe Grangier** (IOGS), **Elham Kashefi (**LIP6 and VeriQloud), **Marc Kaplan (**VeriQloud), **Pascale Senellart (**C2N and Quandela), **Franck Balestro** (UGA, Institut Néel) and **Alexia Auffèves (**CNRS, then at Institut Néel in Grenoble and now MajuLab in Singapore, we are now teaming up as cofounders of the Quantum Energy Initiative), **Matthieu Desjardins** (C12), **Jacqueline Bloch (**C2N), **Iordanis Kerenidis (**CNRS), **Heike Riel** (IBM Zurich) and **Vern Brownell** (then D-Wave CEO).

In 2020, **Artur Ekert** (CQT Singapore), **Patrice Bertet (**CEA SPEC), **Xavier Waintal (**CEA IRIG), **Yvain Thonnart** (CEA LIST), **Rob Whitney** (LPMMC Grenoble), **Damian Markham** (CNRS LIP6 and JFLI in Tokyo), **Robert Whitney** (CNRS LPMMC, also part of the QEI), **Bruno Desruelle (**Muquans), **Georges-Olivier Raymond** and **Antoine Browaeys (**Pasqal), **Théau Peronnin** and **Raphaël Lescanne (**Alice&Bob) as well as **Jeremy O'Brien (**PsiQuantum), **Magdalena Hauser** and **Wolfgang Lechner (**ParityQC), **Roger McKinley** and **Peter Knight** (UK) and the IBM Zurich research teams. I also had discussions with the teams from **Qblox**, **Qilimanjaro**, **Quantum Motion**, **Strangeworks** and **IQM**.

There were these countless discussions with **Jean-Christophe Gougeon** of Bpifrance, **Neil Abroug**, who is since 2021 the coordinator of the quantum strategy in France, as well as **Charles Beigbeder** and **Christophe Jurczak** from Quantonation and Le Lab Quantique, who wrote the foreword of this book, page vii. I should also mention the numerous exchanges related to quantum investments with **Cédric O** and his team, in the French government. He was onboard early on and became its driving force within the government.

The fourth edition in 2021 benefited from the contributions of **Alexia Auffèves** (measurement, energetics of quantum computing, quantum foundations, photon qubits), **Antoine Browaeys** (IOGS and Pasqal, cold atoms), **Christophe Chareton** (CEA LIST, linear algebra, quantum algorithms and development tools), **Cyril Allouche** (Atos, supercomputing, emulators, European projects), **Daniel Esteve** (CEA DRF, superconducting qubits), **Eleni Diamanti** (CNRS LIP6**,** quantum telecommunications and cryptography), **Elvira Shishenina** (BMW, proof-read all the document), **Frédéric Nguyen Van Dau** (Thales, quantum sensing), **Georges Uzbelger** (IBM, quantum algorithms and software tools), **Jonas Landman** (CNRS IRIF, quantum algorithms), **Léa Bresque** (CNRS Institut Néel, quantum physics 101, quantum postulates and measurement), **Marc Kaplan** (Veriqloud, quantum telecommunications and cryptography), **Michel Kurek** (who patiently proof-read several times all the book and checked all hyperlinks), **Peter Eid** (Arm, classical and unconventional computing, telecommunications/cryptography), **Philippe Grangier** (Institut d'Optique, quantum foundations), **Pol Forn-Díaz** (Qilimanjaro, superconducting qubits), **Théau Peronnin** and **Jérémie Guillaud** (Alice&Bob, cat- qubits) and **Valérian Giesz** (Quandela, photon qubits and photonics).

In 2022, I had a chance to discuss about the quantum ecosystem with **Rainer Blatt** (AQT and Munich ecosystem), **Jonathan Home** (ETZ Zurich), **Tommaso Calarco** (Jülich) and **Jay Gambetta** (IBM). I also met with countless other quantum physicists and entrepreneurs.

Reviewers for this fifth and 2022 edition were **Jean-Philippe Fauvarque** (Plassys-Bestek, for the fabs part), **Antoine Gras** (Alice&Bob, also for the fabs part), **Frédéric Wyczisk** (for the quantum matter part, formerly at Thales), **Michel Kurek** (the proof-reading master who does an incredible work spotting all the details), **Antoine Browaeys** (Pasqal/IOGQ, neutral atoms computing), **Bruno Desruelle** (ixBlue, quantum sensing), **Christophe Jurczak** (updated foreword), **Marco Fellous-Asiani** (energetics, control electronics, superconducting qubits), **Clément Barraud** (MPQ, quantum matter), **Georges-Olivier Raymond** and **Nicolas Proust** (Pasqal, cold atoms qubits), **Léa Bresque** (Institut Néel, Quantum technologies energetics), **Luc Gaffet** (Air Liquide, cryogeny), **Olivier Hess** (Atos, software), **Jérémie Guillaud**, **Blaise Vignon** (Alice&Bob, superconducting qubits), **Thomas Ayral** (Atos, various pats), **Loïc Chauvet** (CACIB, software tools), **Daniel Vert** (CEA, quantum annealing), **Xavier Vasques** and **Jean-Michel Torres** (IBM, on IBM quantum software stacks), **Stéphane Louise** and **Christophe Chareton** (CEA LIST, on algorithms), **Marc Kaplan** (VeriQloud, quantum telecommunication and cryptography), **Maud Vinet** (history, silicon qubits) and **André M. Konig** (Global Quantum Intelligence, various places).

And maybe you, next time :)!

Cheers,

Olivier Ezratty, September-November 2022

Bibliography

Here are a few books and other sources of information on quantum technologies that I consulted or discovered to prepare and update this book.

Events

There are numerous conferences on the different scientific branches of quantum technologies and a growing number of quantum "business" conferences associating some scientific content, industry vendors talks (and sponsoring) and customer use cases testimonials.

I found online various inventories of quantum related scientific events on quantum.info (which also inventories some quantum physics predatory journals), Conference service, Conference Index and Quantum Computing Report.

Many of these events are fee based for both participants and speakers. It costs up to $1,000 to participate as an attendee, plus extra-fees for speakers and poster sessions. It's a business!

Figure 925: a yearly timeline of some notable quantum events, from science to business. (cc) Olivier Ezratty, 2022.

Quantum Scientific events

Let's quickly cover the main quantum related events where the audience is mainly made of scientists and the content is likewise highly scientific[3025].

APS March Meeting is the largest physicists conference in the world with over 12K attendees, hundreds of sessions, thousands of presented papers, and a significant part of them are in the quantum physics disciplines, including enabling technologies like cryogeny. Other talks cover different parts of physics likes high-energy particles physics or astronomy. They have over 100 exhibitors. Their industry tracks showcase scientific advancements from the main quantum computing players like

[3025] See Q-Turn: Changing Paradigms In Quantum Science by Ana Belén Sainz, February 2022 (9 pages) about how to organize scientific quantum events.

IBM, Google, IonQ and others. The 2022 edition was in Chicago and will be in Las Vegas in 2023. This four-day event is organized by the American Physical Society which also publish the reference journals PRX Quantum, PRX, PRL (Physical Review Letters) and PRA (Physical Review A), that are frequently mentioned in this book bibliographical references.

Photonics West in January/February is the largest photonics related conference and vendors exhibition, including quantum photonics, their related enabling technologies (lasers, photon counters, …) and also covering medtechs, organized at the Moscone Center in San Francisco. It also hosts industry related events.

Laser World of **Photonics** and the **World of Photonics Congress** is another photonic major congress, happening in Germany. The 2023 edition takes place in June in Munich with over 30K visitors and 6000 congress participants.

QIP (Quantum Information Processing) is an important quantum information conference with prestigious scientific speakers. The 2022 edition was organized in Caltech, California (attendees picture below) and the 2023 edition is planned in Ghent, Belgium in February.

Figure 926: QIP2022 group photo at Caltech.

QUANTUMatter gathers various communities in quantum information and quantum matter involved in all branches of quantum technologies (computing, sensing, telecommunications). Its second edition was organized in Barcelona in June 2022.

QPL (Quantum Physics and Logic) is about the mathematical foundations of quantum computation, quantum physics and related areas with a focus on the use of mathematics, formal languages, semantic methods and other mathematical and computer scientific techniques to the study of physical systems and processes. The 2022 edition was organized in Oxford, in June/July.

IEEE organizes many quantum related scientific conferences including QSW (International Conference on Quantum Software), in Barcelona, Spain in July 2022, the IEEE Quantum Week, in September, 2022 in Broomfield, Colorado and IEDM (International Electron Devices Meeting) in September in San Francisco which covers silicon spin qubits and qubit control electronics among other topics.

ASC (Applied Superconductivity Conference) is a superconducting related event. The 2022 edition happens in Honolulu, Hawaii in October. It covers quantum systems, computation, sensing and networking, control and readout electronics, fabrication, packaging, and scalable infrastructure, and hybrid or novel quantum systems.

SQA (Superconducting Qubits and Algorithms Conference) covers science, technology, and algorithms related to superconducting quantum computing organized by IQM. The 2022 edition takes place, not surprisingly in Helsinki, in August. With prestigious speakers like William D. Oliver (MIT), Andreas Wallraff (ETH Zurich) and Vladimir Manucharyan (Maryland University).

Spin Qubit 5 is a conference on spin qubits organized in Pontresina, Switzerland in September 2022. It covers NV and SiC centers qubits, quantum dots spin qubits and the likes. The conference chair is none other than Daniel Loss.

ICDCM (International Conference on Diamond and Carbon Materials) is the conference were NV center and SiC cavities are talked about. The 2022 edition happened in Lisbon, Portugal, in September.

ICQTQMS is the International Conference on Quantum Technologies, Quantum Metrology and Sensors. The 2022 edition is planned in September in Rome, Italy.

QTML (Quantum Techniques in Machine Learning) focuses not surprisingly on quantum machine learning, gathering researchers and industry players. The 2022 edition takes place in Naples, Italy in November.

QRE is a yearly workshop on Quantum Resource Estimation also dealing with benchmarking and performance analytics. The 4th edition took place in June 2022 in New York.

QTD2022 (Quantum Thermodynamics Conference) took place virtually on Zoom in June/July 2022.

FQMD (Frontiers in Quantum Materials and Devices).

GDR IFQA gathers international quantum scientists covering all fields, with tutorial sessions, docs/post-docs sessions and poster sessions. It has been organized by the research group on quantum technologies from CNRS in France every November since 2011. The 2022 edition takes place in Palaiseau in the Paris region in November.

Quantum Business conferences

And now, onto the quantum business events which usually provide a mix of scientific and business related content.

Q2B is a conference organized by QC-Ware since 2017. Initially happening in California each December, it will also happen in Tokyo in July 2022 and later in Europe. It is a good opportunity to learn about the scientific progress from major industry players in quantum computing.

Inside Quantum Technology is a series of quantum business conferences organized in several like The Hague (February 2022), San Diego (May 2022), New York (October 2022) and San Jose, California (April 2023).

Quantum.Tech is another conference focusing on industry use cases of quantum technologies. The last edition was in Boston in June 2022. A London edition takes place in September 2022.

Commercialising Quantum was organized in May 2022 in London by the Economist, London with a mix of in-person and virtual events.

QHack is a mix of a fan expo, hackathon and scientific conference for quantum software developers. The third edition was organized online in February 2022.

Quantum Business Europe is an international conference launched in 2021 that had a second edition in March 2022 with a mix of vendors, scientists and user talks.

World Quantum Day is a virtual global event, consolidating events happening one day in April all over the world, targeting broad audiences.

Quantum World Congress gathers experts from the industry with plenary sessions and breakout tracks on market acceleration, science and engineering, government and security, complemented by an exhibition. The 2022 edition takes place in Washington DC in November/ December.

France Quantum is a conference that was launched by Startup Inside and OVHcloud in June 2022 at the Eiffel Tower to promote the French quantum ecosystem. The 2023 edition is planned in Paris in June.

Quantum Eastern Europe is a 2-day online event gathering quantum stakeholders from Eastern Europe. The 2022 edition happened in May.

Investment Summit for Quantum Startups was organized in October 2021 at Maryland University as a gathering of investors and startups.

Metaverse Quantum Computing Summit is not a joke. Or still, yes, it's really a gigantic joke. You even have the opportunity to "*Learn best practices, strategies and ideas you can implement today*". This is an extreme case of mixing two trendy B.S. into one compound B.S (source). By the way, none of the speakers talk about the metaverse, but only about crypto-financial stuff.

Websites and content sources

The Quantum Insider (USA, formerly The Quantum Daily) is a quantum news site. Many of the news are broadcasting press releases from vendors, government and research labs and some others are original posts. It is completed by a job board and professional services, exploiting a proprietary database of quantum industry vendors and stakeholders. The company is run by Alex Chahans out of the USA. In October 2021, The Quantum Insider integrated Entangle, a global quantum technology community. The Entangle team is now focused on a crusade around using quantum tech to solve the climate crisis.

Quantum Zeitgeist (USA) is another quantum news media that also maintains an online database of startups in the field and a quantum jobs board. Their about talks about "we" but they provide no name of who's behind the site. The site belongs to a company named Hadamard LLC based in Wyoming, and created in July 2021.

Fact Based Insight (UK) is/was an analyst shop run by David Shaw in the UK. It publishes very interesting charts and analysis on the quantum ecosystem, including some insights on quantum hardware.

Global Quantum Intelligence is an analyst shop created by André M. Konig, David Shaw and Doug Finke that consolidated in 2022 the activities from The Quantum Report (Doug Finke), Fact Based Insight (David Shaw) and André M. Konig's consulting activities. They provide data and insights on an annual subscription basis.

The Quantum Leap is a blog of news on the quantum ecosystem published by Russ Fein, a venture investor passionate of quantum computing and based in the USA.

AzoQuantum (UK/Australia) an information site on quantum science news with a supplier's directory, focused on manufacturing equipment and some interviews, mostly written by young researchers.

Quantum Journal - the open journal for quantum science, a site of scientific news on quantum physics, mostly showcasing preprints published on arXiv.

Quantiki is an information site on quantum computing. It looks like they became mainly a jobs board.

The Qubit Report (USA) is a news media focused on quantum vendors launched in 2017.

Qosf, a site that inventories guides and training for developers of quantum applications.

The Quantum Hubs newsletter (Switzerland) is broadcasting in his website and email newsletter the latest news from quantum research and vendors.

Podcasts

Quantum Tech Pod are podcasts by Christopher Bishop on quantum technology news, published on Inside Quantum Technology's web site. These are mostly half-an-hour interviews of quantum startup founders. It started mid-2021.

Consulting firm Protivity also launched its own series of podcasts, in May 2021. Like Chris Bishop's podcasts, it's about interviewing quantum startup founders. They also last half an hour.

Quantum Computing Now by Ethan Hansen covers quantum computing news, basic concepts, and what people in the field are doing. The first episode was aired in July 2019. They are biweekly and cover news as well as science and learning tutorials.

The Quantum Analysts Roundtable is a podcast launched in January 2022 and run by Doug Finke, David Shaw, Shahin Khan, James Sanders and André M. König.

The Qubit Guy's podcast series is run by Yuval Boger, Classiq's CMO with short-format interviews.

QViews is a news podcast from Anastasia Marchenkova launched in May 2022. It's a pity since it just reads the titles and headlines from press releases.

The Quantum podcasts that I have been recording regularly (in French) since September 2019 with Fanny Bouton (OVHcloud). They are available on all audio platforms (Spotify, iTunes, Deezer, ...) as well as on YouTube in video version. It covers quantum news including what's happening in the ecosystem, with startups and in research. We decipher many lead scientific announcements. Our first episode was on Google's supremacy!

They are complemented by the Decode Quantum interviews that we have been publishing since March 2020 with a great variety of personalities (lead researchers, startup founders, investors, user companies, public servants, etc.) in partnership with Frenchweb. The first episodes featured Pascale Senellart, Alexia Auffèves, Maud Vinet, Eleni Diamanti, Elham Kashefi, Théau Peronnin and Raphaël Lescanne from Alice&Bob, Alain Aspect, Philippe Grangier, Michel Devoret, Daniel Esteve and many others since we had 53 episodes in-store as of November 2022! They last about one hour.

insideQuantum is an equivalent series of podcasts in English which started in 2022 out of Spain with slightly shorter formats.

Books and ebooks

If you wander in Amazon or your other preferred real-life of virtual scientific bookstore or University library, you'll find an abundant literature on quantum physics and quantum information. Many people willing to learn in these domains have a hard time finding the "right" book that is adapted to their existing knowledge and particularly, to their fluency in mathematics. Here's a not-too long list of books for this purpose. It's mostly adapted to students since, if you work in the industry, you probably won't have much time to read many of these thick books. Many of these ebooks are open source and/or free to download[3026].

Quantum physics

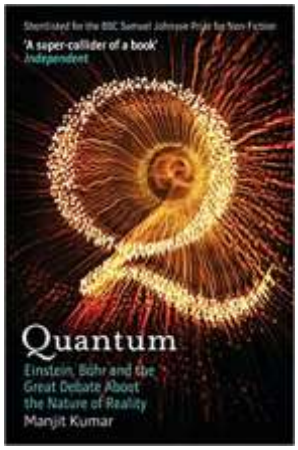
Quantum Mechanics, Volume 1: Basic Concepts, Tools, and Applications, Second Edition, 2017, by Claude Cohen-Tannoudji, Bernard Diu and Franck Laloë (879 pages) is an undergraduate reference series of books to learn quantum physics. It is considered to be the reference or the bible by many students and teachers of quantum physics.

[3026] See Publicly available quantum computing books (WIP) for a list of open access book on quantum computing, a bit lazily done with urls without titles.

Quantum Mechanics, Volume 2: Angular Momentum, Spin, and Approximation Methods, Second Edition, 2017, by Claude Cohen-Tannoudji, Bernard Diu and Franck Laloë (688 pages).

Quantum Mechanics, Volume 3: Fermions, Bosons, Photons, Correlations, and Entanglement, Second Edition, 2017, by Claude Cohen-Tannoudji, Bernard Diu and Franck Laloë (747 pages).

Do we understand quantum mechanics? Second Edition by Franck Laloë, 2019 (550 pages) is an interesting piece that documents the debates on quantum foundations and how to interpret quantum physics. Do we really understand quantum mechanics? by Franck Laloë, 2004 (118 pages) is a shorter and older version of this book, in public access.



Quantum: Einstein, Bohr, and the Great Debate about the Nature of Reality by Manjit Kumar, 2009 (480 pages) is an excellent history book about the creation of quantum mechanics. It centers a lot on the works from Max Planck, Niels Bohr, Albert Einstein, Max Born, Werner Heisenberg and Erwin Schrodinger. It's a good account of the history of ideas and how quantum physics saw the day of light. It also showcases a lot of lesser known scientists who played key roles around the most famous ones and the balance between theoreticians and experimentalists. On top of that, the book scientific content is quite good and easy to understand, without any mathematics! Other history books and papers, mostly available in open access, are also mentioned throughout this book, particularly in the History and Scientists section, starting page 21.

Lecture notes on Quantum Mechanics by Frédéric Faure, 2015 (397 pages) which provided me with some leads to link quantum mechanics to its mathematical formalism and notably to explain the Born equation.

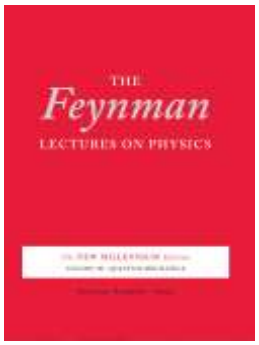
The Feynman Lectures on Physics - Volume III on Quantum Mechanics by Richard Feynman, Robert Leighton and Matthew Sands, (688 pages). It contains lecture notes of Feynman legendary courses from the early 60s. These are treasures of pedagogy with a content that is still up to date to grasp the fundamental of quantum physics. One advantage is it doesn't make any abuse of mathematics.

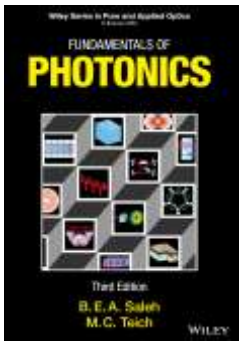
Quantum Optics An Introduction by Mark Fox, 2015 (397 pages) an excellent coverage of the broad field of quantum optics and the second quantization.

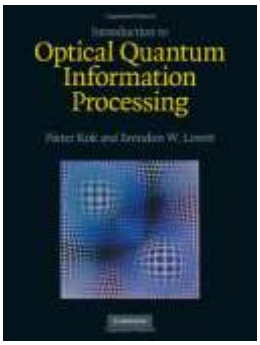
The Quantum Theory of Light by Rodney Loudon, 1973-2001 (450 pages) is a classic book on quantum light, that is useful to later better understand the physics of photon qubits used in quantum computing, telecommunications and cryptography. It classically starts with Planck's radiation law, then covers lasers, light-matter interactions, Mach-Zehnder interferometry, light quantization, single mode, multi-mode and continuous-mode optics and nonlinear optics.

Fundamentals of Photonics by Bahaa Saleh and Malvin Teich, 2019 (1401 pages) is a comprehensive quantum optics books that also covers instrumentation, which means it's good stuff for experimentalists.

Introduction to Optical Quantum Information Processing by Pieter Kok and Brendon W. Lovett, 2010 (506 pages) is another classic quantum photonics books covering quantum information systems.

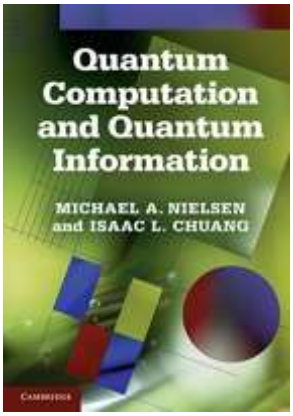




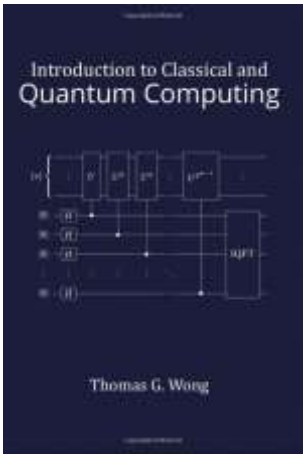


I Don't Understand Quantum Physics by Douglas Ross, 2018 (104 pages) is a nice primer to conceptualize and visualize many quantum phenomena. It describes the founding experiments of quantum physics (blackbody radiation, photoelectric effect, Compton scattering, etc), the wave-particle duality, matter wave, indeterminacy, Schrödinger's equation, superposition and the EPR paradox.

Quantum information



Quantum Computation and Quantum Information by Michael Nielsen and Isaac Chuang, 2010 (10th edition, 704 pages, public access) is the definitive reference on the basics of quantum computing. It answers many key questions, in particular on the mathematical models of linear algebra used in quantum computing. It also covers the basics of quantum physics, quantum postulates, problems complexity classes, quantum measurement, quantum algorithms, how qubits are realized (harmonic oscillators, trapped ions, photons, NMR), the impact of quantum noise and decoherence, how quantum error corrections work, what is fault-tolerant quantum computing, how about Shannon and Von Neumann information entropy and the likes. It also covers quantum key distribution and cryptography.



Introduction to Classical and Quantum Computing by Thomas Wong (2022, 400 pages), a book that is free to download in PDF and available in paperback on Amazon (😊). It makes a good comparison between classical and quantum computing. Like most quantum books for developers, it covers only classical gate-based algorithms with nothing on quantum annealing and quantum simulation. And it says nothing about the hardware and what it can do. It also makes some confusions between phase flip errors and decoherence related errors, which create mixed state when a simple phase error preserves a pure state.

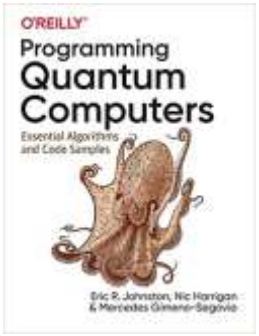
Elements of Quantum Computing by Seiki Akama (133 pages), which is at the same time concise, precise and quite complete on the nuts and bolts of quantum physics and quantum computing, with a good historical overview.

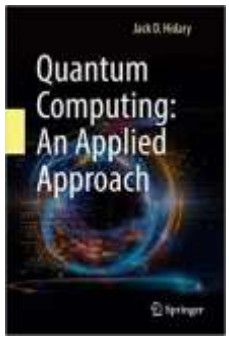
Quantum Information Meets Quantum Matter by Bei Zeng, Xie Chen, Duan-Lu Zhou and Xiao-Gang Wen. It is available in a February 2018 version on arXiv as a free download (373 pages).

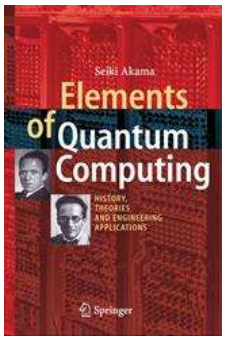
Programming Quantum Computers - Essential Algorithms and Code Samples by Eric R. Johnston, Mercedes Gimeno-Segovia and Nic Harrigan (2019, 336 pages) is an excellent and detailed description of key quantum algorithms like the QFT, phase estimation and the likes.

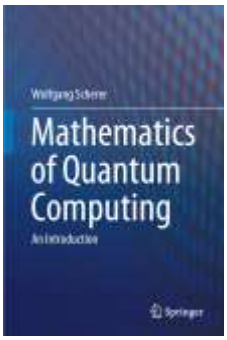
Quantum Computing: An Applied Approach (2021, second edition, 445 pages) by Jack Hidary, a fairly comprehensive book covering quantum algorithms and their mathematical foundations. It briefly describes the different architectures of quantum computers.

Quantum Machine Learning - What quantum computing means to data mining, by Peter Wittek, 2014 (176 pages) is a good introduction to machine learning and quantum machine learning although many progresses were made since this book's publication.





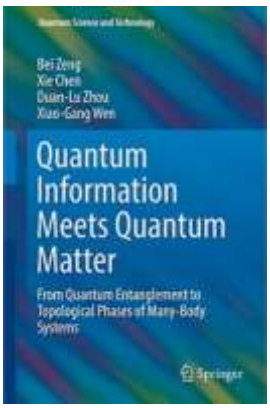


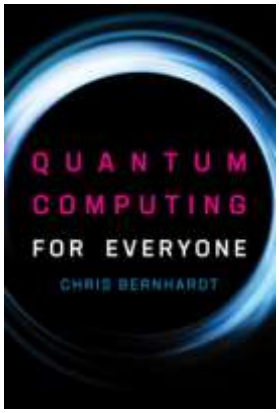


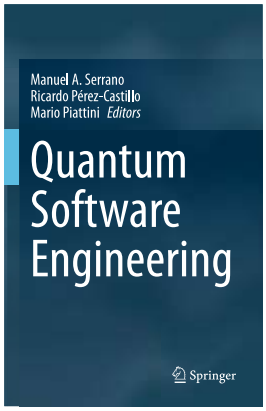
Quantum computing- from quantum physics to quantum programming in Q# by Benoit Prieur, 2019 (244 pages). It starts with the general principles of quantum physics. The section on quantum computers themselves is rather thin and explores only a few technologies (superconductors and NMR, which is little used). The rest is dedicated to learning programming in Q#, Microsoft's quantum programming language.

Principles of Quantum Computation and Information, A Comprehensive Textbook by Giuliano Benenti, Giulio Casati, Davide Rossini and Giuliano Strini, December 2018 (598 pages).

Quantum Computing for Everyone by Chris Bernhardt, 2019 (216 pages) which describes the basics of quantum computing starting with the inevitable qubit, quantum gates, accelerations brought by quantum algorithms and the main components of a quantum computer.







Quantum computing by Joseph Gruska (1999, 390 pages), another fairly comprehensive base covering all aspects of quantum computing and communication.

An Introduction to Quantum Computing by Phillip Kaye, Raymond Laflamme and Michele Mosca, 2007 (284 pages) which starts with some mathematical foundations of quantum physics and quantum computing. By reference authors such as Raymond Laflamme (Canada) who is one of the fathers of error correction codes.

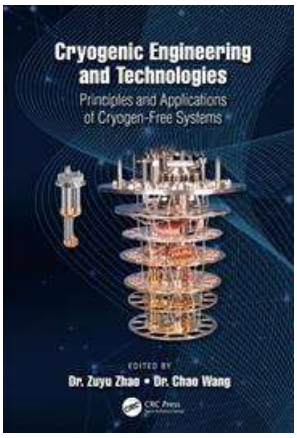
Introduction to quantum computing algorithms by Arthur Pittenberger, 2001 (152 pages) which describes classical quantum algorithms with a good part dedicated to error correction codes.

Quantum Software Engineering is a book edited by Manuel A. Serrano, Ricardo Pérez-Castillo and MarioPiattini from University of Castilla-La Mancha in Spain, 2022 (321 pages). It provides an overview of this emerging discipline, describing key concepts, the related vocabulary and formal methods. It also presents Q-UML, a quantum modeling language.

Quantum Internet, a 60-page magazine presenting the different sides of quantum computing, published by TU Delft (2019).

Quantum computing for dummies by William Hurley, April 2023, has yet to deliver its nuggets!

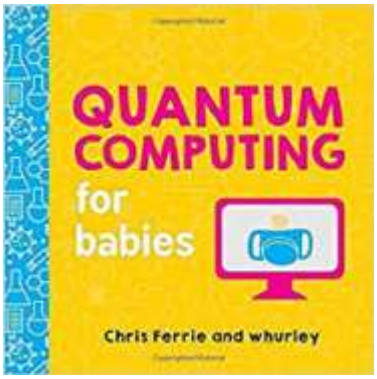
Cryogenic Engineering and Technologies by Zuyu Zhao and Chao Wang, October 2019 (386 pages) is a reference book on cryogenic issues with a very extensive and well-documented history. There is an excellent chapter on dry dilution cryostats used in quantum computers. This helped me to prepare the part of this book on cryogenics (starting page 464) in addition to an interview with the team of the French startup CryoConcept and with researchers from CNRS Institut Néel in Grenoble.

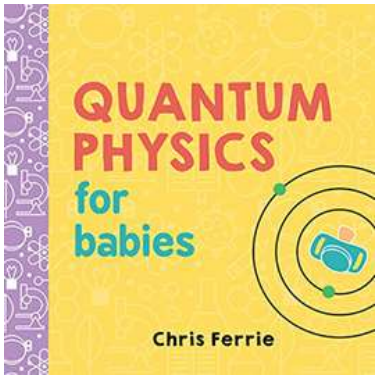


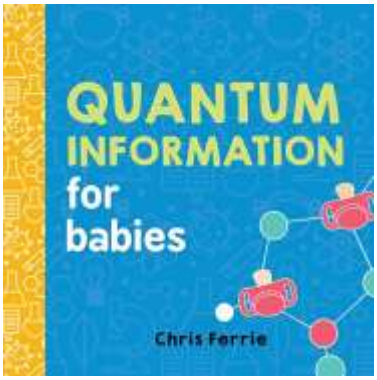
Unconventional Computation by Bruce MacLennan, University of Tennessee, October 2019 (304 pages) which discusses the energy issues of computation (reversible, non-reversible) and various alternative methods of computation including quantum computing and molecular computing.

Comics

Quantum Computing for babies by Chris Ferrie and William Hurley, April 2018, is aimed more at children or even older children. The book popularizes the major concepts of physics and quantum computing in a very colorful way. It comes from a professor of quantum computing at Sydney University of Technology and the founder of the American startup Strangeworks. William Hurley is the founder of **Strangeworks**. Two other books in the same vein from Chris Ferrie were also released: Quantum Physics for babies and Quantum Information for babies, all for less than $10. I "read" the last one (24 pages) and I'm not sure even an adult would really understand how quantum computing after looking at it. This is the danger of oversimplification and information dilution.







Presentations

Here are a few conferences and presentation materials rather well done to popularize quantum computing.

Quantum computing for the determined by Michael Nielsen, a series of 22 videos on quantum computing, 2011, accompanied by a long text of explanations.

CERN's Quantum Computing for High Energy Physics workshop in November 2018, with presentation materials and videos and interesting talks by various players in quantum computing, including Intel, who are not often seen. The specific content may be overtaken by the basic principles remain valid.

Quantum computing Overview by Sunil Dixit, September 2018 (94 slides) is a presentation by Northrop Grumman that takes a fairly broad look at quantum computing and the underlying mathematical models.

A Practical Introduction to Quantum Computing From Qubits to Quantum Machine Learning and Beyond, by Elias Combaro, CERN course, 2020 (251 slides) is a good course on quantum algorithms, debugging, validation, verification and benchmarking.

Quantum computing, a four-part course by Hélène Perrin at Université Paris 13, February 2020 (lecture 1 of 77 slides on trapped ions, lecture 2 of 36 slides on superconducting qubits, lecture 3 of 39 slides on silicon, molecular and NV Centers qubits, lecture 4 of 75 slides on cold atoms). This requires a good background in physics to be understood from start to finish. The references provided allow to deepen the topics covered.

Training

Berkeley courses for 2013: Quantum Mechanics and Quantum Computation on YouTube.

Videos from the Stanford Quantum Computing course.

The Quantum Computing Fundamentals course offered by MIT.

An online training course on quantum programming offered by Brillant in partnership with Microsoft.

The QSIT course (FS 2016) at ETH Zurich with its slides and lecture notes.

Quantum Computing as a High School Module, a curriculum with exercises on the basics of quantum physics for students at the BAC level.

Reports

Inside Quantum Technology, an analyst company dedicated to quantum technologies, which sells industry reports.

You can also find analysts reports on quantum technologies with McKinsey, BCG, Yole Development and other analyst companies.

Miscellaneous

Designing and Presenting a Science Poster, Jonathan Carter, Berkeley (20 slides) which is intended to help researchers design a good research project presentation poster.

Glossary

What is the purpose of a glossary? It allows you to find your way around in a new terminology and to step back to understand new concepts. For the author, it was also a good checkpoint of his own understanding and ability to popularize scientific and technological concepts. Some of these descriptions are simplified versions derived from Wikipedia definitions. Welcome to the lingua franca of quantum sciences and technologies!

137: constant used to compare different equivalent quantities in quantum physics. It turns out that 1/137 is a value that corresponds approximately to the fine-structure constant, a ratio that is found in several places in quantum physics and compares data of the same dimension. It is for example the ratio between the speed of an electron in the lower layer of a hydrogen atom and the speed of light or the probability of emission on the absorption of a photon for an electron. 137 is a bit like 42 in quantum physics. Wolfgang Pauli died after an operation for pancreatic cancer, while his hospital room was number 137.

ADC: analog-digital converter. Converts an analog signal into a digitized signal. In quantum technologies, it is used to convert the reflected microwave signals used in superconducting and electron spin qubits readout.

Adiabatic: quantum computation method used in particular with D-Wave quantum annealing computers. A complex Hamiltonian describing a complex system is first determined whose fundamental state describes a solution to the problem under study. A system with a simpler Hamiltonian is then prepared and initialized in its fundamental state. This Hamiltonian then adiabatically (meaning, with no energy or mass exchange with the outside environment) evolves into the complex Hamiltonian. According to the adiabatic theorem, the system remains in its fundamental state, and its final state describes a solution to the problem under consideration.

Adiabatic theorem: quantum mechanics concept created by Max Born and Vladimir Fock in 1928. It states that a quantum mechanical system subjected to gradually changing external conditions adapts its form, but when subjected to rapidly varying conditions there is insufficient time for the functional form to adapt, so the spatial probability density remains unchanged. This can be used to find Hamiltonian energy minimums with quantum algorithms running on various architectures: gate-based, annealing and quantum simulation.

Advantage: see quantum advantage.

Aka: shortened “also known as”.

Algorithm: a method of problem solving that is made up of a finite sequence of operations or instructions. The word comes from the name of the 9th century Persian mathematician, Al-Khwârizmî.

Algorithmic qubit: benchmark metric proposed by IonQ which corresponds to the number of qubits usable with an equivalent computing depth with a randomized benchmark producing a good result in 2/3rd of the runs. It’s actually $\log_2$ of IBM’s quantum volume.

Amplitude: this term has various meanings depending on the context. It can be the classical amplitude of a wave, i.e. half of its maximal variation, as opposed to its phase. For a quantum object, it can be the complex amplitudes of its basis states or eigenvectors. With a qubit in its Bloch sphere representation, the amplitude is related to the projection of the qubit vector on the z axis. But the $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ describing the qubit vector are also amplitudes, although, precisely, complex amplitudes. These complex amplitudes define the qubit amplitude ($1\text{-}\cos(\theta/2)$) and its relative phase (angle φ).

Anharmonic oscillator: contrarily to harmonic quantum oscillator that have the same energy difference between ach each consecutive energy levels, an anharmonic quantum oscillator has different energy differences between consecutive energy levels. This is the case of superconducting qubits, in order to create two manageable energy levels that are controlled with microwaves with the highest energy transition level of the oscillator.

Angular momentum: generally speaking, speed of rotation of a rotating object. In quantum physics, angular momentum is quantized and can have only discrete values.

Ansatz: another name for the parametrized quantum circuits or parametric quantum circuits that contain rotation gates and the parameters of the problem to encode in a variational quantum optimizer defined by a classical optimizer. Typically used is most QML algorithms.

Anyons: type of elementary particle found in two-dimensional systems. It is a generalization of the concept of bosons and fermions. Anyons have intermediate statistical behaviors between the two types of elementary particles. They are in fact virtual particles that live in two spatial dimensions and are generally based on electrons or electron gaps moving in superconducting metallic 2D structures. Anyons are a particular type of quasi-particles. They are used in topological quantum computers and would be used in particular in computers based on the hypothetical Majorana fermions studied at Microsoft.

arXiv: Cornell University's site that allows researchers to publish scientific papers prior to publication in peer-reviewed journals such as Nature, Science or Physical Review. It can take up to 9 months between publication of an article on arXiv and publication in a peer-reviewed journal. In the latter case, the article will have eventually evolved. The interest of arXiv in literature search is that publications are open and free of charge whereas most of the peer-reviewed journals are not free. The disadvantage is that the articles are not necessarily validated and that one has to make his own evaluation. It should be noted that in a researcher's publication, there are often several authors, up

to several dozen. The first author is generally the PhD student who has carried out a large part of the work, particularly its experimental part. Others are contributors who helped him/her. The last author is the thesis director or principal investigator (PI), the group leader or the laboratory director who has closely or remotely supervised the project. He/she probably contributed significantly to the article writing and cleanup.

Atoms: the smallest constituent element of matter that manifests chemical properties. It consists of a nucleus, with one or more positively charged protons and zero or more neutrally charged neutrons, around which negatively charged electrons gravitate. In a neutral atom, the number of electrons is equal to the number of protons. Otherwise, the atom is negatively or positively charged and forms an ion. The number of protons determines the nature of the atom in Mendeleev's Elements Periodic Table. An atom with one proton is hydrogen, with two protons it is helium, etc. Uranium has 92 protons. The nucleus represents the bulk of the atom mass. The isotopes of an element correspond to variations in the number of neutrons. In general, the number of neutrons of an element is equivalent to that of protons. Electrons are distributed in layers whose number depends on the atomic number. They are numbered from 1 to 7. Each layer can contain a maximum of $2n^2$ electrons, n being the number of the layer (thus 2, 8, 18, 32, 50, 72 and 98). This model was developed by Niels Bohr between 1909 and 1913. The chemical properties of the element depend on the number of electrons of the last layer which is called the valence layer. If this number is $2n^2$, the atom will be inert and will not combine chemically with other atoms. Carbon has three layers of electrons, the last one having 4 which allows it to combine with other atoms such as hydrogen (1 layer, 1 electron) or oxygen (6 electrons in the last layer).

Autonomous quantum error correction (AQEC): quantum error correction codes and architectures that doesn't require error syndrome measurement. It replaces real-time feedback by analog feedback circuits using engineered dissipation with the reservoir engineering technique. It couples the system with a dissipative reservoir to transfer the entropy created by errors to an ancillary system, the reservoir. This entropy is then evacuated via the strong dissipation of the ancilla. This technique is used in cat-qubits.

Back action: in quantum measurement, this is the physical impact of the measurement device on measured quantum objects. Quantum measurement usually modifies the state of the measured quantum object unless it is already in a basis state (mathematically, one of the eigenvectors of the measurement observable operator...). After measuring a quantum object state, performing the same measurement on the already measured system will not provide any additional information. In order to increase our knowledge on the final state of some quantum computation, the only solution is to start again the computation from the beginning and measure again the final state. The subtlety being that this new final state has not yet been measured and thus corresponds exactly to the one we are trying to infer. Then, we compute an average of the obtained results across several experiments. Some measurement techniques like gentle measurement or weak measurement are designed to minimize this back action and are sometimes used in quantum error correction codes.

Balmer series: set of four spectral emission or absorption lines with the hydrogen atom, generated by electron transitions between the second and higher energy levels of the atom.

Beam splitter: optical device that splits a beam of light in two. It's usually made with two glued triangular glass prisms. Polarizing beam splitters are a particular class of beam splitters that use birefringent materials to split light into two beams of orthogonal polarization states.

Balanced beam splitter: beam splitter where the light is equally divided in two streams.

Baryon: class of elementary particles of the first level of the nuclei of atoms. It contains protons and neutrons.

Bell inequalities: Bell's 1964 theorem proves that no hidden variable theory - imagined by Einstein in 1935 - can reproduce the phenomena of quantum mechanics. Bell's inequalities are the relations that measurements on quantum entangled states must respect under the hypothesis of a local deterministic hidden variable theory. Experiments shows that Bell's inequalities and related statistics are systematically violated, forcing scientists to give up one of the three following hypotheses on which Bell's inequalities are based. The first is the locality principle according to which two distant objects cannot have an instantaneous influence on each other, which means that a signal cannot propagate at a speed greater than the speed of light in a vacuum. The second is causality, according to which the state of quantum particles is determined solely by their experience, i.e. their initial state and all influences received in the past. The third is realism, which means that individual particles are entities that have properties of their own, carried with them (source).

Bell states: or EPR states are maximally entangled states of two qubits. There are four of them: $(|00\rangle + |11\rangle)/\sqrt{2}$, $(|01\rangle + |01\rangle)/\sqrt{2}$, $(|00\rangle - 11\rangle)/\sqrt{2}$ and $(|01\rangle - |01\rangle)/\sqrt{2}$. The first of the Bell state is generalized in GHZ states with n qubits and the second is generalized as W states.

Bell test statistic: it is a test of correlation of quantum state detection with two entangled quantum objects which can have values A and A', and B and B'. Quantum entanglement showing a correlation of the values of these two objects will yield and average value of: $|S| = \langle AB\rangle_{lim} + \langle AB'\rangle_{lim} + \langle A'B\rangle_{lim} - \langle A'B'\rangle_{lim} = 2\sqrt{2}$ (about 2.828). In this formula, $\langle A'B\rangle_{lim}$ is the probability to have outcome A with the first quantum object and outcome B' for the second. It's usually a photon polarization. This test is also a way to evaluate the entanglement of two qubits in quantum computers.

Black body: a body that is in thermal equilibrium with the radiation it emits. It can be the inside of a furnace or a star. It is by studying the radiation of the black body and its frequency distribution as a function of the body temperature that Max Planck uncovered the existence of energy quanta

in 1900. Also written blackbody or black-body depending on the source.

Blind Quantum Computing: technique for distributing quantum processing in remote quantum processors and securing the confidentiality of the processing.

Bloch sphere: geometric representation of a qubit state with a vector in a sphere of radius 1. The qubit ground state is an upwardly directed vector $|\mathbf{0}\rangle$ and the excited state is a downwardly directed vector $|\mathbf{1}\rangle$. An intermediate state vector is defined by its amplitude and phase, in line with the wave-particle duality of the qubits. It models of the state of a qubit using polar coordinates with two angles, one indicating the amplitude of the quantum and the other its relative phase.

Born rule: postulate of quantum mechanics created by Max Born in 1926 giving the probability that a measurement of a quantum system will yield a given result. It states that the probability density of finding a particle at a given point, when measured, is proportional to the square of the magnitude of the particle's wavefunction at that point.

Bose-Einstein Condensate, or BEC, state of very low density boson gas cooled to a temperature close to absolute zero (-273.15°C) where a large part of the bosons are in the lowest possible quantum energy state and exhibit particular properties such as interferences. A special case of BEC is superfluid helium, discovered in 1938, which, at very low temperatures, has no viscosity, i.e. it can move without dissipating energy. These condensates were imagined and theorized by Satyendra Nath Bose and then Albert Einstein in 1924. Their existence was demonstrated experimentally in 1995 by Wolfgang Ketterle, Eric Cornell and Carl Wieman who were awarded the Nobel Prize in Physics in 2001. In quantum computing, this field is related to the field cold atom-based qubits.

Boson sampling: typical experiment with photons qubits that mixes photons in an interferometer. It's hard to emulate on a classical computer and is used to show a specific quantum advantage. The only caveat is these experiments are not programmable and are therefore entirely useless and irrelevant to compare any calculation capacity between systems.

Boson: particles with gregarious behavior, which can accumulate in arbitrarily large numbers and in the same state. Bosons comprise photons and composite objects with whole integer spin such as hydrogen, lithium-7, rubidium-87, carbon and silicon atoms in crystalline structures. These particles escape Pauli's exclusion principle. They have a symmetrical wave function.

Bosonic codes: hardware system that implement quantum error corrections with bosonic modes, using a quantum harmonic oscillator with a continuous energy levels. It includes cat-qubits, GKP codes (Gottesman-Kitaev-Preskill) and binomial codes.

BQP (problem class): complexity class of problems that can be handled by quantum algorithms. Means a bounded-error quantum polynomial time. It is the class of problems that can be solved in polynomial time relative to the size of the problem with a probability of obtaining an error not exceeding one third of the results. This class is positioned between the class P (problems that can be solved in polynomial time on a classical machine) and NP (problems for which a solution can be verified in polynomial time on a classical machine).

Bra-ket (notation): A notation model describing the state of a quantum and a qubit in the form $|\boldsymbol{\psi}\rangle$ and $\langle\boldsymbol{\psi}|$. It was created by Paul Dirac in 1939. A bra psi vector is a quantum state described as a column vector. A ket is its transpose, a row vector. It facilitates the writing of operations with quantum states, like inner products $\langle\boldsymbol{\phi}|\boldsymbol{\psi}\rangle$, outer product $|\boldsymbol{\phi}\rangle\langle\boldsymbol{\psi}|$ and projection $\langle\boldsymbol{\psi}|\boldsymbol{A}|\boldsymbol{\psi}\rangle$.

Cavity quantum electrodynamics (CQED): field of quantum physics coupling trapped atoms in physical cavities and microwaves. It is about the interactions between photons and electrons and atoms.

Chandelier: nickname of the quantum computing system located inside the cryostat of a superconducting or electron spins quantum computer. It contains several stages made of copper disks covered with gold. These disks are crossed by numerous coaxial cables that are used to drive the qubits and read their state with microwaves. It is completed by filters, attenuators and amplifiers for the microwaves that circulate in these wires, various sensors, and heat exchangers that cool the copper disks, which in turn cool the elements that are placed on them.

Chi: Greek letter used to define the level of nonlinearity of an optical medium. A $\chi^{(i)}$ medium had a nonlinearity of level i. When i=2, the medium has a second order nonlinearity. It is used for example for the frequency doubling of laser light. With i=3, it is a third order nonlinearity, which is used for example in four-wave mixing. Chi is a coefficient of the polynomial relation between the phase P change of a light beam traversing the medium and the beam energy E, with the formula $P = \epsilon_0(\chi^{(i)}E^i)$.

Circuit quantum electrodynamics (cQED): architecture used in solid state qubits systems using superconducting qubits and microwave photons. Science behind the interactions between microwaves and electromagnetic circuits.

Clifford group: group of unitary quantum gates that can be easily simulated in polynomial time on classical computers according to Gottesman-Knill's theorem. A Clifford gate is a quantum gate that can be decomposed into gates of the Clifford group. It is sufficient to have one unitary gate rotating on the X axis and another on the Z axis to create a complete set of Clifford gates. They must be completed with at least one two-qubit gate as a CNOT. These gates make quarter turns or half turns in the Bloch sphere. They are not sufficient to create a universal gates set. You need non-Clifford gates like the T gate.

Circuit: describes a set of quantum gates applied in an orderly fashion to a register of qubits. In other word, it is a quantum program for a gate-based quantum computing system. A graphical representation of a quantum circuit shows qubits in stacked horizontal lines, quantum gates as boxes labelled X, Y, Z, H and others applied to single qubits and two or three quantum gates with vertical lines

connecting qubits. The X axis represents time and gates are executed from left to right.

Cluster state: the starting point for an MBQC (Measurement Based Quantum Computing) calculation with a grid of embedded qubits that are usually initialized in an entangled state. Used mostly with photon qubits.

CMOS: a common semiconductor fabrication technique used to produce processors and memory, and which is reused to create qubits that manipulate electron spins.

Code distance: notion used in quantum error correction codes and with the stabilizer codes formalism which is linked to the smallest number of simultaneous qubit errors that can be fixed with a given quantum error code. A code distance d means that the error correction code can correct errors for up to (d − 1)/2 qubits. These are usually even numbers (3, 5, 7, …). So a code distance of 7 can correct at most 3 qubits.

Coherence: quantum coherence is the ability of a quantum system to demonstrate interference. The coherence between different parts of a wave function allows for the famous double-slit interference and the formation of short quantum wave packets propagating in space. Two wave sources are coherent when their frequency and waveform (or phase for an electromagnetic signal) are identical. There are temporal coherence (same waveforms with some time delay), spatial coherence (in 2D or 3D such as with plane waves) or spectral coherence (waves of different wavelengths but with a fixed relative phase form a wave packet). In quantum physics, coherence comes with linear superposition of various states of a quantum system containing one or several quantum objects (represented by a wave due to the wave-particle duality). Quantum coherence progressively degrades naturally due to the interactions with the environment and ends after a certain time for qubits (the coherence time) and also when measuring the state of a qubit.

Cold atoms: atoms cooled at very low temperatures, generally with techniques using lasers and the Doppler effect. They are used in certain types of quantum computers called cold atom quantum computers. The atoms used are neutral atoms (not ionized) and quite often rubidium, an alkali metal.

Compatible properties: physical properties of a quantum system that can be measured in any order or simultaneously.

Commutativity: mathematically, two variables A and B commute when A×B=B×A. They do with integers but not with non square matrices. Even square matrices don't necessary commute. They are then "noncommutative".

Commutator or commutation operator: Characterize the level of non-commutativity between two variables, usually matrices. For two matrices A and B, their commutator is [A,B]=AB-BA.

Complementarity: principle of quantum physics introduced by Niels Bohr in 1927 according to which quantum objects have certain pairs of complementary properties which cannot all be observed or measured simultaneously. These are incompatible properties. Another version of this principle is that it's not possible to simultaneously observe a quantum object as a particle and as a wave, like in the Young slit experiments.

Complementary variables: pairs or complementary variables or properties according to the Bohr complementary principle.

Complex number: set of complex numbers created as an extension of the set of real numbers, containing in particular an imaginary number noted i such that $\boldsymbol{i^2 = -1}$. Any complex number can be written in the form a + ib where a and b are real numbers. These numbers are used in particular to describe the state of a qubit and to represent the phase of a quantum object with its complex component.

Complexity (theory): branch of theoretical computer science and mathematics that plays an important role in quantum computing to evaluate its performance compared to traditional Turing/Neumann machine computing. It defines classes of problems by levels of complexity, in terms of computing time or even the memory space required, with, in particular, problems that are solved in polynomial time in relation to their complexity (class P) and whose results are verifiable in polynomial time (class NP). The methods used to solve these problems are most often based on the brute force of navigating through an increasingly large space of combinations to be evaluated according to the size of the problem to be solved.

Compton effect: effect which demonstrates that photons can have some momentum and behave as particles, that was demonstrated by Arthur Holly Compton in 1922 with scattering of X rays and gamma rays photons by atomic electrons.

Computational basis: naming of the basic states of a qubits register. For a single qubit, this corresponds to the $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$ states. For a register of N qubits, the computational basis is made of the 2^N combinations of series of N 0s and 1s, named in Dirac's notation $|\mathbf{000}\ldots\mathbf{000}\rangle$ to $|\mathbf{111}\ldots\mathbf{111}\rangle$. All these states are mathematically orthogonal with each other. A N qubits register in a pure state mode is a linear superposition of all these states using complex amplitudes.

Concatenated codes: describes the recursive application of error correction codes where in an error correction code, a physical qubit is replaced by a logical qubit, and so on.

Condensed matter physics: branch of physics that studies the macroscopic properties of matter (solids, liquids, glasses, polymers) and in systems where the number of constituents is large and the interactions between them are strong. Condensed matter physicists seek to understand the behavior of these phases using the laws of physics (quantum mechanics, electromagnetism and statistical physics). In practice, it mainly covers low temperature superconducting, ferromagnetic, antiferromagnetic and ferrimagnetic phases of spins in crystalline lattices of atoms, spin glasses, spin liquid, and Bose-Einstein condensates. Physicists working on superconducting qubits are part of this discipline.

Conjugate variables: pairs of dynamic variables describing the state of a quantum object, like position and

momentum, that are related to the other with the Heisenberg indeterminacy principle which prevents a precise measurement of both variables.

Continuous variables quantum computing (CV): a type of quantum computer that uses qubits whose values are continuous and not binary. Used in two types of quantum computers: analog quantum simulators (particularly based on cold atoms) and CV photon-based systems.

Cooper pair: pairs of tightly coupled electrons creating electric current flow in superconducting materials, usually at very low temperatures and without resistance. Cooper pairs have an integer spin because they accumulate two electrons with a spin of ½. They become bosons and can accumulate and form macro quantum objects.

Copenhagen interpretation: interpretation of quantum physics elaborated by Niels Bohr in Copenhagen and by Werner Heisenberg, although it was never clearly formalized. Applied to individual quantum objects, it is mostly based on Bohr's correspondence and complementarity principles, Heisenberg's indeterminacy principle, Born's probability interpretation of the Schrodinger wave function and on the wave function collapse and its fundamental indeterminism. It avoids describing any reality beyond what can be measured like an exact position of an electron. The completeness of this theory was challenged by Albert Einstein. Physicists are still debating about this interpretation, as part of the quantum foundation field.

Correspondence principle: principle formulated by Niels Bohr in 1920 which states that the behavior of systems described by quantum physics matches classical physics in the limit of large quantum numbers (large orbits and large energies or electron quantum numbers).

Coulomb blockade: decrease of electrical conductance at small bias voltages of small electronic devices containing at least a low-capacitance tunnel junction. As a result, the conductance of the devices may not be constant at low bias voltages, but disappears for biases under a certain threshold, i.e. there is no current flows.

Coulomb force: electrostatic force between electrically charged particles like electrons and protons. Its strength is inversely proportional to the square of their distance and proportional to the product of their respective charge.

CPTP map: completely positive and trace preserving map or operator also referenced as a quantum channel or superoperator. It is a linear operator that turns a density matrix describing a mixed state system into another density matrix. Its size is then the square of the density matrix size, so 2^{4N} for a system of N qubits. It can describe any operation on a mixed state system: some quantum gates, any sort of measurement, quantum filters, as well as feedback networks in quantum control theory.

Crosstalk: in the qubit field, is a phenomenon where an action on a given qubit or set of qubits has a side effect on other qubits. Of course, various techniques are employed to minimize it like, in the case of superconducting qubits, with using tunable couplers between qubits. Then, there are several crosstalk types like IX, IY, IZ, ZX, ZY, ZZ which depend on the type of interactions between qubits.

Cryogenics: cooling technology. Very low temperature cryogeny is used with superconducting and electron spin qubits computers. The temperatures required to stabilize qubits and reduce their error rate are very close to absolute zero: around 15 mK. The most commonly used systems are dilution refrigerators that use helium-3 and helium-4. Cryogenics is also used for photon generators and photon detection systems, but at a higher temperature situated between 2K and 10K.

CSCO: complete set of commuting observables, the most complete measurement of a quantum system comprised of compatible properties that can be measured in any order.

CVD: chemical vapor deposition, an additive manufacturing technique for semiconductors, where the target surface is exposed to one or more volatile precursors, which chemically react and/or decompose on the target surface to leave a thin film deposit on the target, e.g. using silane SiH_4 to deposit Si on the wafer, generating 2 H_2 molecules.

DAC: digital-analog converter. Classical electronic device converting a digital signal into an analog signal. Is used in the microwave generation systems implemented to control superconducting and electron spin qubits.

Dark count: photons detected by photon detectors that come from the environment and thermal or tunneling effect. This explains why most single photon detectors must be cooled at a temperature usually below 10K.

De Broglie wavelength: wavelength of a particle calculated with its momentum p with h/p, with h being Planck's constant.

Decoherence: marks the end of the coherence of a quantum object or a qubit. It is notably caused by the interactions between the quantum objects and their environment. One often uses indifferently the expression coherence time (time during which the qubits are in a state of superposition and entanglement with other qubits) or decoherence (time at the end of which this superposition and entanglement end), which is the same.

Degenerate: a quantum system energy level is degenerate if it corresponds to two or more different measurable states with different quantum numbers. Mathematically, a quantum state is degenerate when several linearly independent eigenvectors may have the same eigenvalue. A normalized linear combination of these eigenvectors is also an eigenvector with the same eigenvalue. The number of linearly independent eigenvectors having the same eigenvalue corresponds to the degree of degeneracy of the quantum system. The number of different eigenstates corresponding to a particular energy level is the degree of degeneracy of the level. This happens for example when the energy level alone is not sufficient to characterize the state of a quantum system. That's where we need other quantum numbers to characterize the state. This is the case with the hydrogen atom electron. Its energy level depends only on its principal quantum number n (the electron layer), and not the three other electron quantum numbers (orbital angular momentum, magnetic moment and spin, although this degeneracy can be broken with using relativistic quantum mechanics and hyperfine structure splitting of electron energy levels). But you also have degenerate quantum error

correction codes, which are supposed to correct more errors than they actually detect, particularly with noisy quantum channels (meaning practically qubits gates). Another example is an atom's nucleus energy level that is only dependent on its orbital angular momentum in the absence of magnetic field. Different energy levels arise with a magnetic field due to the nucleus magnetic quantum number.

Density matrix: matrix of complex numbers used to describe the statistical state of a physical system that is more precise than the computational state vector used in quantum computing. Density matrices are useful to describe so-called mixed states versus pure states that are sufficiently described with state vectors. They are used to describe what happen to subsystems of entangled systems, when decoherence happens and also, during measurement.

Dequantization: said about some quantum algorithm where an efficient classical equivalent is found. Term initiated with Ewin Tang's work on recommendation systems in 2018, when she found a dequantized classical equivalent to a quantum recommendation algorithm devised in 2016 by Iordanis Kerenidis and Anupam Prakash. Interestingly, quantization is a term used in artificial intelligence and deep learning when the numbers used in these models are integers (or even binary numbers) instead of floating point numbers.

Determinism: situation when events are determined completely by previously existing causes and parameters. Applied to classical mechanics to predict objects position and momentum based on initial conditions. Contrarily, in quantum physics, it is not possible to determine simultaneously the position and momentum of any particle at any instant. This indeterminism is observed with quantum measurement when the quantum object is in a superposed state.

Deutsch-Jozsa (algorithm): quantum algorithm created in 1992 by David Deutsch and Richard Jozsa. It can check whether a given function is balanced or not, i.e. whether it always returns 0 or 1, or 0 and 1 in equal proportions. The alternative between equilibrium (as many 0's as 1's) or not (as many 0's or 1's in output) is a starting postulate. The gain in performance compared to classical algorithms is exponential. In the case of N qubits, the function should be classically evaluated on at least half of the possible input values, i.e. $2^{N-1}+1$. Unfortunately, this algorithm is not very useful.

DFT (Density Functional Theory): mathematical model used to describe the structure of molecules at rest as a function of inter-atomic interactions. Used in high-performance computing as well as in quantum computing for chemical simulation.

Diffraction: phenomenon created when a wave encounters an obstacle or opening, like a small hole or slit. It is generated by the bending of photon waves around the corners of the obstacle. It creates interferences between the passing waves as they are detected in a plane further down the waves path. The phenomenon can be described classically with the Huygens–Fresnel principle that considers points in the hole or slit as a collection of individual spherical wavelets. The interference pattern shows up with laser light and can also be explained by the photon wave functions and their probability distribution. All-in-all, you can consider that a Young single-slit experiment also create quantum interferences!

Dilution refrigerator: name given to the very low temperature cryostats used to cool quantum computers below 1K. They cool superconducting or electron spin chipsets to respectively 15 mK and 100 mK. Dilution is related to the use a mixture of two helium isotopes (3 and 4), which are diluted in a mixing chamber, the two isotopes having slightly different physical properties. A helium 4 cryostat only goes down to about 2.8K, a helium 3 cryostat goes down to 300mK while a cryostat using both goes down to 10mK. The most common variant is the "dry" as opposed to "wet" dilution refrigerator. This version uses less helium and leaves more space in the chandelier to house electronic and quantum devices.

Dirac's notation: see bra-ket.

Dirac constant: Planck constant divided by 2π, also called reduced Planck constant and denoted $\hbar$ (h-bar). Some physicists called sometimes, abusively, this constant "Planck constant".

Discrete log problem: mathematical problem consisting in finding a log of a number that happens to be an integer. It is used in finding the solution of cryptographic problems with quantum algorithms. Shor's dlog algorithm is a quantum algorithm solving discrete log problems.

Distillation: technique used in quantum error correction codes based on magic states. It consists in combining several magic state qubits to feed others with a lower error rate. Distillation has the effect of purifying the state of qubits, meaning turning mixed states into pure states.

Doppler effect: shift in the electromagnetic spectrum due to the speed at which the source moves away from or closer to the observer. If the source moves away from the observer, the light wavelength is shifted towards the red (redshift), otherwise towards the blue. This effect is used in particular in the technique of atoms laser cooling. It consists in illuminating atoms that are in thermal motion with a wavelength that is just below the absorption level of the atoms. Those atoms moving towards the laser beam will absorb the photon, which will reduce their kinetic energy and movement. Those atoms moving in the other direction will not absorb it because the apparent frequency of the photon will be too low to change the energy state of the atoms. As atoms get cooled, the cooling laser wavelength has to be adjusted. This technique allows atoms to be cooled to below mK (milli-Kelvin).

D-Wave: Canadian company designing quantum annealing computers. They do not have the same power as universal gate quantum computers with equal numbers of qubits. The current generation of D-Wave "Advantage" using Pegasus chipsets includes 5000 qubits.

EBL: electron beam lithography, a lithography technique that is focusing a beam of electrons on an electron-sensitive resist film to remove matter in specified areas, without requiring a mask like with photolithography. It is used to create 1nm precision nanostructures like with photon-generating quantum dots and also superconducting qubit

chipsets. It's a rather slow process compared with photolithography that is adapted to low volume and custom productions.

Eigenstate: for a quantum object, these are the elementary wave functions in which it is possible to decompose it. They are represented by eigenvectors.

Eigenvalue: see eigenvector.

Eigenvector: for a square matrix A, an eigenvector x of A is a vector that verifies the equation $Ax = \lambda x$, λ being a real number called eigenvalue. Their direction do not change once multiplied with matrix A.

Electromagnetic spectrum: all electromagnetic radiation from the largest radio waves to X-rays and gamma rays. Visible light is only a very small part in the middle of this spectrum. An EM wave is decomposable in a number of photons, the smallest elementary unit of an EM wave.

Electron: elementary particle found in atoms, orbiting the nucleus, but also in freeform traveling between atoms and creating something we know as being electric current. According to Bohr's model developed in 1913, there is a finite number of electron orbits around the nucleus of atoms. The movement of electrons from one orbit to another corresponds to the absorption or emission of a photon. Electrons are elementary particles in the standard model because it is not composed of sub-particles, unlike neutrons and protons which are composed of quarks. According to quantum physics, the electron as many other particles behaves as a particle and as a wave. Electrons are often used in qubits, in the form of electrons circulating in semiconductors loops or who are trapped in quantum dots or electromagnetic cavities and whose spin is controlled.

Electron gas: describes the behavior of free valence electrons in metals and semiconductors when they move around free of the atom nucleus. Their behavior is governed by the Pauli exclusion principle (1925), Dirac-Fermi statistics (1926) and Arnold Sommerfeld's quantum theory of metal (1927). Electron gas enable the modeling of electric conductivity, electron heat capacity and electric thermal conductivity as well as the Hall and quantum Hall effects. There are 1D, 2D and 3D electron gases. 1D electron gas are observed in semiconductor nanowires and carbon nanotubes. 2D electron gas show up in semiconductor quantum wells and in graphene sheets.

Elliptic Curves Cryptography (ECC): a type of public key cryptography that is potentially broken by Shor's quantum algorithm. One of its advantages is that it requires small keys, about three times smaller in number of bits than RSA public keys.

Energetics of quantum technology: cross-disciplinary research field and sector studying the energetics of quantum computing but also quantum telecommunications, cryptography and sensing. It's about making sure quantum technologies are not power hungry and also dealing with the energetic constraints related to quantum computing scalability. It's about balancing the act between cooling requirements, cabling, control electronics to ensure quantum computers can scale in number of physical and logical qubits.

Entanglement: quantum phenomenon where two quantum objects are related with each other in a way that a measurement done on these two objects generates a correlated (but random) value. Mathematically speaking, two quantum objects are entangled when their quantum state (psi, vector state) cannot be expressed as the tensor product of individual quantum states. This process is used to link qubits together through two or three qubit quantum gates in quantum computers. It is also used in quantum cryptography and telecommunication systems based on entangled photons in QKDs.

Entropy: measures the degree of disorder and randomness of a physical system. Key concept related to the second law of thermodynamics that states that the entropy of an isolated system cannot decrease spontaneously. In quantum mechanics, the (Von Neumann) entropy of a system is $-tr(\rho log \rho)$ where ρ is the density matrix describing the system state.

ERC Grants : European Research Council grants. Funding of European research projects with several levels, the top of which is the Synergy Grant which funds "moonshots" in European research associating at least two principal investigators (PIs) from public or private research laboratories. 14M€ is the maximum funding for such a project with 10M€ of core funding and 4M€ which can notably finance heavy investments or access to large infrastructures. Other levels include the Starting grants with up to 1.5M€ for 5 years and the Consolidator grants with 2M€ also for 5 years.

Ergodicity: capacity of a moving system to explore all parts of the space in which it can move in, in a uniform and random manner. The phenomenon occurs with many physical systems like with electrons. Quantum ergodicity states that in the high-energy limit, quantum objects tend to a uniformly distribute in the classical phase space.

Ergotropy: maximum amount of work that can be obtained from a quantum system.

Error Correction Codes: describes both logical methods and physical architectures to correct physical errors happening in both classical and quantum computing and telecommunication technologies.

Errors: a major concern in the operation of quantum computers. Operations on qubits: one and two qubit gates and qubit readouts generate errors that must be minimized. Error rates are in 2021 between 0.1% and 2% for quantum gates. When several quantum gates are chained together, the rates of correct results (1 - error rate) multiplies quickly to the point of distorting everything. This is avoided either by reducing the physical level error rate like with cat-qubits, using shallow algorithms (low number of gates) or with error correction code systems.

Eta letter: η, used to describe error rates or efficiency, Carnot engine efficiency, and also Landau symmetry breaking.

Exclusion principle: see Pauli exclusion principle.

Expectation value: average or mean value of an observable. With an observable operator A on a quantum state ψ, the expectation value is $\langle a \rangle = \langle \psi | A | \psi \rangle$. In other words, it's a scalar product of the ψ vector and the vector resulting

from the projective measurement of ψ using the observable A. In layman's term for a qubit, it is either the average value that would be obtained when doing an experiment, a large number of times and measure the value of the qubit yielding 0 or 1, and making an average, or the result of its mathematical evaluation if you have a clear idea of the qubit quantum state description. For example, after an Hadamard gate is applied to a $|0\rangle$ qubit, the expectation value of its measurement in in the typical z basis will be 0,5. Some algorithms output like in chemical simulations output real number values that are obtains through expectation value assessment using a large number of computing runs.

Euclidean networks: class of encryption algorithms used in post-quantum cryptography (PQC).

Fabry-Pérot cavities: equipment used in lasers that combines two parallel mirrors, one of which is semi-reflective. This contributes to the creation of the laser effect in the cavity. The length of the cavity is generally a multiple of the laser light wavelength, at least if we want to emit coherent light with photons having all the same phase. The name of the cavity comes from the French scientists Charles Fabry (1867-1945) and Alfred Pérot (1963-1925).

FBQC: fusion-based quantum computation, a variant of MBQC crafted by PsiQuantum that is based on micro-clusters states with groups of 4 qubits connected together and using Resource State Generators (RSGs). It's replacing measurement of entangled states in MBQC with double measurement of non-connected adjacent qubits to create entanglements between them.

Fermi sea: electrons filling the lowest atom orbits or degenerate low-energy states within a solid and at very low temperature near 0 K. It corresponds to low-energy states that do not participate in materials thermal activity.

Fermions: particles with individualistic behavior. Two particles of this type cannot be in the same state at the same place. This includes electrons, quarks, half-integer spin composite objects. For example, deuterium, lithium-6, potassium-40 atoms (source: Jean Dalibard). In contrast, integer spin bosons such as photons and some atoms can accumulate in the same state. In a word, bosons are communists and fermions are ultra-liberals.

Fine structure: splitting of an energy level or spectral line into several distinct components that take into account electron spins and relativistic corrections to Schrodinger's wave equation.

Floquet code or Planar Honeycomb Code is a family of quantum error corrections codes created by Matthew B. Hastings and Jeongwan Haah from Microsoft in 2021. It simplifies toric codes with fewer qubits and stabilizers and is adapted to qubits architectures implementing pair-wise qubit measurements like with the elusive Majorana fermions.

Fluxonium: variation of flux superconducting qubit. It has a better coherence time than transmon, above 100 µs but two-qubit gates are more difficult to implement, and this architecture seemingly has not yet been tested beyond 10 functional qubits.

Flying qubits: qubits that can move, as opposed to stationary qubits that do not move. They are usually photons but there's a small branch of flying qubits studying flying electrons.

Fock space: mathematical object of algebra used to describe the quantum state of a set of identical particles whose number is variable or unknown. It is a Hilbert space made up of the sum of the tensor products of Hilbert spaces for the particles that make up the set.

Fock state: defines a group of quantum objects, like photons, who have the same quantum numbers and are indistinguishable. They are defined by their number, a photon number in the case of photons, and their common quantum numbers describing the quantum objects state.

Flux biasing: technique used to control with some direct current the resonant frequency of a frequency-tunable superconducting.

Fourier Transform: mathematical decomposition of a time domain signal into elementary single frequency signals with their frequency, amplitude and phase. It is a complex value function of time with, for each frequency, a magnitude (real part) and a phase offset (complex part) of the sinusoid of this elementary frequency. The inverse Fourier transforms that frequency decomposition function back into its original compound signal.

FPGA: Field Programmable Gate Arrays. Integrated circuit where some or all functions can be dynamically defined and program on-demand. It can have analog and digital features. Modern FPGAs also embed full-fledge processing units (Arm cores, GPUs, neural processing units, networking units). FPGAs are used in qubit control electronics for reading out the signals coming from the resonators attached to superconducting and electron spin qubits. It measures the phase and amplitude of the reflected microwaves after they are converted from analog to digital with an ADC (analog-digital converter) that can be embedded in the FPGA.

Fredkin gate: quantum gate operating on three qubits that inverts the state of the second and third qubit if the first qubit is 1. Also called CSWAP gate (conditional SWAP).

FTQC: Fault-Tolerant Quantum Computer. Error-resistant quantum computer that is based on logical qubits made of many physical qubits and implementing quantum error correction. Fault-tolerance is based on the error correction making sure errors don't propagate to many qubits.

FTDQC: Fault Tolerant Distributed Quantum Computation, and extension of the FTQC concept to distribution quantum computing.

Gate-based quantum computing: the broader category of quantum computing system based on qubits and quantum circuits implementing quantum gates on 1, 2 and 3 qubits at a time.

Gaussian Boson Sampling (GBS): variation of a boson sampling experiment that uses Gaussian states photons as input. It's a physical model that is even more difficult to digitally simulate than a boson sampling since the

underlying mathematical object is a Hafnian instead of a permanent, that is even more complicated to compute.

Gaussian state: describe particular photon states that are classical. The gaussian curve is the form in three dimensions of Wigner's function which describe the phase and amplitude distribution of the photon. It is opposed to non-Gaussian states which are non-classical, with some negative Wigner function values and a non-Gaussian form for the 3D function.

GHZ: means something other than giga Hertz in quantum computing! It is a three-qubit Greenberger-Horne-Zeilinger superposed state that allows to demonstrate the inexistence of hidden variables in the quantum entanglement of at least three particles and with a finite number of measurements. The concept dates back to 1989 and has been experimentally validated in 1999.

GKP qubits: error corrected qubits according to a method proposed by Gottesman, Kitaev and Preskill that encodes a qubit in a harmonic oscillator. It is works with photon qubits using linear elements for Clifford gates.

Gleason's theorem: according to Andrew M. Gleason's theorem proved in 1957, the functions assigning probabilities to measurement outcomes are projection operators that must be expressible as density operator and follow the Born rule. This determines the way to calculate probabilities and the set of possible quantum states.

GPGPU: General Purpose Graphical Processing Unit, used for simulation, scientific computing and machine learning, like the Nvidia V100, A100 and H100. These are coprocessors which are mostly not anymore used for graphics software or gaming but more for machine and deep learning and scientific computing, thus the "general purpose" nickname addition.

Grotrian diagram: diagram used to show the various electronic energy transitions for a given atom, introduced in 1928 by the German physicist Walter Grotrian. The indicated frequencies of transitions to higher energy levels provide an indication of their source like lasers (in the hundreds of nm wavelengths) or microwaves (in the 4-20 GHz frequency regimes).

Ground state: lowest energy state of an atom, other states being excited states. The hydrogen atom ground state happens when its electron occupies the lowest energy level (with main quantum number = 1). More generally, is said of a qubit that is in its ground basis state $|\mathbf{0}\rangle$.

Grover (algorithm): quantum algorithm for finding an element in a non-indexed array or a unique element for which an oracle function returns 1.

H-bar: see Dirac constant.

Hadamard (gate) : quantum gate creating a superposed state between $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$ in a qubit when starting with $|\mathbf{0}\rangle$ or $|\mathbf{1}\rangle$.

Hall effect: production of a voltage difference across an electrical conductor that is transverse to an electric current in the conductor and to an applied magnetic field perpendicular to the current. The effect was discovered by Edwin Hall in 1879.

Hamiltonian: equation describing the total and potential energy of a system of quantum objects. It is the global operator of the right part of Schrödinger's equation. This notion is used in D-Wave quantum annealing computers and with quantum simulators. "Preparing a Hamiltonian" in this kind of computer is equivalent to setting up a matrix of qubits linked together by potentials and which will seek a minimum energy resulting in a balanced Hamiltonian corresponding to the solution of the problem to be solved. The solution is about finding the right combination of qubits states (up/down for quantum annealing) that minimizes the energy of the whole system.

Hamming distance: metric used to compare two binary data strings of equal lengths. It is the number of bit positions in which the two bits are different. For two strings a and b, it is denoted as d(a,b).

Harmonic oscillator: in classical mechanics, system that, when displaced from its equilibrium position, experiences a restoring force proportional to its displacement x with a frequency that does not depend on the amplitude. Quantum physics formalize the whereabouts of many harmonic oscillators including photons in cavities, superconducting qubits, phonons, diatomic molecules, etc.

Hartree-Fock: method to compute atomic structures using the time dependent Schrödinger's wave equation.

Heisenberg (principle of indeterminacy): fundamental principle of quantum mechanics which postulates that there is a lower limit to the precision with which one can measure two independent parameters relating to the same object such as its speed and position or the energy emitted and the duration of emission.

Heisenberg limit: in quantum sensing, like with interferometry, the optimal rate at which the accuracy of a measurement can scale with the energy used in the measurement. More precisely, not every quantity is a quantum observable that can be measured directly. The estimation of such quantity, however, can be performed by measuring a state whose probability distribution depends on it. To evaluate the accuracy of this estimation, one often considers the variance of the estimated quantity. When using, for instance, an ensemble of photons as the meter probing our parameter of interest, if these photons are allowed to be initially entangled, then this variance is lower bounded by the fundamental Heisenberg limit. As for the standard quantum limit, it implies that the more resources, the more accurate the measurement. However, only quantum probing resources can reach the Heisenberg limit which states that our estimation's standard deviation is at best inversely proportional to the size of the meter, hence here the number of photons. The Heisenberg limit can be reached in quantum sensing with using entangled objects with a precision that scales better at a rate of 1/N instead of $1/\sqrt{N}$ with the standard quantum limit. The Heisenberg limit is reached with using so-called NOON states superposing N (bosonic) objects (like photons) in a state with all the objects being in one or the other of two modes.

Helium 3: a rare isotope of helium that is used in cryogenic quantum computer systems to generate temperatures below 1K as part of dilution refrigeration systems. It is

usually produced from tritium in specialized nuclear power plants, including the US Department of Energy's Savannah River nuclear power plant.

Helium 4: a common helium isotope that is also used in cryogenic systems.

Heralded single-photons: pairs of single photons can be generated in highly correlated states from using a single high-energy photon to create two lower-energy ones. One photon from the resulting pair is detected to "herald" (or "signal") the other so its state is pretty well known prior to its own detection or whereabouts. The two photons need not be of the same wavelength, but the total energy and resulting polarization are defined by the generation process. Two commonly types of heralded single-photon sources are SPDC (spontaneous parametric down-conversion with line width in the THz range) and SFWM (spontaneous four-wave mixing with line width in the MHz range or even narrower). It's used with QKD.

Heterodyne measurement: method used for extracting information from an oscillating signal along two orthogonal components in phase space like the in-phase and quadrature signals coming out of an I/Q mixer. In this type of measurement, two conjugate operators are measured simultaneously, which create added noise.

Hilbert (space): vector space of real or complex numbers with a Euclidean or Hermitian scalar product, which is used to measure distances and angles and to define orthogonality. It is an n-dimensional extension of the concept of three-dimensional Euclidean space. In quantum mechanics, the state of a quantum is represented by a vector in a Hilbert space with as many dimensions as the number of basic (or observable) states of this quantum. These are geometrical spaces which are used in particular to measure lengths and angles, to make projections on dimensions and to define the orthogonality between vectors.

Hidden variables: interpretation proposals of quantum physics based on the use of (yet) unobservable hypothetical entities what would explain phenomena like entanglement and describe reality. Bell's theorem implies that local hidden variables of certain types cannot exist. Based on the assumption, promoted by Albert Einstein in the famous 1935 EPR paper, that quantum physics is an incomplete theory.

Homodyne measurement: method used for extracting information encoded as modulation of the phase and/or frequency of an oscillating signal. It compares that signal with a standard oscillation carrying no information. Homodyne detection uses a single frequency where heterodyne detection uses dual frequencies. Since we measure only one characteristic of the signal, it can yield a better precision than with heterodyne measurement which captures two characteristics using two conjugate operators.

HPQC: High Performance Quantum Computing, a quantum analogue of HPC (High Performance Computing). These are currently theoretical models of quantum mainframes comprising giant matrices of qubits that can be partitioned for shared use by several users. See High Performance Quantum Computing, 2011 (7 pages).

Hubbard model: physics simulation model of mixed conducting and isolated systems based on a simple Hamiltonian. Mentioned in the sizing benchmark used by Amazon for its cat-qubits fault-tolerant quantum computing system being currently designed.

Hybrid quantum algorithm: an algorithm that combines classical processing running on classical computers and some processing performed on quantum computers, where needed.

Hyperfine structure: small splitting of atomic energy levels or spectral lines with electrons with the same quantum numbers into several distinct components that are explained by the interactions between the nucleus and electron clouds.

Indistinguishability: relates to bosons quantum objects that have the same quantum state in a given location and are impossible to separate with any measurement tool.

Indistinguishable photons: see Indistinguishability, photons being a common type of boson.

Integrated Quantum Photonics (IQP): technologies exploiting photons as quantum information carriers and implemented on chipsets using wafer-scale fabrication, mostly in silicon-based CMOS or with III/V materials like gallium arsenide (GaAs) and indium phosphide (InP). IQP is used in quantum telecommunications and computing. It is using optical waveguides to guide and route single-photons, provides miniaturized split and phase control circuitry, entangled state generation, overall manipulation and sometimes even photons generation and photons detection.

Interference: fundamental phenomenon of quantum physics used with the wave aspect of quantum objects, when several waves can add or annihilate with constructive and destructive interferences. Is the basis of gate-based quantum algorithms!

Invertible computation: involves computations that run both forwards and backwards so that the forward/backward semantics form a bijection. In classical computing, it can correspond to some symmetric logical circuits that can process data forward and backwards with both ends used as inputs and outputs. It's used for example in MemComputing classical processors. The principle was created by Supriyo Datta from Purdue University in Indiana, USA.

Irreversible: said in computing of a calculation that makes it impossible to compute the initial values with using the result of the calculation. This is the case with all two-classical bits gates (NOR, OR, AND). Contrarily, quantum computing gates are mathematically reversible since relying on unitary transforms that, multiplied with their transconjugate, generate an identity operator. In plain language, if you apply an unitary (set of quantum gates) to a set of qubits, you can reverse this computing with the transconjugate of this unitary. Practically, it means playing in reverse order the gates initially applied. This technique is used in the uncompute trick that we describe elsewhere.

Ion: non-neutral atom, which has a positive or negative electric charge. It is negative if its number of electrons

exceeds the number of protons (anions) and positive in the opposite case (cations).

IonQ: an American startup from the University of Maryland that pioneered the first commercial quantum computers using ion traps. Their operational record as of 2021 was 11 qubits with 32 qubits to be made readily available.

I/Q mixer: in phase and quadrature mixer, which adds two pulse signals of same frequency but with different amplitude and phase. The In-phase signal is a sinusoid and the quadrature signal is a cosine. They have a delay of $\pi/2$ or 90°. When added up in the mixer, the sum of both signals create an arbitrary phase and amplitude signal of the same frequency.

Ising (model): a statistical physics problem that can be simulated and solved using quantum algorithms, especially on quantum annealers like those from D-Wave. It models the interactions between two-levels particles (spin, ferromagnetism). All algorithms for D-Wave annealers are reduced to solving an Ising model.

Isotopes: variations of atoms where the number of protons and electron is the same, sharing the same atomic number, but when the number of neutrons is different. For example, helium can exist in the for He^3 and He^4 with one and two neutrons. Many materials involved in quantum technologies are used with particular isotopes, like Si^{28} in silicon wafer used with electron spin qubits, the reason being the number of neutrons has an influence on atom nucleus spins, that can interfere with their electron spins.

IT: information technologies.

Jaynes-Cummings Hamiltonian: Hamiltonian used to describe the total energy of a system linking a resonator usually implemented as a coplanar waveguide (CPW) resonator with a superconducting circuit.

JJ: "jay-jay", nickname for Josephson junctions.

Josephson (effect): physical phenomenon happening in a superconducting current loop traversing a thin insulating barrier known as a Josephson junction (JJ) like some non-superconducting metal thanks to the tunneling effect. It enables the creation of a multiple level energy or phase state for the superconducting current. This technique is used in superconducting qubits from quantum systems such as those of IBM and Google. It is also used in quantum sensing with SQUIDs (superconducting quantum interference devices) that are used as very sensitive magnetometers.

JPA (Josephson Parametric Amplifiers): simple amplifiers, using one or two Josephson junctions that are used for the first stage amplification of readout microwaves in superconducting or silicon spin qubits. Their narrow bandwidth prevents their implementation with frequency-domain qubits readout multiplexing.

Kerr effect: when some materials refractive index is modified in a nonlinear (quadratic, second-order nonlinear) manner as a function of the electric field applied to them. Is a variant of Pockels effect.

Ket: vertical vector describing in Dirac's notation the state of a quantum object, with the symbols | and ⟩ forming a psi vector noted $|\psi\rangle$. It contains complex number amplitudes defining the relative weights in the computational basis. For a qubit, it's a 2 complex numbers vector. For a register of N qubits, it's a 2^N size vector of complex numbers defining the amplitudes of each combination of N 0s and 1s, which are orthogonal states in the 2^N state vector Hilbert space.

Kochen-Specker theorem: no-go theorem that states that it is impossible to assign simultaneously values with certainty to all observables in all possible contexts. This simple observation contradicts classical physics, where such an assignment is quite possible. It is the formal proof of quantum contextuality.

Larmor frequency: frequency of the Larmor precession (magnetic moment rotation). It is frequently mentioned in papers related to electron spins qubits.

Larmor precession: rotation of the magnetic moment of an object like an electron when it is exposed to an external magnetic field. This rotation happens along the axis of the magnetic field.

Laser: coherent light source invented in 1960 and used in many fields such as CD and DVD players, fiber optic communications, surgery, ophthalmology and dentistry, LiDARs. They are also often found in quantum computing to control cold atoms or manage photon-based qubits as well as in quantum cryptography and telecommunications (QKD & co). Laser means Light Amplification by Stimulated Emission of Radiation. It is a source of coherent light, i.e. it consists of photons of the same polarization, phase and wavelength, and emitted in the same direction in a narrow beam. Light amplification uses a process of stimulated emission in an amplifying active medium made of solid, fiber, liquid, gas or semiconductor which is placed in the center of a resonant optical cavity with a reflecting mirror on one side and a semi-reflecting mirror on the other side, which allows the light beam to exit. The wavelength and power of the light radiation depends on many parameters. The energy comes from an excitation or pumping system: primary laser, laser diode, flash lamp or electric discharge.

Leggett-Garg inequality: mathematical inequality fulfilled by macroscopic physical theories and systems. It says that a macroscopic object which has two or more distinct states, is at any given time in of those states. And it is possible in principle to determine which of these states the system is in without any effect on the state itself, or on the subsequent system evolution. This inequality is violated by quantum systems when superposition and entanglement are put in play like in interference processes.

Lindblad equation: equation describing the time evolution of the density matrix ρ of a quantum system that preserves the laws of quantum mechanics, meaning it preserves the trace and positiveness of the matrix. But the transformation is usually not a unitary due to decoherence. Also named a Lindbladian, a quantum Liouvillian, and in the long form, a Gorini–Kossakowski–Sudarshan–Lindblad equation (GKSL equation, for Vittorio Gorini, Andrzej Kossakowski, George Sudarshan and Göran Lindblad).

Linear algebra: branch of mathematics that is used in quantum physics and quantum computing. It is based on

the manipulation of vectors and matrices within Hilbert spaces. In particular, the state of a sets of qubits is represented by vectors in a Hilbert space of size 2^N when N is the number of qubits. Computing with qubits consists in applying linear transformations.

Linear optics: field of quantum mechanics that manipulates photons based on their classical properties: polarization, phase or frequency.

Locality (principle): in classical physics, principle according to which distant objects cannot have a direct influence on each other. An object can only be influenced by its immediate environment. This principle derived from Albert Einstein's restricted relativity is questioned by quantum mechanics, non-locality and quantum entanglement observed experimentally since at least 1982 with photons, in Alain Aspect's famous experiment (with Philippe Grangier and Jean Dalibard). But there are various interpretations of quantum physics which explain entanglement without resorting to non-locality.

Logical Qubit: an assembly of physical qubits implementing hardware and software quantum error correction. Seen from the software developer's point of view, it creates a virtual logical qubit with a very low error rate. The fidelity of logical qubits depends in particular on the number of physical qubits they contain, the quality of the error correction codes and the qubits fidelity stability with the increase in the number of physical qubits.

LSQC: Large Scale Quantum Computing also frequently called FTQC for fault tolerant quantum computing. Category of future fault tolerant quantum computers. These will be based on the use of numerous physical qubits assembled into logical qubits with a very low error rate as seen from the software. Precisely, an LSQC implementing fault-tolerance has error corrections codes with at least two characteristics: it must not propagate errors broadly in the physical qubits and it must be able to implement non-Clifford group qubit gates like the single qubit gate T or the three qubits gate Toffoli. But LSQC definition is not clear yet. It could pertain to a large number of physical qubits (not necessarily arranged in logical qubits) or a large number of logical qubits, way beyond the first generations of FTQC. The jury's out to settle dusts with this terminology.

Magic states distillation: process that converts a set of noisy qubits into a smaller number of qubits with a lower noise. It is particularly useful for non-Clifford group quantum gates that bring universal computing power and exponential speedup. It is one of the ways to create fault-tolerant quantum computers but it has a high overhead cost with physical qubits. It was proposed in 2004 by Emanuel Knill, Sergey Bravyi and Alexei Kitaev.

Magneto-Optical Trap (MOT): device used to cool down and trap a cloud of neutral atoms. It uses a combination of magnetic trapping using two coils and Doppler effect in three orthogonal directions for cooling. The technique is used in cold atom interferometry (cold atoms gravimeters) and cold atom computers.

Majorana fermion: an electron-based quasiparticle in superconducting materials that could be used to manage reliable qubits in so-called topological computing. This virtual particle was imagined by Ettore Majorana in 1937. Microsoft intends to build a quantum computer based on these quasiparticles. But their very existence has not yet been really demonstrated.

Manifold: corresponds to the discrete controllable states of a quantum object.

Matrix: mathematical object made of rows and columns of values.

Matter wave: principle of quantum physics enacted by Louis De Broglie in 1924 according to which massive objects can also behave as waves. The De Broglie wavelength of a massive particle is the Planck constant divided by its momentum.

MBE: molecular beam epitaxy, a variety of PVD process (thin-film deposition), used to create a single orderly crystal structure in semi-conductor manufacturing. Is notably used to produce semi-conductors quantum dots in III/V materials.

MBQC: Measurement Based Quantum Computing, a quantum computing method invented in 2001 by Robert Raussendorf and Hans Briegel that uses a high number of groups of pre-entangled qubits, called cluster states, embedded in two-dimensional grids in which qubit state readouts modify the grid structure and help create quantum gates. The last measured qubit gives the result of the algorithm. This technique is particularly useful with flying qubits like photons because it can be implemented in a highly parallel way and support the finite depth of quantum gates that these qubits enable.

Mesoscopic: subdiscipline of condensed matter physics that deals with materials of an intermediate size. The size ranges from a couple atoms to a μm.

Metal layers: in semiconductor chipsets, correspond to the layers containing wires connecting the various transistors and other electronic elements. These layers are surrounded by some insulator (silicon oxide or other). In typical CMOS processors, you have over 12 metal layers of decreasing density as you move father from the logic layer, In superconducting qubits, you have no metal layers on top of the Josephson junctions since it must be as isolated as possible.

Microring resonator: tiny optical waveguides looped back onto themselves in circle or spiral which enable interference phenomena, the creation of delay lines, and various other optical devices used for example in entangled photon generation.

Mode-locked laser: pulse laser generating streams of very short pulses of light formed of wave-packets in the picosecond to femtosecond range. These pulses are generated thanks to the emitted photons being synchronized in phase. A synonym of mode-locked is phase-locked!

Mott insulator: material that are expected to conduct electricity but are actually insulators, particularly at low temperatures, and under certain conditions which can be controlled, leading to so-called Mott transitions.

Mott transition: change in a condensed matter material's behavior from insulating to metallic generated by multiple factors like and ambient electric field changing the band structure of the material like with some metal oxides.

MVP: Minimum Viable Product. Concept used mostly in startups consisting in creating the simplest form of a product before starting to sell it. Opposite to full-fledged product with tons of R&D and an ever-lasting perfectionist approach.

MINLP: Mixed Integer Non Linear programming, a class of complex problems that can potentially be solved with quantum algorithms. It is about finding the minimum(s) of nonlinear functions and under constraints that aim to respect nonlinear functions. The variables in the equation are a combination of integers and floating-point numbers. The applications are numerous in all cases where one seeks to optimize a constrained function (energy distribution, optimum take-off of an aircraft, optimization of financial portfolio, minimizing risk in insurance or credit, etc.).

Mixed state: quantum objects state that is a classical statistical combination of several pure states. They can be prepared with physically associating several sources of pure states, like with merging two laser beams in one beam. A subsystem of an entangled quantum objects system is also a mixed state. A mixed state is mathematically represented by a density matrix operator, providing all the information that can be obtained about the related quantum system.

Momentum: physical property of an object or particle that for a massive particle is equivalent to its mass multiplied by its velocity. Usually denoted p. A (massless) photon has a momentum equal to their wavelength multiplied by Planck's constant.

Multimode: said of an optical fiber with a larger core (about 50 to 62 μm) where several light beams can be transported, usually with different wavelengths. Light propagation use bouncing inside the fiber walls. These fibers are used for short distances communications of less than a kilometer and with bit rates reaching 200 GBit/s. The contrary of multimode fibers are monomode fibers. Also said of multimode photons, with an entirely different meaning and a way more complicated one, never explained in plain language by quantum photonicians. Its contrary is single mode photons. A single mode photon has one complex amplitude while a multimode photon is a mixed state of single mode photons with several independent complex amplitudes. If you want to know more, you get to use a complicated mathematical formalism.

Mutually unbiased bases: it is a concept mostly used in quantum key distribution. A bases is a set of orthogonal vectors in a Hilbert space. Mutually unbiased bases are two bases where the measurement of one of the vectors of one basis will yield a random result on the other base.

NISQ: Noisy Intermediate-Scale Quantum, a name for current and near future gate-based quantum computers, which are intermediate in terms of number of qubits (a few tens to hundreds) and subject to quantum noise that limits their capabilities. This acronym was created by John Preskill.

No-go theorem: theorem that demonstrates that a physical phenomenon is not possible. In quantum physics, famous no-go theorems are Bell's theorem and the Kochen–Specker theorem which con-strain hidden variable theories trying to explain non-locality and entanglement with an underlying deterministic model featuring hidden states and variables. You also have the no-cloning and no-deleting theorems which prevents the cloning and deletion of a quantum object state.

Non-Clifford gates: said of quantum gates that are outside the Clifford group itself based on combining Pauli gates (half-turns in Bloch's sphere), Hadamard gates (quarter turns) and CNOTs for entanglement. To make things simple, non-Clifford gates enable the creation or arbitrary rotations in Bloch's sphere and their multi-qubits gates derivatives. The single qubit T gate (one eighth turn in Bloch's sphere) is the minimum additional gate, that, combined with the others, enable by approximation the creation of any arbitrary gate and unitary transformation.

Non cloning theorem: prohibits the identical copy of the state of a quantum. Therefore, it is impossible to copy the state of a qubit to exploit it independently of its original. Any copy destroys the original!

Nonlinear optics: field of optics where the optical properties of materials depend on the light amplitude and lead to the creation of new frequencies. Nonlinearity qualifies the response of a medium to an excitation that is generally quite energetic from intense fields, mainly from lasers, especially femtosecond pulsed lasers. In this case, the response of a material to the sum of two electromagnetic fields is not equal to the sum of the response to each individual field. Nonlinear optics can be used to create two-photon quantum gates with continuous variables photons. See also Chi.

Non-locality: principle allowing a (quantum) object to influence the state of another (quantum) object at a distance, which can be very large. Contradicts the principle of locality, which means that an object can only influence another object at close range. Photons quantum entanglement at great distances verifies the non-locality. However, the initial quantum state of both objects is always random. So it doesn't transmit a predetermined information per se from one place to the other.

NMR: Nuclear Magnetic Resonance, a type of qubit that was investigated in the 1990s and early 2000s and was then nearly abandoned. The reason is it didn't scale well at all and these were very noisy qubits and difficult to entangle. It was based on exploiting quantized states of atoms nuclei spins. However, the Chinese startup SpinQ is offering a desktop NMR-based quantum computer with 2 to 5 qubits. It's useful only for educational tasks.

Non-classical light: forms of light and electromagnetic fields treated as quantum systems. It contains single photon wave packets, pairs of entangled photons and squeezed states of light.

Non-demolition measurement: see QND.

NOON state: many-body entangled state superposing N quantum objects, usually bosons, in two modes. Namely, it

superposes all the objects in one mode and all the objects in the other mode. This kind of superposition is used in quantum metrology to obtain a precision reaching the Heisenberg limit, which is better than a standard quantum limit based measurement.

Normalization: in quantum physics, normalization is used in many situations like with scaling wave functions so that the sum of probabilities equal one. This 1 is considered as a normalization constant or constraint.

NP (problem class): class of problems whose solution is verifiable in a polynomial term relative to the size of the problem. It includes the so-called exponential or intractable problems, whose solution time is exponential with respect to their size. A quantum computer is supposed to solve some NP problems in a tractable way, meaning, not exponential time.

NP-complete (problem class): decision problem for which it is possible to verify a solution in polynomial time and for which all problems of the NP class are reduced to it via a polynomial reduction. This means that the problem is at least as difficult as all other problems of the NP class. The problems of the traveling salesperson and the knapsack problem are Complete NP problems. The concept dates from 1971 and comes from Stephen Cook.

NP-difficult (problem class): problem to which any problem of the NP class can be reduced by a polynomial reduction. If it is also in the NP class, it is said to be an NP-complete problem. If $P \neq NP$, then NP-difficult problems cannot be solved in polynomial time.

Observable: equivalent in quantum mechanics of a physical quantity in classical mechanics, such as position, momentum, spin or energy. In quantum physics, an observable is a mathematical operator used for the measurement of one property.

ODMR: optically detected magnetic resonance is a quantum sensing testing is a double resonance technique where the electron spin of a crystal defect like a NV center is optically pumped for initialization and readout with a green laser light. It radiates some red light or nothing depending on the cavity electrons spin. It uses the Zeeman effect in unpaired electrons. With NV^- centers, it is used for high-precision magnetometry and medical imaging with a sensitivity ranging from 10^{-9} to 10^{-15} T/√Hz, the unit of magnetometry precision.

On-premises: said of hardware that sits in a customer site or datacenter. It is the opposite of sitting in a datacenter from a cloud vendor.

Optical molasses: gas of cold neutral atoms whose cohesive strength is of the viscous type. It is cooled with lasers using the Doppler effect, usually with three pairs of lasers in three orthogonal directions.

Optical pumping: technique used to modify the states of atoms by increasing their energy level using polarized photons. Alfred Kastler, invented it in 1950 and was awarded the Nobel Prize in Physics in 1966. The technique is used in lasers and quantum sensing. Optical pumping passes through three to four energy levels of atoms (E0, E1, E2, E3). Pumping moves an atom from its fundamental level E0 to E3. A (mechanical) relaxation brings the atom back from the E3 state to E2. In lasers, this generates a population inversion between the E1 and E2 states, so that there are more atoms in the E2 state than in the E1 state. The spontaneous and stimulated emission of photons of E2-E1 energy can then take place. The atom in the E1 state then returns to the E0 state by relaxation.

Orbital angular momentum (OAM): is one of the two angular momenta of photons with spin angular momentum. Discovered in 1992 by Les Allen et al from Leiden University, this phenomenon is more difficult to visualize than spin angular momentum. With OAM, the photon itself is rotating along its propagation axis or vector. One analogy with the Earth is its own rotation (spin angular momentum, defining days) and its rotation around the Sun (orbital angular momentum, defining years). This orbital angular moment is quantified with integers times the reduced Planck constant. It can be any integer! One record OAM number of 10.100. Being quantified, it can lead to superposition and entanglement. It can also be used to encode information on fibers.

P (problem class): problem that can be solved in polynomial time with respect to its size, on a deterministic Turing machine.

Paramp: parametric amplifier using a parametric nonlinearity and a pump wave. Paramps exist for photos in the visible spectrum (these are OPA for optical parametric amplifiers) as well as for microwaves. In this last case, they are used to amplify readout microwaves from superconducting or silicon spin qubits. The most recent breed of paramps are the TWPAs.

Pauli (exclusion principle): postulates that two fermion particles cannot be in the same quantum state. Two electrons or two neutrons cannot be in the same place with the same energy level. If an external force such as gravitation forces them to be in the same place, they cannot have the same energy, i.e. the same speed. If a set of fermions has to be in the same place, they will have to have different velocities. Fermions have half-integer spins.

Permanent: real number resulting from n! additions of multiplications of n values of a square matrix n*n. They are used to evaluate the complexity of matrices representing graphs.

Phase Estimation Algorithm: algorithm created by Alexei Kitaev in 1995 and used to find the phase of an eigenvector of a unitary operator U. This algorithm is based on an inverse QFT. It is used as part of period finding in Shor's factoring algorithm and in quantum chemistry algorithms.

Phase: an important physical properties of quantum objects given they all can behave as waves. It explains interferences between all sorts of quantum objects, like electrons on top of photons.

Phasor diagram: two-dimensional diagram describing electromagnetic field quadratures positioning the statistic characteristics of a photon source, with X1 and X2 orthogonal axis corresponding to two oscillating electric fields that are out of phase by 90°.

Phonon: collective excitation in a periodic, elastic arrangement of atoms or molecules in condensed matter, specifically in solids and some liquids. In quantum information technologies, it is mostly used with trapped ions to provide a n-to-n connectivity between qubits.

Photoelectric effect: emission of electrons from a material like a metal when electromagnetic radiation above a certain minimum frequency strikes it, independently of its intensity. Formalized by Albert Einstein in 1905.

Photolithography: patterning process in semiconductor manufacturing used to define in which zones matter must be removed or added in subsequent steps. It uses ultraviolet rays illuminating a photomask that exposes a photoresist film or coating. For very high densities, the exposure is done with extreme ultra-violet waves. The related manufacturing tools are now produced by a single company in the world, ASML (The Netherlands).

Photon: quantum of energy associated with electromagnetic waves ranging from radio waves (long waves, low frequencies) to gamma rays (very short waves, very high frequencies) through visible light. Its mass is zero. Its spin is 1 and it is therefore part of the bosons. Photons are absorbed an emitted by atoms during energetic levels changes.

Photon measurement: measurement of a photon where the degree of freedom is the excitation quanta. It can yield a number of superposed photons that we try to detect, but not their characteristics like their phase or frequency, which requires homodyne or heterodyne measurement.

PKI: Public Key Infrastructure, set of roles, policies, hardware, software and procedures used to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

Planck constant: fundamental constant of quantum physics ($h=6.626x10^{-34}$ Js). Created in 1900 with Max Planck's explanation of black body radiation spectrum and then used in most other quantum physics equations, including Schrodinger's wave equation.

Pockels effect: effect used in optical modulators where a medium refraction index changes in a linear manner as a function of the electric field applied to it.

Polarized Beam Splitter (PBS): class of beam splitters that use birefringent materials to split light into two beams of orthogonal polarization states.

Polaritons: quantum quasi-particles with strong interactions between light and matter in semiconductors. It results from the coupling between photons and an electrical polarization wave which occurs in particular in plasmons (oscillations of free electrons in metals), phonons (oscillations of atoms, especially in crystalline structures) and excitons (pairs of electron holes generated by photons in semiconductors).

POVM: Positive Operator-Valued Measure, quantum measure generalizing Projection-Valued Measures (PVMs) which is useful when the measurement basis is not made of orthogonal states in their Hilbert space. POVMs that are not PVMs are called non-projective measurements. They have many use cases like enhancing quantum states tomography, help detect entanglement and allow unambiguous state dis-crimination of non-orthogonal states, with applications in quantum cryptography and randomness generation

PQC: Post Quantum Cryptography, cryptography resistant to quantum computers-based codebreaking algorithms. It is based on the use of public keys that are not decomposable with conventional or quantum computers.

PQS: Programmable Quantum Simulator, or analog quantum computers.

Private Key: key used in private key encryption systems. Keys are exchanged beforehand by the parties using an encryption algorithm, often hash or Diffie-Hellmann algorithms.

Property: physical characteristic of a physical object. In quantum physics, observables are the mathematical operator used to compute properties values using the quantum object state vector. For a photon, it can be for example its phase, polarization and wavelength. In quantum physics, it's not possible to evaluate the values of all properties of quantum systems to describe it, due to Bohr's complementarity principle.

Public key: an encryption system that involves sending a public key to an interlocutor who will use it to encrypt a message sent in the other direction. The elements used to create this public key are used to decrypt the message sent. It is normally impossible or very difficult to decompose the public key to find the elements that were used to create it. PQCs are based on public keys.

Purcell effect: relaxation or loss of energy of a superconducting qubit through its readout resonator. More generally, it's the enhancement of a quantum system's spontaneous emission rate by its environment, discovered in the 1940s by Edward Mills Purcell with the spontaneous emission rates of atoms when incorporated into a resonant cavity.

Purcell filter: high and low-band filter that reduces the Purcell effect between a superconducting qubit and its readout resonator.

Pure state: quantum state of an isolated quantum system of one or several objects constructed as a linear superposition of the states from its computational basis.

Purification: process applied to a mixed which integrates it in a larger system to create or recon-struct a pure state. It can be applied to a set of entangled qubits as well. It is used in some error-correcting codes both in quantum telecommunications and quantum computing.

PVD: physical vapor deposition, is a material deposition technique in semiconductor manufacturing where the material to deposit is first turned into vapor and then condenses on the target surface. There are various PVD methods like sputtering that is using ion projection to pull material from a source and deposit it on the target,

PVM: Projective Value Measurement, used in quantum computing, consists in doing a geometrical vector projection of your qubit pure state on any axis in the Bloch sphere.

Q factor: quality factor, dimensionless value defined as the ratio between the energy stored in a resonator and the energy dissipated per oscillation cycle times 2π. With the frequency of the oscillator, it provides an indication on the oscillator lifetime. In a superconducting qubit, it characterizes the stability of its oscillation and determines its T_1 or relaxation time. The greater the Q factor is, the longer the T_1 is. The higher the better, this factor can exceed 10^7. The dissipation comes from cavity losses and depends on the materials and structure of the electromagnetic cavity. Another definition for Q factor for an oscillator is the ratio between the main resonance frequency and its bandwidth.

QCaaS: quantum computing as a service, a fancy acronym for quantum computing running in the cloud.

QFHE: Quantum Fully Homomorphic Encryption. A method of quantum information encryption allowing to perform processing on encrypted data.

QFT: Quantum Fourier Transform. Quantum variation of the Fourier transform. The classical Fourier transform allows to decompose a signal (as in audio) into frequencies (or frequency spectrum). The QFT does this on a sequence of integers and determines its largest observable frequency.

QIP: Quantum Information Processing, a name sometimes used to information tools based on second-generation quantum technologies. It contains quantum computing, quantum simulation, quantum cryptography and quantum telecommunications.

QHO: quantum harmonic oscillator.

QIR (Quantum Intermediate Representation): an intermediate representation for quantum programs launched in September 2020, serving as a layer between gate-based quantum programming languages and target quantum computers. It can also be used to run code on an emulator. It is supported by the QIR Alliance launched in November 2021 and is part of the Linux Foundation. The Alliance founding members are Honeywell, Microsoft, the DoE Oak Ridge National Laboratory, Quantum Circuits Inc. and Rigetti Computing.

QKD: Quantum Key Distribution, a secure protocol for sending symmetrical keys via an optical link based on quantum entanglement (fiber or satellite). These keys are tamper-proof, or at least an interception of the key is detectable.

QLM: Quantum Learning Machine, name of the Atos quantum emulator appliances using classical hardware (Intel and/or Nvidia).

QMA: Quentin Merlin Arthur, a class of problems that is verifiable in polynomial time on a quantum computer with a probability greater than 2/3. It is the quantum analogue of the "traditional" NP complexity class. QML: Quantum Machine Learning. Branch of quantum algorithms used in machine learning.

QML: Quantum Machine Learning. Class of quantum algorithms implementing machine learning or deep learning techniques.

QND: quantum non-demolition measurement, a sequence of measurements where results are completely predictable using the result of the first measurement. Practically, it stays the same. Let's say we measure the state of a qubit that yields a $|0\rangle$ or a $|1\rangle$. The measurement is a QND one if a new measurement will yield the same $|0\rangle$ or a $|1\rangle$ coming out of the first measurement and so on. In mathematical parlance, it means the measurement observable commutes with itself at different times. How about a destructive measurement of a qubit? It can happen for example with a photon detector which absorbs it. The photon is then entirely destroyed (and converted to some current in the detector) and cannot be measured a second time. Usually, a QND signal is quantum and extremely weak and is obtained with a quantum probe.

QRNG: Quantum Random Number Generator, the optical random number generators used in quantum cryptography, like those of the Swiss IDQ.

QSVT (Quantum Singular Value Transformation): quantum algorithm that performs a polynomial transformation of the singular values of a linear operator embedded in a unitary matrix. Was created by András Gilyén, Yuan Su, Guang Hao Low and Nathan Wiebe in 2018.

Quantization: in quantum physics, happens with quantum objects having some physical properties that are discontinuous and not continuous, like electron energy levels and electron spins.

Quantum accelerator: quantum computer used as a complement to a supercomputer or HPC, usually to run hybrid algorithms like VQE (Variational Quantum Eigensolvers) combining a classical part that prepares the data structure that feeds a quantum accelerator.

Quantum advantage: occurs when a quantum computer executes some processing faster than its optimum equivalent adapted to a supercomputer, with a useful algorithm. This advantage can be declined on another aspect than the duration of the calculation. For example, a quantum energy advantage relates to energy consumption instead of computing time.

Quantum annealing: technique used to find the global minimum of a given objective function over a given set of candidate solutions, based on using quantum fluctuations. It is used to solve combinatorial optimization problems with a discrete search space. This computational process is in D-Wave quantum computers.

Quantum channel: transformation of a quantum state resulting from any kind of interaction with a quantum environment. It is modelized with a density matrix super-operator. It is useful to modelized subsystems, decoherence, quantum error correction and qubits noise.

Quantum Chaos: branch of physics studying how chaotic classical dynamical systems can be described with quantum theory. It deals with the relationship between quantum mechanics and classical chaos and with the boundaries between classical and quantum physics in modelling chaos.

Quantum chromodynamics: describes the strong interaction, one of the four fundamental forces, that governs the interactions between quarks and gluons and the cohesion of atomic nuclei. Why "chromo"? Because we describe the states of elementary particles with color codes: blue, green

and red for particles, then anti-blue, anti-green and anti-red for anti-particles. This theory is based on the quantum field theory. This part of quantum physics is not used in the creation of qubits. It is used for the physics of elementary particles and is verified in large particle accelerators such as the CERN LHC in Geneva.

Quantum circuit: see circuit.

Quantum cognition: descriptive model of the functioning of human knowledge (language, decision-making, memory, conceptualization, judgment, perception) based on the mathematical formalism of quantum mechanics, proceeding mainly by analogy, without going through physical explanations or quantification of the neurosciences, which themselves fall within the "quantum mind" field resulting from the work of Roger Penrose.

Quantum dots: we can mention at least three different types of quantum dots: the powders used in LCD screens that convert the blue backlighting LED light into green or red light based on their grain size. Then we have the quantum dots used to generate single photons. At last, we have quantum dots used to trap electron spins in spins qubits.

Quantum Electro-Dynamic (QED): branch of quantum physics, or QED, which is "*a physical theory that aims to reconcile electromagnetism with quantum mechanics using a relativistic Lagrangian formalism. According to this theory, electric charges interact by photon exchange*" (Wikipedia). This is the basis of the quantum field theory which applies to all elementary particles.

Quantum emulator: a software and/or hardware system using a conventional computer to run and test some software programmed for a quantum computer. This makes it possible to test quantum programs without a quantum computer. The execution speed is not as good as on a quantum computer as soon as you exceed a few tens of qubits. And beyond about fifty qubits, the capacity of classical machines is insufficient to perform it properly. Emulation should not be confused with quantum simulation, which simulates quantum physics phenomena with an analog quantum processor like those using cold atoms.

Quantum engineering: is about developing quantum technologies in computing, telecommunications, cryptography and/or sensing with a pluridisciplinary approach merging quantum physics and other related sciences and technologies like thermodynamics, cryogeny, electronics, semiconductors, cabling, mathematics, information theory, programming and the likes.

Quantum foundations: branch of science philosophy that aims to build some understanding and description of the real world in quantum physics and, as such, associate it to some ontology.

Quantum gates: operations modifying the state of one or several qubits. Multi-qubit gates (Toffoli, Fredkin, ...) exploit the principle of quantum entanglement. The operations of quantum gates are generated by physical actions on the qubits which depend on their nature. For superconducting qubits, this involves sending microwaves between 5 and 10 GHz via electrical conductors. For trapped ions, these are laser-controlled operations. For electron spins qubits, these are a mix of electrical voltages and microwave pulses. For qubits based on mass particles (electrons, ions, cold atoms), quantum gates act on the qubits but these do not move in space. For flying qubits based on photons or electrons, these circulate and cross quantum gates which modify their state (phase, frequency, or other).

Quantum Hall effect (QHE): or integer quantum Hall effect is a quantized version of the Hall effect which is observed in two-dimensional electron systems at low temperatures and under a strong magnetic field, in which the Hall resistance Rxy has quantized values. It is related to the field of quantum matter. The effect was discovered by Klaus von Klitzing from the MPI in Germany in 1980 and was awarded the Nobel prize in physics in 1985.

Quantum hydrodynamics: studies the hydrodynamic effects of quantum systems such as superfluid elements (helium at very low temperature) or polaritons and associated light fluids.

Quantum Internet: marketing term describing a quantum network enabling the quantum telecommunications based on entanglement, particularly to connect quantum systems like quantum computers and quantum sensors. By extension, it also includes quantum key distribution infrastructures that are used to secure information exchange with encryption keys that are shared quantumly between senders and receivers.

Quantum medicine: in general, false science and charlatanism based on a totally fanciful interpretations of quantum mechanics.

Quantum Non Demolition measurement (QND): type of measurement in which the uncertainty of the measured observable does not increase from its measured value during the subsequent normal evolution of the system. QND measurements are the least disturbing type of measurement in quantum mechanics. In other words, for a qubit, it would mean that after a $|\mathbf{0}\rangle$ or $|\mathbf{1}\rangle$ is measured, subsequent measurements will always yield the same $|\mathbf{0}\rangle$ or $|\mathbf{1}\rangle$ that was obtained in the first place.

Quantum number: variables describing quantum objects physical quantities or variables that are discrete. Electrons have four quantum numbers: principal quantum number (energy level or electron shell), angular momentum also named azimuthal or orbital quantum number describing electron subshell, magnetic quantum number describing the electron energy level within its subshell and spin projection quantum number, being either +1/2 or -1/2, in a given spatial direction.

Quantum postulates: basis of quantum physics formalism. These are postulates and not laws because it describes a mathematical formalism that cannot be proved per se. There are many different presentations of quantum postulates in reference sources (Nielsen & Chuang, Preskill, Cohen-Tannoudji, Wikipedia, ...). Depending on the sources, you'll find 3, 4, 5, 6 or even 7 of them.

Quantum Physical Unclonable Functions (qPUF): quantum based physical identifiers that can be used to create unique and unclonable security keys.

Quantum reservoir computing: specific category of recurrent neural networks used to process time series. It uses a set of neuron weights and links between neurons randomly fixed in the reservoirs, all with nonlinear activation functions. The hundreds of neurons in a reservoir are fed by input data stored in the reservoirs. The activation functions nonlinearity makes this memory evanescent. The training parameters of these networks are located in the weights of the neurons that connect the reservoirs to the output data

Quantum reservoir engineering: set of techniques for managing qubits through their interaction with a "quantum thermal bath" (quantum bath) to reduce energy consumption, reduce the duration of the measurement of the state of the qubit and allow a non-destructive and reversible measurement of this state ("Quantum non-demolition" or QND). Reservoir engineering is used in cat-qubits.

Quantum simulator: name given to analog quantum computers that are capable of simulating quantum objects and solving related problems, particularly in materials physics. By abuse of language, the name is used for supercomputers capable of executing quantum algorithms by numerical simulation. In this case, it is preferable to use quantum emulator.

Quantum state: mathematical object used to compute at a given time the probabilities of a quantum object or set of object property values that would be obtained when measuring it and to predict their evolution over time. It is usually represented by a vector in a Hilbert space (linear, metric and complete). This is however only the case for a pure state. A mixed state is represented by a density matrix. The notion of quantum state is usually the first quantum postulate.

Quantum state tomography: technique used to characterize the quality of qubits and qubits gates or any quantum channel. It is used to experimentally reconstruct a density matrix of a set of qubits. It also requires a lot of classical computing to process the experimental data obtained with repeated state preparation and measurements.

Quantum Steering: quantum measurement phenomenon when one subsystem can influence the wave function of another subsystem by performing specific measurements.

Quantum supremacy: describes a situation where a quantum computer can perform some computation that is inaccessible to the best current supercomputers with the best classical algorithm and in a humanly reasonable time. The computing time differential between quantum computing and classical computing must be several orders of magnitude. It can deal with a useful calculation or not. Thus, the quantum supremacy claimed by Google in October 2019 dealt with a random algorithm that had no practical interest. The term was coined by John Preskill in 2011. Nowadays, the trend is to use the quantum advantage denomination.

Quantum switch: consists in creating a series of qubit transformations that can be implemented simultaneously in different orders, creating an indefinite causal order computing flow.

Quantum teleportation: technique used to transfer the state of one qubit to another location. It is usually performed with three communication links: a pair of previously entangled photons and two classical bit links. It has many uses such as in quantum cryptography (QKD). The no-cloning theorem also says that the state of a teleported quantum disappears from the source after teleportation. It can be used to transmit a rich quantum state of several qubits and can enable distributed quantum computing.

Quantum variational circuits: type of quantum algorithm used to implement machine learning.

Quasi-particles: physical concept which treats elementary excitations in solids like spin waves, as particles. As the particles do not consist of actual matter, they are called quasi particles. Majorana fermions and polaritons are examples of quasi-particles.

Qubit or physical qubit: the elementary unit of information in quantum computing in quantum computers and quantum telecommunication. It stores a quantum state associating two distinct states of a particle or of a quantum system (electron spin, energy level of a superconducting loop, energy level of a trapped atom or ion, polarization or other property of a photon). Its mathematical representation is a vector comprising two complex numbers in a Bloch sphere.

QUBO: Quadratic Unconstrained Binary Optimization problem. It is a generic NP hard combinatorial optimization problem and its related algorithm which can help solve many applications in finance, logistics and other domains. Many classical combinatorial problems like maximum cut, graph coloring and the partition problem, can be turned into a QUBO problem. QUBO problems can be solved on all three quantum computer paradigms (gate-based, annealing, simulation).

Qudits: generic form of qubit that has d possible quantum states instead of two. The approach is rarely used, at least in quantum computers outside research laboratories.

Qunat: another name for qubits based on continuous variables.

Qutrit: it is a form of qubit which instead of having two possible quantum states, has three. It is a special case of qudits.

Rabi (oscillation): oscillations between states of a two-level system excited at a frequency close to its resonance. This phenomenon is observed between two spin states in nuclear magnetic resonance as well as when an electric field acts on the transitions from one electronic state of a system to another for an atom or molecule. The curve describing the oscillation resembles a sinusoidal curve that attenuates over time. Isidor Isaac Rabi is an American physicist of Hungarian origin (1898-1988) who was awarded the Nobel Prize in Physics in 1944. Rabi's oscillations can be found almost everywhere, especially in the operation of superconducting qubits with microwave pulses.

Raman cooling: variant of the Doppler effect using the Raman effect used to cool atoms below the limit of Doppler-based cooling, under 1μK. It uses two counter-

propagating laser beams. This effect is used in cold atom based interferometry in absolute gravimeters. Also known as Raman sideband cooling.

Raman effect or Raman scattering: shift in wavelength of an inelastically scattered radiation where an incident monochromatic photon energy and momentum are both changed. Discovered by Chandrasekhara Venkata Raman (1888-1970, India), Nobel Prize in physics in 1930. This is a small effect that accompanies the predominant Rayleigh scattering of light (unchanged wavelength). The incident polarized light is scattered at its original frequency (Rayleigh elastic scattering) and with higher and lower frequencies (Raman stokes and anti-stokes anti-elastic scattering).

Raman spectroscopy: determines vibrational and rotational level spacings from the energy (wavenumber) shifts of inelastic scattered light (*aka* Raman scattering). It is used to analyze multi-atoms molecules through their vibrational modes, particularly in organic chemistry.

Raman transition: couples two atomic levels by the absorption of a photon in one Raman beam (pump beam) and by stimulated emission of another one in the other beam (Stokes beam). It is used in cold atom interferometry to split a cold atom cloud into two superposed matter waves of different energy levels and vertical velocity.

Ramsey experiment: technique used to measure the T_2^* of a superconducting qubit, with applying one Hadamard gate, waiting a time t, then applying another Hadamard gate, and measuring the output. The sinusoid curve amplitude slowly decreases around a probability 0.5. T_2^* is obtained when the probability reaches 1/e.

Rayleigh scattering: predominantly elastic scattering of electromagnetic radiation by particles that are much smaller than the radiation wavelength. Elastic scattering happens with incident photons whose direction is changed but not their energy (color or wavelength). It explains why the sky is blue, linked to blue light being more scattered than green and red light, and also polarized.

Realism: in science, philosophical view according to which there exists a reality independently of an observer. The Copenhagen interpretation of quantum physics is non-realist since it believes reality is only what can be observed and measured.

Reduced Planck constant: see Dirac constant.

Reflectometry: technology used with superconducting and electron spin qubits readout. It consists in sending a microwave to the qubit and to analyze the reflected microwave, which can have different phase and amplitude depending on the measured qubit state.

Register: set of bits or qubits. In the case of qubits, it provides an exponentially growing computational base space with the number of qubits.

Relaxation: corresponds to the T_1 or lifetime of a qubit, which defines when the qubit loses its amplitude.

Renyi entropy: generalized version of entropy that can be used as a measure of entanglement. Shannon entropy is a special case of Renyi entropy.

RIE: reactive ion etching, a process used to remove some material on a semiconductor target using accelerated molecular or atomic ions in vacuum.

RSA: a public key encryption system based on the difficulty of factoring a public key formed by multiplying two very large prime numbers. This factorization is theoretically possible with Peter Shor's quantum algorithm. However, it requires a very large number of qubits to break the most common RSA keys at 1024 or 2048 bits. For 2048-bit keys, 20 physical million qubits with a 99,9%+ fidelity are required, which is very long-term in quantum computer roadmaps.

Rydberg (atoms): excited state of an atom having one or more electrons and whose principal quantum number n (index of the electron layer in the atom which is an integer between 1 and the number of electron layers in the atom) is very high. These atoms are generally of large size, proportional to n^2, and with very strong inter-atomic interactions. These interactions are used to build entanglement between atoms. These atoms have been used by Serge Haroche's team to detect non-destructively the presence of a photon in a cavity, and thus study quantum decoherence. Hydrogen can also be a Rydberg atom if it is excited with high energy levels.

Sapphire: aluminum oxide crystals (Al_2O_3) that is sometimes used as a substrate instead of silicon for the manufacturing of superconducting qubits chipsets. In that case, wafers are made of synthetic sapphire.

SAT: class of logic problem or Boolean satisfiability problem, of 0-order logic. It is a decision problem, which, given a propositional logic formula, determines whether there is an assignment of propositional variables that makes the formula true. As when looking for Boolean variables x, y and z that satisfy the equation $(x \vee y \vee z) \wedge (\bar{\mathbf{x}} \vee \bar{\mathbf{y}}) \wedge (\bar{\mathbf{x}} \vee y \vee z)$, $\wedge$ meaning "and", and $\vee$ "or" or "and". $\bar{\mathbf{x}}$ being the negation of x. The problem becomes very complex if the number N of variables becomes very high because to test their combinatorics with brute force, we will have to test 2^N combinations. This problem has been highlighted by Cook's theorem according to which the SAT problem is NP-complete. The SAT problem also has many applications, notably in constraint satisfaction, classical planning, model verification, diagnostics, up to the configurator of a PC or its operating system: we go back to propositional formulas and use a SAT solver.

Scale-out: generic information technology term describing the capacity to expand computing power with several processors connected to the other. This is done in classical server clusters and datacenters, using both hardware (multiple processors on same board, high-speed connectivity between boards and servers, high-speed data storage, ...). Such techniques are envisioned with quantum computing, consisting in connecting different processing units, usually with using photons and entanglement resources.

Scattering: deflection of moving particles by some physical medium or radiations.

Schrödinger (equation, wave function): describes the evolution in time and space of the wave state of a quantum

object with a mass like an electron, i.e. the probabilities of finding the object at a given place and time in time.

Schrödinger wave function collapse: in the case of a qubit, happens at the end of the coherence (superposed state) which is generated by its state readout, bringing it back to one of its basis states (|**0**⟩ or |**1**⟩). This collapse is also caused by the interaction between the qubit and its environment and after qubit measurement.

Second quantization: field of quantum physics that deals with many-body quantum systems. It was introduced by Paul Dirac in 1927 and developed afterwards by Vladimir Fock and Pascual Jordan.

Second quantum revolution: covers advances in quantum physics since the 1980s, when we began to control the properties of individual quanta, at the level of photons (polarization, ...), electrons (spin) and atoms and also use superposition and entanglement. It covers in particular the uses of these properties in cryptography and telecommunications, quantum computing and quantum sensing. The term was created simultaneously in 2003 by Alain Aspect, Jonathan Dowling and Gerard Milburn.

Semi-classical light: describes interactions between quantized matter (atoms, electrons) and classical light fields. Laser light belongs to this category.

Shor (algorithm): integer quantum factorization algorithm invented by Peter Shor in 1994. It would theoretically allow to break RSA public keys by decomposing them into prime numbers.

Silicon 28: Silicon isotope allowing the creation of silicon wafers suitable for the creation of silicon qubits. Silicon 28 has a zero spin that does not affect the spin of the trapped electrons used to manage the qubits. It is purified in Russia and can then be deposited in a thin layer in the gas phase on conventional silicon.

Single mode: said of an optical fiber using a small core (around 9 µm) and transporting a single light beam that doesn't bounce off the inside walls of the fiber. It has low loss and is adapted to long distance transport, usually in the 1310 nm or 1550 nm wavelengths. These cables still use multiple wavelengths, with WDM (wave-division multiplexing). Also said of a single mode photon, see Multimode.

SPAC: special purpose acquisition company. A funding mechanism used by IonQ and HQS (Honeywell Quantum Systems) consisting in getting acquired by an investment fund creating a dedicated fund for the company and raising money on both limited partners (individual corporate ventures and the likes) and on the stock market like the NASDAQ.

SPAM: State Preparation And Measurement, a sequence of operations after which the fidelity of qubits is measured. This fidelity reflects that of an initialization sequence, the application of single qubit gates and the measurement of the qubit state.

Spectral lines: lines obtained graphically after decomposing an electromagnetic radiation into frequency components, usually with some spectrography apparatus. You have absorption and emission spectral lines depending on the source of light (indirect, direct). Each line corresponds to the emission or absorption of photons in atoms at particular energy levels, then wavelength and frequency.

Spectral decomposition: mathematically, spectral decomposition of a pure state vector in a Hilbert space is its eigenstates $|i\rangle$ and eigenvalues λ_i. It can be related to the wave-duality aspect of all quantum objects. A quantum object pure state is indeed decomposable in a coherent superposition of elementary waves, the eigenstates.

Spin: quantized angular momentum of elementary (like electrons or photons) or composite particles (like atoms) that cannot be described or explained in classical physical terms. The spin of composite particles is the addition of its components spin. A proton and a neutron have a spin of 1/2. An electron has a spin of +1/2 or -1/2. A photon also has a spin, which relates to its circular polarization. Spin help distinguish fermions who have half integer spins from bosons who have integer spins.

Spintronics: a set of technologies based on the manipulation of electron spin. It is found in memristors as well as in hard disks using giant magnetoresistance (GMR). The latter was discovered by Albert Fert (France) and Peter Grünberg (Germany) independently and the same year, in 1988. This got them the Nobel Prize in Physics in 2007.

Spontaneous emission: when an atom emits a photon resulting from the transition of an electron from an excited to a lower energy state.

Spontaneous Four-Wave Mixing (SFWM): photons pairs source category based on pumping nonlinear optical waveguides or cavities.

Spontaneous Parametric Down-Conversion (SPDC): system converting high-energy photons into pairs of photons of lower energy, based on pumping nonlinear optical waveguides (crystals) or cavities. It can be used to create pairs of entangled photons as well as single photons sources.

Squeezed states of light: correspond, in a quadrature or phasor diagram representation, to wave functions which have an uncertainty in one of the quadrature amplitudes (phase or photon number) smaller than for the groundstate corresponding to the vacuum state. It can be generated by different means like a parametric down conversion. In other words, it's a way to increase the measurement precision of one of the photons characteristics at the expense of another characteristic.

SQUID: Superconducting Quantum Interference Device, a magnetometer that measures the direction of current in a superconducting qubit. It is notably used by D-Wave and in some quantum sensors.

Stabilizer gates: quantum gates that are used in error correction systems: CNOT, H (Hadamard) and P (phase).

Standard quantum limit: to estimate a system's parameter, one usually uses light as the meter by making it interact with the system and thereby extracts some information. The standard quantum limit, also known as shot noise, states that the variance of this estimation is larger than the

inverse of the square root of the number of times the measurement is made. It limits the precision of quantum sensing using non-entangled quantum states. See Heisenberg limit.

Stark shift or Stark effect: shifting and splitting of spectral lines of atoms and molecules due to the presence of an external electric field. This is the electric-field analogue of the Zeeman effect which is linked to the effect of the magnetic field,

State reduction: consequence of the measurement of the state of a quantum or a qubit, which modifies its (superposed) state into a stable state (not superposed). For a qubit, it is one of the two basic states: excited or non-excited, horizontal or vertical polarization for a photon, spin orientation for an electron, excited state for an ion or a cold atom, etc.

State vector: Hilbert space vector representing a pure state of a quantum object.

Stationary qubits: stationary (or static) qubits, which do not move in a circuit. This is the case of superconducting qubits, trapped ions and cold atoms qubits as well as electron spin qubits. They are opposed to flying qubits that move, like photons.

Stern-Gerlach experiment: deviation of projected atoms placed under an intense magnetic field, which is explained by electron intrinsic angular momentum or spin.

Stimulated emission: when an incident photon is not absorbed by an excited atom but stimulates the atom to emit a second photon with the same wavelength. This principle is used in lasers to amplify light in their cavity.

Sturm–Liouville problem: mathematical problem consisting in solving some second-order differential equations where the unknown is a density function and finding eigenvalues and eigenvectors and satisfying bound limits. Solving Schrodinger's wave equation is a particular case of such a problem.

Superconductivity: the ability of some materials to conduct electricity without resistance. It generally occurs at low temperatures. It is linked to the behavior of electrons in some crystalline structures who happen to gather in pairs, Cooper pairs, who become bosons, and have a collective behavior enabling them to move around within the structure. Superconducting and electron spins qubits use this effect. The first with superconducting loops traversing a Josephson barrier and all of them with cabling and some surrounding electronics.

Superdense coding: technique used to send two bits on a single (optically transmitted) qubit between two points when they are already connected by a pair of entangled photons. It is a communication protocol imagined by Charles Bennett and Stephen Wiesner in 1992 and experimented in 1996 by Klaus Mattle, Harald Weinfurter, Paul Kwiat and Anton Zeilinger. The initial entanglement preceding the transmission of the two bits in the qubits avoids violating Holevo's theorem that a set of qubits cannot carry more information than the equivalent number of classical bits.

Superoperator: linear operator that transforms a linear operator like a density matrix. It must be a CPTP map, completely positive and trace preserving map (see CPTP definition).

Superposition: property of quantum objects and qubits to be able to be in several states at the same time. This can be explained by the wave-like nature of quantum objects. A superposition is a linear combination of quantum eigenstates (the $|0\rangle$ and $|1\rangle$ in the case of qubits).

Surface codes: type of quantum error correction code that is tolerant to high qubits error rates and require a larger number of physical qubits per logical qubits and have a design constraint for physical qubits that must be connected to their immediate neighbors in a 2D structure. This is the QEC architecture chosen by Google.

SVD: singular value decomposition, a mathematical process to factorize any mxn complex values matrix into three matrices: a unitary mxm matrix, a rectangular diagonal mxn matrix (which has no zero values only in its diagonal) and a unitary nxn matrix. SVD is used in QSVT algorithms.

SWAP: quantum gate that inverts the state of two qubits. It is very useful since most qubit geometries don't allow an any-to-any qubit connection. The SWAP gate enables this kind of connection that is mandatory for many quantum algorithms.

Symmetry: of Schrödinger's wave function, with bosons. Fermions have an antisymmetric wave function. It is the mathematical consequence of Pauli's exclusion principle which states that two fermions with the same quantum numbers cannot cohabit while two similar bosons can.

T gate: single qubit gate implementing a "quarter turn" phase rotation around the Z axis in the Bloch sphere. It is a very important gate enabling (on top of the three-qubit Toffoli gate) the creation of a universal gate set.

T-count: number of T gates required in a quantum algorithm. It is an important metric since T gates are the most expensive to correct with FTQC.

T-depth: number of circuit layers implementing one or several T gates in a quantum algorithm.

T_1: qubit amplitude coherence time, which indicates the end of coherence of the qubits linked to a loss of amplitude ("energy relaxation"). Aka qubit lifetime.

T_2: phase related coherence or time when some phase shift occurs, i.e. a rotation around the z axis in the Bloch sphere of the qubit state.

Tensor: in multilinear algebra and differential geometry, a tensor designates a very general object whose value is expressed in a vector space. In quantum physics and computing, tensors are used to describe the state of a compound quantum object with several quanta or qubits. A qubit is represented by a vector of 2 complex numbers. A register of N qubits is represented by a vector with 2^N complex numbers resulting from the tensor product of N vectors of 2 complex numbers. In a way, the tensor product represents the combinatorial space of the values that a combination of qubits can take. Before entanglement comes into play to mix things up and create non separable vector states, i.e.,

which cannot be expressed as tensor products of individual quantum states.

Thermodynamics first law: the internal energy of an isolated system is a constant, applying the principle of the conservation of energy. Inside the system, the form of energy can however be transformed.

Thermodynamics second law: the entropy of a closed system cannot decrease. In other words, heat does not flow spontaneously from cold to hot objects. Was formalized by Rudolph Clausius in 1854.

Time crystal: also, DTC for discrete time crystal is a topological state of condensed matter at very low temperature where atoms in their ground state are periodically arranged in both space and time with in a permanently oscillating structure with a given period (for discrete time crystals).

Time domain: deals with the evolution of some value and signal over time. It's frequently opposed to frequency domain where a signal is analyzed with decomposing it into frequencies (mathematically, with a Fourier transform).

Time reversal: clearly a misnomer. It describes situations when from a given point in time, for some physical property like energy, a system presents a symmetry when you evaluate it with look forward or backward at time. It's a mathematical symmetry. You don't change the arrow of time backwards. Time reversal is not a time machine!

Toffoli (gate): also called CCNOT is quantum gate operating on three qubits which modifies the value of the third qubit if the value of the first two is 1.

Topological: topological quantum computing is based on the notion of anyons which are "quasi-particles" integrated in two-dimensional systems. The anyons are asymmetric and two-dimensional physical structures whose symmetry can be modified. This allows the application of topology principles with sets of successive permutations applied to pairs of anyons that are in proximity in circuits. The associated algorithms are based on the concepts of topological organizations of braids or nodes ("braids"). There is an algorithmic equivalence between computation with universal gated qubits and topological qubits.

Transmon: transmission-line shunted plasma oscillation qubit, variation of superconducting qubit with superconducting current oscillating at two different frequencies across a Josephson junction. The difference between these two frequencies corresponds to the energy of the microwave pulses sent to the qubit to drive single qubit gates.

Transpiler: source-to-source compilers used in classical computing and quantum computing to optimize the source code based on some hardware constraints like to fit with the universal gate set available in the quantum processor. It can help reduce the number of gates to execute and as a result, reduce errors (particularly with NISQs) and reduce the algorithm execution time.

Transpilation: code conversion and optimization achieved by transpilers.

Transversal gates: relates to quantum error correction and fault tolerance. These are gates implemented with QEC where there is a 1-1 correspondence and link between all qubits from a given corrected qubit with a similar corrected qubit, when they are assembled through concatenation. This mechanism limits the propagation of errors between logical and physical qubits.

Trapped ions: these are ions used in certain types of quantum computers. They are usually trapped magnetically or electrically, and their state is controlled with lasers. Their readout uses a laser excitation and an imager readout of the resulting ions fluorescence.

Tunnel effect: property of a quantum object to cross a potential (or energy) barrier even if its energy is less than the minimum energy required to cross this barrier. This effect is used in D-Wave's quantum annealers to quickly determine the minimum energy of a complex system ("Hamiltonian" implemented as an Ising model).

Two-Level Systems (TLS): other descriptor of quantum systems used to implement qubits. A qutrit is a three-level system.

TWPA (Travelling Waves Parametric Amplifiers) microwave readout amplifiers implemented in a long array of SQUIDs. Their broad bandwidth that can reach 2 GHz with a 15 dB amplification enables up to 20 qubits readout multiplexing. But it depends on the gate speed since the faster the gate, the smaller the microwave pulse bandwidth will be large.

UHV: Ultra High Vacuum, the ultra-high vacuum required to operate certain types of qubits. It is mainly used for cold atoms and trapped ions. Superconducting qubits are integrated in a vacuum cryostat that does not require ultra-high vacuum.

Ultraviolet catastrophe: expression of Paul Ehrenfest, linked to the Rayleigh-Jeans law proposed in 1900 to explain the black body radiation spectrum, which was diverging to infinite values as the temperature was growing, when reaching ultraviolet wavelengths. Planck's law based on quanta solved the problem and got rid of the ultraviolet catastrophe.

Unary gates: single qubit gates. Not to be confused with unitary operations that are the result of the combination of all qubit gates on a given set of qubits. A unitary transformation of the computational state vector is a matrix operator that is equal to its transconjugate. It is a mathematically reversible operation.

Unconventional Computing: computing methods that do not fall under the classical computing principles of Turing and Von Neuman machines. Covers non-traditional tools and methods that include, but are not limited to, quantum computers. It also includes molecular computers and neuromorphic processors.

Unitary operation: linear operation on a vector that preserves its length. In the case of qubits whose vector always has a length of 1, the unitary quantum gates apply on it a transformation that preserves this length and is also reversible. In the representation of qubits in the Bloch sphere, the operation rotates the vector representing the state of the qubit in this sphere.

Universal quantum computer: most generic form of a quantum computer exploiting a universal quantum gate set, and which can both simulate quantum physics and implement any operations of a classical computer.

Universal quantum gates: sets of quantum gates from which all other quantum gates can be reproduced to create any unitary transformation on any number of qubits (by approximation and under a given error rate). It requires a non-Clifford group gate, like a T gate or a Toffoli gate.

Unruh effect: relativistic thermodynamic effect with a black body radiation showing up in vacuum at relativistic speed. Il has some connection with quantum noise.

VQA (Variable Quantum Algorithm) more generic quantum hybrid algorithm than VQE. It combines a classical optimizer that is used to train a parametrized quantum circuit. It could lead to obtain some quantum advantage with NISQ quantum computers. VQA has a broad set of applications: finding ground and excite states, quantum simulations, machine learning and optimizations.

VQE (Variational Quantum Eigensolver): hybrid quantum algorithm used in chemical simulation created in 2013. Its main contributor is Alán Aspuru-Guzik, a researcher at the Zapata Computing startup. It is also used in machine learning tasks. VQE was the first proposed VQA.

Wave packets: is a burst of electromagnetic wave that travels as a unit. It is formed by the addition of an infinite number of sinusoidal waves of different frequencies, phases and amplitudes creating constructive and destructive interferences on a small region in space, and destructively elsewhere. Wave packets are used in many quantum technologies such as with microwaves sent to superconducting and electron spin qubits or by femto- and picoseconds lasers. In these cases, their decompositions in frequencies lead to so-called frequency combs.

Wave-particle duality: the property of elementary particles such as electrons, neutrons, atoms and photons to behave as both particles with momentum and waves that can generate interference. It is verified with the famous Young's slits experiment which shows these interferences with both photons and electrons.

Wien's displacement law: describes the relationship between peak wavelength and temperature in black body energy spectrum. Discovered by Wilhelm Wien in 1893.

Wigner function: representation of a quantum state used to measure the level of quantumness of a light pulse. It has the particularity of having negative values for entangled and non-gaussian states. It is usually visualized in a 3D chart with peaks and lows. Also called Wigner quasiprobability distribution or Wigner-Ville distribution. It was created by Eugene Wigner in 1932.

X: quantum gate at a qubit that inverts its amplitude, goes from $|\mathbf{0}\rangle$ to $|\mathbf{1}\rangle$ or from $|\mathbf{1}\rangle$ to $|\mathbf{0}\rangle$ for the basis states.

XY gates: two qubit entangling gate.

Y: single-qubit quantum gate that performs a 180° rotation around the Y axis in the Bloch sphere.

Z: quantum gate to a qubit that applies a sign change to the β component of the qubit vector, i.e. a phase inversion and a 180° rotation with respect to the Z axis. More generally, Z gates is also a denomination for phase change gates.

Zeeman effect: splitting of spectral lines when atoms are placed in a static magnetic field. Explained by the different electron's magnetic moment and/or by the atom nucleus spin for the nuclear Zeeman effect. There are two Zeeman effect, the normal and abnormal effect, differentiated with the off/even spectral rays generated and generated by different orbital angular momentum (normal) and spin (abnormal).

Zeeman cooling or slower: use of the Zeeman effect to cool atoms at a lower temperature than with a simpler Doppler effect. Invented by William D. Phillips (Nobel prize in physics in 1997), it consists in adjusting the atoms resonant frequency with a magnetic field as the atoms are slowing down when implementing the Doppler effect.

ZX calculus: graphical language and formalism used to visualize in quantum programming the notions of entanglement, complementarity, causality and their interactions. It can be used for Measurement Based Quantum Computing (MBQC), the creation of error correction codes and compiler optimization techniques.

Index

Table of figures

Revisions history

This book improved over time with successive revisions. The first editions from September 2018, 2019 and 2020 were published in French and this fifth one is the second published in English. It is freely downloadable on:

https://www.oezratty.net/wordpress/2022/understanding-quantum-technologies-2022/

Different PDF formats are available: **A4 in full resolution in a single volume** (87 Mb), **A4 in reduced resolution in two volumes** (to fit under the 32 Mb threshold for some ebook readers) and the same in **Letter format** for USA and Canada readers who would like to print it on their own.

After a post-publication proof-reading and correction couple weeks period, I also published it during October 2022 on **arXiv** (https://arxiv.org/abs/2111.15352) and in printed paperback editions on most **Amazon** web sites.

Version and date	Modifications
1.0 (332 pages) September 29th, 2018	First version of this document published in French and consolidating 18 posts published between May and September 2018 on www.oezratty.net.
2.0 (504 pages) September 20th, 2019	Second edition, also in French. New content on superconductors, superfluidity, quantum sensing, quantum supremacy, quantum computing emulation, cryogeny, hybrid algorithms, algorithms certification, quantum teleportation, blind computing. Addition of a glossary and bibliography.
3.0 (684 pages) September 7th, 2020	Third edition, also in French. New content on Maxwell, Schrödinger and Dirac's equations, relativistic quantum chemistry, how research works, lasers and masers, polaritons, extreme quantum, linear algebra, quantum gates classes, quantum error correction codes, cryo-electronics, MBQC, quantum cloud, qubits technologies, unconventional classical computing, quantum hype cycle, quantum foundations and on the influence of science fiction.
4.0 (838 pages) September 27th, 2021	Fourth edition, the first one in English. Main new features vs the 3.0. on top of updates nearly everywhere: New section on quantum physics postulates, page 86. More on wave-particle duality and on photon qubits physics. Improvements and extensions on linear algebra, on quantum measurement and quantum memory. New part on vacuum in enabling technologies. Much improved section on algorithms, including data preparation and debugging. Expanded part on QRNG. Went from 265 to over 450 vendors covered in the various sections of the book. More on ethical issues and gender balance. Additional covered countries: Belgium, Portugal, Italy and Abu Dhabi and nice ecosystems maps for the USA and the UK. Added an index with company names, people and some scientific terms and many terms in the glossary (from 179 to >280).

From October 2021 to January 2022	The two-volumes printed version of the book was made available to purchase at an affordable price on most **Amazon** sites. Added a new graph explaining Dirac $\langle A\|B\|C\rangle$ notations in the measurement section starting page 185. Added a roadmap for managing the energetic footprint of quantum computing. Added American Binary (Ambit) in the quantum cryptography vendors section that starts page 859. Small update related to D-Wave gate-based quantum computing announcement in the quantum annealing section that starts page 277. Added Energetics of quantum technology, Quantum postulates, QML, QLM and scale-out in the glossary. Corrected wrong naming for Atos QLM (instead of Atos QML or Atos aQML). Update on Origin Quantum and their cloud quantum emulation offering. Added StarX Electronics in the inventory of enabling technology vendors and Chipiron in quantum sensing imaging, starting page 896. Added Two-Level Systems in glossary. Added a chart from Joseph Bardin describing the various microwave and other signals used to drive superconducting, electron spin and trapped ions qubits. Added Algorithmic qubit, anharmonic oscillator, cQED, CQED, fluxonium, Q-factor, Dirac and Reduced Planck constants, homodyne detection and Universal quantum computer in the glossary. Updates on IBM and its 127 qubits processor announced in November 2021, the related qubits fidelities chart with the best-in-class IBM 27, 65 and 127 QPUs. Some updates on IQM and OQC (on Amazon Braket). Updates on Kipu Quantum and on Quantinuum (new name for HQS/CQC merger). Added a mention on Alexia Auffèves quantum energy initiative. Updates on Quandela, Qu&Co (acquired by Pasqal) and Rahko (acquired by Odyssey Therapeutics). Added Mikhail Lukin in the quantum computing physicists section. Added Black Quant and Runa Capital in the quantum investors section.
5.0 (1128 pages in single volume version) September 2022	Many updates everywhere, including… **Why**: new intro, rearranged and updated the part on Moore's law. Removed the long abstract from the previous version. **History and scientists**: updated scientists with more stuff on Marc Benioff, David Deutsch, David Hilbert, Daniel R. Simon, Erwin Schrodinger and new bios for Andrew G. White, Gaston Floquet, Bruce Kane, Daniel Kleppner, Daniel Loss, Frank Wilczek, Gerhard Rempe, Herbert Walther, James Clarke, Jeff Kimble, Jian-Wei Pan, Leo Kouwenhoven, Menno Veldhorst, Steven Girvin, Rob Schoelkopf, Roy J. Glauber, Jay Gambetta, Alexandre Blais, Robert Raussendorf, Maciej Lewenstein, Ronald Walsworth and Philip W. Anderson. More details on how research works, papers published and evaluated. **Quantum physics 101**: added a table listing the various quantum physics postulates versions, added nuclear quantum numbers in quantization, added a part on quantum matter, including on quantum batteries, time crystals and skyrmions. **Gate-based quantum computing**: various updates on quantum gates, added illustrations on quantum computing dimensionality, better differentiation between quantum emulation and quantum inspired software. **Quantum computing engineering**: simplified qubit type descriptions, update content on exotic qubits, better explained how error rates are measured, many updates on quantum error

	corrections, definitions of FTQC, universal QC and LSQC. Described in detail the whereabouts of the Quantum Energy Initiative. Added a definition of quantum switch. **Quantum computing hardware**: added vendor investment comparisons per type of qubit, types of use cases per qubit type, inventory of scalability challenges per type of qubit, rearranged and standardized the presentation of each qubit type with history, science, qubit operations, research and vendors. More schematics. More science on quantum annealing. Genealogy of superconducting qubits. Updated content on IBM, Google, Rigetti, IQM, OQC and added Atlantic Quantum, Baidu and Toshiba in superconducting computers vendors. Comparisons of different types of quantum dots spin qubits. Added Diraq in quantum dots spin qubits vendors, XeedQ in NV centers qubits vendors, It's Q, Quantum Source Labs and TuringQ in photonic qubits vendors and Crystal Quantum Computing and Planqc in neutral atoms qubit vendors, and Hon Hai / Foxconn in the trapped ions vendors list. Added coherent Ising machine in quantum photonics systems. Archer Materials, Atom Computing, Bleximo, BosonQ Psi, Nord Quantique and QBoson. **Quantum enabling technologies**: rearranged the section on control electronics. Added ICE, Maybell Quantum and FormFactor, and updated myCryoFirm in cryostats vendors, Active Technologies, Keysight, QuantrolOx and Scalinq in control electronics vendors, Qubic Technologies, Raditek, QuinStar Technology, RF-Lambda, Wenteq Microwave Corp, Holzworth Instrumentation, apitech, Analog Quantum Circuits, CryoHEMT and Silent Waves in cryoelectronics vendors, CryoCoax, XMA and Rosenberger Group in cable and filtering vendors and Alcyon photonics, Teem photonics and Scintil Photonics in photonic enabling technologies vendors, AnaPico, Diatope, HiQeTe Diamond, Orsay Physics, QuantTera and Quantum Diamant in other enabling technologies vendors. Added a new part on fabs, processes and manufacturing tools. Added here many manufacturing tools vendors like BESI, PlasmaTherm, Picosun Group, NanoAcademic Technologies and QuantCAD. Updates on raw materials. **Quantum algorithms**: added a part on tensor networks. Significant updates on quantum machine learning. **Quantum software development tools**: updates on emulation software, restructured and updated the part on benchmarking. **Quantum business applications**: updated all vertical case studies lists. Added Arclight Quantum, Allosteric Bioscience, Artificial Brain, ColibrITD, Dirac, Foqus, GenMat, Good Chemistry Company, Ingenii, Qbraid, QEDma, Qoherent, Quanscient, Quantagonia, Sanctuary, SavantX, Tinubu Software and Turing in the software and tools vendors inventory. Created a section on IT service vendors working on quantum technologies. Added DN-Quantum Computing, Kvantify, Plantagenet Systems, Protiviti, Psi-Ontic, Quantum Computing Engineering, Quanvia, quGeeks, Quant-X Security & Coding, Qubitech and Unitary Zero Space. Updated information on AegiQ, Azurlight Systems, Cogniframe, exaQ.ai, Horizon Quantum Computing, HQS Quantum Simulations, Multiverse Computing, and Nomidio, Phasecraft, OTI Lumionics, Q.ant, Quantum Computing Inc, QunaSys, Q-Ctrl, Strangeworks and Terra Quantum. **Quantum enabling technologies**: I singled out this part and moved it to the second volume. Content has been sporadically updated. **Quantum telecommunications and cryptography**: added a part on quantum photon sources and detectors in the QKD section, improved description of trusted nodes and repeaters, rearranged and enriched the quantum interconnect and telecommunication part. Update on PQC with NIST 2022 selection results. Added Abelian, ComScire in QRNG vendors, Bohr Quantum Technology, Photoniq and Entanglement Networks in quantum telecommunications, NodeQ, Patero, QANplatform, Quantum Collective, SandboxAQ, Synergy Quantum and ThinkQuantum in quantum telecommunications and cryptography vendors. Updated information on Post-Quantum, IDQ, Qnu Labs, QphoX and, Qunnect. **Quantum sensing**: added new parts on quantum sensing taxonomy and on quantum pressure sensing. More details on quantum thermometers. Added OK Quantum and Zero Point Motion in quantum gravimeters and accelerometers, Improved the technical description of a quantum gravimeter. QuSpin, Siloton, QLM Technology and Mag4Health in imaging sensors and qdm.io and Elta Systems in quantum magnetometers. Updated information on Chipiron.

	Quantum technologies around the world: updates in investments data, new part disappeared startups, SPACs, government spending and quantum national initiatives rationales. Added Finland, Norway, Hungary, Ireland, and Qatar in countries overview and Intqlabs startup in UAE. Updated nearly all other countries quantum activities. Added a map of Canada's quantum ecosystem. **Quantum technologies and society**: added EFEQT in scientific education and on quantum technologies marketing. **Bibliography**: reshuffled the quantum events section, added an events timeline. **Glossary**: added Ansatz, Bell state, Chi (nonlinearity order), Circuit, Coulomb blockade, crosstalk, CVD, Fermi sea, Floquet code, EBL, electron gas, FTDQC, Flux biasing, Gaussian Boson Sampling (GBS), Hall effect, Heterodyne and Homodyne measurements, I/Q mixer, Jaynes-Cummings Hamiltonian, JPA, Leggett-Garg inequality, MBE, Magneto-Optical Trap, mesoscopic, metal layers, microring resonator, Mott insulator and Mott transition, Mutually unbiased bases, no-go theorem, normalization, on-premises, ODMR, paramp, photolithography, Purcell effect, Purcell filter, purification, PVD, Quantum Hall effect, QHO, QND, QSVT, QUBO, quantum steering, quantum switch, Ramsey experiment, relaxation, Renyi entropy, RIE, Sapphire, surface code, SVD, time crystals, time reversal, TWPA, Stark shift, Unruh effect and Zeeman cooling. Added over 900 figure captions with sources and sorting out how figures are referenced in the text (mostly).
5.1 (1128 pages in single volume version) October 12th, 2022	Added Nobel prize mentions for John Clauser, Alain Aspect and Anton Zeilinger. Integrated some corrections suggested by André Konig. Modifications in the FTQC/LSQ nomenclature proposed in Figure 246 with suggestions from Alastair Abbott and Tristan Meunier and thoughts about the progressive growth of logical qubits fidelities. Presentation improvements in quantum physics simulation algorithms. Various improvements in the part on quantum error correction page 235. Various edits in satellite QKD, China funding, Google Sycamore, NV centers frequency analyzers in sensing.
5.2 (1130 pages in single volume version) October 16th, 2022	Updates on Alain Aspect's experiment and its explanation. Updates in insurance use cases. Added the class NISQ in quantum complexity classes. Added quantum amplitude estimation in the algorithms toolbox. Precisions on transpilers and transpilation in the gates section and with the glossary. Added T gate, T-count and T-depth in the glossary. Added IonQ, Rigetti and D-Wave quarterly revenue in the investor section. Added a reference to the book "Quantum Software Engineering" in the bibliography. Index cleanup and various edits elsewhere.
5.3 (1132 pages) October 23th, 2022	Changed page formatting at the beginning of volume 1 to accommodate Amazon's stringent rule for paperback edition support on KDP. Added a new partnership between Switzerland and the USA.
5.4 (1132 pages) October 25th, 2022	Updated the record "non-Shor" integer factoring algorithms in the quantum cryptoanalysis threat section.
5.5 (1132 pages) October 31th, 2022	Several corrections in the precursors and founders sections with errors in Einstein's photoelectric and Dirac's relativistic equations and other hidden details. Updated chart on algorithms per computing paradigm and UK industry ecosystem.

5.6 (1132 pages) November 27th, 2022	Updates on Keequant, Orca Computing, Quantopticon, Quantum Brilliance, QuiX, Q.ANT, Qunnect and XeedQ using content from the Optica Conference in November 2022. Updates on M Squared and Exail (formerly ixBlue) in the quantum sensing part. Added LuxQuanta in QKD vendors.
5.7 (1132 pages) December 1st, 2022	Added Siquance in the silicon qubits startups.

I update the book on a regular basis as I find editorial issues, mistakes, misspellings, and the likes. You can submit me any comment, correction, suggestion or even request for digging into some untapped topic (olivier@oezratty.net).

page intentionally left blank.

page intentionally left blank.

back-cover flip page.

le lab quantique

⟨ Aage Niels Bohr | Abner Shimony | Adi Shamir | Akira Furusawa | Alain Aspect | Alain Ravex | Alain Sarlette | Alán Aspuru-Guzik | Alastair Abbott | Albert Einstein | Alberto Bramati | Alexander Andreev | Alexander Holevo | Alexander Prokhorov | Alexandre Blais | Alexandre Zagoskin | Alexei Bylinskii | Alexei Grinbaum | Alexei Kitaev | Alexia Auffèves | Alfred Kastler | Alfred Pérot | Alonzo Church | Amir Naveh | André Luiz Barbosa | Andrea Morello | Andrea Rodriguez Blanco | Andreas Wallraff | Andrew Childs | Andrew Cross | Andrew Gle | Andrew White | Andy Matuschak | Anne Broadbent | Anne Canteaut | Aram Harrow | Arieh Warshel | Arthur Holly Compton | Arthur Leonard Schawlow | Artur Ekert | Astrid Lambrecht | Audrey Bienfait | Axel Becke | Benjamin Huard | Benoît Valiron | Bettina Heim | Bob Wiens | Boris Podolsky | Brian Josephson | Bruce Kane | Bruno Desruelle | Bryce DeWitt | Carl Wieman | Carlo Rovelli | Chad Rigetti | Charles Bennett | Charles Fabry | Charles Hard Townes | Charles Hermite | Chien Shiung Wu | Christiaan Huygens | Christian Weedbrook | Christine Silberhorn | Christophe Jurczak | Christophe Solomon | Christophe Vuillot | Christopher Monroe | Christopher Papile | Claude Cohen Tannoudji | Claude Weisbuch | Clauss Jönsson | Clinton Davisson | Cornelis Dorsman | Cristian Calude | Cristina Escoda | Cyril Allouche | Damien Stehlé | Daniel Esteve | Daniel Gottesman | Dave Wecker | David Bohm | David Deutsch | David DiVincenzo | David Gosset | David Hilbert | David J. Thouless | David Wineland | Dennis Dieks | Dieter Zeh | Dirk Bouwmeester | Don Coppersmith | Don Misener | Donna Strickland | Dorit Aharonov | Douglas James Scalapino | Earle Hesse Kennard | Ed Sperling | Edward Farhi | Edward Fredkin | Edward Tang | Elena Calude | Eleni Diamanti | Elham Kashefi | Elisabeth Giacobino | Elvira Shishenina | Emanuel Knill | Emmy Noether | Enrico Fermi | Eric Cornell | Ernest Rutherford | Ernst Ising | Erwin Schrödinger | Etienne Klein | Ettore Majorana | Ewin Tang | Fabio Sciarrino | Faye Wattleton | Felix Bloch | Francesca Ferlaino | Franck Balestro | François Le Gall | Frédéric Grosshans | Frédéric Magniez | Freeman John Dyson | Friedrich Hund | Friedrich Paschen | Geordie Rose | George Uhlenbeck | Georges Paget Thomson | Georges Zweig | Georges-Olivier Reymond | Gerard Milburn | Gerrit Jan Flim | Gil Kalai | Gilles Brassard | Gilles Holst | Giorgio Frossati | Gordon Baym | Gordon Gould | Guang-Can Guo | Haig Farris | Hans Albrecht Bethe | Hans Jürgen Briegel | Hantaro Nagaoka | Harald Fritzsch | Hartmut Neven | Heike Kamerlingh Onnes | Heinrich Hertz | Hélène Bouchiat | Hélène Perrin | Hendrik Anthony Kramers | Hendrik Casimir | Hendrik Lorentz | Henri Poincaré | Hermann Minkoswki | Hermann Weyl | Hugh Everett | Hui Khoon Ng | Ilana Wisby | Ilya Mikhailovich Lifshitz | Immanuel Bloch | Iñigo Artundo | Iordanis Kerenidis | Irfan Siddiqi | Isaac Chuang | Isaac Newton | Itamar Sivan | Jacqueline Bloch | Jacques Salomon Hadamard | James Chadwick | James Clarke | James Clerk Maxwell | James Park | Jared Cole | Jason Alicea | Jay Gambetta | Jean Michel Raimond | Jean-François Roch | Jean-Michel Gérard | Jean-Philip Piquemal | Jian-Wei Pan | Jelena Vučković | Jelena Vucokic | Jeremy O'Brien | Joannes van der Waals | Joe O'Gorman | Johann Balmer | Johannes Pollanen | John Bardeen | John Clauser | John Frank Allen | John Hall | John Levy | John Martinis | John Morton | John Rowell | John Smolin | John Stewart Bell | John Von Neumann | John Watrous | John Koomey | Jonathan P. Home | José Capmany | José David Domenech | Jose Ignacio Latorre | Joseph Jo | Josh Nunn | Juan Ignacio Cirac | Julia Kempe | Julian Schwinger | Julien Bobro | Kevin Young | Kirill Tolpygo | Kohei Itoh | Kristel Michielsen | Krysta Svore | Léon Brillouin | Leon Neil Cooper | Leonard Adleman | Lester Germer | Llewellyn Thomas | Loïc Henriet | Louis Cauchy | Louis de Broglie | Lu Jeu Sham | Ludwig | Luigi Frunzio | Magdalena Hauser | Marcus Doherty | Marcus Huber | Martin Karplus | Masahide Sasaki | Masahiro Kitagawa | Masahito Haya | Matthieu Desjardins | Maud Vinet | Max Born | Max Planck | Michael Ben-Or | Michael Frank | Michael Freedman | Michael Horne | Michel Devoret | Michelle Simmons | Mikhail Dyakonov | Mikhail Lukin | Nathanaël Cottet | Niccolo Somaschi | Nick Farina | Nicolas Gaude | Nikolay Basov | Nir Minerbi | Nobuyuki Imoto | Oleg Mukhanov | Olivier Carnal | Pascual Muñoz | Patrice Bertet | Patty Lee | Paul Benioff | Paul Dirac | Paul Hiria | Peter Knight | Peter Leek | Peter Shor | Peter Zoller | Philip W. Anderson | Philipp Le | Pierre Hohenberg | Pierre Rouchon | Pieter Zeeman | Pranav Gokhale | Pyotr Kapitsa | Raymond Laflamme | Rebecca Krauthamer | René Descartes | Richard Feynman | Richard Murray | Rob Schoelkopf | Rob Whitney | Robert Andrews Millikan | Robert Dennard | Robert König | Robert McDermott | Roy J. Glauber | Robert Raussendorf | Robert William Boyd | Robin Blume-Kohout | Roger Penrose | Roland | Roman Lutsiv | Ron Rivest | Roy Glauber | Ronald Walsworth | Rudolf Grimm | Ryan Babbush | Samuel Goudsmit | Sandu | Sara Ducci | Sarah Sheldon | Satyendranath Bose | Scott Aaronson | Sébastien Balibar | Sébastien Tanzilli | Serge Haroche | Sergey Bravyi | Seth Lloyd | Shengtao Wang | Shi Yaoyun | Shin'ichirō Tomonaga | Silvano de Franceschi | Simon Benjamin | Simon Perdrix | Simone Severini | Sophia Economou | Stefanie Barz | Stephanie Wehner | Steve Girvin | Steve Lamoreaux | Taki Kontos | Tauqir Abdullah | Terry Rudolph | Théau Peronnin | Theodor Hänsch | Theodore Lyman | Theodore Maiman | Thibault Jacqmin | Thierry Lahaye | Thomas Monz | Thomas Young | Tommaso Calarco | Tommaso Toffoli | Tracy Northup | Travis Humble | Tristan Meunier | Umesh Virkumar Vazirani | Urmila Mahadev | Valerian Giesz | Vasilis Armaos | Vincent Bouchiat | Virginia D'Auria | Vlad Anisimov | Vladan Vuletic | Vladimir Fock | Walter Brattain | Walter Kohn | Walter Houser Brattain | Walther Meissner | Walther Nernst | Wassim Estephan | Werner Heisenberg | Wilhelm Wien | William Rowan Hamilton | William Shockley | William Wootters | Willis Eugene Lamb | Winfried Hensinger | Wojciech Zurek | Wolfgang Haken | Wolfgang Lechner | Wolfgang Paul | Wolfgang Pauli | Wolfgang Ketterle | Xavier