Understanding Quantum Technologies

Ninth edition - 2026 Key Takeaways

Olivier Ezratty

le lab quantique

le lab quantique

Le Lab Quantique is a supporter and promoter of this book, but not its publisher or editor.

Understanding Quantum Technologies

Ninth edition - 2026 Key Takeaways - Version 9.0

Olivier Ezratty

Generated on September 28, 2026

About the author

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

Olivier Ezratty is an author, academic, teacher and advisor on quantum technologies. He started this endeavour in 2018.

He is the author of the reference book "Understanding Quantum Technologies" (September 2021, 2022, 2023, 2024, 2025 and 2026) following three previous editions in French in 2018, 2019 and 2020. The 2025 edition is also available in paperback version on Amazon. This 2026 edition's Amazon print version will be available before the end of 2026.

Since 2021, he has been teaching quantum technologies at EPITA, an IT engineering school in France, at Ecole Normale Supérieure Paris-Saclay since 2024 and CentraleSupelec since 2005. He's affiliated with the EPITA Research lab for his various research writings.

He is a cofounder of the Quantum Energy Initiative in 2022 with Alexia Auffèves (CNRS MajuLab Singapore), Robert Whitney (CNRS LPMMC) and Janine Splettstoesser (Chalmers University, Sweden), and member of its scientific board.

He acts as an independent expert for Bpifrance and at the Agence Nationale de Recherche (ANR) to evaluate quantum R&D projects, as a member of the European Quantum Computing Advisory Board (Q-CAB) since April 2026, and of the Inria expert group for the selection of risky research projects (Programme PIQ) since June 2024.

Since 2018, he has spoken in a large number of quantum technology events such as the Q2B Paris and Santa Clara organized by QC Ware, France Quantum, Lindau Nobel Laureate meeting, DPG, Q-Expo and other events, on top of presentations at Société Générale, BNPParibas, Crédit Agricole, Michelin, Adéo, L'Oréal, FIECC, IHEDN, Business France, CentraleSupelec, Avolta Partners, IHEDN, etc.

He coproduces two series of podcasts on quantum technologies along with Fanny Bouton (in French): a monthly "Quantum " on tech news (since September 2019) and Decode Quantum (2020-2026), with entrepreneurs and researchers, with a total of about 170 episodes as of September 2026.

He also lectures or lectured in various universities such as CentraleSupelec, ENSTA, Telecom Paristech, Les Gobelins, HEC, Neoma Rouen and SciencePo, on artificial intelligence, entrepreneurship and product management (until 2020) and on quantum technologies (since 2018), 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).

Beforehand, Olivier Ezratty was specialized in many other topics since 2005, like digital television, internet of things and artificial intelligence. As such, he carried out various strategic advisory missions, conferences, or training assignments in different verticals and domains such as media and telecoms, finance and insurance, industry and services and the public sector.

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 initiated 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 an extensive experience in many areas of the marketing mix: products, channels, markets and communication. He launched in France 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.

Cover illustration credits: 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 terms from the book glossary. This book contains about 1,325 illustrations. I have managed to give credit to their creators as much as possible. Most sources are credited in the captions. Only scientists' portraits are not credited since it's quite hard to track their original source. I have added my own credit in most of the illustrations I have created or modified. 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

Table of contents iii

1 About these takeaways 1

2 Why... 2

3 Quantum physics history and scientists 4

4 Quantum physics 101 6

5 Gate-based quantum computing 8

6 Quantum computing engineering 10

7 Quantum computing hardware 12

8 Enabling technologies 14

9 Unconventional computing 16

10 Algorithms 18

11 Software tools 20

12 Applications 22

13 Communications and cybersecurity 24

14 Quantum sensing 26

15 Quantum technologies throughout the world 28

16 Quantum technologies and society 30

17 Quantum fake sciences 31

1 About these takeaways

"Understanding Quantum Technologies" was released at the end of September 2026 in its Ninth edition. This version is about 1,822 pages long and is available as a free-to-download PDF in various formats (A4, Letter, single or five parts) on this link.

It will also be available as a paperback edition in five volumes on Amazon (prologue, computing hardware, computing software, communications and sensing, ecosystem).

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 in the quantum ecosystem from researchers to industry vendors and policy makers, and finally scientific students who would like to investigate quantum technologies as an exploratory field.

> "*Knowledge is a process of piling up facts; wisdom lies in their simplification*".
>
> Martin H. Fischer, German-born American Physician - Teacher - Author (1879-1962).

It is a very large book, but it can also be considered a collection of books. One on quantum physics history and fundamentals, another on quantum computing hardware, one on quantum computing programming, software and applications, yet another one on quantum communication and cryptography, and on quantum sensing, on quantum geopolitics, an inventory of quantum industry vendors with over 970 being described in the book, etc. But they are all tied together in a consistent manner.

For your convenience, I have extracted the key takeaways that are at the end of each part and included a couple of key illustrations in this short version to create this 42-page special edition of the book.

Olivier Ezratty, September 2026

2 Why...

- This book is unique in its shape, structure and length. It covers quantum technologies with a 360° approach. It is more scientific than most broad-reach publications, outside research review papers. It is a good appetizer for those who want to investigate the matter whatever the angle. It covers the broad field of quantum science and technologies with fundamental science and engineering viewpoints, but also through an economic and geopolitical lens. It contains an extensive bibliography with over 11,700 references, mostly scientific papers. It tries to answer many commonplace questions that are not well addressed in broad audience scientific and business publications.
- Many enabling devices used in existing digital technologies, including transistors and lasers, rely explicitly on quantum physics and are commonly associated with the "first quantum revolution". They exploit light-matter interactions in large ensembles of quantum objects such as electrons, atoms and photons and in semiconductors. The "second quantum revolution" is an expression coined in 2003 for a newer generation of quantum technologies that relies on a variable mix of superposition, entanglement and control of individual quantum objects. It usually includes quantum computing, quantum telecommunications, quantum cryptography and quantum sensing. Quantum matter applications are a newer addition to this list that is also described in this book.
- Quantum technologies are at the crossroads of many scientific domains encompassing physics, mathematics, computing, social sciences and economics. This creates new educational and pedagogical challenges that must be addressed in innovative ways and customized for various audiences. This book targets broad audiences with a technical background, including computer science engineers, but also quantum physicists and quantum information scientists who want to have a broad view of the field and its burgeoning ecosystem.
- Quantum computing may accelerate selected problems for which suitable quantum algorithms and favorable end-to-end resource scaling are known. It does not make all classically intractable problems tractable. Enormous challenges must still be overcome to scale quantum computers beyond today's relatively modest systems. In the interim, noisy intermediate-scale quantum computers (NISQ) may provide useful improvements for some specific tasks, while analog quantum computers are other candidates for demonstrating quantum advantage on selected problems.
- Moore's law has not ended yet, particularly with regard to the number of transistors per chip. Classical computing continues to advance and remains much better suited than existing quantum computers to workloads involving large volumes of classical data. Data loading speed and big-data applications will remain key strengths of classical computing for the foreseeable future.
- Other new technologies may compete with quantum computing and belong to the broad "unconventional computing" category. Some may provide advantages for specific problem classes, including combinatorial optimization, but no generic exponential computing capacity should be inferred without a problem-specific complexity analysis and comparison with the best classical methods. Other approaches may instead provide benefits such as lower energy consumption. Technologies based on superconducting electronics and adiabatic or reversible computing could also help enable scalable quantum computing, particularly with superconducting qubits.
- At last, this part contains an inventory of 12 key misconceptions on quantum computing.

Common quantum technologies misconceptions

Misconception	Explanation
Quantum computing is fast or instantaneous.	While quantum algorithms may be faster than their classical equivalents in a quantum advantage regime, they can be quite slow and run for hours, days if not months and more.
Quantum computing speedups are explained by the Hilbert space dimension of a qubit register (2^N).	The number of computational-basis states indeed scales exponentially with the number of qubits but it doesn't explain the potential quantum algorithms speedups. It depends on many factors like the type of qubit gates used, how the data is loaded in the quantum circuit, its degree of entanglement and, above all, the structure of the problem.
Quantum computers will soon break RSA keys and all Internet cybersecurity.	We'd need at least 100,000 physical qubits to break an RSA-2048 key in less than a year according to the latest 2026 estimates. We are many years away if not largely more than a decade away from this mark at best. So far, progress has been better with reducing quantum circuit size than improving hardware scaling.
Quantum computing will enable larger big data applications.	Not really. Quantum computers are slower by several orders of magnitude to feed with data compared to classical computers. This could slightly improve with the use of quantum sensor data or with advanced compression techniques.
Quantum computing will solve the LLM energy crisis.	Probably not. Loading both training data and a trained model in a quantum circuit would be prohibitively slow even for modest-size LLMs, and just for getting one response token!
Quantum computing will progress following some Moore's exponential law.	While qubit numbers are making progress and did fit some exponential trend for some time, and then stalled, it is not the case with qubit fidelities and many other figures of merit, particularly at scale. Researchers are still struggling to scale the number of qubits and keep good fidelities.
Quantum computing is business-ready now.	Many analysts and vendors would like you to believe it with NISQ, but it is not yet the case for industry grade applications. The few applications nearing quantum advantage are most of the time physics simulations far from industry use cases.
Quantum computing will (soon) help fix climate change.	It may enable some research in innovative chemical engineering, but this will require large-scale fault-tolerant quantum computers which are decades away. We'd better fix climate change with classical methods in the meantime.
China is investing between $15B and $25B in quantum technologies and is beating all other geographies.	This is probably not true or at least not verified nor decomposed in detail. Estimates range from $5B to $10B over 10 years. The $15B to $25B investment mark comes from a questionable 2017 statement on the Hefei lab buildup. This number has not changed since 2017! But China is faring well in many domains like in photonic quantum computing, quantum communications and quantum sensing.
Government funding and private investment means it will work.	Money can buy time, but the laws of physics make this hard. Creating viable quantum computers requires more iterations in component design and manufacturing, along a complex value chain.
Quantum communication will replace the Internet with faster transmission speed.	Quantum communication's main purpose is to enable the creation of symmetric encryption keys between trusted parties, not to speed up data communications. It will also enable the connection between multiple quantum computers by entanglement-based quantum communication links, but not faster than light. All these techniques need some classical links on top of quantum links.
Quantum computers will save energy.	We are not so sure about it, particularly with large scale fault-tolerant systems. This is an area of investigation and optimization.

Table 1: 12 misconceptions on quantum computing and communications

3 Quantum physics history and scientists

- A first wave of 19^{th} century scientists laid the groundwork that helped create quantum physics afterwards (Young, Maxwell, Boltzmann, mathematicians). The photoelectric effect, black body spectrum, atomic emission or absorption spectra as well as the Zeeman effect could not be explained with the theoretical frameworks of classical physics and thermodynamics of the 19^{th} century.
- Starting with Max Planck in 1900, a second wave of scientists (Einstein, De Broglie, Schrodinger, Heisenberg, Dirac, Born, Von Neumann, ...) created the field of quantum mechanics, or quantum physics, to describe light-matter interactions, energy quantization and wave-particle duality. It explained many previously unresolved 19^{th} century experiments while raising new questions about the nature of reality at the nanoscale. 1925 was a pivotal year with the work of Werner Heisenberg, Erwin Schrödinger and Max Born, who laid much of the groundwork of quantum physics as it is still used today.
- Many of these scientists made major theoretical contributions, while other researchers made landmark experimental discoveries such as superconductivity, electron interference and the Stern-Gerlach experiment. Some scientists contributed to both theory and experiment. Quantum physics also relies on a significant body of mathematics, including linear algebra and group theory. After World War II, enabling device technologies such as transistors and lasers increasingly relied explicitly 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 (atoms, electrons, photons) 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.
- This part showcases many contemporary quantum scientists in quantum physics and quantum information science from around the world with their key contributions. This hall of fame covers many generations, including young brilliant scientists in their 30s.
- While the first quantum revolution was driven by research coming mostly out of Europe, the last wave comes out of all countries across several continents (North and South America, Europe, Asia/Pacific).
- This book also describes how research works in general and particularly in quantum physics and information science. It explains how scientific papers are written and communicated, how researchers are evaluated, and how quantum-technology readiness level can be assessed. It provides some insights on how to analyze and rate scientific papers. It also describe how LLM-based generative AI is transforming, if not disrupting, this whole field like most scientific fields.

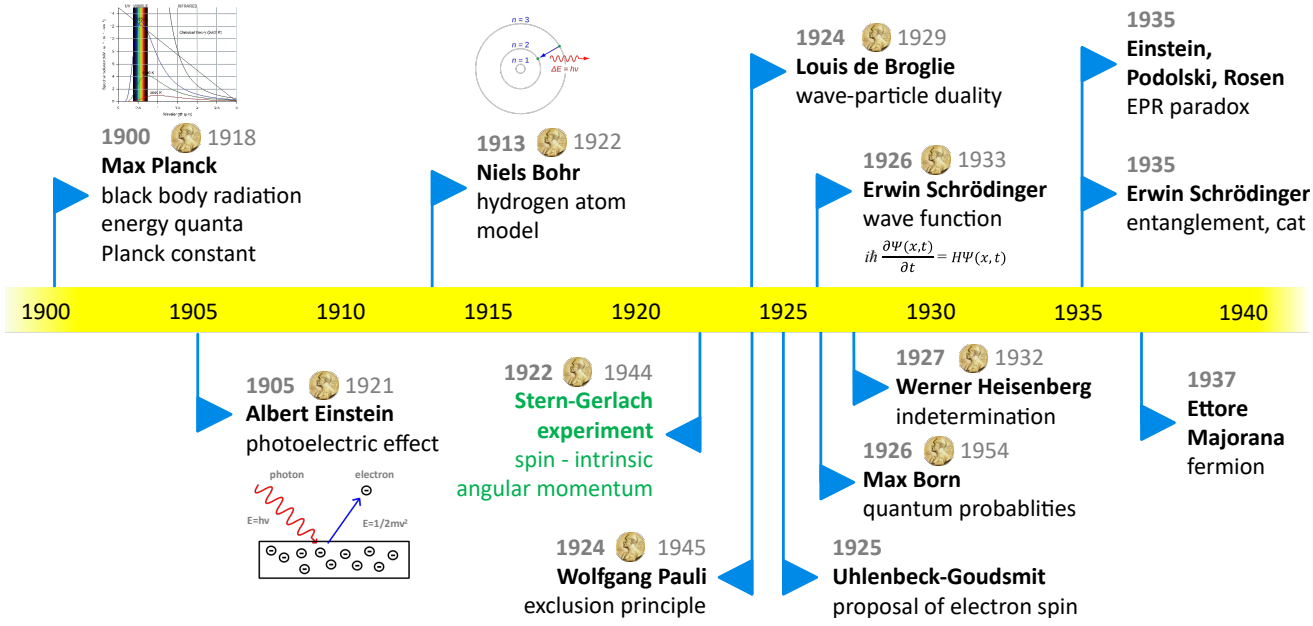


Figure 1: Quantum physics foundational years timeline. In green, experimentalist works, in black, theoretician works. The gold coins represent a Nobel prize. © Olivier Ezratty, 2021-2025.

4 Quantum physics 101

- Quantum physics is based on a set of postulates and a 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 interpretations in quantum physics. One big underlying question is "what is reality". But although deemed incomplete, the theory has been validated by an incredible number of experiments and to extreme precision.

- Quantum physics describes the behavior of matter and light at the nanoscale level, but it can in some conditions extend to larger objects like molecules or even artificial atoms like superconducting currents, Bose Einstein condensates and quantum dots. 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, ...). However, we don't use or need to look at this level of granularity in most quantum technologies.

- Quantumness comes from the quantization of many properties of light and matter that can take only discrete values, from the wave-particle duality of massive particles such as atoms and electrons and massless particles such as photons, and from phenomena such as superposition and entanglement. Atoms, electrons, nucleons and photons can be described by quantum numbers associated with particular observables, while quantum systems can also have continuous observables such as position and momentum. Schrödinger's cat is a thought experiment about measurement, entanglement and macroscopic definiteness. Macroscopic quantum superpositions are not forbidden merely by an object's size, but environmental decoherence suppresses their observable coherence extremely rapidly in ordinary conditions.

- The Heisenberg uncertainty principle states that the statistical uncertainties of incompatible observables obey uncertainty relations, for example $\Delta x\, \Delta p \geq \hbar/2$ for position and momentum. Quantum squeezing can reduce the uncertainty of one observable at the cost of increased uncertainty in an incompatible observable. Optical squeezing is used in gravitational-wave interferometers such as LIGO and in other areas of quantum photonics and sensing. The uncertainty principle is not restricted to continuous observables: incompatible discrete observables also obey uncertainty relations, whereas commuting observables can in principle be measured jointly. This part also looks at the role of measurement and symmetries in quantum physics.

- 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 phenomena such as skyrmions, magnons, topological insulators and quantum batteries. They could lead to a new chapter in the second quantum revolution.

- 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 quantum physics phenomena described in this section have or will have some use cases in quantum information science and technologies. Sometimes, the same quantum objects and properties like cold atoms can be used across quantum computing, quantum sensing and quantum communications.

- Quantum foundations is the branch philosophy of science 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 among them.

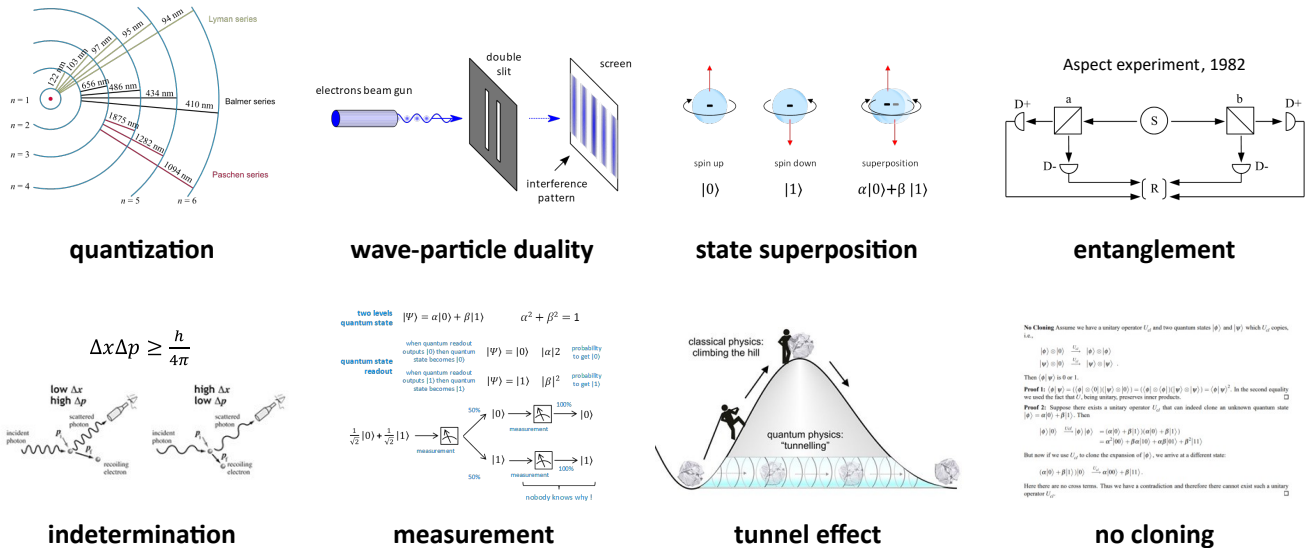


Figure 2: Eight key basic principles (quantization, wave-particle duality, state superposition, entanglement and indetermination), postulate (measurement), effects (tunnel effect) and theorem (no-cloning) of quantum physics. © compilation Olivier Ezratty, 2021-2025.

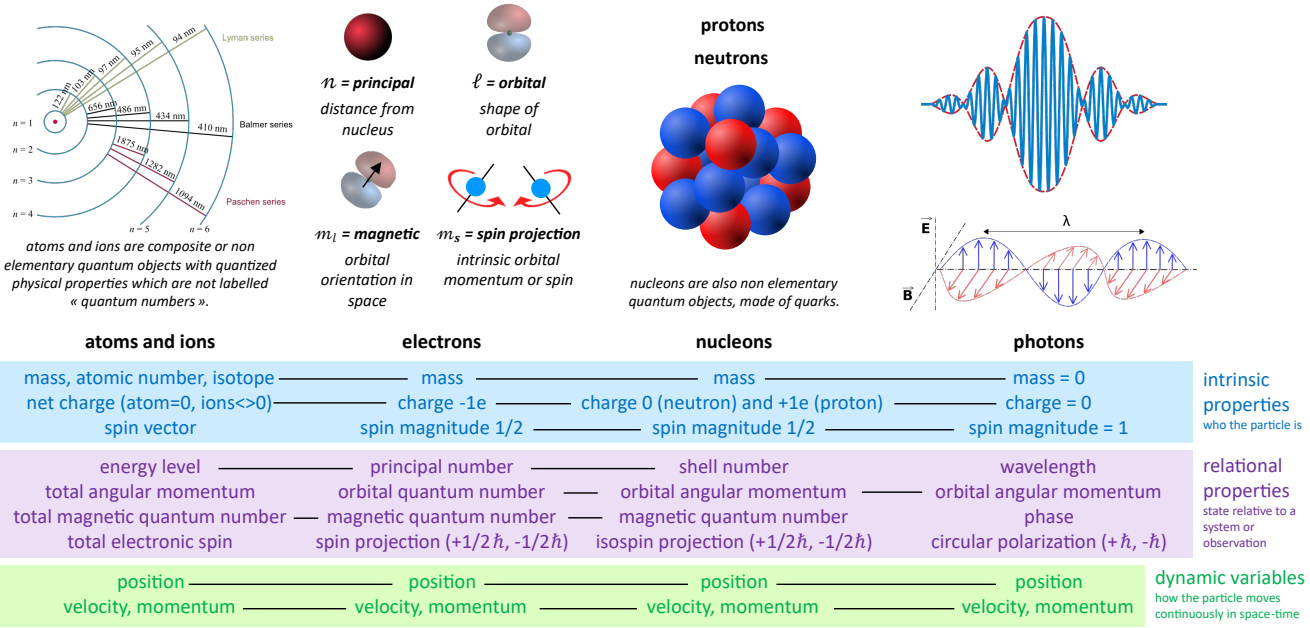


Figure 3: The three kinds of properties for atoms, electrons, nucleons and photons: their intrinsic properties which are related to the particle type and have a single possible value (mass, charge, spin magnitude), the relational quantized properties which are relative to a system (the electron in an atom) or observation (spin projection on an axis, the photon relative to an observer), and the dynamic variables which are continuous and relative to a referential. The table shows the correspondence between atoms, electrons, nucleons and photons. Only elementary particles like electrons and photons have "quantum numbers", atoms and nucleons being composite quantum objects made of electrons and quarks only have "quantum properties". The properties in bold are those which are quantized. The photon wavelength, OAM and phase are continuous variables and their value is relative to the observer. The polarization is a bit subtle. The helicity or circular polarization is observer independent while a linear polarization is dependent on the observer, depending on the chosen polarizer angle (more on photon properties in 3.2.4). Quantized properties are used to create qubits or qudits in quantum computing with distinct states and at the particle scale (atoms, electrons, photons). © Olivier Ezratty, 2022-2026, with some Wikipedia image sources.

5 Gate-based quantum computing

- Gate-based quantum computing is the main quantum computing paradigm. It relies on qubits and finite sequences of quantum gates acting on individual qubits or on two or more qubits, called "circuits". Other paradigms include analog quantum simulators (Pasqal, QuEra) and quantum annealers (D-Wave). The boundary of a quantum algorithm depends on the abstraction level. An abstract algorithm specifies the mathematical procedure that generates a quantum circuit, the logical circuit specifies encoded operations and measurements, and a compiled implementation adds hardware-specific gates, scheduling and control. Classical optimization, adaptive feedforward, error mitigation, quantum error-correction gadgets and decoding may be integral to an end-to-end implementation even when they are treated as separate layers in a software stack.

- The mathematical effects of quantum gates on qubits are relatively simple linear algebra operations. A set of qubits lives in a large-dimensional Hilbert space made of vectors, using complex numbers, vectors, and matrices. A qubit register supports a vector with 2^N complex numbers. A quantum gate applied a so-called "unitary" operation on this vector. Mathematically, it's a matrix multiplied by the register vector, which changes the vector. The Dirac Bra-Ket notation helps manipulate vectors and matrices in that formalism. It is often used to describe quantum states, for the decomposition of quantum algorithms and for quantum measurements.

- A qubit is encoded in a two-level quantum degree of freedom with basis states represented by $|0\rangle$ and $|1\rangle$. A pure qubit state can be a superposition of these two states, $\alpha|0\rangle + \beta|1\rangle$, with complex amplitudes satisfying the normalization constraint $|\alpha|^2 + |\beta|^2 = 1$. It is well represented with a vector on a Bloch sphere surface. Quantum circuits exploit phase control, interference and entanglement, which can be generated by two-qubit gates such as CNOT and CZ. Entanglement is a nonseparable property of the joint quantum state. It is usually created, transformed and removed during the circuit execution using conditional multi-qubit gates.

- A qubit register of N qubits can handle 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 a potential polynomial or exponential speedup with quantum computing. You need a lot of entanglement and some non-obvious quantum gates like arbitrary angle rotation gates (NISQ) or T gates (FTQC).

- While the computational space grows exponentially with the number of qubits, you don't really store information in the qubit register per se since retrieving it would require an exponential number of circuit execution and qubit readouts. You feed it with some problem and the circuit output is a relatively simple value of interest made of N classical bits. You must deal with it when designing quantum circuits. A quantum circuit won't generate a lot of data like an image, a video or a stream of text. There are still problems where some values of interest can be extracted that are just real numbers, like in quantum chemistry where you are looking for an energy value.

- A quantum circuit must usually be executed a large number of times, and its results averaged due to the probabilistic nature of qubit measurement. The number of "shots" depends on the algorithm structure and its distribution output, programming paradigm and type of error correction or error mitigation. Running the circuit multiple times and processing the results is called "sampling" a circuit.

- Qubit 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 and not destroy it. Other techniques are used that are useful for qubit quality characterization and for quantum error correction like a quantum state or quantum gate tomography.

		bits: 0 or 1		qubits: coherent superposition of 0 and 1
states	mathematical bit	2 possible exclusive states, 0 or 1	mathematical qubit	linear combination of |0⟩ and |1⟩
initialization		0 or 1		|0⟩ basis state
dimensionality		1 binary digit => two possible values		2 real numbers => one point on Bloch sphere
modifications		logic decision tables, irreversible		reversible unitary transformations
readout		0 ou 1, deterministic		0 or 1, probabilistic
errors		no error, perfect mathematical object		no error, perfect mathematical object
physical implementation	physical bit	current/no current in a logic electronic circuit and two states memory device bit	physical qubit	quantum object with two exclusive states for one property
computing vs memory		separate devices and parts of processors		all done in qubits and with quantum gates
computing operations		transistors based logic		amplitude and phase change + entanglement
errors sources		cosmic rays, transistors leakage		decoherence, thermal, electromagnetic, radioactivity…
error levels		2.5×10^{-11} bit per hour error rate		usually ≫ 0,1% with qubit gates and readout (*)
information redundancy	logical bit	parity bits	logical qubit	large number of physical per logical qubits (*)
error correction		ECC (memory), MCA (CPU), RAID (storage)		quantum error correction codes and FTQC
error level after correction		negligible		under an acceptable threshold for fault tolerance

Figure 4: Detailed comparison between classical bits and qubits by separating the mathematical logic, the physical implementation and error correction techniques. © Olivier Ezratty, 2021.

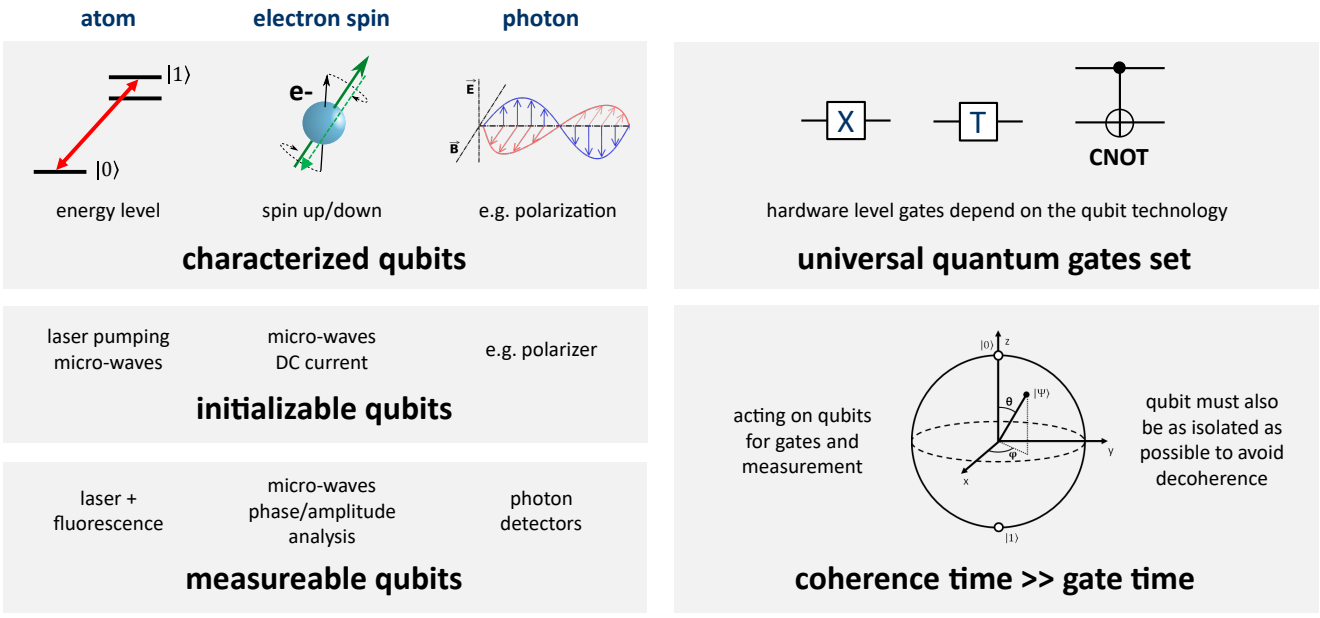


Figure 5: DiVincenzo gate-based quantum computing criteria. © Olivier Ezratty, 2021-2025, inspired by a slide from Pascale Senellart.

6 Quantum computing engineering

- A quantum computer uses physical qubits of different nature, the main ones being superconducting qubits, electron spin qubits, 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.
- Many key parameters are required to create a functional quantum computer. It must rely on two-level quantum systems used as qubits. These must be initializable and manipulable with a universal gate set that can approximate any unitary transformation on the relevant qubits to the desired accuracy. Qubits must be measurable when required by the algorithm. More general quantum channels are not arbitrary gate operations and require open-system dynamics or constructions involving ancillas, measurements or discarding subsystems. Coherence times and physical error rates must be compatible with the required circuit depth and error-management scheme.
- Most quantum computers are composed of several parts: a qubit chip (for solid-state qubits but also for trapped ions), vacuum enclosures (particularly with cold atoms and trapped ions) or sources, waveguides and detectors (photons), usually housed in a cryogenic vacuum chamber, some electromagnetic waves conveyed to the qubits with laser beams, or coaxial cables guided microwaves or direct currents, and a classical computer driving these electronic and photonic components. Qubits are driven by electromagnetic waves in various parts of the spectrum: UV, optical photons, infrared photons, microwave and radio-frequency signals.
- Errors are unwanted effects happening with qubits during initialization, gate operations, idle times, and readouts which affect the quality of the results. Noise is the main type of error source of stochastic nature that can be endogenous or exogenous. Decoherence progressively destroys superposition and entanglement in, and between qubits. Scientists devised quantum error mitigation (after computing) and active correction (during computing) schemes to address these problems. Quantum error correction relies on creating logical qubits composed of many physical qubits, the number depending on the quantum circuit size and many other parameters. A logical qubit is not a "perfect" qubit. It has a residual error rate designed to support the quantum circuit size. The number of physical qubits per logical qubit depends on it, the error correction codes, the qubits' physical connectivity and the physical qubit error rates. This creates huge scalability challenges, many of them with classical qubit control technologies. Fault-tolerant quantum computing (FTQC) is not just about using logical qubits. Error correction must happen faster than error creation and errors must not propagate within the quantum computer when logical gates are implemented.
- Many quantum circuits also require data preparation or storage, for example in quantum machine learning or oracle-based algorithms such as Grover search. Quantum-state memories exist in experimental and limited practical forms. They should be distinguished from qRAM, which aims at coherent random access to a large classical or quantum-addressed data set, and from circuit-based QROM. Large-scale fault-tolerant qRAM with efficient coherent random access is not currently available.
- 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, control electronics, lasers, cabling as well as the available space to house cabling and cryo-electronics. Based on vendor roadmaps, there seems to be a 1 to 100 scale of power consumption for future FTQC quantum computers. This explains the creation of the Quantum Energy Initiative in 2022, which gathers a community of researchers and industry vendors and organizations working collectively on this topic.
- The book describes the Lieb-Robinson bounds, which quantifies how fast information and entanglement propagate in a quantum system, and its potential impact on quantum-computing systems architectures from hardware to compilers and error correction.
- The economics of quantum computers are still uncertain due to their immaturity and the current low manufacturing volume. Uncertainty is also strong with regard 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. Another one is about expanding the limits in our ability to control a large number of entangled quantum objects, and with excellent fidelity.

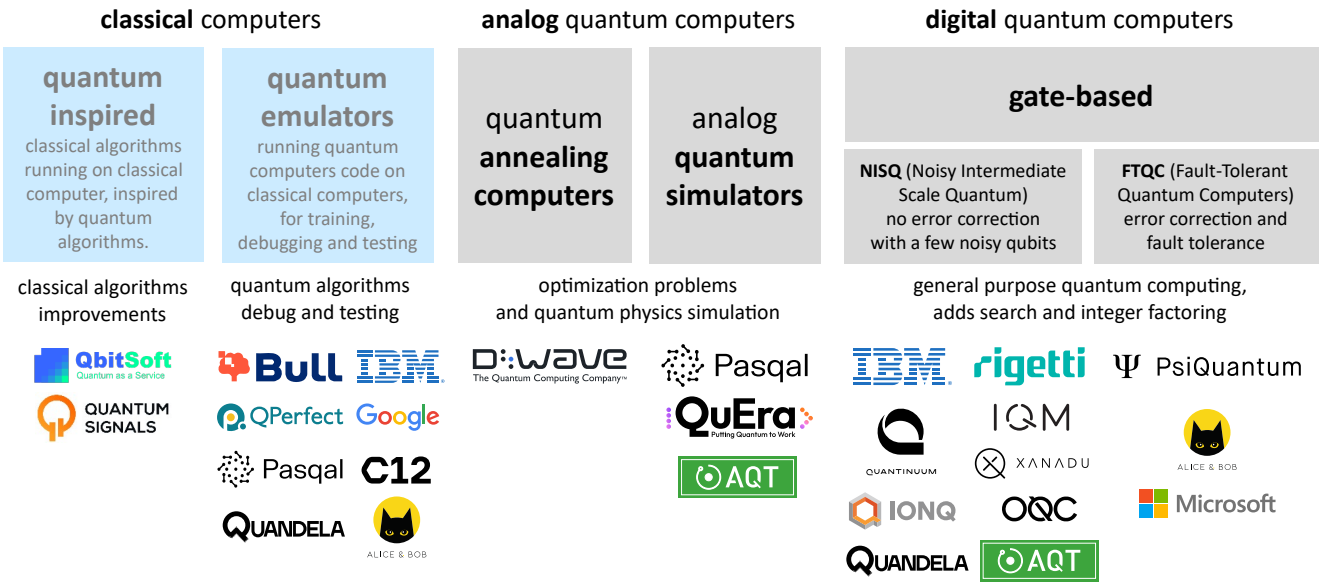


Figure 6: The different computing paradigms with quantum systems, hybrid systems and classical systems. © Olivier Ezratty, 2022-2026.

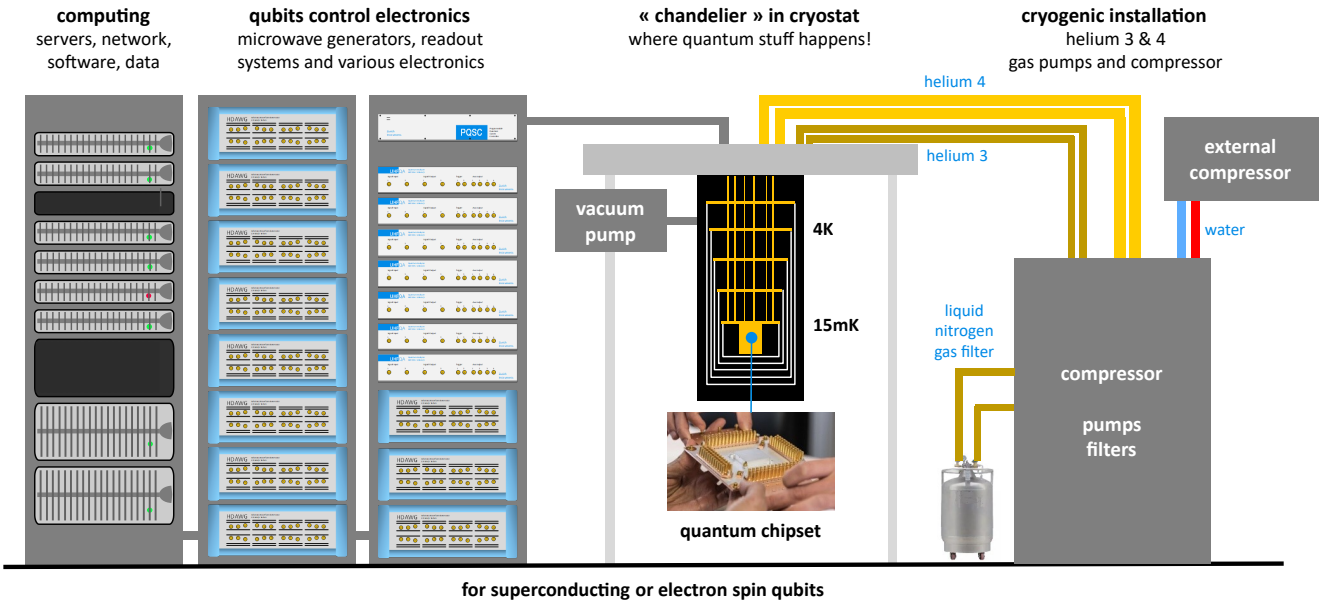


Figure 7: Typical physical components of a superconducting qubit quantum computer. It contains a classical computer that drives the whole system. © Olivier Ezratty, 2020-2025.

7 Quantum computing hardware

- Superconducting qubits are among the most common approaches today, implemented by IBM, Google, Rigetti, IQM and Origin Quantum among others. They remain noisy and face scaling challenges, particularly in control electronics, cabling and readout. One approach is to use bosonic encodings such as GKP and cat qubits, which combine microwave modes stored in cavities with superconducting circuits for manipulation and readout (Alice & Bob, AWS, Nord Quantique). Fluxonium qubits seem promising, but only a few vendors pursue them, including Google, which acquired Atlantic Quantum in October 2025. Alibaba was active in that segment but ended its quantum computing R&D in late 2023.
- Quantum-dots spin qubits could scale well due to their small size, the reuse of classical CMOS semiconductor manufacturing known-how, their higher working temperature enabling the usage of control cryo-electronics. They have however been demonstrated only at a very low scale at this stage.
- NV-center qubits have the benefit to be stable and to work potentially at ambient temperature. An increasing number of startups are playing in this field, like Quantum Brilliance (Australia and Germany). None of these commercial products support more than 10 qubits and it's been the case for several years. Don't count on it for scalable quantum computing and scalable room temperature operations. There are variations with other cavities and defects like with silicon-carbide (SiC) and SnV (tin vacancy color centers) but their technology readiness level remains very low as well.
- Topological qubits aim to obtain intrinsic protection against some classes of errors and could improve scalability if a suitable topological platform is demonstrated. Experimental solid-state platforms investigate Majorana zero modes, which are emergent quasiparticle excitations and should not be conflated with hypothetical elementary Majorana fermions. Microsoft's Majorana-1 and -2 announcements in 2025 and 2026 do not yet validate the architecture which is still lacking operational metrics. Microsoft's 2029 FTQC objective is a roadmap target whose feasibility remains uncertain if not totally unrealistic.
- Trapped-ion qubits have achieved very high fidelities and provide a credible approach for running NISQ algorithms. They have historically faced scaling challenges, with the current record as of September 2026 being Quantinuum's Helios 98-qubit processor. Recent progress with QCCD architectures shows additional scaling potential. One key limitation is slower gate speed, partly offset by high qubit-to-qubit connectivity that can reduce routing overhead and circuit depth, as well as potentially lower hardware and energy requirements in some architectures.
- Cold-atom qubits are widely used in quantum simulation, where systems can scale to hundreds or thousands of atoms, and they can also be used for gate-based quantum computing. Key demonstrations at the end of 2023, particularly with QuEra, increased interest in scaling these systems in gate-based mode and with quantum error correction. Pasqal (France), QuEra (USA), Infleqtion (USA), Atom Computing (USA) and planqc (Germany) are among the industry vendors in this field. New players entered the field in 2025-2026, including Q-Factor (Israel), Logiqal, Oratomic and Google (USA).
- Photonic qubits are flying qubits, propagating from sources to detectors through optical components that implement state preparation, transformations and measurements. The main encodings include discrete-variable and continuous-variable photonic schemes. Scalability remains challenging, particularly because of photon generation, loss and detection efficiency. Limited deterministic gate availability motivates measurement-based approaches such as MBQC and fusion-based quantum computing (FBQC), the latter being pursued by PsiQuantum. Quandela (France), Xanadu (Canada) and QuiX (The Netherlands) are other key players in this space. A key capability for measurement-based schemes is the generation of large, high-fidelity entangled photonic resource states, which remains an active research and engineering challenge.
- There are many other qubit types proposed by academic research teams, including molecular, nanomechanical and other emerging approaches. These generally have a very low technology readiness level, and many have not yet demonstrated a complete gate set or reported gate fidelities. Some may nevertheless represent promising approaches worth monitoring.

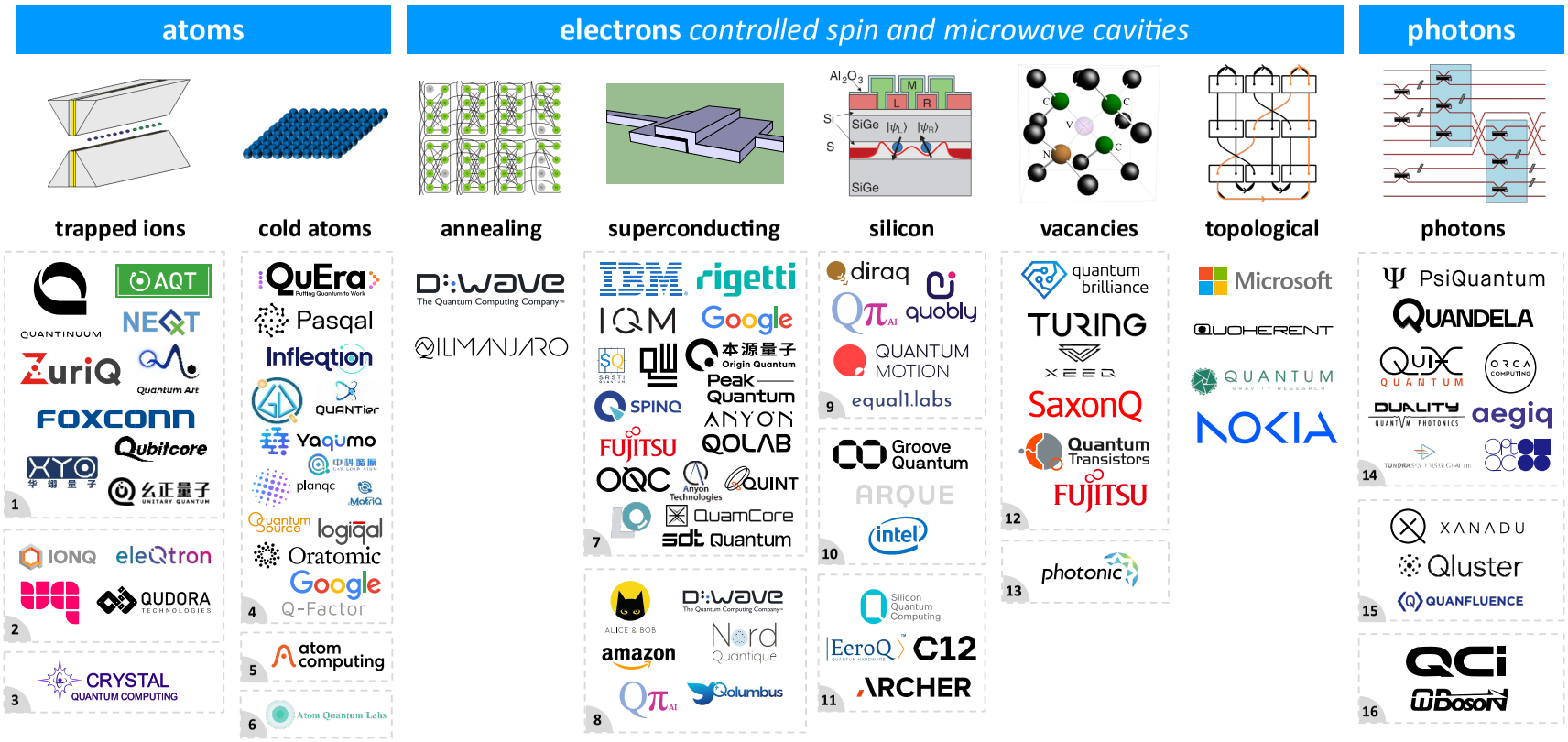


Figure 8: Map of the 90+ industry vendors in quantum computing hardware per qubit type. Some qubit categories are organized in subclasses as follows: (1) for laser driven ions, (2) for microwave driven ions, (3) for ions in Rydberg states, (4) for regular cold atoms, (5) for cold atoms with nuclear spin manifold, (6) for a variant of cold atoms with ionization preparation, (7) for transmon superconducting qubits, (8) for other superconducting qubits like bosonic qubits, dual-rail qubits and fluxonium qubits, (9) for silicon spin qubits, (10) for silicon-germanium qubits, (11) for other spin variant qubits like nanosphere and nanotubes, spin on helium and donor spin, (12) for NV centers qubits, (13) for silicon vacancies qubits, (14) for discrete-variable photon qubits, (15) for continuous variable photon qubits and (16) for coherent Ising model photonics systems. © Olivier Ezratty, September 2026.

8 Enabling technologies

- Quantum enabling technologies cover a broad field with cryogenics and vacuum pumps, control electronics, photonics including lasers, photon sources and detectors, photonic integrated circuits, semiconductor manufacturing techniques and even specific materials production. They are strategic to enabling future quantum systems, particularly scalable quantum computers. From a business standpoint, they are the equivalent of shovels in the gold rush. Many of these technologies have use cases beyond quantum technologies.

- Cryogenics is a key enabling technology for quantum computing, particularly for solid-state qubits operating at temperatures between roughly 15 mK and 1 K. Dilution refrigerators use mixtures of ^{3}He and ^{4}He to reach the lowest temperatures. Other cryogenic technologies target approximately 3 K to 10 K and can be used for some photonic sources and detectors. Large photonic quantum-computing projects may also require substantial cooling in the 2 K to 4 K range for sources, circuits, detectors and control electronics. A new trend for large-scale cryogenic systems for superconducting qubits is the use of helium centralized liquefiers (LHe).

- Cabling and filters play another key role, particularly with solid-state qubits. Cryogenic and superconducting cables can be expensive, with prices and supplier availability depending strongly on cable type, attenuation, thermal load, bandwidth and connector specifications. Signal multiplexing may reduce cabling requirements, including microwave multiplexing and microwave-to-optical conversion approaches.

- Microwave generation and readout systems used with superconducting and quantum-dot electron-spin qubits are other key enabling technologies. The challenge is to miniaturize them, lower their power consumption and, where useful, place some control electronics closer to the qubits at cryogenic temperatures while simplifying system cabling. This is important for physical-qubit scalability and quantum error correction. Many different technologies compete here, mostly around cryo-CMOS and SFQ superconducting electronics. Other components deserve attention, including circulators and parametric amplifiers that we cover in detail. Lastly, error correction requires extensive classical processing that is frequently omitted from fault-tolerant quantum-computing resource estimates.

- Many lasers and photonic components are used with cold atoms, trapped ions and photonic qubits, as well as in quantum telecommunications, cryptography and sensing. These include indistinguishable single-photon sources, single-photon detectors and photon-number-resolving detectors. The laser field is also very diverse, with products covering different wavelength ranges, powers and continuous-wave or pulsed operation. Cold-atom technologies can require relatively high optical power with low phase noise. Laser reliability is also a concern for production use. Cold-atom systems additionally rely on light-shaping devices such as SLMs, AODs, optical arrays and metasurfaces designed to control large numbers of atoms.

- Manufacturing electronic components for quantum technologies is a strategic topic covered extensively in this book with a description of generic fab techniques and some that are specific to quantum technologies as with the fabrication of superconducting qubits and quantum dots.

- Quantum technologies use many different raw materials, some of them rare but required only in small quantities. Some materials may carry significant environmental or supply-chain costs, while others are available from multiple sources. Examples include ^{3}He for sub-1 K cryogenics, isotopically enriched ^{28}Si for silicon-based quantum technologies, and atomic isotopes such as ^{87}Rb and ^{171}Yb. A key challenge is to analyze full product life-cycle costs and reduce the environmental footprint of emerging quantum technologies, particularly for components that may eventually be manufactured at scale.

Figure 9: Market map of key enabling technology vendors. © Olivier Ezratty, 2020-September 2026.

9 Unconventional computing

- Various non-conventional computing technologies may compete with classical and quantum computing or provide useful enabling capabilities. Many of them are now positioned as enabling a reduction of the energy consumption for AI-related tasks. Reversible and superconducting technologies, for example, may help create cryogenic electronics for scalable quantum computers. Because these approaches rely on very different physical principles, they require careful evaluation and benchmarking by both physicists and computer scientists. None has demonstrated a scalable polynomial-time solution to generic NP-complete problems or a broadly applicable advantage over the best classical baselines. We also cover in this part the realm of classical supercomputing, which provides some comparable on system size and capabilities.
- Digital annealing computing is mostly proposed by Japanese companies like Fujitsu and Hitachi, using classical CMOS chipsets. These solutions are supposed to solve intractable problems faster than classical computers, but their scalability remains questionable according to existing benchmarks. Their commercial traction seems to be limited to the Japanese market.
- Reversible and adiabatic computation have been researched for a long time and has not yet developed into broadly deployed commercial computing products. It may be more useful for reducing energy dissipation than for increasing computational speed, with potential applications in quantum-computing enabling technologies as well as in artificial intelligence application inferences.
- Superconducting computing is an interesting area of research to create more energy efficient supercomputers, despite the cooling cost that, fortunately, 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 computing is an interesting research area. These solutions may be competitive for solving specific combinatorial and decision problems.
- Optical processors are mainly investigated in the deep-learning space to accelerate training and inference for selected neural-network operations. Some variants target combinatorial optimization problems, where fault-tolerant quantum computers may also face substantial resource requirements. This is a dynamic sector with several well-funded startups.
- Chemical computing is one of the many other areas in unconventional computing that may be interesting but have probably various scaling limitations. Other unconventional computing such as DNA computing and other variations are not studied here, particularly since they are not deemed to solve intractable problems.

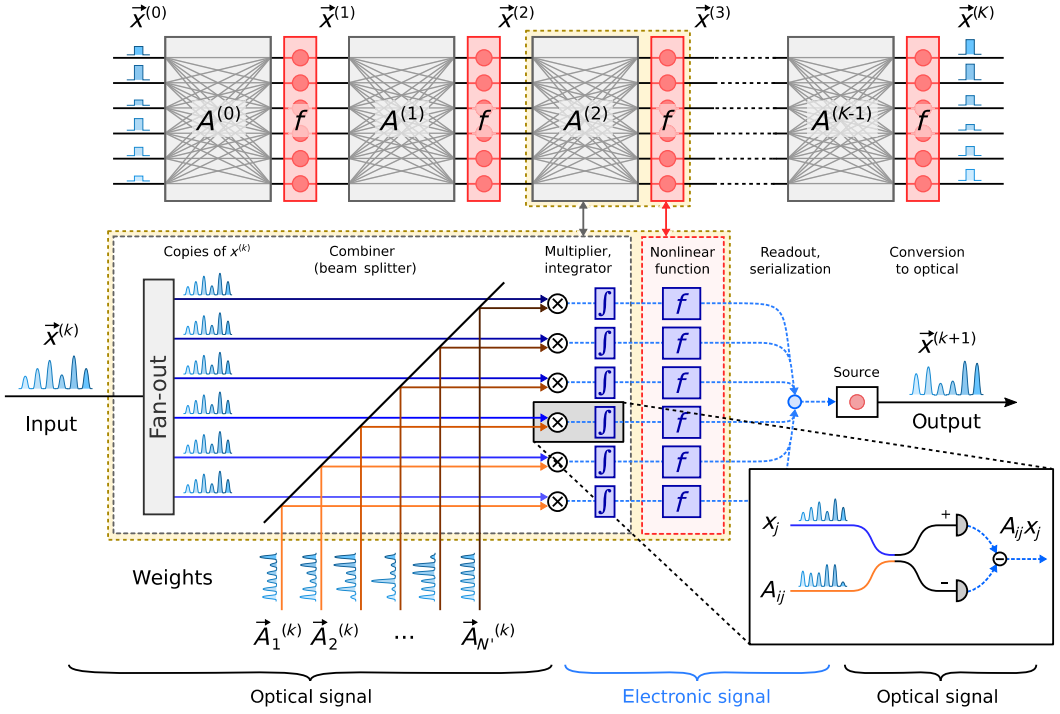


Figure 10: Source: "Large-Scale Optical Neural Networks Based on Photoelectric Multiplication" by Ryan Hamerly, Physical Review X, May 2019. Added in 2023.

10 Algorithms

- Quantum algorithms have been created since the early 1990s, many years before any quantum computer was prototyped in a research laboratory. They manipulate quantum amplitudes through coherent unitary transformations, interference and measurement, and in many important algorithms, entanglement. Their mathematical description relies on vectors, matrices and linear operators acting in Hilbert spaces whose dimension grows exponentially with the number of qubits.

- The main algorithm classes are oracle based and search algorithms, optimization algorithms, quantum physics simulation algorithms, and quantum machine learning algorithms. There is also a more generic class of algorithms solving linear systems and partial differential equations.

- Quantum algorithms are interesting when they provide some quantum advantage compared to their equivalent best-in-class classical equivalents. It can be a theoretical and practical speedup, better result quality such as chemical simulation accuracy or better heuristics, less required training data in some machine learning cases, or, potentially, a lower computing cost including energy consumption. Quantum speedups must be practical and incorporate all classical and quantum computing costs, including error detection and mitigation (NISQ) or QEC/FTQC overheads. A polynomial quantum speedup can be a limiting factor, like with Grover's search algorithm, particularly if its oracle implementation is not well specified.

- Another key aspect of quantum algorithms is data loading and/or preparation. It is often overlooked and can have a significant time cost. For algorithms relying on amplitude encoding, loading an arbitrary N-dimensional classical vector generically requires $O(N)$ resources in one form or another unless exploitable structure or an efficient state-preparation mechanism is available. Some algorithms assume the use of qRAM, which is not yet available at useful scale. These constraints make quantum computing not well adapted to big-data workloads such as conventional large-language model (LLM) training and inference. Any serious resource estimate should include the circuit and data-access costs required to prepare the quantum state that is then processed by components such as phase estimation, amplitude amplification or quantum simulation.

- Relatively few quantum algorithms provide a theoretical computing time exponential or superpolynomial speedup, the main one being Shor's integer factoring and discrete log algorithms. Any exponential speedup for most other classes of algorithms like HHL to solve linear systems is usually conditioned by specific criteria like data sparsity and the existence of some structure in the problem. The 2024 DQI (Decoded Quantum Interferometry) from Google generated a lot of hope to solve optimization problems efficiently, but the related resource estimates are quite significant.

- Gate-based computers, quantum annealers and analog quantum-simulator algorithms are all hybrid, combining a classical (preparation) part and a quantum part (a quantum circuit, or an annealing process). A special breed of quantum algorithms are the variational quantum algorithms (VQA) and their variants for optimizations (QAOA), chemical simulations (VQE) and machine learning (QML) that target NISQ systems (noisy intermediate quantum computers). These combine classical preparation and adjustment of a Hamiltonian that computes a cost function with several classical optimization steps and quantum computing circuit executions. Algorithms based on a Quantum Fourier Transform (QFT) and modular exponentiation require a fault-tolerant quantum computer with quantum error correction. But they are also hybrid since they need some classical software that prepares the circuit to run, a task that may be highly resource demanding and in some cases, that requires an HPC.

- Quantum-inspired algorithms run on classical computers and borrow mathematical representations, sampling techniques or algorithmic ideas from quantum information and many-body physics. Tensor networks, including MPS and DMRG, form one major family, but other approaches include sample-and-query dequantization, neural quantum states, Pauli and Majorana propagation, matchgate and fermionic-Gaussian simulation, and annealing-inspired optimization. They can improve classical computing solutions and are useful for classical simulations of quantum systems. Progress in these methods continuously raises the classical baseline against which quantum advantage must be evaluated, including in quantum chemistry where increasingly large active spaces can now be treated classically.

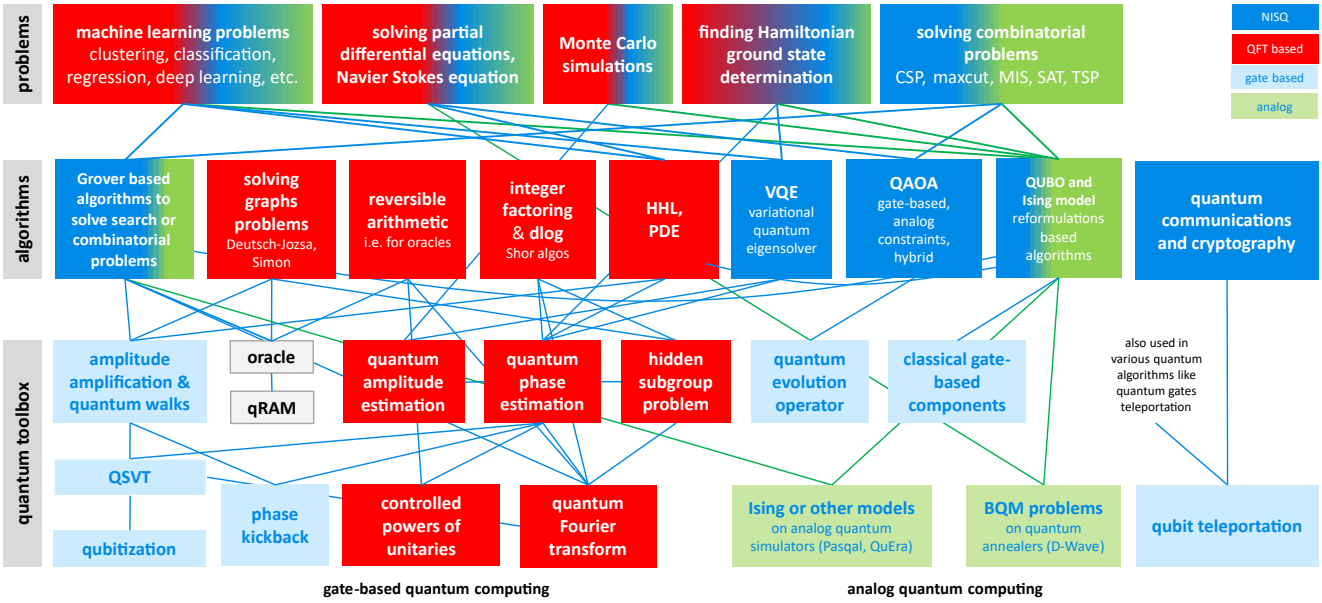


Figure 11: Simplified quantum algorithms inventory with problems (top), key algorithms (middle) and basic algorithm components (bottom). The color code is red for FTQC problems/algorithms relying on the QFT (quantum Fourier transform) and/or modular exponentiation, blue for problems/algorithms corresponding to other gate-based algorithms that may work in NISQ QPUs and green for problems/algorithms related to analog quantum computing paradigms like quantum annealing (*ala* D-Wave) and quantum simulations (*ala* Pasqal). Many high-level problems can be solved using an FTQC QFT-based version and some analog equivalents, usually based on a QUBO or Ising problem formulation. © Olivier Ezratty, 2023-2025.

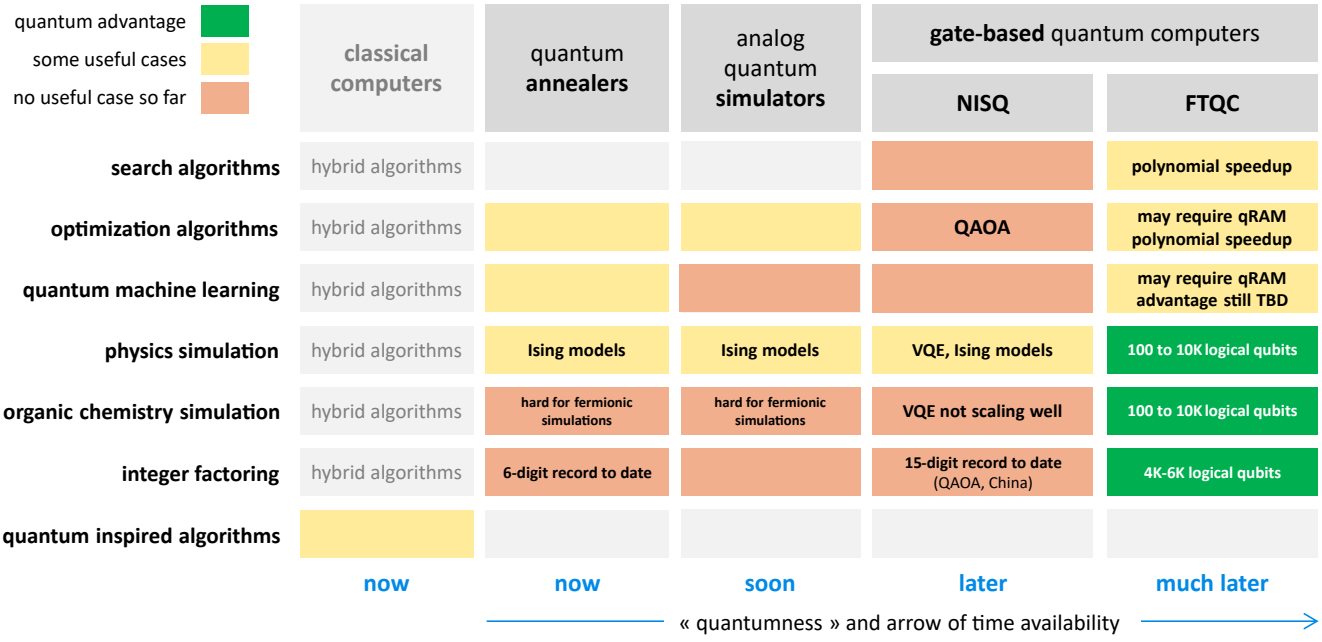


Figure 12: Classes of problems and the quantum computing paradigms (gate-based, analog-simulation annealing) which can solve them, and a related time scale for their practical availability. Surprisingly, integer factoring algorithms are also available on quantum annealers and simulators, but it may not scale as well as future FTQC systems. There are subtle nuances on the scalability of all these platforms, including analog quantum computers. Analog quantum computing platforms can theoretically solve a lot of problems, but are particularly well suited to solve graph problems and Ising models in fundamental physics, while the FTQC paradigm is the most generic one. But its advent is still uncertain and in a time window between 5 and 15 years depending on the estimates. In the FTQC regime, search, optimization and machine learning algorithms have an uncertain fate due to either a polynomial speedup that may not turn into a practical speedup, or unproven speedups. © Olivier Ezratty, 2021-September 2026.

11 Software tools

- Gate-based programming involves either graphical circuit design (mostly for training purposes) and (usually) Python based programming when qubit-gate structures must be designed in an automated way. Key components of the software development toolset are compilers and optimizers as well as resource estimators, which help figure out the hardware configuration required to run some quantum circuit.
- Python-based programming relies 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.
- Current NISQ quantum computing commonly relies on repeated circuit executions, often thousands or more, to estimate output probabilities or expectation values. In variational algorithms, a classical optimizer repeatedly updates circuit parameters between groups of quantum executions. A single run yields one probabilistic measurement outcome, while statistical estimates converge as the number of shots increases. VQE may require many circuit executions to estimate the expectation values of Hamiltonian terms with sufficient precision while a classical optimizer updates the ansatz parameters. Large circuits on fault-tolerant quantum systems may also require repeated executions depending on the algorithm and desired success probability, including algorithms using quantum phase estimation (QPE).
- 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, OVHcloud and Scaleway. Similar offerings are available in China and Japan. In the long term, cloud quantum computing services architectures will need to be distributed and require dynamic routing of photonic entanglement resources to enable the creation of large virtual QPUs.
- Quantum emulators are very useful to learn programming, and test circuits until the emulators reach the limits of classical emulation. They support up to 20 qubits on a laptop, 40 on a server appliance and 50-55 on an HPC in state vector mode. It can exceed 100 qubits with using tensor-network-based emulators for shallow circuits. Emulators can help debug small-scale quantum algorithms. When these emulators include physical simulators of the underlying qubit physics as with Bosonic Qiskit and Quandela Perceval, they help create algorithms that are error-resilient and design new quantum error correction codes. Quantum emulation is an indispensable part of any quantum cloud offering. Emulator are often called "simulators" which is a misnomer creating confusion with quantum simulators which are classical and quantum systems that can simulate quantum systems in general.
- Gate-based circuit 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. Another key discipline is resource estimation, with tools that help figure out the hardware configuration necessary to run a given algorithm. It also provides indications on the related computing time which may be prohibitive and require future optimization techniques.
- Benchmarking quantum computers remains an unsettled field with many competing approaches, including methods used to assess claims of quantum supremacy or quantum advantage. Such claims must specify the computational task, the best classical baseline, the cost metric, the hardware and error-mitigation assumptions, and whether the result has been peer reviewed or independently reproduced. By 2026, several experiments had reported computational or scientific utility on NISQ hardware, especially for quantum-physics problems, but this does not by itself establish an industry-relevant quantum advantage. The book therefore distinguishes claimed advantage, peer-reviewed evidence and independent validation and advances in dequantization and quantum inspired classical techniques.

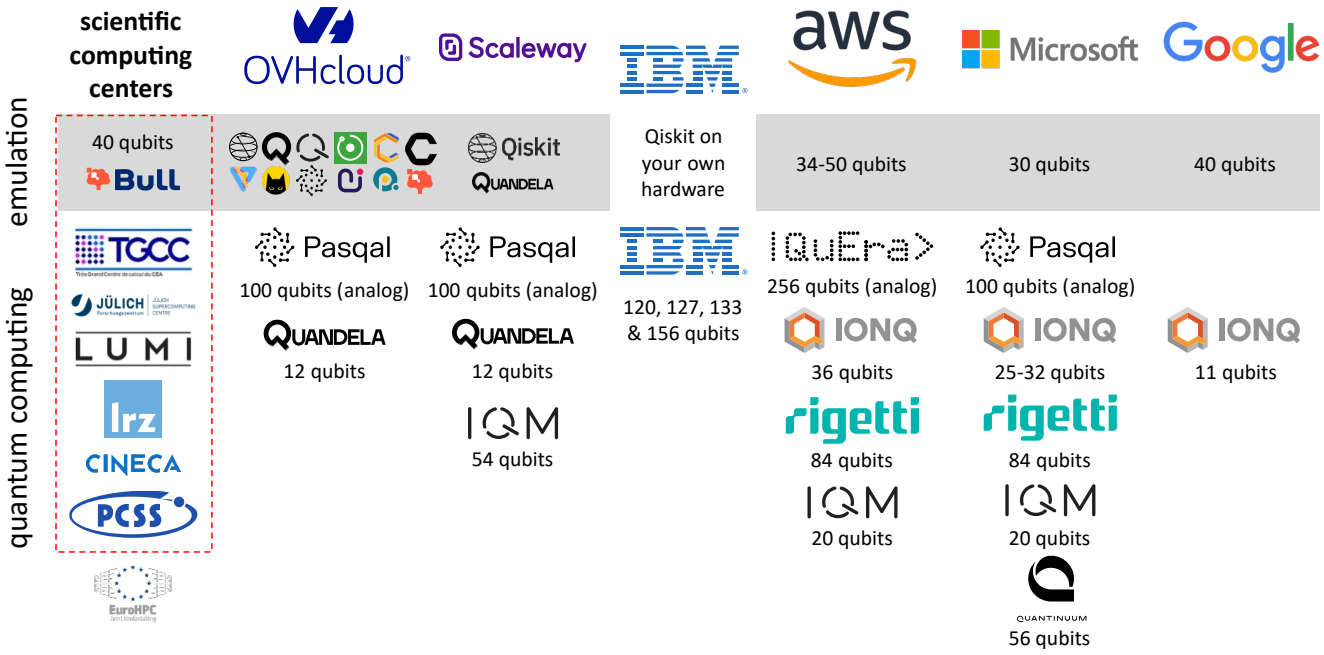


Figure 13: Main quantum cloud emulation and QPU offerings in the USA and Europe. IBM discontinued its online Qiskit emulator in May 2024. It can be used on customer's laptops or with other cloud vendors like OVHcloud. The book contains a similar map for China and Japan. © Olivier Ezratty, 2021-September 2026.

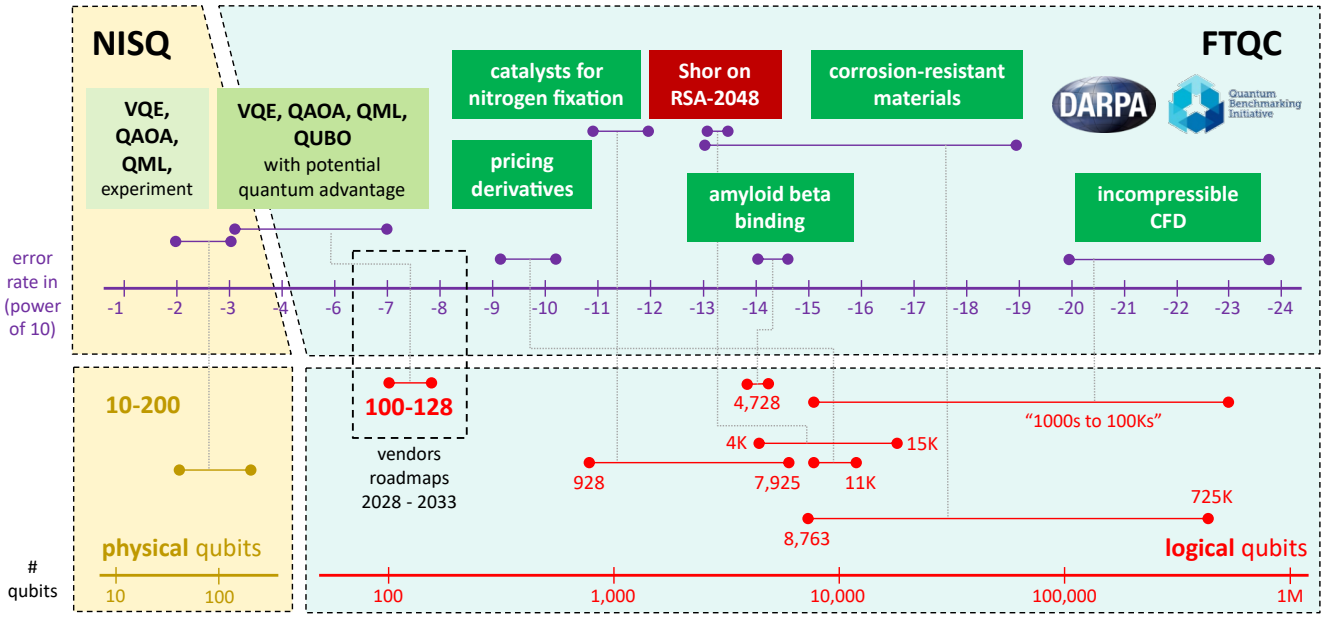


Figure 14: Compilation of some algorithmic-level resource estimates for key algorithms which have some industry relevance. The top part contains some typical algorithms, and their resource estimated ranges in gates, T gates or Toffoli gates. These resource estimates correspond to an error rate for the qubits (physical in NISQ and logical in FTQC) in the purple scale crossed by the dotted lines. In a simplified manner, it corresponds usually to the two-qubit gate error rates which are usually the higher vs single qubit gates. Below in orange and red are the related resource estimates in physical (NISQ) and logical (FTQC) qubits, regardless of the implementation. Physical qubits (in NISQ) and logical qubits (in FTQC) are on a similar log scale. What determines the physical per logical qubit count is not shown in the chart. The best algorithms for early FTQC systems may be NISQ variational algorithms which require deeper circuits than NISQ QPU + QEM can enable. © Olivier Ezratty, 2024-2025.

12 Applications

- Most quantum computing market forecasts are highly optimistic and assume an early advent of scalable quantum computers. They also sometimes tweak forecasts by pushing business value numbers instead of an actual market for quantum technologies. These numbers are confusing and sometimes taken as market sizes, which fools some investors.
- 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 (FTQC). Others may find their way on analog quantum simulators.
- This book contains a framework proposal to assess the interest and relevance of published use cases. It helps separate marketing claims from practical evidence. Under a strict criterion requiring an independently documented production deployment and a demonstrated advantage over the best practical classical baseline, no qualifying corporate quantum-computing application was identified by the book's September 2026 cutoff. Many documented NISQ use cases run on fewer than 30 physical qubits and can therefore often be emulated classically at lower cost and sometimes faster. Without credible resource estimates or benchmarking against strong classical baselines, such case studies are primarily useful for learning, workflow development and algorithm exploration. The book contains a list of items to watch for in documented case studies (retrospective) and use cases (prospective).
- In some cases, the potential use cases are in the overpromising twilight zone such as simulating very complex molecules, improve climate modeling and develop innovations to fixing climate change, curing cancers or optimizing large fleets of autonomous vehicles. All these are dubious long-term promises. Serious case studies contain resource estimations. The use cases bringing significant business value frequently require a large number of logical qubits, in the thousands, and usually, rather long computing times. There is still a lot of room for quantum-algorithms optimizations.
- One purveyor of case studies is D-Wave with its quantum annealer although it has not yet demonstrated a real quantum advantage. IBM is second there, having evangelized a broad number of customers and developers since 2016, particularly around the theme of "quantum utility" which has not yet reached the realm of industry relevant applications even though they switched gears on "quantum advantage" in August 2026 with three case studies that are still far from being industry related. IonQ and Quantinuum are also publicizing case studies, but they are usually below a quantum advantage level, using fewer than 25 qubits. Quantinuum is making progress with its 56 and 98 qubits quantum processors.
- Beyond computing time, a quantum advantage can also come from the system's energetic footprint and/or the precision of the outcome. Specific cases can claim to be in that situation with analog quantum simulations.
- There are already many software vendors in the quantum-computing space despite the limited availability of hardware demonstrating practical quantum advantage. Their activities include pilot projects, software frameworks, hybrid quantum-classical algorithms, and quantum-inspired algorithms running on classical hardware, and engineering or consulting services. This book also covers the growing IT and consulting-services ecosystem around quantum technologies.

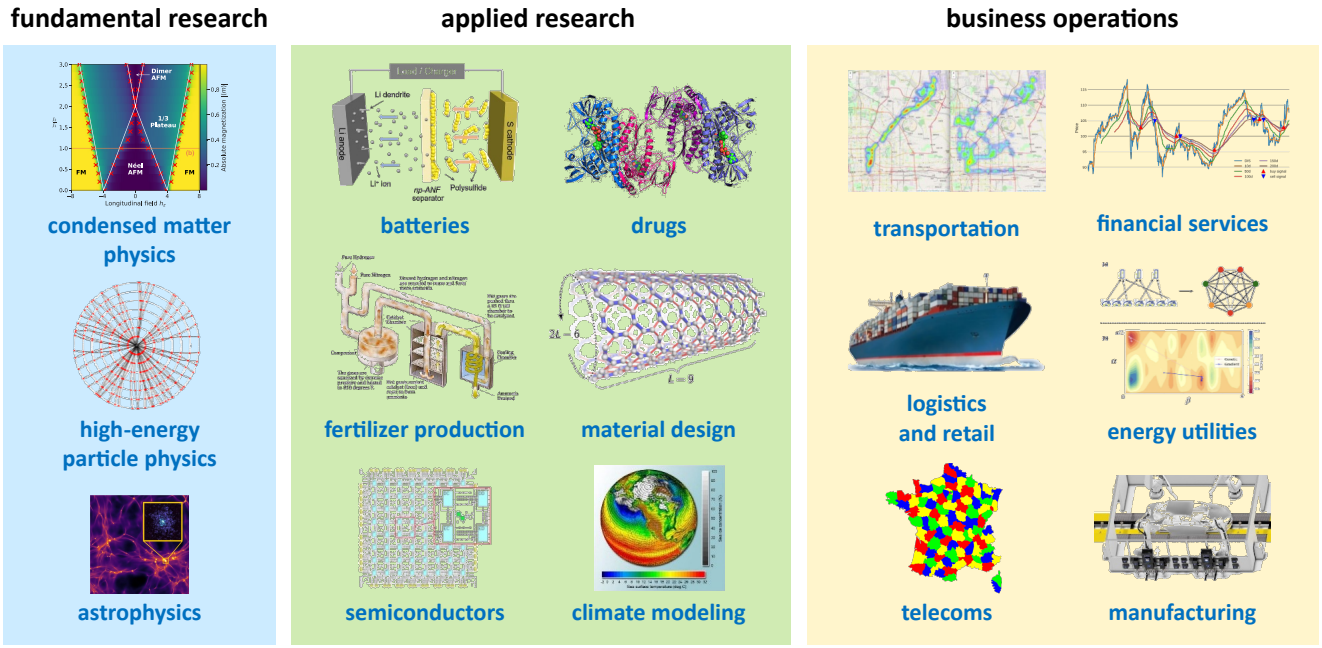


Figure 15: Map of the main solution domains for quantum computing applications separating research-oriented use cases and operation-level use cases. The use cases on the left and middle are the most credible ones while optimization-based use-cases are based on quantum algorithms which do not yet provide some exponential speedup. This turns into algorithms that do not bring some practical speedup due to so-called prefactors, one being that quantum gates are relatively slow. © Olivier Ezratty, 2022-2025.

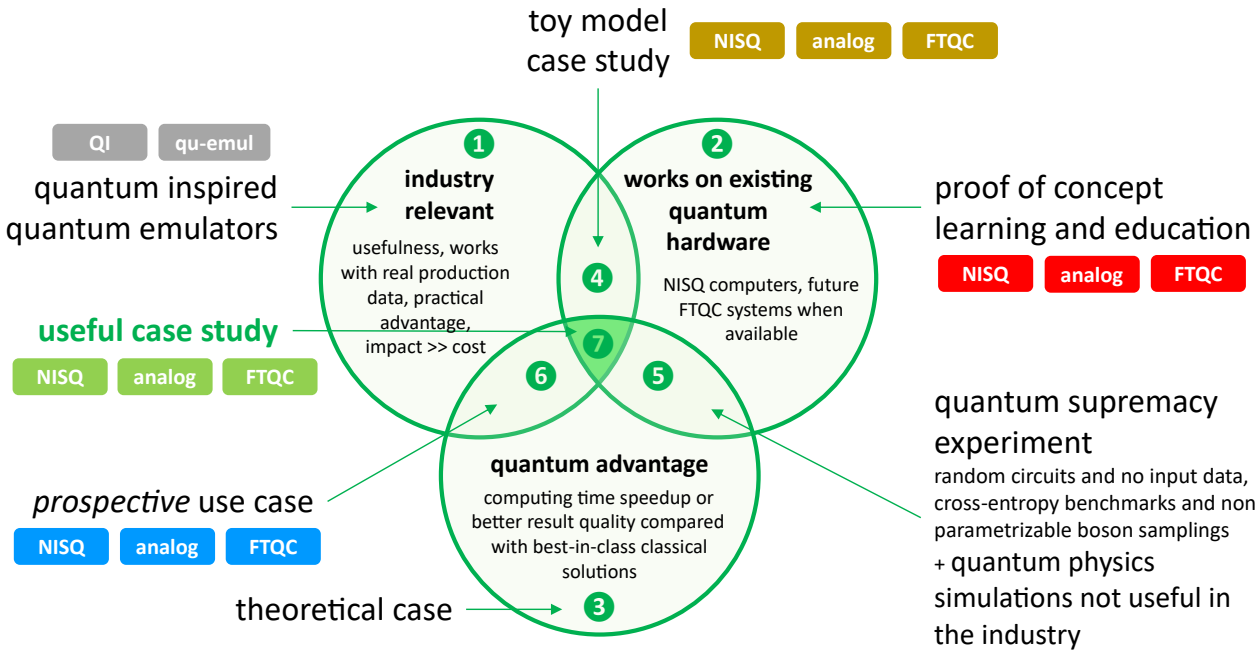


Figure 16: Semantics segmentation between three zones (industry value, runs on quantum hardware, provides some quantum advantage) and their potential overlap. It creates seven zones with distinct scenarios, which are detailed in the main text. Badge color codes: red for no industry value and no quantum advantage, orange for industry value without a quantum advantage, blue for future systems and green for quantum advantage on existing hardware and industry value. © Olivier Ezratty, September 2026.

13 Communications and cybersecurity

- Quantum computing poses a theoretical threat to widely used public-key cryptography based on integer factoring or discrete logarithms. Shor's algorithm could, on a sufficiently large fault-tolerant quantum computer, recover the private information underlying schemes such as RSA from public data. Symmetric cryptography is affected differently, most notably through the quadratic search speedup provided by Grover's algorithm rather than through public-key distribution. The migration urgency is partly driven by the "store now, decrypt later" threat and by planning rules such as Mosca's inequality, which motivate deployment of quantum-resistant protections before cryptographically relevant quantum computers exist.
- Two broad families of countermeasures are commonly discussed: post-quantum cryptography (PQC), based on classical cryptographic algorithms believed to resist known quantum attacks, and quantum-communication techniques such as QKD. NIST launched its PQC standardization process in 2016 and selected algorithms for standardization in July 2022. In August 2024 it finalized FIPS 203, FIPS 204 and FIPS 205, covering ML-KEM, ML-DSA and SLH-DSA. FN-DSA, derived from FALCON, is planned for FIPS 206 and remains in development. PQC security must still be assessed against cryptanalysis, implementation flaws and side-channel attacks.
- Quantum key distribution (QKD) uses a quantum communication channel, together with an authenticated classical channel, to establish shared symmetric key material between remote parties. Protocols can use prepare-and-measure schemes or entanglement-based schemes, including architectures relevant to future quantum networks connecting computers and sensors. QKD does not transmit or protect public keys, and it does not require a general-purpose quantum computer. The generated key material is normally used with conventional symmetric cryptographic mechanisms for subsequent data protection.
- Quantum random-number generation (QRNG) can provide entropy for classical and quantum-communication cryptographic systems, including key generation, nonces and other protocol randomness. A QRNG does not by itself guarantee the security of a public or private key, which also depends on the cryptographic algorithm, implementation and threat model. QRNGs also have applications wherever high-quality randomness is useful in classical computing, including lotteries and Monte Carlo simulations.
- Quantum telecommunications can also use quantum entanglement to enable communications between quantum computers and/or quantum sensors. Distributed quantum computing has two potential benefits: scaling quantum computing beyond the capacity of individual quantum computers and enabling safe communications between quantum computers. There is a huge technology challenge with interconnecting quantum computers. It is about creating entanglement resources between distant qubits, sometimes using transduction between different wavelengths, and then, gate teleportation protocols to enable two-qubit gates between distant quantum processors. Distributed quantum sensing can also enable more accuracy sensing.
- Quantum Physical Unclonable Functions (qPUFs) are proposed authentication primitives whose security claims must be stated under a defined threat model, including assumptions about enrollment, verification and resistance to attacks. No physical authentication method is literally unfalsifiable, and qPUF technology remains immature.
- There are already many startups in the QKD and PQC scene. Deployments have already started worldwide, particularly in China with both landline fiber and satellite links. Europe is also experimenting quantum communication networks. PQC deployment is a priority for most governments and sensitive verticals (defense industry, financial services, healthcare, automotive).

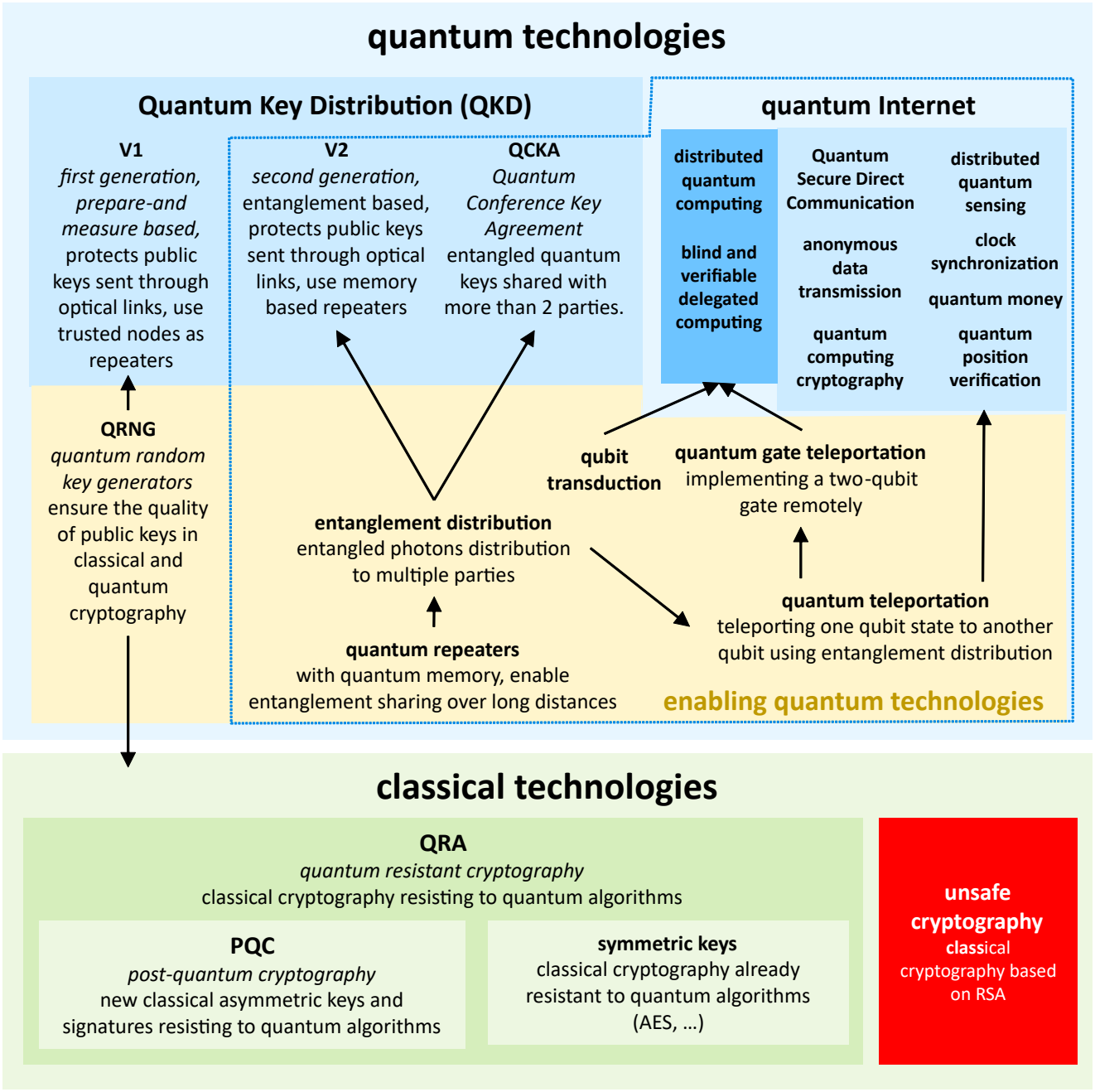


Figure 17: The various types of communications and cybersecurity technologies covered in the book and their relationship. © Olivier Ezratty, 2023-2024.

14 Quantum sensing

- Quantum sensing is a slightly more mature and overlooked market in quantum technologies, one potential reason being its fragmentation and currently limited large-scale use cases. It is perceived as having a higher technology readiness level (TRL) than quantum computing. But these sensors are still not easy to design from an industrial point of view and their actual accuracy and sensitivity do not always match expectations.
- Quantum sensing enables more precise measurement of nearly any physical parameter: time, distance, temperature, movement, acceleration, pressure, gravity, magnetism, light frequency, radio spectrum and the chemical composition of matter.
- The 2019 revision of the International System of Units (SI) fixed exact numerical values for several defining physical constants. Quantum electrical standards, atomic clocks and other precision-measurement techniques are central to the realization and dissemination of several SI units, but it is more accurate to describe them as part of precision metrology than to say that quantum sensing itself "updated" the SI.
- Lasers and optical frequency combs are used for extremely precise frequency and time metrology, including comparisons involving optical atomic clocks that can outperform cesium microwave clocks in stability and accuracy. Frequency combs are commonly generated with mode-locked lasers producing trains of ultrashort, often femtosecond, pulses.
- Nitrogen-vacancy (NV) centers in diamond are one of the most widely studied solid-state quantum-sensing platforms. They can measure magnetic fields and, through adapted protocols, other parameters such as temperature, pressure or electric fields, with applications ranging from materials characterization to biomedical research. Their practical performance depends on trade-offs among sensitivity, spatial resolution, bandwidth, stand-off distance and form factor. Many implementations are still moving from laboratory demonstrations toward robust products.
- Another important approach is cold-atom interferometry, implemented in gravimeters, accelerometers and inertial sensors relevant to PNT, meaning "positioning, navigation, and timing". Atomic systems can also be used for radio-frequency sensing and are being investigated for searches for some forms of dark matter.
- China supposedly built some quantum radars using photon entanglement and up/down converters between visible photons and radar frequencies, but the real performance of these devices is questionable, particularly their range, and is driving a lot of skepticism in the Western world. But the related research is still going on and quantum LiDARs seem to make progress. Quantum sensing can also potentially improve the sensitivity of classical radars.

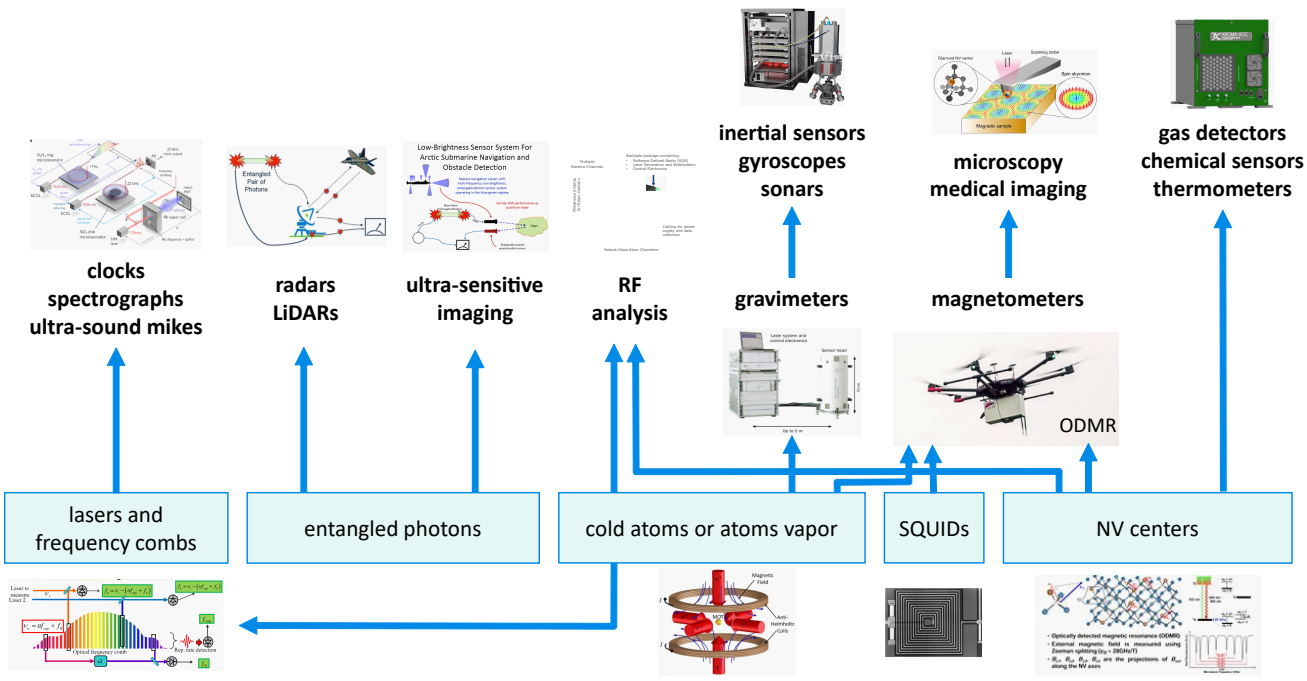
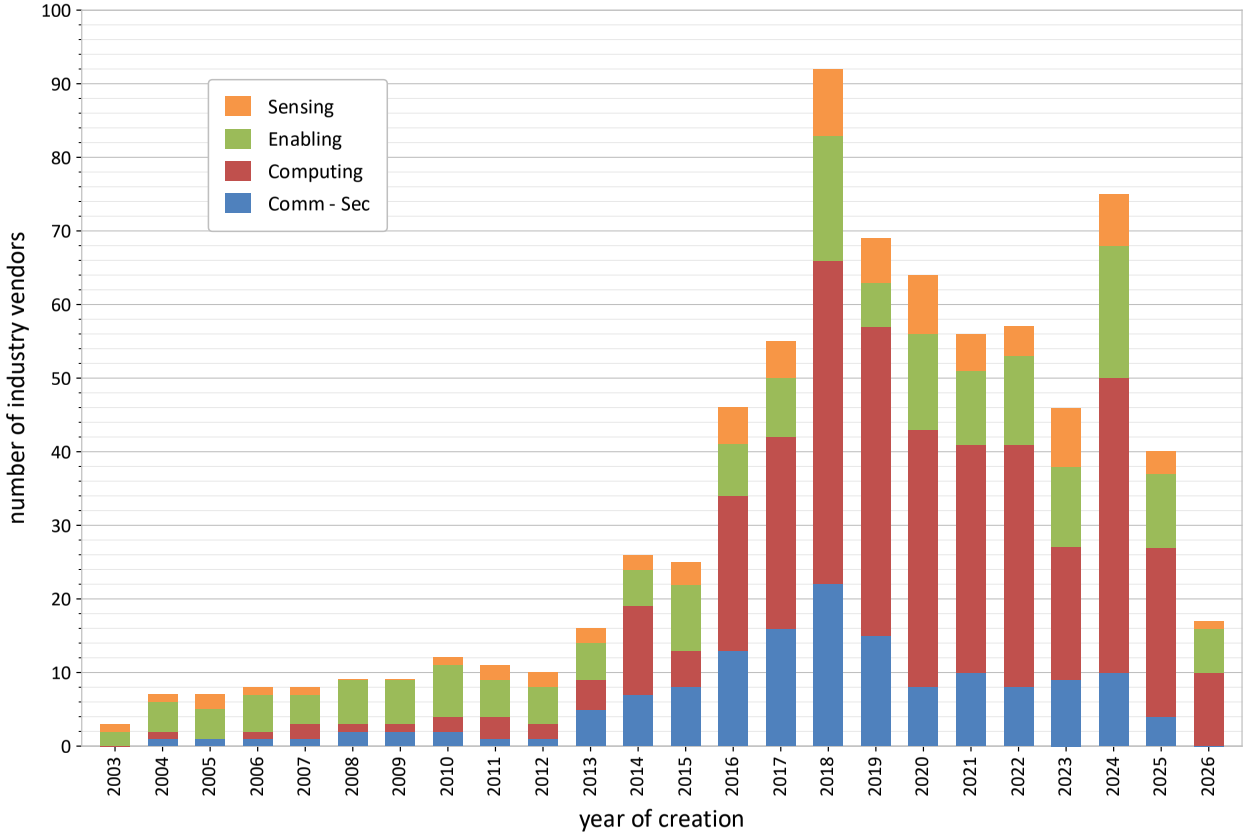


Figure 18: A (partial) map of various quantum sensing basic technologies and use cases. © Olivier Ezratty, 2021-2025.

15 Quantum technologies throughout the world

- The quantum startup scene saw 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 startup funding. The investors FOMO (fear of missing out) and the "winner takes all" syndromes explain this situation. But startup funding in the quantum space is faring relatively well considering the long-term business prospects, particularly with the surge of SPACs and IPOs for companies like D-Wave, IonQ, Rigetti, Infleqtion, Xanadu, and Pasqal. Quantinuum also did its IPO in 2026, without a SPAC. We describe these funding mechanisms in the book. We show the dominance of the USA in the private sector investment, which adds the best funded startups in the world to large established companies significant investments, topped by IBM's recent $10B 5-year plan announced in June 2026.
- Most developed countries now have national quantum plans, often with a strong emphasis on quantum computing. Cross-country investment comparisons require explicit accounting rules because announced totals can mix incremental and pre-existing funding, different time windows, public and private investment, and supranational programs such as European Union funding. Meaningful comparisons therefore require a common normalization period, source date and inclusion rule. These plans generally support fundamental research, industrial ecosystems and workforce development, while governments also support suppliers through procurement programs.
- China's public investment in quantum technologies is difficult to compare with that of the United States or Europe because program scope, disclosure practices and accounting conventions differ. Published estimates such as $15B to $25B can't be compared directly with US or European investments unless they use the same time window and include the same categories of spending. The book therefore treats such country totals as ranges or source-dependent estimates rather than precise figures.
- Europe and the United States are among the largest investors in quantum science and technology, but their relative ranking depends on the accounting perimeter, time window and treatment of national, supranational and private investment. Europe has substantial public investment through both the European Union and member states, while the United States has major private investment from large technology companies and venture-backed startups.
- Many countries have placed quantum technologies in the critical field of "digital sovereignty" like if they were some sort of nuclear weapon equivalent. Many countries launched specific defense related quantum investment plans and competitions like DARPA's QBI, and equivalent programs in France, Germany and elsewhere.
- Each country has its own strengths and specialties 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 coming both from the academic and industry vendor spaces. The intensity of the hype is very strong in this industry, but so far, it has resisted the bubble burst effect.



Country	Computing	Enabling	Sensing	Comm - Sec	Total
USA	90	61	24	41	216
Germany	33	28	9	9	79
UK	25	22	8	22	77
France	23	36	9	8	76
Canada	35	13	6	19	73
China	18	8	6	11	43
Japan	17	12		4	33
India	20	5	2	4	31
Netherlands	10	11	3	4	28
Switzerland	6	14	1	4	25
Australia	8	5	7	2	22
Israel	10	2	2	4	18
Italy	5	6	2	4	17
Denmark	5	6	3	2	16
Spain	9	4		3	16
Sweden	3	11	2		16
Finland	6	6		3	15
South-Korea	9	3		3	15
Singapore	8	2	1	2	13
Poland	5	2		3	10
Austria	4			4	8
Russia	1	2		4	7
Taiwan	1	2		2	5
Estonia	3			1	4
Belgium	1	2			3
Chile	1			2	3
Slovenia	1	1		1	3
UAE	2			1	3
Bulgaria	1			1	2
Czechia				2	2
Greece	2				2
Hong-Kong	2				2
Turkey		1	1		2
Belarus	1				1
Brazil	1				1
Columbia	1				1
Libya	1				1
Lithuania				1	1
Luxembourg		1			1
Sri Lanka	1				1
Ukraine	1				1
Uruguay	1				1
Total	**371**	**266**	**86**	**171**	**894**

Figure 19: Chart of the creation year of small businesses and startups in "second revolution" quantum technologies. © Olivier Ezratty, September 2026.

16 Quantum technologies and society

- Quantum technologies can become one expression of humanity's technological ambitions, pushing the limits of what can be measured, simulated and computed, as artificial intelligence has done in other domains. Quantum computing nevertheless has fundamental and practical limits. No finite model can reproduce every detail of the universe without assumptions and finite resource bounds, and quantum computing does not make arbitrary future prediction possible. Claims about determinism, free will or the ultimate social impact of quantum technologies require more careful philosophical and scientific qualification. The quantum revolution may therefore be oversold when such claims go beyond demonstrated capabilities.
- Science fiction has built an imaginary around quantum technologies, including teleportation, superluminal travel, extreme entanglement and miniaturization, parallel worlds and time travel. These ideas do not all have the same scientific status. Some conflict with established physical constraints, while others are speculative interpretations, limited laboratory phenomena or capabilities that are simply not technologically realizable today. Science fiction can nevertheless inspire scientific vocations and motivate new generations to solve real problems.
- The quantum scientific community is investigating the ethics of quantum technologies. As with artificial intelligence, it will be questioned on algorithm 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 for specialists. There's a need for better pedagogy, accessible educational content and for sound fact-checked information, and for the creation of suited teams for both creating and using quantum technologies.
- Gender balance remains an issue in quantum technologies, with women underrepresented in many parts of the field, particularly among technology vendors. There are nevertheless many women scientists and entrepreneurs who can serve as role models for girls and young women. Numerous initiatives around the world have been launched to improve participation and representation.
- Finally, quantum-technology vendors marketing must be watched carefully. It is and will be full of exaggerations and approximations. The worst is found with vendors from outside the quantum technology sphere.

Figure 20: Some women role models around the world, from research to the industry. © montage by Olivier Ezratty, 2021-September 2026.

17 Quantum fake sciences

- Quantum physics has been for a while integrated in highly dubious offerings, particularly in the healthcare and energy production domains.
- There is a proliferation of products and services making unsupported health claims based on electromagnetic waves, vaguely defined "energies" or alleged restoration of a body's "balance". Expectation and placebo responses do not establish that such a product has the claimed therapeutic efficacy. These claims should be evaluated against controlled clinical evidence, plausible mechanisms and applicable regulatory findings. Otherwise, these are just scams.
- Some proposals attempt to explain consciousness using quantum physics, but broad claims of this kind currently have limited theoretical and experimental support. This form of reductionism has very limited theoretical and experimental grounds. Likewise, products marketed around scalar-wave detectors or generators, healing crystals, structured water or "quantum" medallions are also pure scams.
- This part of the book proposes a simple methodology for identifying unsupported or misleading healthcare claims using scientific evidence, reproducibility, plausible mechanisms and regulatory information.
- 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 which have nothing quantum at all to offer. It spans a large number of product and service sectors.

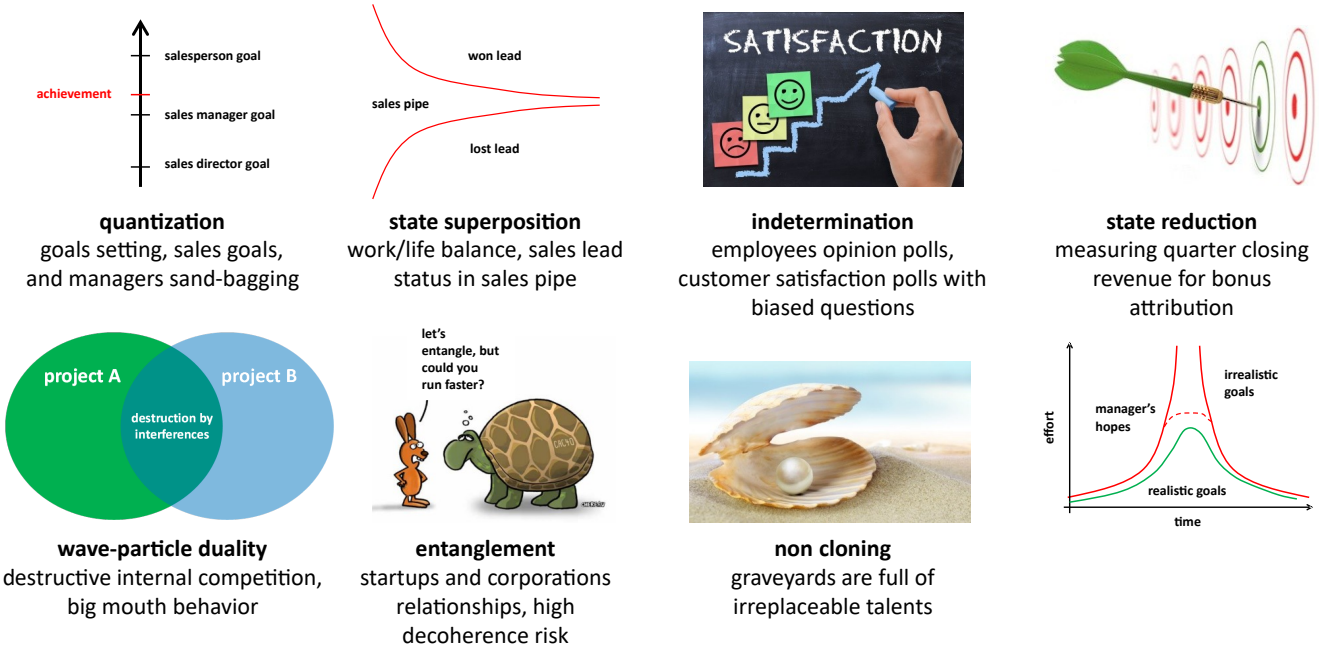


Figure 21: A useless framework for quantum management. © Olivier Ezratty, 2022.

Year	Hardware	Software	Ecosystem
2018	• IBM 20-qubit QPU. • IonQ 11-qubit QPU. • Preskill's NISQ concept. • IQM, Atom Computing, QuEra, Quantum Machines, Qblox creation.	• IBM open-source QASM. • Ewin Tang's QML tensorisation. • Quantum Error Mitigation. • Google Cirq. • DAQC.	• EU Quantum Flagship. • US NQIA launch. • Israel NQI. • Peak year in startup creation. • QED-C creation.
2019	• Google 53-qubit supremacy. • IBM Q System One. • Oxford Ionics, Nord Quantique creation. • Pasqal creation.	• Gidney Shor-2048 estimate. • ADAPT-VQE. • Amazon Braket. • Multiverse creation.	• UK quantum strategy renewal. • Russia Quantum Technologies Roadmap.
2020	• D-Wave Advantage. • Quantinuum 20-qubits QPU. • IBM, Google first roadmaps. • Alice&Bob, C12, Eleqtron creation. • Jiuzhang 1.0 GBS.	• Quantum kernel methods. • Algorithmiq, Classiq, ParityQC, Qedma creation.	• Germany's €2B quantum plan. • USA NQIA extension. • First India quantum plan.
2021	• IBM Eagle 127-qubit QPU. • Quantinuum creation. • PsiQuantum FBQC proposal. • First logical qubits. • Jiuzhang 2.0 GBS.	• Floquet Code. • XZZX surface code. • Kipu Quantum creation. • Nvidia cuQuantum.	• France NQS launch. • IonQ and Rigetti IPO. • QuiC consortium creation. • First English edition of this book.
2022	• Xanadu quantum advantage. • Diraq, Quobly, Planqc, Welinq creation.	• NIST PQC draft standards. • Nvidia CUDA-Quantum.	• Aspect-Clauser-Zeilinger Nobel laureates. • D-Wave IPO. • QEI launch.
2023	• QuEra logical qubits. • IBM Heron and Condor. • IBM quantum utility Nature paper. • Jiuzhang 3.0 GBS. • ETH superco QPU interconnect.	• VQE and QAOA refinements.	• India National Quantum Mission. • South Korea quantum plan.
2024	• Google Willow. • Origin Quantum Wukong. • Quantinuum H2 56-qubits QPU. • 6,100 controlled atoms at Caltech. • Qolab creation.	• FTQC advances. • FTQC vendor roadmaps. • Google DQI algorithm. • Zapata bankrupt. • LLMs getting used in quantum computing. • NIST PQC standards.	• UK NQCC inaugurated. • First QPUs delivered to EuroHPC. • PsiQuantum deal with Australia.
2025	• Microsoft Majorana-1. • IBM Nighthawk. • IBM 122-qubits GHZ state. • D-Wave Advantage 2. • Oxford Ionics acquisition by IonQ. • Equal1 and Quantum Motion full-stack QPUs. • Jiuzhang 4.0 GBS.	• D-Wave quantum advantage on Ising model. • Google Magic state cultivation. • IBM bivariate bicycle qLDPC code. • EU AI/quantum white paper. • Zapata back from the dead. • Google Echoes-OTOC experiments.	• EU Quantum Strategy. • DARPA QBI selection. • US NQIA renewal in the making. • PsiQuantum raises $1B. • Record funding year (>$2B WW). • Clarke-Devoret-Martinis Nobel laureates.

Table 2: Some key events in quantum computing since 2018. © Olivier Ezratty, November 2025.

Year	Hardware	Software	Ecosystem
2026	• More logical qubits experiments, like with Quantinuum Helios. • Oratomic creation and funding. • Microsoft Majorana-2. • Modular cryostats at Bluefors, Maybell Quantum and IBM.	• New QEC/FTQC architectures and resource estimations for breaking RSA-2048 and ECC-256 keys. Iceberg Quantum Pinnacle, Oratomic, Q-CTRL, Google, IonQ, and Quandela. • IBM "quantum advantage" claims with U. Chicago, Qedma and Algorithmiq. • Q-CTRL quantum advantage paper. • Accelerated PQC migration timelines.	• USA POTUS Quantum Executive Orders, Dept Commerce led $2B manufacturing investment and DoE's Quantum Genesis program and competition. • IBM's $10B 5-year quantum investment announcement. • France National Quantum Strategy renewal. • Infleqtion, Xanadu, Horizon Quantum, IQM, Quantinuum and Pasqal IPOs. • Another record funding year.

Table 3: Some key events in quantum computing in 2026. © Olivier Ezratty, September 2026.

Page intentionally left blank.

Page intentionally left blank.

le lab quantique