

Understanding Quantum Technologies

Fifth edition

Key takeaways

2022

Olivier Ezratty



le lab quantique

cover back page

#QEI
the quantum energy initiative

discover the [QEI](#)

Understanding Quantum Technologies

Fifth edition
Key takeaways
2022

Olivier Ezratty

About the author

Olivier Ezratty

consultant and author



[olivier \(at\) oezratty.net](mailto: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 was 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 paperback 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 project with Alexia Auffèves (CNRS MajuLab Singapore). He is a member of the strategic board of QuantAlps, the quantum ecosystem in Grenoble, since January 2022.
- He is an expert on quantum projects for Bpifrance, 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 CentraleSupélec, 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 CentraleSupélec in 2015.

This document is provided to you free of charge and is licensed under a "Creative Commons" license.
in the variant "Attribution-Noncommercial-No Derivative Works 2.0".



see <http://creativecommons.org/licenses/by-nc-nd/2.0/> - web site [ISSN 2680-0527](http://www.issn.org/ISSN_2680-0527)

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

Understanding the key take aways	6
Why... ..	7
Quantum physics history and scientists	8
Quantum physics 101.....	9
Gate-based quantum computing.....	10
Quantum computing engineering.....	11
Quantum computing hardware	12
Quantum enabling technologies.....	13
Quantum algorithms.....	14
Quantum software development tools.....	15
Quantum computing business applications	16
Unconventional computing.....	17
Quantum telecommunications and cryptography	18
Quantum sensing.....	19
Quantum technologies around the world.....	20
Quantum technologies and society	21
Quantum fake sciences	22

About these key takeaways

“Understanding Quantum Technologies” was released at the end of September 2022 in its 5th edition. This quite large sequel is 1128 pages long and it may frighten you. It is available as a free to download PDF in various formats (A4, Letter, single or two volumes) here:

<https://www.oezratty.net/wordpress/2022/understanding-quantum-technologies-2022/>

This book is a kaleidoscope for quantum technologies with a 360° perspective encompassing historical, scientific, technological, engineering, entrepreneurial, geopolitical, philosophical, and societal dimensions. It is not a quantum for dummies, babies, or your mother-in-law book. It mainly targets three audiences: information technologies (IT) specialists and engineers who want to understand what quantum physics and technologies are about, and decipher its ambient buzz, all participants to the quantum ecosystem from researchers to industry vendors and policy makers, and at last scientific students who would like to investigate quantum technologies as an exploratory field.

For your convenience, I have extracted the key takeaways that are at the end of each part and included a key illustration in this short version to create this special edition of the book.

Olivier Ezratty

October 2022

Why...

- All existing digital technologies are already quantum and belong to the first quantum revolution including transistors, lasers and the likes, leveraging our control of light-matter interactions with large ensembles of quantum objects (electrons, atoms, photons). The second quantum revolution is about using a variable mix of superposition, entanglement and individual quantum objects. It usually contains quantum computing, quantum telecommunications, quantum cryptography and quantum sensing.

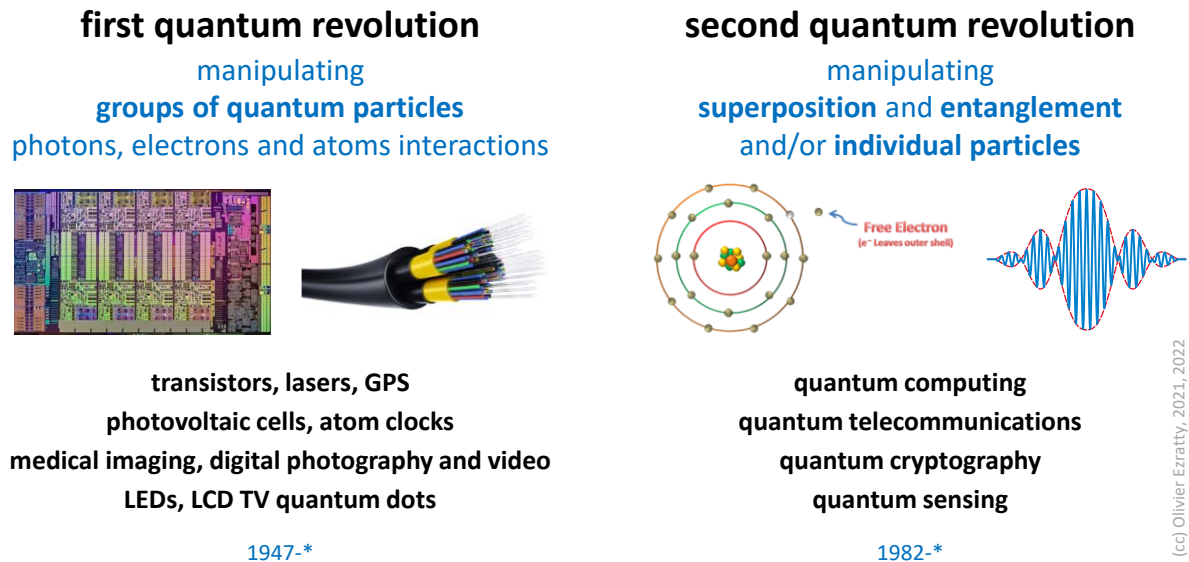


Figure 1: first and second quantum revolution definition and related use cases. (cc) Olivier Ezratty, 2020-2022.

- Quantum technologies are at the crossroads of many scientific domains encompassing physics, mathematics, computing, social sciences and the likes. It creates new educational and pedagogy challenges that must be addressed in innovative ways and customized according to various audiences. This book targets broad audiences with some technical background, including computer science engineers.
- Quantum computing promise is to solve so-called intractable problems whose computing complexity grows exponentially with their size. These can't be solved with classical computing, whatever happens with Moore's law. But we're not there yet since there are many challenges to scale quantum computers beyond what can be done today. In the interim, some marginal improvements will come with noisy intermediate scale computers, including better and more precise solutions in various domains.
- Other new technologies may compete with quantum computing, belonging to the broad "unconventional computing" category. Only a very few of these could also bring some exponential computing capacity. Most others bring other benefits compared with classical computing like in the energy consumption domain. Some of these technologies like superconducting electronics and adiabatic/reversible computing could also be helpful as enablers of quantum computing scalability.

Quantum physics history and scientists

- A first wave of 19th century scientists laid the groundwork that helped create quantum physics afterwards (Young, Maxwell, Boltzmann, mathematicians). The photoelectric effect, black body spectrum and atoms emission or absorption spectrum were not explained with the current theoretical frameworks.
- Starting with Max Planck, a second wave of scientists (Einstein, De Broglie, Schrodinger, Heisenberg, Dirac, Born, Von Neumann) created quantum physics to describe light/matter interactions, energy quantification and wave-particle duality. It solved most of the 19th century unexplained physics experiments.

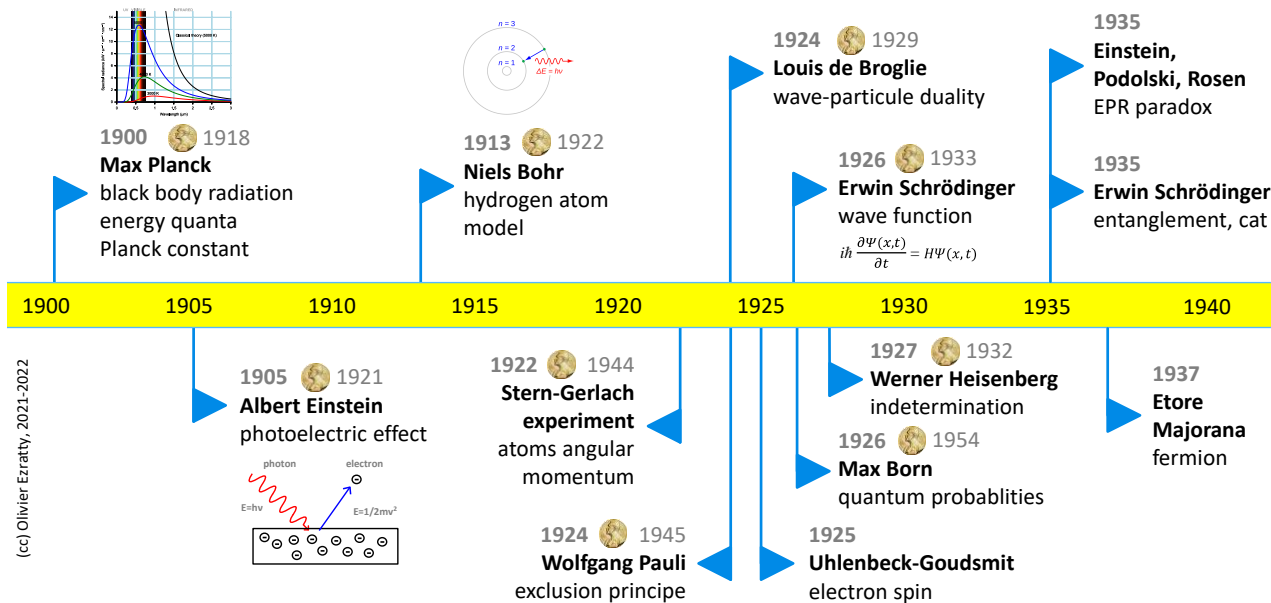
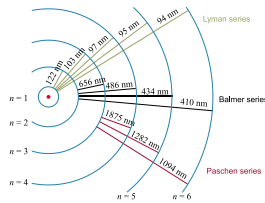


Figure 2: quantum physics foundational years timeline. (cc) Olivier Ezratty, 2021-2022.

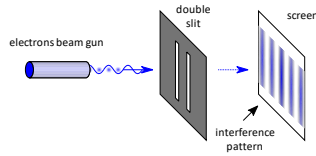
- These scientists were theoreticians while many lesser-known researchers were experimentalists with landmark discoveries (superconductivity, electron interferences, Stern-Gerlach experiment, ...).
- After World War II all digital technologies (transistors, lasers, telecommunications) were based and are still based on quantum physics, as part of what is now called the first quantum revolution.
- Since the 1980s and thanks to advances in individual quantum objects control and the usage of quantum superposition and entanglement, new breeds of technologies were created, most of them belonging to the “quantum information science” field and being part of the second quantum revolution.
- Many of these research programs were funded by governments after Peter Shor’s integer factoring algorithm was created.
- While the first quantum revolution was driven by research coming mostly out of Europe, the last wave comes out of all developed countries across several continents (North America, Europe, Asia/Pacific).

Quantum physics 101

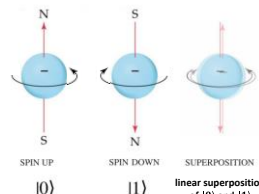
- Quantum physics is based on a set of postulates and a strong linear algebra mathematical formalism. Surprisingly, there are many variations of these postulates. There is not a single bible or reference for these, illustrating the diversity of pedagogies and opinions in quantum physics. But although deemed incomplete, the theory has been validated by an incredible number of experiments.
- Quantum physics describe the behavior of matter and light at nanoscopic levels. It deals not only with atoms, electrons and photons which are used in quantum information technologies but also with all elementary particles from the standard model (quarks, ...).



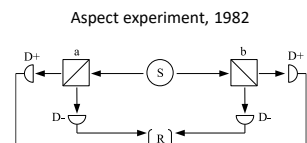
quantization



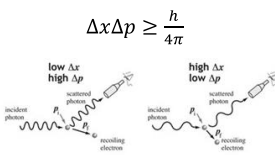
wave-particle duality



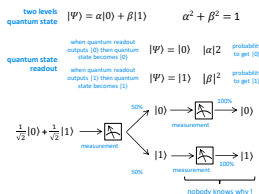
state superposition



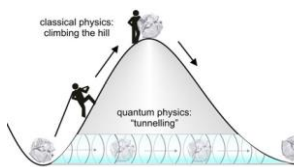
entanglement



indetermination



measurement



tunnel effect

No Cloning Theorem: Assume we have a unitary operator U and two quantum states $|\psi\rangle$ and $|\phi\rangle$ which U copies, i.e.,

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$$

$$U(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle$$

Then $\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2$.

Proof 1: $\langle\psi|\phi\rangle = \langle\psi|\phi\rangle \langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2$ if $\langle\psi|\phi\rangle \neq 0$, then $\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2$. In the second equality we used the fact that U being unitary preserves inner products.

Proof 2: Suppose there exists a unitary operator U that can indeed clone an unknown quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Then

$$U(|\psi\rangle \otimes |0\rangle) = (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

$$= \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$$

But since if we use U to clone the expansion of $|\phi\rangle$, we arrive at a different state:

$$U(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle = \alpha^2|00\rangle + \beta^2|11\rangle$$

Thus there are no clones. Thus we have a contradiction and therefore there cannot exist such a unitary operator U .

non cloning

Figure 3: eight key dimensions of quantum physics that we are dealing with. (cc) compilation Olivier Ezratty, 2021.

- Quantumness comes from the quantification of many properties of light and matter that can take only discrete values, from the wave-particle duality of massive (atoms, electrons) and non-massive (photons) particles, and from wave-particle duality and its consequences like superposition and entanglement. By the way, a cat can't be both alive and dead since it's not a nanoscopic quantum object. Forget the cat and instead, learn Schrodinger's equation!
- Indetermination principle states it's impossible to measure with an infinite precision quantum objects properties that are complementary like speed and position. You can use this principle to improve measurement precision in one dimension at the expense of the other. It is used in photons squeezing, itself applied in the LIGO giant gravitational waves interferometer.
- Quantum matter and fluids are showing up with composite elements associating light and matter, or with superfluidity and superconductivity where boson quantum objects can behave like a single quantum object. You find there a wealth of strange phenomenon such as skyrmions, magnons, topological insulators and quantum batteries.
- Quantum physics also explains weird effects like vacuum quantum fluctuation, although it doesn't violate the second principle of thermodynamics, nor can it lead to the creation of some free energy sources.
- Most of quantum physics phenomena have or will have some use cases in quantum information science and technologies.

Gate-based quantum computing

- Gate-based quantum computing is the main quantum computing paradigm. It relies on qubits and finite series of quantum gates acting on individual qubits or two and three qubits. The main other paradigms belong to analog quantum computing and include quantum simulators and quantum annealers.
- To understand the effect of qubits and quantum gates, you need to learn a bit of linear algebra. It deals with Hilbert vector spaces made of vectors in highly multidimensional spaces, matrices and complex numbers. The Dirac Bra-Ket notation helps manipulate vectors and matrices in that formalism.

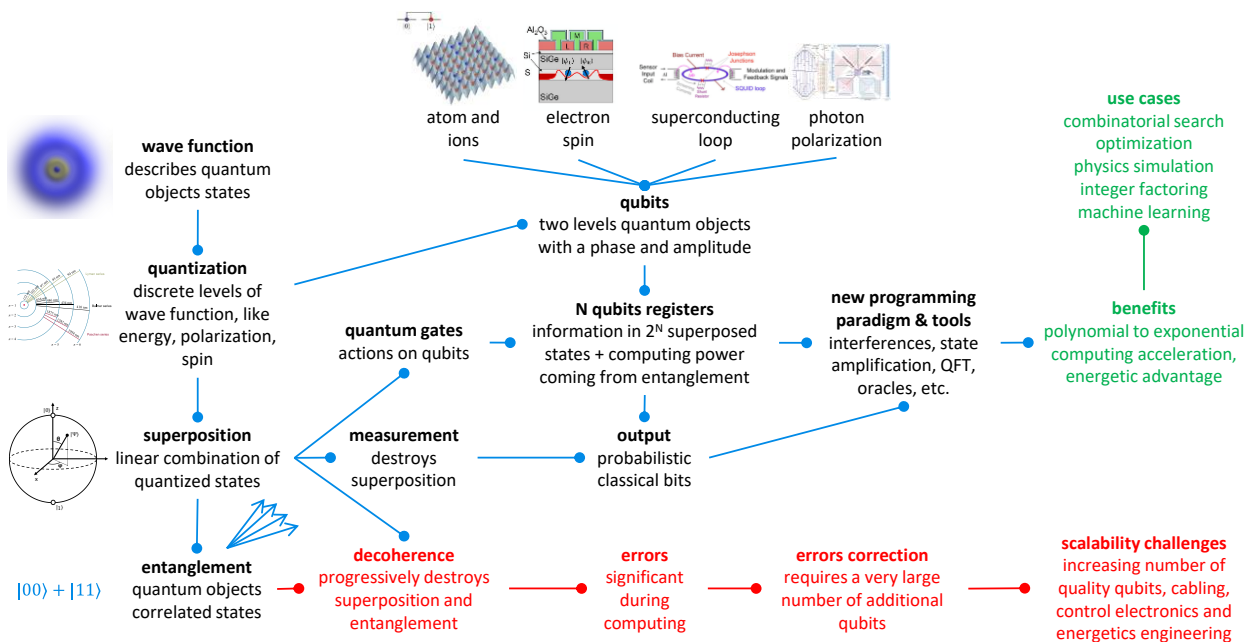


Figure 4: a single schematic to describe quantum physics and quantum computing. (cc) Olivier Ezratty, 2021.

- A qubit is usually represented in a Bloch sphere, reminding us of the wave nature of quantum objects during computation. This wave nature is exploited with qubits phase control and entanglement which provokes interferences between qubits. Qubits entanglement is created by conditional multi-qubit gates like the CNOT.
- A qubit register of N qubits can store a linear superposition of 2^N basis states corresponding to the qubit computational basis, each associated with a complex number. But surprisingly, this exponential growth in size is not enough to create an exponential speedup for quantum computing.
- While the computational space grows exponentially with the number of qubits, a qubit register measurement at the end of quantum algorithms yields only N classical bits. You have to deal with it when designing quantum algorithms.
- Computation must usually be done a great number of times and its results averaged due to the probabilistic nature of qubits measurement.
- Qubits measurement can be done in various ways, the main one being a classical projective measurement, if possible a non-demolition one (QND) that will maintain the qubit in its collapsed state after measurement. Other techniques are used that are useful for qubits quality characterization and for quantum error corrections.

Quantum computing engineering

- A quantum computer is based on physical qubits of different nature, the main ones being superconducting qubits, electron spin qubits, NV centers, cold atoms, trapped ions and photons. They all have pros and cons and no one is perfect at this stage. Future systems may combine several of these technologies.

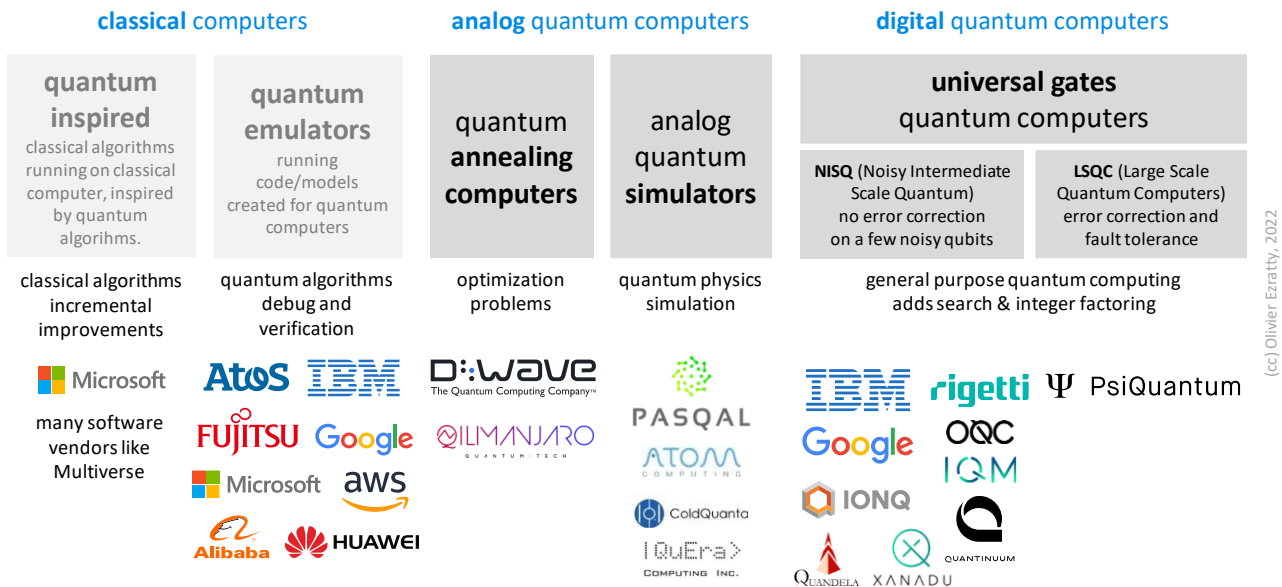


Figure 5: the different computing paradigms with quantum systems, hybrid systems and classical systems. (cc) Olivier Ezratty, 2022.

- Many key parameters are required to create a functional quantum computer. It must rely on two-states quantum objects (qubits). These must be initializable and manipulable with a set of universal gates enabling the implementation of any linear transformation of qubit states. Qubits must be measurable at the end of algorithms. Their coherence time must allow the execution of a sufficient number of quantum gates. Decoherence and errors must be as low as possible.
- Most quantum computers are composed of several parts: the qubit circuit (for solid-state qubits), vacuum enclosures (particularly with cold atoms and trapped ions) or waveguides (photons), usually housed in a cryogenic vacuum chamber (with the exceptions of photons and NV centers), some electronics sending laser rays or coaxial cables guided microwaves or direct currents onto qubits and a classical computer driving these electronic components.
- Since qubits are noisy, scientists have devised quantum error correcting schemes. These rely on creating logical “corrected” qubits composed of a lot of physical qubits, up to 10,000. This creates huge scalability challenges, many of them with classical enabling technologies like cabling, electronics and cryogeny. The science of quantum error correction, quantum error mitigation (a new section in this edition) and fault-tolerant quantum computing is a realm in itself.
- Many quantum algorithms also require some form of quantum memory, either for data preparation and loading (such as with quantum machine learning) or to access efficiently classical data (such as with oracle based algorithms like a Grover search). These quantum memories don’t exist yet.
- The energetic cost of quantum computing is both a potential benefit but also an immense challenge, particularly when a large number of physical qubits are required to create large scale fault-tolerant computers. All components must be carefully designed to take into account the cryogenic cooling power as well as the available space to house cabling and cryo-electronics. This explains the creation of the **Quantum Energy Initiative** by Alexia Auffèves, Olivier Ezratty and Robert Whitney, which creates a community of researchers and industry vendors and organizations working collectively on this topic.
- The economics of quantum computers are still uncertain due to their immaturity and the current low manufacturing volume. Uncertainty is also strong with regards to the feasibility of scalable quantum computers. The scalability challenges ahead are enormous. One of them is to benefit from actual algorithm speedups when including all end-to-end computing operations.

Quantum computing hardware

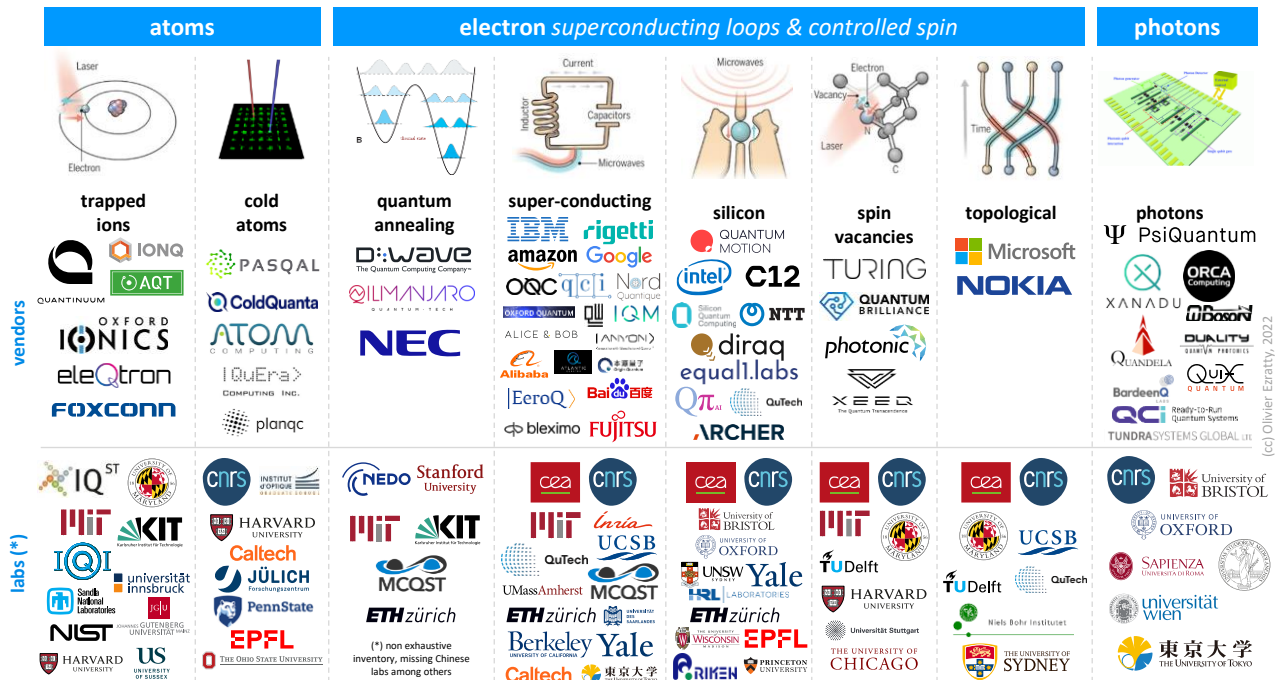


Figure 6: a map of key research lab and industry vendors in quantum computing hardware per qubit type. (cc) Olivier Ezratty, 2022. Qubits drawing source: [Scientists are close to building a quantum computer that can beat a conventional one](#) by Gabriel Popkin in Science Mag, December 2016. I consolidated the logos lists since 2018. It's incomplete for the research labs at the bottom but rather exhaustive for the vendors at the top.

- Superconducting qubits are the most common nowadays, implemented by IBM, Google and Rigetti among others. But they are noisy and do not scale well. One solution may be cat-qubits which combine trapped microwave photons in cavities and superconducting qubits for their manipulation and readout (Alice&Bob and Amazon).
- Quantum dots spin qubits could scale well due to their small size, the reuse of classical CMOS semiconductors manufacturing known-how, their higher working temperature enabling the usage of control cryo-electronics. They have however been demonstrated at a relatively low scale at this stage.
- NV centers qubits have the benefit to be stable and to work potentially at ambient temperature but there are not many vendors involved there, besides Quantum Brilliance (Australia and Germany).
- Topological qubits could bring the benefit of being resilient to some quantum errors and to scale better than other solid-state qubits. It doesn't really exist yet, particularly the Majorana fermions species looked after by Microsoft.
- Trapped ions qubits have the best fidelities so far, but they are hard to scale beyond about 40 qubits, at least with their main vendor, IonQ, Quantinuum and AQT.
- Cold atoms qubits are mostly used in quantum simulation where it could scale up to a thousand qubit and it could potentially also be used in gate-based quantum computing although it's not really demonstrated at a large scale. Pasqal (France), Cold Quanta (USA), QuEra (USA) and Atoms Computing (USA) are the industry vendors in this field.
- Photon qubits are flying qubits, moving from a source to detectors and traversing optical devices implementing quantum gates. There are many investigated techniques, with the distinction between single/discrete variable photons and continuous variable photons. Scalability is also an issue, particularly with photon sources and the probabilistic nature of photons generation. Their limited quantum gates computing depth requires the implementation of specific computing techniques like MBQC and FBQC, this last one being used by PsiQuantum, the best funded quantum computing startup with IonQ as of 2022. Quandela (France), Xanadu (Canada) and Orca (UK) are other key players in that space. One key capability to implement MBQC is the generation of high volume cluster states of entangled photons.

Quantum enabling technologies

- Cryogeny is a key quantum computing enabling technology particularly for solid-state qubits which work at temperatures between 15 mK and 1K. These systems rely on a mix of helium 3 and 4 in so-called dry-dilution refrigeration systems. Other simpler cooling technologies target the 3K to 10K temperature ranges that are used with photon sources and detectors, as used with photon qubits systems.

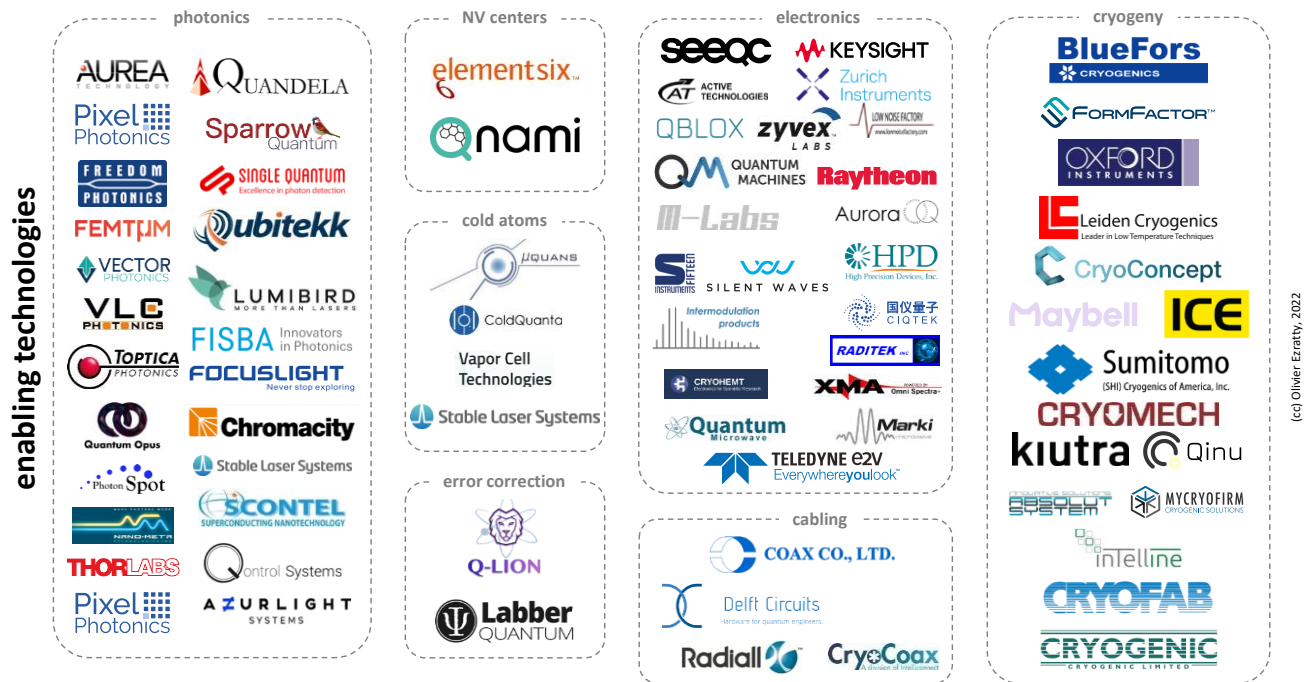


Figure 7: a market map of key enabling technology vendors. (cc) Olivier Ezratty, 2022.

- Cabling and filters play another key role, particularly with solid-state qubits. Superconducting cables are expensive with 3K€ per unit and come from a single vendor source from Japan. Signals multiplexing is on the way!
- Microwave generation and readout systems used with superconducting and quantum dots electron spin qubits are other key enabling technologies. The challenge is to miniaturize it and lower their power consumption and, if that makes sense, to put them as close as possible to the qubits, operate them at cryogenic temperatures and simplify system cabling. It's a key to physical qubits scalability. A lot of different technologies compete here, mostly around cryo-CMOS and superconducting electronics. Other components deserve attention like circulators and parametric amplifiers that we cover in detail in this new edition.
- Many lasers and photonics equipment are used with cold atoms, trapped ions and photon qubits and also quantum telecommunications, cryptography and sensing. It includes single indistinguishable photon sources as well as single photon detectors. The lasers field is also very diverse with product covering different ranges of wavelengths, power, continuous vs pulsed lasers, etc.
- Manufacturing electronic components for quantum technologies is a strategic topic covered extensively in this book for the first time with a description of generic fab techniques and some that are specific to quantum technologies like with the fabrication of superconducting qubits and quantum dots.
- Quantum technologies use a lot of various raw materials, some being rare but used in very small quantities. While some materials may have some incurred environmental costs, most of them do not seem to be scarce and they have multiple sources around the planet.

Quantum algorithms

- 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 theoretical 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.

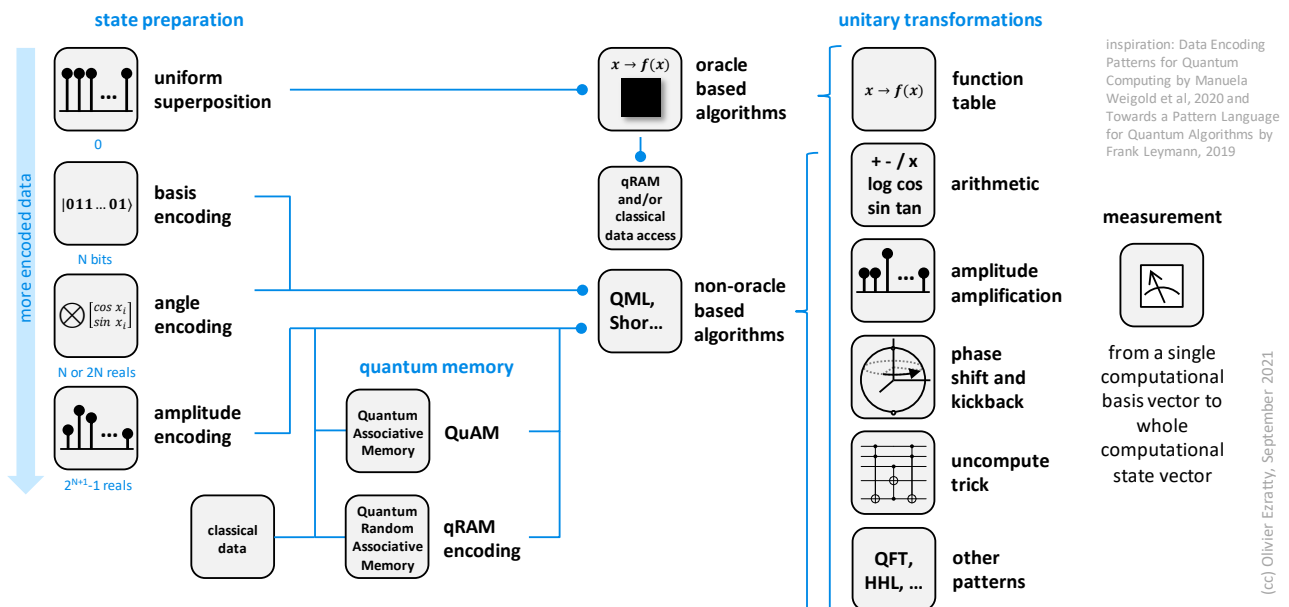



Figure 8: how is data fed into a quantum algorithm depending on whether it uses or not an oracle. (cc) Olivier Ezratty, 2021.

- 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 use some form of quantum mathematical models like interferences and signals decomposition (Fourier series/transforms).

Quantum software development tools

- 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.



	Q Experience	Forest			Quantum Playground	Visual Studio		
visual programming and integrated development environments								
thematic quantum libraries (chemistry, finance, machine learning, ...)	Qiskit Aqua	OpenFermion	Quadrant, Qsage, ToQ	PENNY LANE	OpenFermion	Quantum Chemistry PNNL	PENNY LANE	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 9: 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.

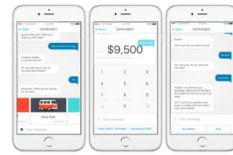
- Quantum computing is based on running code multiple (thousands...) times and averaging the results. A single individual run yields a probabilistic outcome while many run averages will converge into deterministic ones.
- Most quantum computers are used in the cloud, through offerings coming from the 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 Quandel 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 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.



energy and materials
batteries design
renewables optimization
materials design
fertilizers production improvements



finance and insurance
risk assessment
portfolio optimization
fraud detection



healthcare
molecular simulation
drug discovery



defense and intelligence
machine learning
optimizations
cryptology



transports and logistics
travel optimization
fleet management
electric vehicles recharging

(cc) Olivier Ezratty, 2021-2022

Figure 10: typical quantum computing use cases where a quantum speedup brings clear benefits. These are still “promises” since the capable hardware to implement many of these solutions with a quantum speedup remains to be created and it may take a while up to several decades! (cc) Olivier Ezratty, 2020.

- 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

- 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.

Appealing Feature of SFQ Circuits

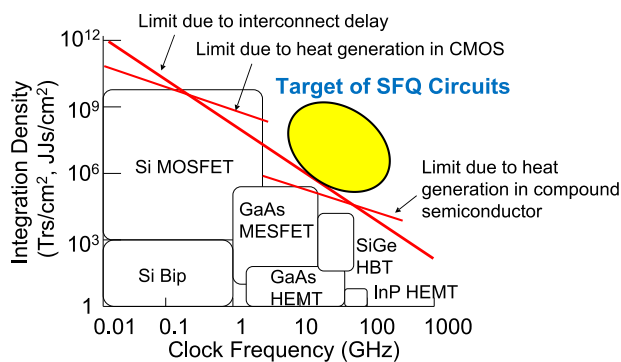


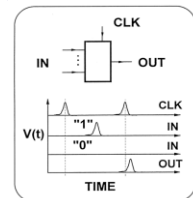
Figure 11: schematic positioning SFQs in terms of clock speed and integration compared to traditional electronic components.
Source: [Impact of Recent Advancement in Cryogenic Circuit Technology](#) by Akira Fujimaki and Masamitsu Tanaka, 2017 (37 slides).

RSFQ - Rapid Single Flux Quantum

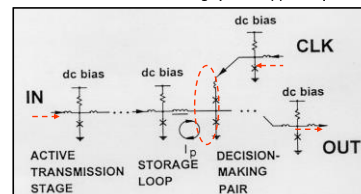
Timeline:
invented in 85-86, generally accepted in 90, adopted in the US in 91, became the main digital superconducting electronics by mid-end of 90s, first product by mid-00s

$$\int V dt = \Phi_0 = h/2e = 2.07 \text{ mV} \cdot \text{ps}$$

$$E_{\text{SFQ}} = 10^{-19} \text{ J}$$



Both Data and Clock are SFQ voltage pulses $V(t)$ with quantized areas



- 750 GHz digital frequency divider demonstrated
- internal memory
- gate-level pipelining
- high-throughput
- low switching power
- dc bias only
- local timing
- amendable for synchronous and asynchronous schemes

- 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 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.

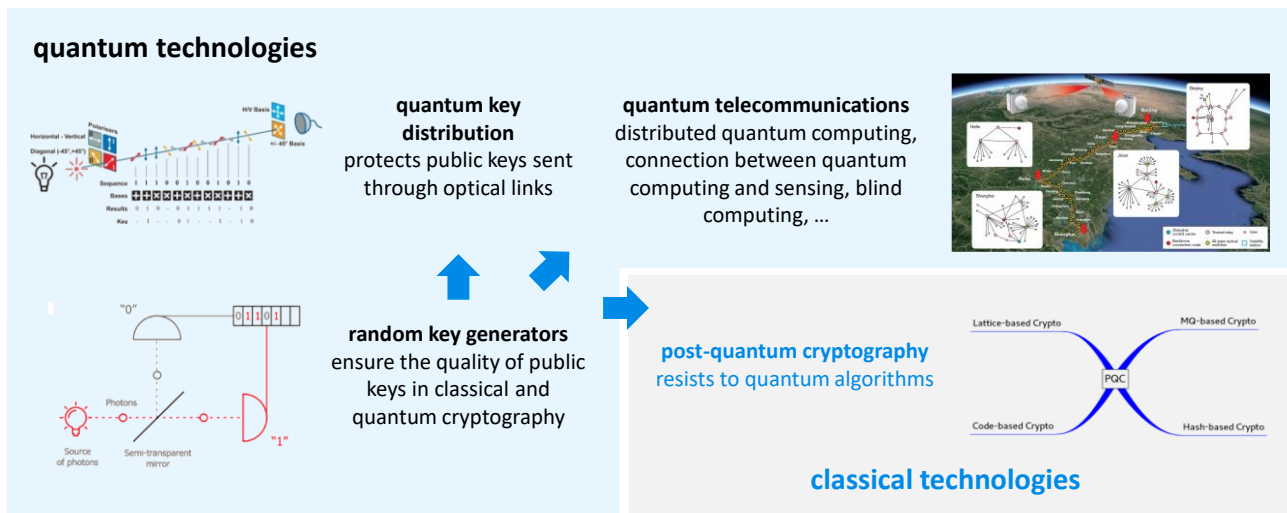


Figure 12: the four classes of technologies covered in this part. (cc) Olivier Ezratty, 2020.

- 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. Distributed quantum sensing can enable better accuracy sensing.
- 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.
- Quantum Physical Unclonable Functions are cryptographic solutions used to authenticate physical objects in an unclonable quantum way. It is however still an immature technology.
- There are already many startups in the QKD and PQC scene. Deployments have already started worldwide, particularly in China.

Quantum sensing

- 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.

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	X											X				
		NV/SiC center ensembles	X			X			X					X	X		X	
	single spins	P donor in Si	X											X				
		quantum dot	X	X										X	X			
		single NV center	X			X			X				X	X				
superconducting circuits		SQUIDs	X	X										X				
		flux qubits	X											X				
		charge qubits		X												X		
single electron transistor		charge eigenstates	X												X			
optomechanics		phonons	X				X	X						X		X		
interferometer		photons, atoms	X	X	X					X			X					

© Olivier Erratty, 2022, based on Quantum sensing by C. L. Degen, F. Reinhard and P. Cappellaro, June 2017

Figure 13: quantum sensing taxonomy. Source: table reconstructed from [Quantum sensing](#) by C. L. Degen, F. Reinhard and P. Cappellaro, June 2017 (45 pages).

- 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.

Quantum technologies around the world

- 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.

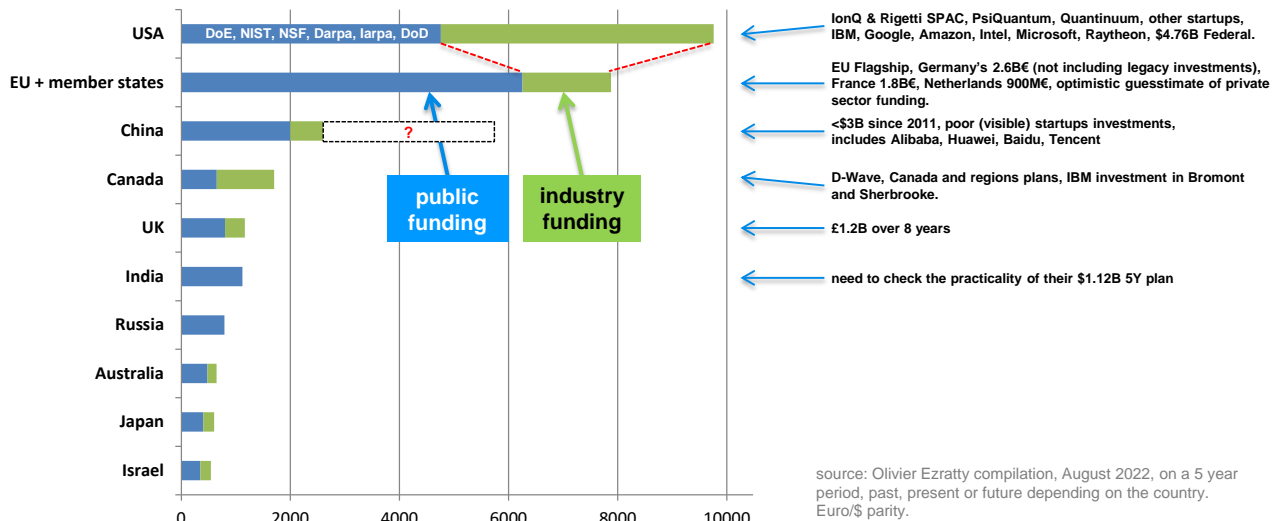


Figure 14: a consolidation of quantum technologies public and private investments with some raw estimated for large IT vendors. It creates a very different picture than what is commonly thought about the place of China and Europe. (cc) Olivier Ezratty, 2022.

- 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.

Quantum technologies and society

- 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 (ψ 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.



Figure 15: some women role models around the world, from research to the industry. (cc) Olivier Ezratty, 2021-2022.

- 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.

Quantum fake sciences

- 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.



Figure 16: quantum medallions and 5G quantum keys are fancy gadgets for the gullible. That's a huge market!

- Quantum physics is sometimes used in management and marketing. This book offers you a nice in-depth parody of these methodologies.

<p>quantization goals setting, sales goals, and managers sand-bagging</p>	<p>state superposition work/life balance, sales lead status in sales pipe</p>	<p>indetermination employees opinion polls, customer satisfaction polls with biased questions</p>	<p>state reduction measuring quarter closing revenue for bonus attribution</p>
<p>wave-particle duality destructive internal competition, big mouth behavior</p>	<p>entanglement startups and corporations relationships, high decoherence risk</p>	<p>non cloning graveyards are full of irreplaceable talents</p>	<p>tunnel effect give false hopes, irrealistic sales goals</p>

(cc) Olivier Ezratty, 2021

Figure 17: my useless framework for quantum management. (cc) Olivier Ezratty, 2022.

- At last, we showcase a few companies using quantum in their branding when they have nothing quantum at all to offer.

back-cover flip page.

le lab quantique



$|0\rangle$

$|1\rangle$