Quantum technologies and industry

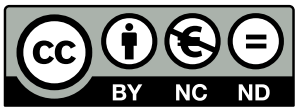
Kenneth Maussang

UNIVERSITÉ DE MONTPELLIER

Quantum technologies and industry

Kenneth MAUSSANG

Version du 25 janvier 2024



Contents

Chapter I

Quantum revolution(s)

1. Innovation and industry

1.1. Innovation strategies

From invention to innovation: market or technology driven?

An innovation strategy guides decisions on how resources are to be used to meet innovation objectives and thereby deliver value and competitive advantage. An innovation strategy identifies the technologies and markets that the company should better develop and exploit to create and capture value [18]. A strategy is nothing more than a commitment to a set of coherent, mutually reinforcing policies or behaviors aimed at achieving a specific competitive goal. Two visions that help guide a company's innovations are usually used: "technology push" and "market pull".

As stressed out by Bary P. Pisano in Harvard Business Review [43], lack of innovation strategy often results in frustrating pursuit in many companies, with frequent failure of innovation initiatives, despite massive investments of management time and money. Successful innovators such as Nokia, Yahoo or Hewlett-Packard have hard tome sustaining their performances.

Fig. I.1. The very first digital camera created by Steven Sasson in 1973. This prototype was the basis for the US patent issued on December 26th, 1978. `https://lens.blogs.nytimes.com/2015/08/12/kodaks-first-digital-moment/`

A striking example is the case of the company Kodak. Kodak was the world's largest photography company that pioneers the snapshot camera. It is best known for photographic film products. Kodak was founded by George Eastman and Henry A. Strong on September 4, 1888. During most of the 20th century, Kodak held a dominant position in photographic film. Kodak began to struggle financially in the late 1990s, as a result of the decline in sales of photographic film and its slowness in transitioning to digital photography. Ironically, Kodak as developed the first digital camera in 1975. The first prototype was designed by Steven Sasson, a 24 years old engineer in charge to see whether there was any practical use for a charged coupled device (C.C.D.), which had been invented a few years earlier. In 1989, he created the first modern digital single-lens reflex camera, with 1.2 megapixel sensor, and used image compression and memory cards. **But Kodak's marketing department was not interested in it. Steven Sasson was told they could sell the camera, but wouldn't — because it would eat away at the company's film sales.**

So digital cameras have been developed by other players, and fortunately the invention had been protected with a US patent, which helped Kodak to earn billions of dollars of royalties [1]. But the patent expired in USA in 2007. Of course, Kodak has begun to focus on digital photography and digital printing in the late 1990s, as a part of a turnaround strategy. But it fully embraced that market until it was too late: after an attempt to generate rev-

1. President Barack Obama awarded Steven Sasson the National Medal of Technology and Innovation at a 2009 White House ceremony.

enues through aggressive patent litigation, Kodak filed for bankruptcy in 2012. Kodak sold many of its patents for approximately $ 525 millions to a group of companies (including Apple, Google, Facebook, Amazon, Microsoft, Samsung, Adobe Systems, and HTC). But the company still exists: Kodak has announced in September 2013 that it has emerged from Chapter 11 Bankruptcy Protection.

Technology push

Technology Push is when research and development in new technology, drives the development of new products. In other words, **research labs are working on technological developments without any specific issues to solve on the market, but aim at creating new objects. This new objets will found their market (or not) afterwards**. Technology Push usually does not involve market research. It tends to start with a company developing an innovative technology and applying it to a product. The company then markets the product. **It's usually the situation when innovation occurs from fundamental research in an academic laboratory.**

Example of technology push good: touch screens

Touch Screen technology appeared as published research by E.A. Johnson [2] at the Royal Radar Establishment, a research center in United Kingdom, in the mid 1960s. This discovery has been published in a research journal entitled *Electronics Letters* [29]. In the 1980s, Hewlett Packard introduced a touch screen computer. In 1993 hand writing recognition is introduced by Apple's Newton personal digital assistant (PDA). In 1996, Palm introduced its Pilot Series of personal assistant. A milestone has been reached with the development of smartphones, in which touch screen becomes a central element, followed by tablets. If today a touch screen is a natural objet in our all-day life, nobody was asking for a touch screen in the 1960s! That is why it is a technology push innovation, because the technology has created a market without any demand from consumers.

The first research paper on the topic (1965) has been published more than forty years before its final most common application, with the presentation of the first smartphone in 2007.

Market pull

The term "Market Pull" refers to the need for a new product or a solution to an identified problem. In a sense, **the consumer require a technological solution to a problem he has, and companies are developing a technology with a well-defined goal: solving this problem**. The need is identified with a market analysis or by potential customers. Then, a product or an ensemble of products are developed, in order to solve the market's need identified. Market pull could be initiated by the claim of consumers for improvements to existing products (for example, cars with lower gasoline consumption and/or less polluant emission). Consumers groups or professional association may have a central role in market pull innovation, testing a concept design or an existing product. For example, in automotive industry, concept cars and automotive courses, such as Formula 1, are important in the innovation process.

Example of market pull good: the digital camera

Twenty years ago, there was a "market" requirement for a camera that could take endless photographs, that could be viewed almost immediately. A premise of solution was the invention of Polaroid camera, but remains limited in number of pictures. A milestone has been reached when the first digital cameras have been developed. Making them smaller and easier to use, it has permit to revolutionize the camera market, and also photo editing software market. There was a real rush of people who are taking photos everywhere and processing them, and so the market really was telling companies that what we need is an easy way to handle all these digital photos with smaller and more efficient devices. And so the market did respond to that. Market pull led to electronics companies developing digital cameras, miniature digital storage, processing power and improved battery performance was available. Market pull ensured that photo editing software also developed, in parallel with the development of digital camera technology.

2. Detailed history of touch screens may be found at the following address: `https://arstechnica.com/gadgets/2013/04/from-touch-displays-to-the-surface-a-brief-history-of-touchscreen-technology/`

1.2. *The Structure of Scientific Revolutions* - thinking out of the box

The Structure of Scientific Revolutions is a book written by the philosopher Thomas S. Kuhn in 1962. Kuhn challenged the then prevailing view of progress in "normal science". Normal scientific progress was viewed as "development-by-accumulation" of accepted facts and theories. Kuhn argued for an episodic model in which periods of such conceptual continuity in normal science were interrupted by periods of **revolutionary science**. The discovery of "anomalies" during revolutions in science leads to new paradigms. New paradigms then ask new questions of old data, move beyond the mere "puzzle-solving" of the previous paradigm, change the rules of the game and the "map" directing new research.

Kuhn explains the process of scientific change as the result of various phases of paradigm change.

Phase 1: pre-paradigm At the beginning, there is no consensus on any particular, well constructed, theory. This phase is characterized by several incompatible and incomplete theories.

Phase 2: normal science In this phase, puzzles are solved within the context of the dominant paradigm. As long as there is consensus within the discipline, normal science continues. Over time, progress in normal science may reveal anomalies, facts that are difficult to explain within the context of the existing paradigm. While usually these anomalies are resolved, in some cases they may accumulate to the point where normal science becomes difficult and where weaknesses in the old paradigm are revealed.

Phase 3: crisis If the paradigm proves chronically unable to account for anomalies, the community enters a crisis period. Crises are often resolved within the context of normal science. However, after significant efforts of normal science within a paradigm fail, science may enter the next phase.

Phase 4: scientific revolution A scientific revolution consists in a paradigm shift, a phase in which the underlying assumptions of the field are reexamined and a new paradigm is established.

Phase 5: post-revolution The new paradigm's dominance is established and so scientists return to normal science, solving puzzles within the new paradigm.

A science may go through these cycles repeatedly, though Kuhn notes that it is a good thing for science that such shifts do not occur often or easily.

The first quantum revolution analyzed further might been seen as an example of Thomas Kuhn's scheme of science progress.

1.3. Innovation in industry

Sustaining innovation

A sustaining innovation is an innovation that does not significantly affect existing markets. It may be either evolutionary or revolutionary.

An evolutionary innovation improves a product in an existing market in ways expected by the market itself (*i.e.* the customers). For example, it might be innovation for better fuel injection in gasoline motors, in order to decrease consumption and obtain better performances.

A revolutionary sustaining innovation is unexpected by the market, but nevertheless does not affect existing markets. For example, the first cars developed in the end of the 19th century were luxury goods, very expensive. So most people could offer themself such a luxury item and only few of them were sold.

Disruptive innovation

In business theory, a disruptive innovation is an innovation that creates a new market and value network and eventually disrupts an existing market and value network. Not all innovations are disruptive, even if they are revolutionary. For example, the first automobiles in the late 19th century were not a disruptive innovation, because early automobiles were expensive luxury items that did not disrupt the market for horse-drawn vehicles. The market for transportation essentially remained intact until the debut of the lower-priced Ford Model T in 1908. The *mass-produced automobile was a disruptive innovation*, because it changed the transportation market, whereas the first thirty years of automobiles did not.

Disruptive innovations tend to be produced by outsiders and entrepreneurs in startups, rather than existing market-leading companies. The business environment of market leaders does not allow them to pursue disruptive innovations when they first arise, because they are not profitable enough at first and because their development can take scarce resources away from sustaining innovations (which are needed to compete against current competition).

A disruptive process can take longer to develop than by the conventional approach and the risk associated to it is higher than the other more incremental or evolutionary forms of innovations, but once it is deployed in the market, it achieves a much faster penetration and higher degree of impact on the established markets.

A disruptive innovation disrupted a market, not necessarily with a novel technology, but with a alternative approach of the market. But disruptive innovation might appears thanks to a novel technology. For example, CDs ans USB flash drivers have disrupted the market of data storage which was dominated by floppy disk. Writable CDs have been developed photosensitive polymers while USB sticks have been developed based on the discovery of giant magnetoresistance (GMR), discovered in 1988 by Albert Fert and Peter Grünberg [3], awarded Nobel Prize in 2007 for their contribution to that topic.

Disruptive innovations can hurt successful, well-managed companies that are responsive to their customers and have excellent research and development. These companies tend to ignore the markets most susceptible to disruptive innovations, because the markets have very tight profit margins and are too small to provide a good growth rate to an established (sizable) firm. Disruptive technology provides an example of an instance when the common business-world advice to "focus on the customer" can be strategically counterproductive. For example, text message (SMS) were not a demand of customers: nobody wanted to write short messages with a 9 touches keyboard. But it was a success.

Disruptive technologies

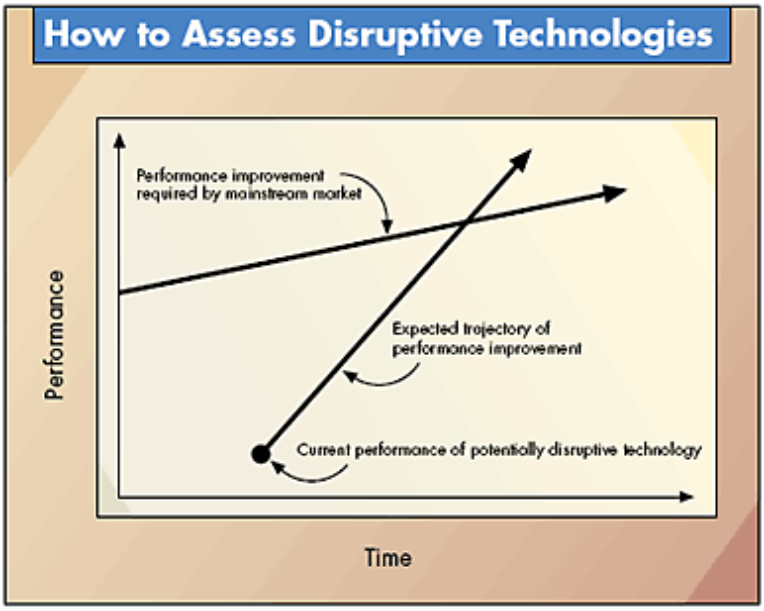


Fig. I.2. Role of disruptive technologies in innovation, especially the increase in performances. `https://hbr.org/1995/01/disruptive-technologies-catching-the-wave`

Technology always evolves: it starts, develops, persists, mutates, stagnates, and declines. When a new high-technology core emerges, it challenges existing technologies which are forced to coexists with it. A Technology Support Net (TSN) is the required physical, energy, information, legal and cultural structures that support the development of technology core. When a new technology emerges, it fits into the existing TSNs, then high-technologies becomes regular technologies, fitting the same TSN. This established technology then resists being interrupted by a technological mutation; then new high technology appears and the cycle is repeated. This cycle is somewhat similar to Thomas Kuhn's scheme of scientific revolution. The technology has impact on the job market, shaping the relative demand for certain skills in labor markets [4].

In his article *Disruptive Technologies: Catching the Wave* [9], published in 1995 in Harvard Business Review, Clayton M. Christensen as introduced the notion of *disruptive technologies*. The article is aimed at management executives who make the funding or purchasing decisions in companies, rather

3. `https://en.wikipedia.org/wiki/Giant_magnetoresistance`
4. World development report: The changing nature of work.
`http://documents.worldbank.org/curated/en/816281518818814423/pdf/2019-WDR-Report.pdf`

than the research community. He has been developed the concept further in his book The Innovator's Dilemma, published in 1997. In that book, he studied the case of the disk drive industry and the excavating equipment industry. In that book, Christensen recognized that few technologies are intrinsically disruptive or sustaining in character; rather, **it is the business model that the technology enables that creates the disruptive impact.** Christensen's evolution of view from a technological focus to a business-modelling focus is central to understanding the evolution of business at the market or industry level. The concept of disruptive technology continues a long tradition of identifying radical technical change in the study of innovation by economists, and the development of tools for its management at a firm or policy level.

In keeping with the insight that what matters economically is the business model, not the technological sophistication itself, Christensen's theory explains why many disruptive innovations are not "advanced technologies", which a default hypothesis would lead one to expect. Rather, they are often novel combinations of existing off-the-shelf components, applied cleverly to a small, fledgling value network.

In 2009, Milan Zeleny (an american economist) described high technology as disruptive technology and raised the question of what is being disrupted. According to Zeleny, the support network of high technology is disrupted [57]. For example, introducing electric cars disrupts the support network for gasoline cars (network of gas and service stations). On a long term timescale, disruptive technologies upgrades or replaces the outdated support network of the established regular technology. Consequently, **a disruptive technology may dramatically transforms some industries through its requisite its own TSN.** This risk on established companies has been pointed out by Joseph L. Bower, Professor of Business Administration at Harvard Business School, in the reference [21]

> *When the technology that has the potential for revolutionizing an industry emerges, established companies typically see it as unattractive: it's not something their mainstream customers want, and its projected profit margins aren't sufficient to cover big-company cost structure. As a result, the new technology tends to get ignored in favor of what's currently popular with the best customers. But then another company steps in to bring the innovation to a new market. Once the disruptive technology becomes established there, smaller-scale innovation rapidly raise the technology's performance on attributes that mainstream customers' value.*

For example, electric cars preceded the gasoline automobile by decades and are now turning to replace the traditional gasoline automobile. Another historical example is AC electricity. The first electrical generators were delivering DC current. Thomas Edison has developed his company, General Electric, on this technology. However, it has strong limitation especially of electrical energy transportation. Transport line were limited to only few kilometers, limited by ohmic losses and voltage reduction with distance. Moreover, different networks were used depending on the voltage required by the device connected (it was not possible to change the voltage value). Nikola Tesla was working for General Electric and proposed a novel type of technology based on AC current (AC motor and AC voltage generator). Tesla proposed in 1884 to Edison to use AC current instead DC current in order to solve issues of the later one. But Edison refused, because Tesla's solution would require to rethink completely its industrial installation, including the electrical network and power-generating plant. Moreover, if Edison adopts Tesla's solution, he would have renounced to the royalties he got from his patents on DC current technologies. He also argued that AC current transportation would be a more costly infrastructure. Indeed, transportation of DC current requires 3 cables while AC current transportation requires 5 cables. For Edison, the cost of additional copper cables would increase significantly the cost of the AC current infrastructure. Finally, the implementation of a distribution system using alternating current requires very advanced knowledge in physics and mathematics, knowledge that Thomas Edison did not have. Edison refused to adopt Tesla's solution, but promised him a reward of \$50,000 [5] if he succeeded in developing a reliable AC system. After several months of work, he presented Thomas Edison with an alternative generator with improved performance. Tesla a deposed the US patent #US359748A entitled *Dynamo-electric machine* in 1886 and the US patent #US382279A entitled *Electro-Magnetic Motor* in 1888. But when Tesla asked for his reward, he was told by Edison that it was a joke and that there was no reward. Rather than \$50,000, he offered him a raise of \$10 a week. Tesla resigned and founded his company, the *Tesla Electric Light Company*. Under

5. equivalent to actual M\$1.5 today!

pressure from investors, he resigned from the company he founded, only two years later, losing the savings he had invested but also losing the use of his patents. He was then hired by George Westinghouse to work in his electrical equipment business. Then, General Electric adopted the AC current solution due to its technological superiority and its benefits in term of performances.

1.4. Gartner's hype cycle

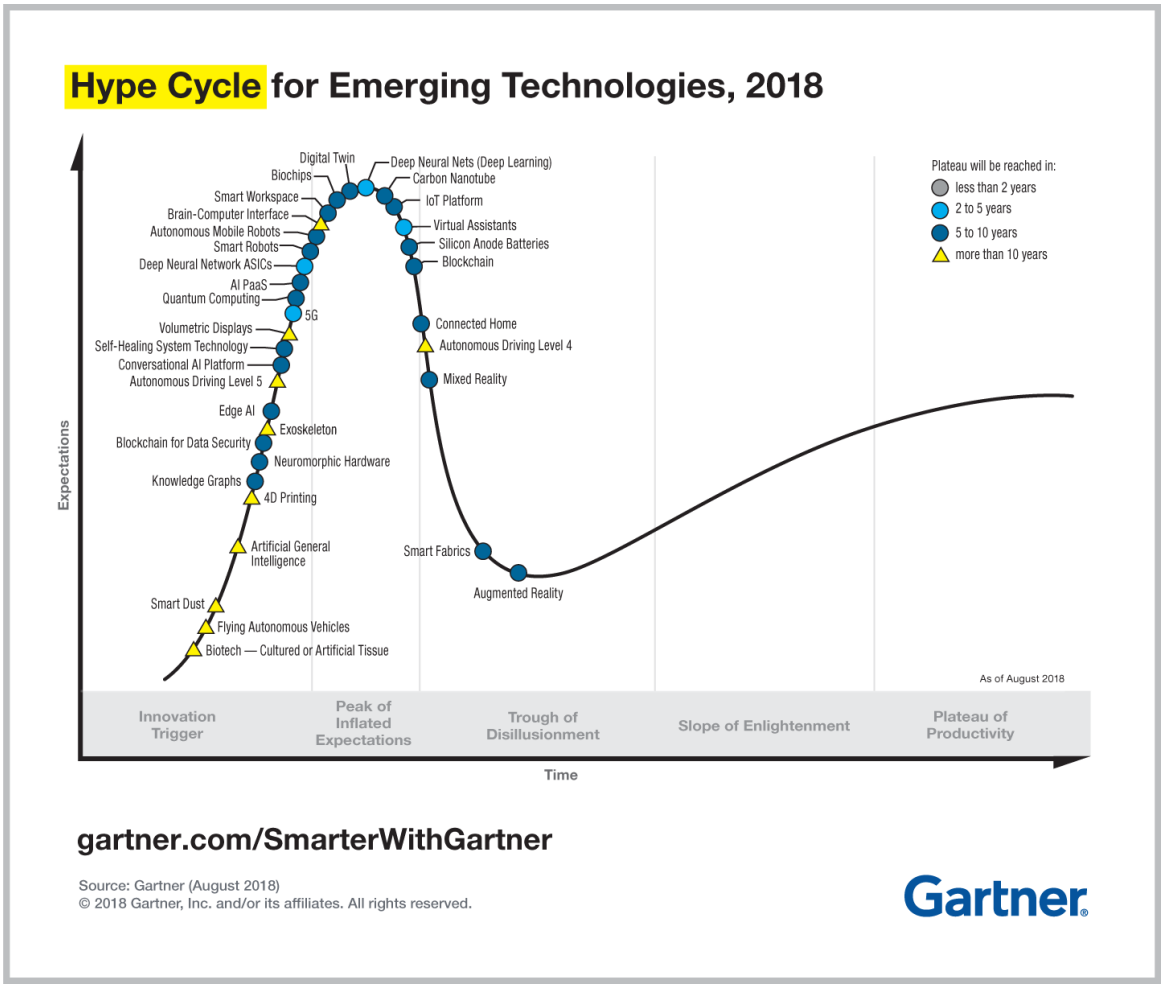


Fig. I.3. Gartner's hype cycle 2018. Quantum computers are in the end of the technology trigger phase.

Gartner Inc. is a private company is a global research and advisory firm which provides information and advice in IT, finance, human ressources, customer service, marketing ,sales and supply chain. Gartner provide every year a *hype cycle* of emerging technologies, *i.e.* a graphical and conceptual representation of the maturity of emerging technologies through five phases [6]

1. **Technology Trigger:** a potential technology breakthrough kicks things off. Early proof-of-concept stories and media interest trigger significant publicity. Often no usable products exist and commercial viability is unproven.
2. **Peak of Inflated Expectations:** early publicity produces a number of success stories — often accompanied by scores of failures. Some companies take action; many do not.
3. **Trough of Disillusionment:** interest wanes as experiments and implementations fail to deliver. Producers of the technology shake out or fail. Investments continue only if the surviving providers improve their products to the satisfaction of early adopters.

6. description extracted from `https://www.gartner.com/en/research/methodologies/gartner-hype-cycle`

4. **Slope of Enlightenment:** more instances of how the technology can benefit the enterprise start to crystallize and become more widely understood. Second- and third-generation products appear from technology providers. More enterprises fund pilots; conservative companies remain cautious.
5. **Plateau of Productivity:** mainstream adoption starts to take off. Criteria for assessing provider viability are more clearly defined. The technology's broad market applicability and relevance are clearly paying off.

The 2018 Gartner's hype cycle has entering phase 2, the peak of inflated expectations (Fig. I.3). It results in important invest in that technology and appearance of several company involved in hardware and software development.

2. First quantum revolution

2.1. Quantum mechanics: half a century of elaboration

Until the 20th century, so-called classical physics has permitted to provide an ensemble of theory and models that explained almost all physical phenomena observed. But two remaining problems were still unsolved: the black-body radiation spectrum and the discrete radiation spectrum of light source made of electrical discharge in atomic vapor. Several models were proposed in order to try to explain these phenomena but with severe difficulties to provide a general theory. A paradigm shift has been introduced by the construction of quantum mechanics that has permit to understand those phenomena in a complete different formalism. This new theory has offered a novel vision of matter and consequently has resulted in many scientific and technological developments.

However, one has always to remind that the construction of a science takes decades. Indeed, for quantum mechanics, it started in 1877 when Ludwig Boltzmann suggested that the energy states of a system might be discrete. From an experimental point of view, a second milestone has been reached when Heinrich Hertz discovered in 1887 the photoelectric effect, where light might cause electrons to be ejected from metals only if the frequency of the electromagnetic wave is high enough. It has been followed in 1900 by the quantum hypothesis by Max Planck, which assumes that any atomic system emits radiation with an energy that is an integer discrete number of 'quanta', *i.e.* energy unit ε. These quantas ε are proportionnal to the frequency ν of the radiation, such that

$$\varepsilon = h\nu,$$

where h is a universal constant called Planck's constant. This model has permitted to derive a formula for the observed frequency dependence of the energy emitted by a black body, called Planck's law, that included a Boltzmann distribution

$$I(\nu,T) = \frac{2h\nu^3}{c^2}\frac{1}{e^{\frac{h\nu}{k_BT}}},$$

where $I(\nu,T)$ is the surfacic power emitted in the normal direction per unit solid angle per unit frequency for a black body at temperature T, h Planck's constant, c speed of light, k_B Boltzmann constant and ν the radiation frequency. Then, In 1905, Albert Einstein explained the photoelectric effect using Planck's quantum hypothesis that light is made of individual particles, each one having an energy $h\nu$. Albert Einstein has been awarded the Nobel Prize of physics 1921 "*for his services to Theoretical Physics, and especially for his discovery of the law of the photoelectric effect*". These particles have been then called *photons* in 1926 by Gilbert N. Lewis.

In 1913, Niels Bohr used Planck's quantum theory to calculate the magnetic moment of the electron (the magnetron), and explained the spectral lines of the hydrogen atom in his paper intituled *On the Constitution of Atoms and Molecules* [7].

However, despite they were successful, these theories were strictly phenomenological: there was no rigorous justification of the quantization of energy exchange.

In 1923, Louis de Broglie proposed another approach, in which he argues that particles can exhibit wave characteristics and waves may have particles behavior. His theory of matter waves basically introduced the notion of *wave-particle duality*. This theory has been elaborated for a single particle, derived initially from special relativity theory.

Building of modern quantum mechanics as started only in 1925, 48 years after Ludwig Boltzmann's quantization of energy levels. While Werner Heisenberg and Max Born developed matrix mechanics in 1925, Erwin Schrödinger invented simultaneously wave mechanics and the non-relativistic Schrödinger equation as an approximation of de Broglie's theory general case. Heisenberg formulated his uncertainty principle in 1927, while the Copenhagen interpretation of quantum mechanics started to shape. In 1928, Paul Dirac derived its equation, so-called Dirac equation, describing the wavefunction of an electron in the relativistic limit, and unified quantum mechanics with special relativity. He also introduced the bra-ket notation.

It took almost half a century from initial model to initiate really the construction of a new theory called *quantum mechanics*, which will result in a scientific revolution in the sense of Thomas Kuhn. This scientific revolution has resulted in many technological development during the second half of the 20th century, referred as the **first quantum revolution**.

2.2. First quantum revolution

The first quantum revolution refers to all technological innovations which have resulted from quantum mechanics theories. Most of those innovations hade resulted from a major paradigm shift introduced by quantum mechanics: the wave-particle duality.

The wave nature of matter

Matter may behave has a wave (*i.e.* the wavefunction). The wave nature of matter is particularly important when one describes electrons dynamics in atoms or solids. The quantum description of electrons in atoms, especially the atom of hydrogen, has permits to explain the discrete spectrum of light emitted by excited atomic vapor, and resulted in the concept of atomic and molecular orbitals. Quantum mechanics has then offer the appropriate formalism to describe atoms and molecules structure, and consequently material structures and electronic properties. In particular, it has results in band theory of matter and more specifically the physics of semiconductors. Then, semiconductors have permit the development of integrated circuits, and therefore all the modern electronic has been developed thanks to quantum mechanics. In particular, applications of electronics have expanded dramatically since the first transistor was invented in 1948. It has resulted in **the industry of semiconductors**, which has impact almost all sector of goods thanks to microelectronics and miniaturization. The latter has permitted the development of computers, and the development of automation. Productivity in industry has been increased thanks to the use of computer, automation and robots: this evolution is called **industry 3.0** (or third industrial revolution).

More recently, the development of IoT (*Internet of Things*) results from the interconnexion between Internet and objects. The development of internet results from the progress of telecommunications technologies. WiFi and wireless communications used in IoT are based on high frequencies (GHz typically) semiconductors. These technologies has initiate the emergence of **industry 4.0**, which is a trend towards automation and data exchange in manufactoring technologies and processes which include cyber-physical systems (CPS), IoT, industrial IoT (IIoT), cloud computing, cognitive computing and artificial intelligence.

The particle nature of light

On the other side, wave-particle duality has permit to think the concept of photon for the description of light, with a better description of light-matter interaction. Two majors inventions have resulted from this concept:

— LASER sources of light;

— photonic devices.

A major technological breakthrough is the development of laser sources of light, continuous-wave (CW) or pulsed ones. It has permit the development of light source of high power, high directivity and high coherence. Lasers have wide applications in industry [7]:

— alignement;

— laser velocimetry;

7. `https://en.wikipedia.org/wiki/List_of_laser_applications`

— distance measurements;
— profilometer (surface inspection);
— scientific lasers for spectroscopy;
— multiphotonic microscopy;
— laser soldering, melting or sublimation (fast marking);
— heat treatment;
— LIDAR;
— laser printer;
— laser scanner;
— military applications (guidance, disorientation, target designator, firearms, defensive countermeasures);
— medical applications (eye's surgery, dermatology);
— CD, DVD;
— ...

Photonic devices are components for creating, manipulating or detecting light. This can include laser diodes, light-emitting diodes, solar and photovoltaic cells, displays and optical amplifiers. Other examples are devices for modulating a beam of light and for combining and separating beams of light of different wavelength.

Applications of photonics included all areas from everyday life to the most advanced science [8], *e.g.*

— light detection;
— lighting;
— telecommunications;
— information processing;
— photonic computing;
— metrology;
— spectroscopy;
— holography;
— medicine (endoscopy, health monitoring);
— art diagnostics (involving InfraRed Reflectography, Xrays, UltraViolet fluorescence, XRF);
— agriculture;
— robotics;
— aviation (photonic gyroscopes);
— military applications (IR sensors, command and control, navigation, search and rescue, mine laying and detection);
— solar cells and photovoltaic generation of electricity;
— ...

2.3. An example: the smartphone

A smartphone is an interesting example to illustrate the impact of the first quantum revolution on our all-day-life.

Materials

Quantum mechanics explains the structure of atoms, molecules and materials. Smartphones are made out of semiconductors, which properties are explained by quantum mechanics. Electronics inside requires elements such as silicon, phosphorous, gallium, arsenic, antimony and indium. Mechanical elements (for acoustic functions) are made out of dysprosium, praseodymium, neodymium, boron and iron. The packaging itself is made out of aluminium and AlSi glass. The screen is made of Indium Oxide and liquid crystal. Finally, battery are made out of lithium, cobalt, oxygen, carbon and aluminium. All those elements have been development in materials which properties have been understand thanks to quantum mechanics.

8. `https://en.wikipedia.org/wiki/Photonics`

Phases

An other contribution of quantum mechanics consists in a better understanding of phases transitions in material (ferromagnetic, ferroelectric, liquid crystal,...). Better understand of phases transistions have opened the way of technological development exploiting them for application, such as liquid crystal display for screens, or magnetic memories in computers.

If one considers a smartphone, such phases transitions are present in almost every part of it. Indeed, electronics is made of material that might be either semiconductor, insulator or conductor. The packaging is made out of conductor and glass. The battery is made of electrolyte, insulator and conductor. The screen is made of transparent conductor and liquid crystal. Acoustic elements are made out of ferromagnetic and ferroelectric.

Miniaturization of devices

The disruptive innovation proposed by Apple in 2007 with the first smartphone relies on combining several devices in a single object: a phone, a camera, a music player, an agenda,... If the innovation relies in this paradigm shift, it has been possible only because all those devices have been miniaturized. This miniaturization results essentially from progress in semiconductors technologies and photonics.

The smartphone might be seen as a small computer with a processor, memory and wireless emitters/recievers. Technological progress in semiconductor industry has permitted to decrease severely transistor size (Moore's law) and permit to obtain miniaturized chips with enough calculation ability for a smartphone. Optical elements such as camera ou LED flash light are only few millimeter size now. The display is governed by miniaturized LCD display (liquid crystal), with tactile ability thanks to microfabrication.

Fig. 1: Smartphone sensors.

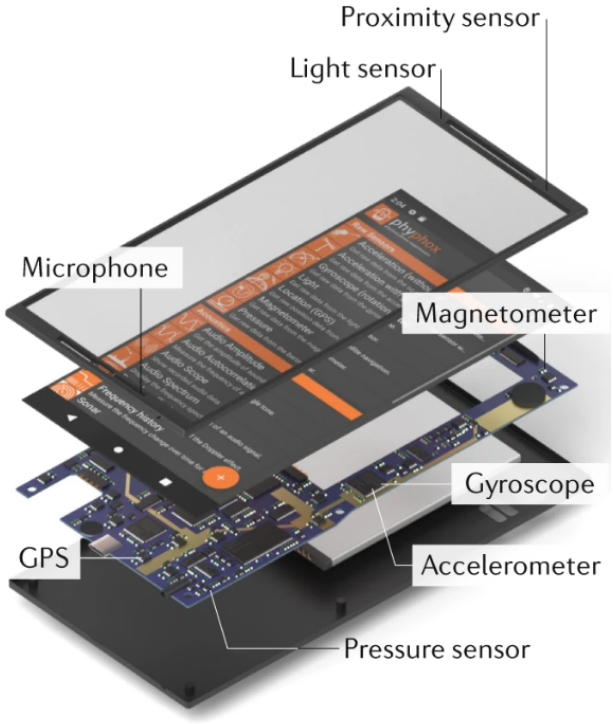


Fig. I.4. Anatomy of a modern smartphone. Extracted from [49].

Such miniaturization has been predicted by Richard Feynman, in his 1959 talk entitled "There's Plenty of Room at the Bottom" (delivered more than 50 years ago) [16]. Feynman proposed shrinking computing devices toward their physical limits, where "wires should be 10 or 100 atoms in diameter". Several devices have been reported with sizes lower than 15 nm, which is to say, with wires at Feynman's 100-atom scale. When Feynman spoke, a single computer could fill a room. Feynman suggested that focused electron beams could write nanoscale features on a surface; this is now called "e-beam lithography". He pointed to complex, active, nanoscale biological mechanisms as an inspiration for nanoscale technology; these have become the basis of what is called "biotechnology", which has delivered what are in some ways the most advanced nanotechnologies developed to date. **Feynman was the first to outline a world of technologies that would work and build at the ultimate, atomic scale.** He viewed this world from a top-down perspective, as the ultimate frontier for miniaturization

This ultimate atomic scale has permit to initiate the second quantum revolution.

3. Second quantum revolution

3.1. Quantum engineering

In the 20th century quantum mechanics revealed the secrets of the nature at atomic scales. Then we used this knowledge do design some classical machines either novel or with significantly higher efficiency in compare to their old ancestor. In the 21st century, we are going to make quantum machines, complex systems governed by the laws of quantum physics.

— Miniaturization is the dominant trend in modern technology. The electronic, optical and mechanical devices are reaching to the length scales that need design based on quantum principles.
— The principles of quantum mechanics offer the promise of exceptional performance over what classical physics has offered to us.

As a consequence, technologies are oriented toward systems so small that it requires to deal and to control quantum effects. Furthermore, it opens the possibility to fully exploit the quantum strangeness, with the development of individual quantum systems. **This is the second quantum revolution** [14]. The fundamental difference with the first quantum revolution relies in the manipulation of individual quantum systems. It permits to fully exploits two majors aspects of quantum effects that were not in the first quantum revolution:

— entanglement (*i.e.* fundamental quantum correlations between states);
— quantum state superposition.

This second quantum revolution is expected be responsible for most of the key physical technological advances for the 21st century [14]. Such technologies are then called **quantum technologies**. Quantum technology allows us to organise and control the components of a complex system governed by the laws of quantum physics. This is in contrast to conventional technology which can be understood within the framework of classical mechanics (including transistor developed in the context of the first quantum revolution). There are two imperatives driving quantum technology. The first is practical : the dominant trend in a century of technological innovation is miniaturisation. To build devices on a smaller and smaller scale. Ultimately this will deliver devices at length scales of nanometres and action scales approaching Planck's constant. At that point design must be based on quantum principles. The second imperative is more fundamental. The principles of quantum mechanics appear to offer the promise of a vastly improved performance over what can be achieved within a classical framework.

In the **first quantum revolution**, we used quantum mechanics to understand what already existed. We could explain the periodic table, but not design and build our own atoms. We could explain how metals and semiconductors behaved, but not do much to manipulate that behavior. The difference between science and technology is the ability to engineer your surroundings to your own ends, and not just explain them.

In the **second quantum revolution**, we are designing quantum object with expected properties that results from quantum mechanics law, for our own purpose. For example, in addition to explaining the periodic table, we can make new artificial atoms—quantum dots and excitons — which we can engineer to have electronic and optical properties of our own choosing. These new man-made quantum states have novel properties of sensitivity and nonlocal correlation that have wide applications to the development of computers, communications systems, sensors and compact metrological devices. Those applications are so-called quantum technologies. While quantum mechanics is a mature science, all its direct application have resulted in the first quantum revolution. Nowadays, quantum engineering as a technology is now emerging on its own right. Quantum engineering is the key feature of the development of quantum technologies in this second quantum revolution.

3.2. Quantum technologies

Quantum technologies is an emerging field of physics and engineering, which relies on the exploitation of quantum physics law on individual quantum systems. Quantum Technologies result from our ability to detect and manipulate single quantum objects, such as atoms, photons or electrons. They represent an intermediate step in the second quantum revolution, between academic fundamental research activities and industrial products. It is about creating practical applications such as quantum computing, quantum sensors, quantum cryptography, quantum simulation, quantum metrology and quantum imaging—based on properties of quan-

tum mechanics, especially quantum entanglement, quantum superposition and quantum tunnelling. Therefore, their development inherently involve cooperation between academic labs and industrial players.

Chapter II

Quantum technologies

Quantum technologies might be subdivided in four type of applications
— quantum computers;
— quantum simulators;
— quantum communications;
— quantum sensors and metrology.

1. Quantum technologies and the second quantum revolution

1.1. Quantum computers

Quantum computation is among the most far-reaching and challenging of quantum technologies. Based on quantum bits that can be zero and one at the same time and instantaneous correlations across the device, a quantum computer acts as a massive parallel device with an exponentially large number of computations taking place at the same time. A quantum computer has the ability to process information contained in qubits for quantum calculations, thanks to quantum algorithms. Some quantum algorithms achieved on a quantum computer are predicted to be significantly faster than even the largest classical computer available today. There already exist many algorithms that take advantage of this power and that will allow us to address problems that even the most powerful classical supercomputers would never solve.

Quantum computers are expected to have a number of significant applications in computing fields such as optimization and machine learning. The most famous application is Shor's algorithm, which can be used to factorise large numbers which are mathematically important to secure data transmission (RSA protocol for encryption).

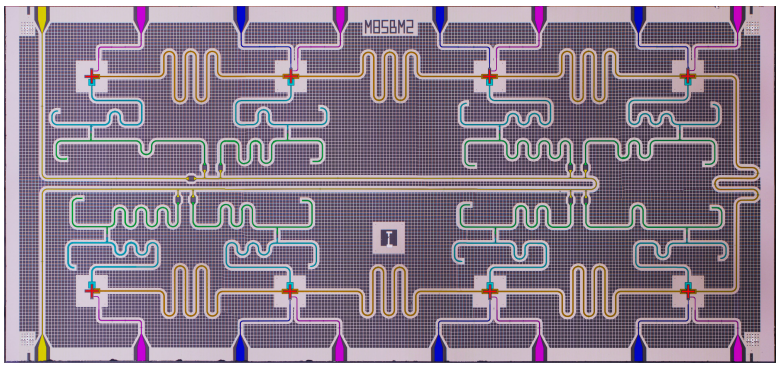


Fig. II.1. 8-Qubit superconducting quantum processor fabricated at ETH Zurich. Image extracted from `https://qt.eu/discover/technology/`

Several quantum computers prototypes have been demonstrated over the last two decades. The most advanced ones relies either on trapped ions and superconducting circuits for implementation of qubits. Typically 10-15 qubits have already run basic algorithms and protocols. More recently, industrial players have reported chips within the 50-72 qubits range (IBM, Rigetti, Intel and Google), all of them based on superconducting qubits.

Other implementations of qubits are also investigated, either in solid-state systems (electrons spins in semiconductors, nuclear spins in solids, Majorana zero modes) or atomic and optical systems (nuclear spins in molecules, hyperfine states and Rydberg states in atoms).

The end of Moore's law, referring to the limit that transistor and processor power seems to reach with standard silicon technologies, make industrial players show interest in quantum computing as a disruptive technology that could outperform standard silicon transistor technology for computers. Then, most of global IT companies have been taking an increased interest in quantum computing in the last decade, but also start-ups and GAFAM

like Google, Microsoft and Amazon [1]. Recent advances in quantum computer design and development, error correction codes, fault-tolerant algorithms and novel fabrication process are promising milestones towards the achievement with a couple of decades of a prototype that could outperform classical computation in some applications.

Nowadays, with these recent developments, the real question is not if there will be a quantum computer, but which market will profit of it within which business model (including the hardware production, *i.e.* which company will fabricate it). Companies like Intel, HRL laboratories and NTT have chosen to develop spin qubits in semiconductors. IBM, Google, Rigetti and Intel are developing superconducting qubits chips, that are already integrated so that simple algorithms have been demonstrated experimentally. The most powerful chip available and integrated by IBM is made out of 53 qubits, while Google reported a 72 qubits chips.

The company D-wave is producting a superconducting quantum annealer, which does not permit implementation of quantum algorithms but could be used for optimisation problems. Microsoft has chosen an audacious strategy, working on the development of topological qubits, which could benefit of topological protection and consequently be more robust against decoherence. Lockheed Martin and Infineon companies are supporting research with trapped ions as qubits, manipulated with lasers beams.

1.2. Quantum simulators

Nowadays, industry uses supercomputers facilities in their R&D development. They are particulary useful in the context of complex objects design such as aircrafts, buildings or cars. By contrast, simulating behaviors at microscopic remains an important challenges where supercomputers might be overwhelmed. One is currently not able yet to predict of a material composed of few hundred of atoms will conduct electricity or behave as a magnet. One can not yet predict if a chemical reaction will take place between complex molecules. But all those small systems are fundamentally quantum systems. In a lecture entitled *Simulating Physics with Computers* [17], Professor Richard Feynman talked about why physicists need computers, and what they require of these devices [2]. But difficulties appears when one want to simulate a large quantum system such as a molecule with a classical computer governed by classical physics. If physics is too hard for classical computers, then build a physical computer that exploits that power, *i.e.* a quantum computer. R. Feynman noticed also that *"it does seem to be true that all various field theories have the same kind of behavior, and can be simulated every way."* And he concluded that *"Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."* Quantum simulators are a subclass of quantum computers, less sensitive to decoherence and environmental noise. They are dedicated to physical simulation of systems. Quantum simulators based on the laws of quantum physics will allow us to overcome the shortcomings of supercomputers and to simulate materials or chemical compounds, as well as to solve equations in other areas, like high-energy physics. Quantum simulators can be viewed as analog versions of quantum computers, dedicated to reproducing the behaviour of materials where quantum phenomena arise and give rise to their properties (at low temperature or for chemical reactions). Their main advantage over all-purpose quantum computers is that quantum simulators

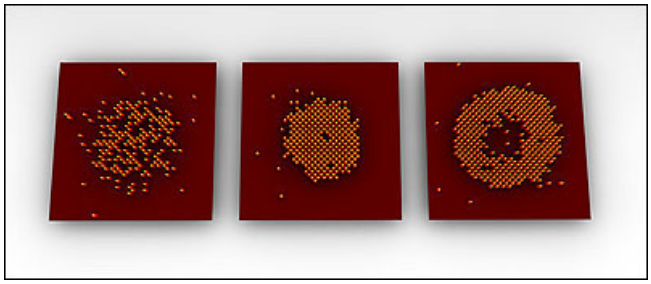


Fig. II.2. Single atom resolution microscope that permits to accesss directly to information of an atomic system at single atom level. Measured atom distribution of an ultracold quantum gas held in a two-dimensional crystal of light for the two distinct quantum phases of a Bose-Einstein condensate (BEC) (left) and Mott insulators with increasing particle numbers (middle & right). Image from Immanuel Bloch's group at MPQ Munich. Extracted from `https://www.photonics.com/Quantum_Particles_in_Perfect_Order_/a43862`

1. Amazon proposes a cloud access to quantum computer facilities through AWS.
2. `http://physics.whu.edu.cn/dfiles/wenjian/1_00_QIC_Feynman.pdf`

do not require complete control of each individual component, and thus are simpler to build and more tolerant to noise.

Several quantum simulators are under development, including ultracold atoms in optical lattices (Fig. II.2), trapped ions, arrays of superconducting qubits or of quantum dots and photons. First prototypes have already been able to perform simulations on specific problems beyond than what is possible with current supercomputers. Quantum simulators are expected to impact deeply material science, and for instance help in the understanding of high-T_c supraconductivity [3], with applications in energy storage and distribution and in transportation. It also should benefits to pharmaceutical, chemical and petrol industries, offering a unique tools to simulate molecules and predict chemical reactions.

1.3. Quantum communications

Communication security is of strategic importance to consumers, enterprises and governments alike. At present, it is provided by encryption via classical algorithms, which could be broken by a quantum computer. This motivates the development of quantum-safe cryptography, that is, encryption methods that quantum computers could not break. Quantum communications relies on the use of entanglement in order to secure communications. One significant component of a quantum secure communication systems is expected to be Quantum key distribution, or "QKD": a method of transmitting information using entangled light in a way that makes any interception of the transmission obvious to the user. Entangled states are fundamentally sensitive to measurement. Therefore, if a spy intercepting the message sent, the measurement while project the entangled state on the measured states. If the entanglement is broken by the measurement, it is possible for the sender/reciever to know that it happened. Several protocol might be used to achieved that, such as the BB84 protocol.

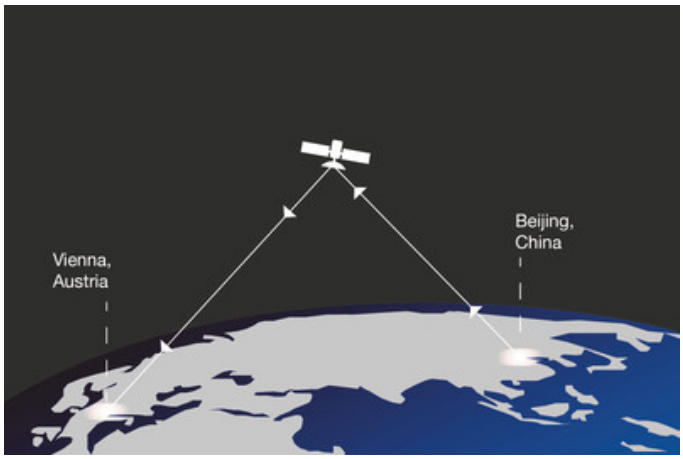


Fig. II.3. Principle of the QUESS project: intercontinental secured quantum communication between China and Austria. The image is a simplified illustration. In reality the satellite will first fly over Beijing and then over Austria. Image ©ÖAW. Extracted from `https://www.oeaw.ac.at/en/oeaw/press/public-relations-and-communications/pressefotos/first-quantum-satellite-successfully-launched/`

Another technology in the field of quantum communications is the quantum random number generator used to protect data. Indeed, it is not easy to produce random number classically. But when a quantum system is in a superposition state such as

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$$

the probability to measure $|0\rangle$ is fundamentally random, with 0.5 probability of success. When such a state, it is then possible to generate random binary number, with perfect randomness insured by quantum mechanics. This produces truly random number without following the procedure of the computing algorithms that merely imitate randomness.

Secure solutions based on quantum encryption are also immune to attacks by quantum computers, and are commercially available today, as is quantum random number generation – a key primitive in most cryptographic protocols. But quantum encryption is based on the transmission of entangled states which are fragile states. Then, theses fragile states might be affected by decoherence (and "accidental" projective measurement) during the propagation in the communication channel. Currently, quantum communication systems can only function over distances of less than 500 km. While in classical communication systems repeaters allows amplification of signal, quantum information is secure because it cannot be cloned. But for the same reason it cannot be relayed through conventional repeaters.

3. if high-T_c supraconductivity has been discovered more than thirty years ago, it's still not properly understood.

Instead, repeaters based on trusted nodes or fully quantum devices, possibly involving satellites, are needed to reach global distances. It has been realized in the chinese project called *Quantum Experiments at Space Scale* (QUESS). QUESS is a proof-of-concept mission designed to facilitate quantum optics experiments over long distances to allow the development of quantum encryption and quantum teleportation technology. By producing pairs of entangled photons, QUESS will allow ground stations separated by many thousands of kilometres to establish secure quantum channels QUESS itself has limited communication capabilities: it needs line-of-sight, and can only operate when not in sunlight. The mission cost was around $100 million in total. Secured quantum communication has been demonstrated between the Institute for Quantum Optics and Quantum Information in Beijing (China) and Vienna (Austria), separated by a ground distance of 7,500km, enabling the first quantum secured intercontinental video call in 2016 [55, 11]. Previously, Anton Zeilinger and his team had already been able to observe these phenomena in many experiments on ground up to a record distance of 144 kilometres. Longer distances on the Earth's surface are impossible due to disturbances in the atmosphere and the Earth's curvature.

Then, to reach intercontinental distance, secured quantum communications requires either the use of satellites or quantum repeaters, devices still in the phase of development at the academic level. The advantage of quantum repeaters lies in extending the distances between trusted nodes. The building blocks for fully quantum repeater schemes are twofold: a small quantum processor and a quantum interface to convert the information into photons similar to the optoelectronics devices used in today's internet, but with quantum functionality. These building blocks have already been demonstrated in the lab, but years of R&D are still needed for them to reach the market.

1.4. Quantum sensors and metrology

Quantum superposition states can be very sensitive to a number of external effects, such as electric, magnetic and gravitational fields; rotation, acceleration and time, and therefore can be used to make very accurate sensors. The most known application of atomic metrology is probably atomic clock with precision so high that, for the most performant academic lab atomic clocks, one has an error of 1 second in a span of about one-hundred million years! This makes them one of the most accurate devices in human history, at least when it comes to keeping time. The main application of atomic clocks is geopositioning and UTC time definition.

UTC stands for Universal coordinated time. UTC is an official world-wide atomic clock time standard. National laboratories around the world have atomic clocks synchronised to this atomic time standard. Leap seconds are introduced at pre-defined intervals to compensate for variations in the earths rotation.

The Global Positioning System (GPS) operated by the US Air Force Space Command provides very accurate timing and frequency signals. A GPS receiver works by measuring the relative time delay of signals from a minimum of four, but usually more, GPS satellites, each of which has at least two onboard caesium and as many as two rubidium atomic clocks. The relative times are mathematically transformed into three absolute spatial coordinates and one absolute time coordinate. GPS Time (GPST) is a continuous time scale and theoretically accurate to about 14 ns [1]. However, most receivers lose accuracy in the interpretation of the signals and are only accurate to 100 ns. The Galileo Global Navigation Satellite System is operated by the European GNSS Agency and European Space Agency and is expected to achieving full operating global coverage soon. It is the first non-military operated Global Navigation Satellite System, and it should offers 30 ns timing accuracy, equipped with two passive hydrogen maser and two rubidium atomic clocks for onboard timing.

Quantum sensors are based on superposition states, which are naturally very sensitive to the environment, and can therefore be used to make very accurate sensors. Recent efforts are being made to engineer quantum sensing devices, so that they are cheaper, easier to use, more portable, lighter and consume less power. If this goal is achieved, then it develop an important market regarding applications such as monitoring of oil and gas deposits. As a result of steady progress in material quality and control, cost reduction and the miniaturisation of components such as lasers, these devices are now ready to be carried over into numerous commercial applications. Solid-state quantum sensors, such as NV centres in diamond, have been shown to be useful for measuring very small magnetic fields. This in turn may help with multiple applications, ranging from biosensors to magnetic resonance imaging and the detection of defects in metals.

Another topic in quantum sensing is quantum imaging. Quantum imaging devices use entangled light to extract more information from light during imaging. This can greatly improve imaging technologies. For example, it could consists in producing an image by measuring one single photon which is entangled with a second, differently colored and entangled photon that is being used to probe a sample.

Regarding navigation devices, atomic and molecular interferometer devices use superposition to measure acceleration and rotation very precisely. These acceleration and rotation signals can be processed to enable inertial navigation devices to navigate below ground or within buildings. Such devices can also be used to measure very small changes in gravitational fields, magnetic fields, time or fundamental physical constants.

1.5. Applications of quantum technologies

There's plenty of applications of quantum technologies. Here are listed only few examples. Applications involving quantum computers will be detailed in chapter V.

Clocks and network synchronisation

A new generation of quantum enhanced optical clock is now emerging showing significantly improved accuracy with respect to the present atomic clocks, with further possibilities for sensing. In GNSS applications, geopositioning relies on time measurements. In this case it is of fundamental importance that all clocks of the constellation are in phase within few ns (clock synchronization). Error of 1 ns corresponds to 30 cm error in determining the user position on the ground. Most common clock synchronization method is based on the use of satellite. This technique allows an accuracy ranging from 100 ns to 500 ps depending on the details of the system. Emerging technique is optical fiber synchronization, which allows to increase the synchronization accuracy to few tens of ps. Many applications of quantum enhanced optical clocks will require to make clock accuracy available outside metrological labs, and to be able to accurately compare remote clocks. This is possible only if the clock frequency is distributed by means of dedicated optical fiber links. A technology that is being tested and developed currently, and has already been proved to improve satellite distribution and comparison techniques by orders of magnitude.

Quantum communications

The most mature quantum technologies in quantum communications are **quantum key distribution (QKD)** and **quantum random number generators (QRNG)**. Integrated photonics is playing an important role here in making these devices and systems more robust, compact and cheaper, thus facilitating their exploitation. An increasing number of security applications are being built on GKD beyond simply secret key distribution, such as ensuring the long term security of stored health records and data in general. QRNGs have found unexpected interest from the gaming industry but are also proving to be an important element in securing our infrastructure such as energy grids.

The future holds even more potential, but it also presents more challenges. Developing more complex system based on and exploiting entanglement will allow quantum resources, such as qubits, entanglement and randomness to be distributed over pan-European distances for what is being called a **quantum internet**. But this would require the development of a key element: the quantum repeater, required for long distance quantum state propagation. It requires elements that can store quantum states, so-called **quantum memories**. Long distance quantum communication would also requires the development of satellite-based protocols, as demonstrated between China and Austria, in order to develop a global **quantum network**.

Quantum network could be an infrastructure used for QKD, but would also provide an infrastructure to connect quantum sensors in an appropriated network, for example quantum clocks for improved timing precision.

Quantum-optical metrology and imaging

In quantum-optical metrology and quantum imaging, quantum effects of light, and in particular quantum entanglement, are exploited to improve the sensitivity in phase measurements or the spatial resolution of optical

systems. In optical metrology, optical phase is measured by the mean of interferometers (for instance a Mach-Zehnder interferometer): a phase shift is converted in intensity difference variation at the outputs ports.

Interferometers: standard quantum limit and Heisenberg limit

In the general case, the Heisenberg principle stipulate that for two observables $\hat{A}$ and $\hat{B}$, their standard deviation verify the following inequality

$$\Delta\hat{A}\Delta\hat{B} \geq \frac{1}{2}\left|\left\langle\left[\hat{A},\hat{B}\right]\right\rangle\right|.$$

In the case of a flux of light, the number of photons N and their phase φ are conjugated variables so that Heisenberg uncertainty becomes

$$\boxed{\Delta\hat{N}\Delta\hat{\varphi} \geq 1}.$$

Therefore, quantum mechanics affects sensitivity of interferometer as a results of the fundamental Heisenberg principle (uncertainty $\Delta\hat{\varphi}$.

The sensitivity of the phase measured is also fundamentally limited by the shot noise at the measurement of the intensities. This shot noise is fundamentally associated to the wave-particle duality of light. When a photoreceptor measures N photons, the measurement provides n photoinduced electrons in the detectors with a quantum efficiency $\eta < 1$. From the discrete nature of photons, the measurement of n photoinduced electrons is associated to a quantum uncertainty of $\Delta n = \sqrt{n} = \sqrt{\eta N}$. The relevant information in intrumentation is the **signal-to-noise ratio** (SNR), a comparison between the signal and the associated noise. In the case of photodetection, the SNR is limited fundamentally by quantum fluctuations following

$$\text{SNR} \leq \text{SNR}_{\text{quantum limit}} = \frac{n}{\sqrt{n}} = \sqrt{n}.$$

This limit may be reformulated in term of number of photons N and quantum efficiency

$$\text{SNR} \leq \text{SNR}_{\text{quantum limit}} = \sqrt{\eta}\sqrt{N}.$$

As expected, SNR limit increases when the intensity of the probed beam increases, but more importantly, the better the detector quantum efficiency is, the higher is the fundamental limit on the SNR.

This fundamental limit, associated to Heisenberg uncertainty principle applied to the observable used for detection, is called **the standard quantum limit**, associated to the detection quantum noise called *shot noise* scaling in $\sqrt{N}$.

But can show that the absolute limit given by quantum theory is the considerably lower than the quantum standard limit: this limit is called **Heisenberg limit**. A known strategy consists in using **squeezed light**, a state of light in which uncertainty is redistributed between the two conjugated variables $\hat{\varphi}$ and $\hat{N}$. In a classical Mach-Zehnder interferometer, no light is introduced in the second input port. If a squeezed light is put into this second input port, it possible to reduce the phase noise considerably. Another strategy consists in using entangled states of light to improve sensitivity, with a NOON state. A NOON state is a superposition of a state where N photons are in the first arm and 0 in the second arm and a state where 0 photons are in the first arm and N in the second arm. With a NOON state instead of a classical coherent state, the interferometer noise falls down the Heisenberg limit and reach a so-called **super-sensitivity**.

Entanglement is the key point that permits to increase the sensitivity of interferometers further than the quantum limit. With a state of maximal entanglement (such as a NOON state), it is possible to reach the maximal sensitivity at the Heisenberg limit.

The use of entangled state is a milestone to improve the sensitivity of interferometers for metrology. Such type of interferometers are already used. Gravitational waves are detected with large Michelson type interferometer (VIRGO and LIGO projects for instance), with arms in the kilometer range. A gravitational wave induces a modulation of the index of refraction of vacuum that is expected to be probed with these interferometers. But the relative variation of index is expected to be in the 10^{-21} range, below the standard quantum limit. Then, thanks to the used of squeezed light in the arms of the interferometers, this limit has been outreached so that it permitted to detect the first gravitational waves in 2015 (and awarded Nobel prize in 2017).

If production of squeezed states, which are entangled states, is widespread in research laboratories, it is still very difficult to produce NOON states to reach Heisenberg limit. Another challenge is the measurement: the photon detectors need to be able to distinguish photon numbers at the level of single photons.

Quantum imaging

In quantum imaging, quantum effects of light are used to improve optical imaging. NOON states can be used to beat the Rayleigh diffraction limit for the resolution of an imaging system. A completely different technique is ghost imaging: the object and the detector used for imaging are illuminated by two spatially separated but correlated light beams. The image is obtained by measuring intensity correlations.

Sensing with NV centers

A NV center is a point defects in the diamond lattice. It consists of a nearest-neighbor pair of a nitrogen atom, which substitutes for a carbon atom, and a lattice vacancy. NV center in diamond behaves like an artificial atom trapped in the diamond crystal with a position controlled at the nanometer scale. The quantum state of a NV center can be manipulated coherently, just like a single atom, at room temperature with laser light, RF-waves and microwaves. NV centers are used as sensors to measure magnetic fields, electric fields, temperature or pressure.

The huge advantage of NV center is that they act as a very small probe. In 2017, NV centers have been demonstrated as a local probe of magnetic field, resolving the magnetic field of nanoscale write heads of hard-disk-drive [28]. In magnetic storage devices, fields are on the order of 1 T over length scales of less than 100 nm, and are switched at GHz bandwidth. Such fields are also essential elements for precision coherent control of spinson nanoscale dimensions in quantum spintronics. In reference [28], gradients of magnetic field have been measured up to 10 mT/nm, and all components of a static and dynamic magnetic field have been measured, independent of its orientation. This results in a milestone for future miniaturization of magnetic memories devices.

NV center have been used in NMR scheme to probe individual proton spins in a single protein [36]. Scanning-NV magnetometry has also shown to be ideally suited to investigate complex antiferromagnetic orders at the nanoscale through. It has permits the first real-space visualization of a cycloidal antiferromagnetic order in a thin film of bismuth ferrite $BiFeO_3$ [25]. Moreover, individual nanoscale antiferromagnetic domains in a thin film of chromium oxide Cr_2O_3 have been imaged with NV centers. These domains have been visualized across the paramagnet-antiferromagnet phase transition. These results might have an important impact in the emerging field of antiferromagnetic spintronics.

NV centers are really promising devices for the development of sensors with spatial resolution lower than 100 nm and high sensitivity. They act like artificial atoms and consequently might be used as magnetic or electric field sensors.

2. Miniaturization as a catalyzer for the second quantum revolution

2.1. From invention to innovation

Research, development and industrialisation are three aspects inherent to the development of new products and technologies. Research is dedicated to the study of the feasibility of a concept or fundamental studies. Fundamental studies may permit to discover a phenomena that nobody expected, which will then result in a technological innovation. Sometimes, fundamental researches requires technological development that found applications in industry or for the development of new commercial products. That is the case of the World Wide Web, which has been invented in 1989 by Tim Berners-Lee, a british research of CERN, the european center for subatomic physics research. The project was originally designed and developed so that scientists working in universities and institutes around the world could exchange information instantaneously. It was adapted for an organization like CERN, where more than 17,000 scientist work from more than 100 different countries.

Development is another step of technological innovation process. Once a physical phenomena has been demonstrated, most of times the first prototype is not useable directly; either due to low performances or due

to bulky setups, non integrable or non scalable solutions. The development phase consists in the optimization of the invention, improving the corresponding technology, the overall performances so that a useable prototype might be obtained. An interesting example are semiconductor lasers. Coherent light emission from a gallium arsenide (GaAs) semiconductor diode (a laser diode) was demonstrated in 1962 by two US groups led by Robert N. Hall at the General Electric research center and by Marshall Nathan at the IBM T.J. Watson Research Center, based on theoretical work by William P. Dumke at IBM's Kitchawan Lab. Diode lasers of that era operated with threshold current densities of 1000 A/cm^2 at 77 K temperatures. Such performance enabled continuous-lasing to be demonstrated in the earliest days. When operated at room temperature, threshold current densities were two orders of magnitude greater, or 100,000 A/cm^2 in the best devices. The dominant challenge was to obtain low threshold current density at 300 K and thereby to demonstrate continuous-wave lasing at room temperature from a diode laser. The innovation that met the room temperature challenge was the double heterostructure laser (awarded by the 2000 Nobel prize in Physics).

Once the development has permit to obtained a prototype of a devices with performances good enough and size acceptable for commercialization, the last step is industrialisation. It consists in the development of a fabrication process compatible with factory mass production, with reasonable cost so that the produced device could be sold at a competitive price regarding its application.

2.2. Technology readiness level

In recent years, the public has often associated technological innovation with the most successful private companies in the world, such as Apple, Google, and Microsoft. One of the fundamental drivers of innovation remains technology research. Unlike traditional research — which aims at obtaining new knowledge about the real world — technology research aims at producing new and better solutions to practical problems. But a significant portion of the technologies leveraged by the iPhone, for example, was originally conceived in research conducted by the public sector. The journey of new technology from research to commercialization goes through a number of so-called technology readiness levels (TRLs). TRL levels are a method for understanding the maturity of a technology, and allow engineers to understand the evolution of a technology, regardless of their technical background. These levels were first developed at NASA between the 1970s and the 1990s. The latest version of the scale from NASA includes nine TRLs and has gained widespread acceptance across governments, academia, and industry. The European Commission adopted this scale in its Horizon 2020 program.

Fig. II.4. Technology readiness level (TRL). Extracted from `https://www.twi-global.com/technical-knowledge/faqs/technology-readiness-levels`

The nine technology readiness levels are:

TRL 1 Basic principles observed.

TRL 2 Technology concept formulated.

TRL 3 Experimental proof of concept.

TRL 4 Technology validated in lab.

TRL 5 Technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies).

TRL 6 Technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies).

TRL 7 System prototype demonstration in operational environment.

TRL 8 System complete and qualified.

TRL 9 Actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space).

Figure 1 General overview of funding and Stakeholders type according to R&I activities and beyond

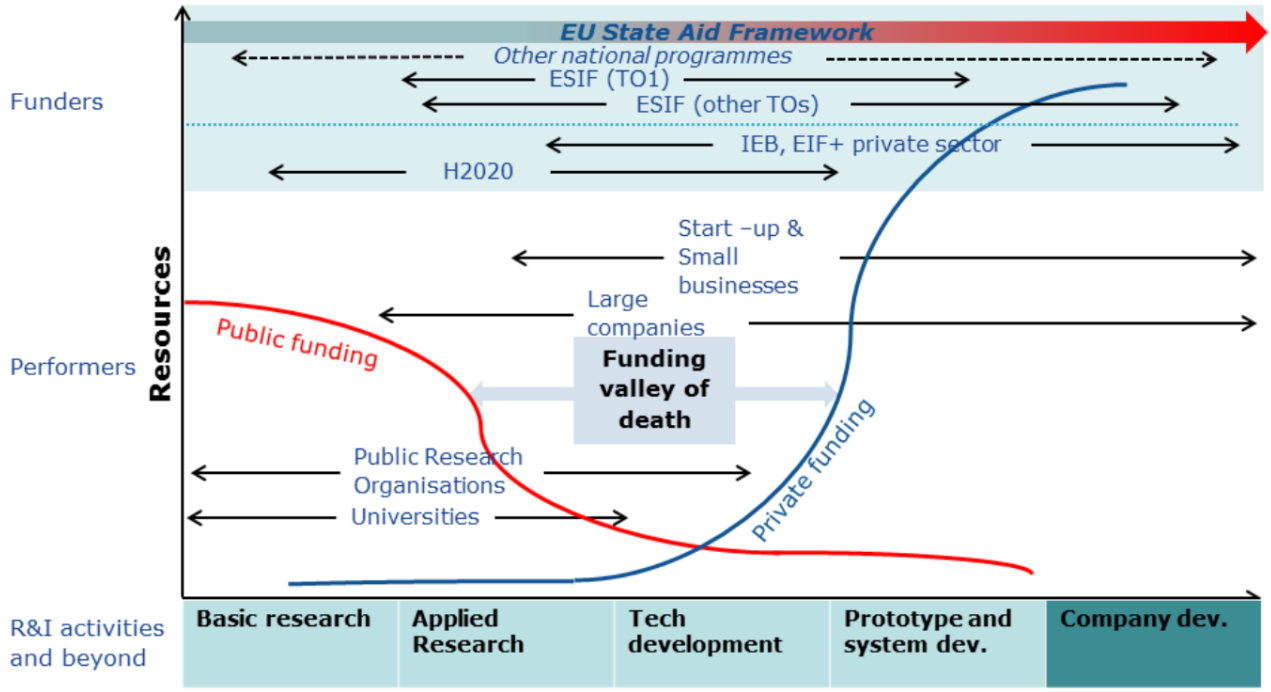


Fig. II.5. Ressources for technological development at different maturity level and "valley of death". Public funding are important for TRLs 1-4 while private funding invests for TRLs 7-9. TRLs 4-7 suffers from lake of investments called "valley of death". Extract from *Drawing funding and financing scenarios for effective implementation of Smart Specialisation Strategies*, European Commission JRC technical report (2018). `https://s3platform.jrc.ec.europa.eu/documents/20182/201464/Drawing+funding+and+financing+scenarios+for+effective+implementation+of+Smart+Specialisation+Strategies/4296838f-13ea-433e-88c2-689456f01b95`.

Some tech giants are large enough to fund research units and work at all levels of this scale, but most companies cannot afford the high investments and specialized competencies this approach requires. Either way, in today's dynamic and volatile markets they have to aim at doing the disrupting in order to avoid being disrupted. Companies that cannot afford research units have to innovate by relying on research conducted elsewhere, and the natural candidate is academia.

Academia tends to focus on TRLs 1–4, whereas industry prefers to work with TRLs 7–9, rarely 6. The term *Valley of Death* represents the often neglected addressing of TRLs 4 through to 7, where neither academia nor the private sector prioritise investment. Consequently, many technologies, even if they are promising, reach TRLs 4–6 and die there.

The issue of the valley of death has been studied extensively, and the scientific literature offers several proposals for bridging the gap. Alessandro Rossini, senior manager at PWC, has summarized the results of these studies in five recommandations [4]

1. Academia and industry should better understand each other's culture;
2. Academics should better understand real-world industrial challenges;
3. Practitioners should stay up-to-date with the state-of-the-art;
4. Industry should hire more PhDs;
5. Academia and industry should conduct more joint research projects.

2.3. Getting out of the lab: miniaturization

Quantum technologies are based of two major fundamental physics phenomena: entanglement and quantum superposition. These phenomena have been studied in academic lab with complex and bulky experimental setups, because nobody was expecting such experiment to be used in industry or in commercially available devices. It's was basic research at TRL 1-2 level. But quantum technologies nowadays are emerging in industry also because technological progress have permit to develop more compact and more stable experimental setups for manipulations and measurements on individual quantum systems. These progresses have lead to miniaturization of experimental setups. The miniaturization dynamics is actually recurrent in technological innovation. For instance, the first lasers were very bulky and expensive systems, with amplification media based on excited gases with high-voltage discharges. Such devices were too bulky and fragile for many applications. A milestone has been reached with the development of semiconductor lasers. After decades of development, semiconductor lasers are powerful, efficient and low-cost solutions for integrated laser source of very small sizes. It has permit its integration in devices such as CD-R or DVD players for example.

Semiconductor devices have stimulated the technological development of microfabrication techniques in clean room facilities, such as photolithography, molecular beam expitaxy,... These technological developments have been used in other fields for miniaturization of lab experimental setup. That is the case of microfluidics, which refers to the behaviour, precise control, and manipulation of fluids that are geometrically constrained to a small scale (typically sub-millimeter) at which capillary penetration governs mass transport. It is a multidisciplinary field that involves engineering, physics, chemistry, biochemistry, nanotechnology, and biotechnology. It has practical applications in the design of systems that process low volumes of fluids to achieve multiplexing, automation, and high-throughput screening. Microfluidics emerged in the beginning of the 1980s and is used in the development of inkjet printheads, DNA chips, lab-on-a-chip technology, micro-propulsion, and micro-thermal technologies.

Quantum technologies have also benefits from such miniaturization. Ultracold experiments were bulky and complicated experimental setup, requiring ultra-high vacuum systems, lasers and their associated optics, and electronics for computer interfacing of the experiment. In such experiments, atoms need to be trapped with a magnetic field. The later is created with coils in which an important electrical current flow, requiring an external cold water circulation to cool them. These coils were the main reason for the limitation in size of the apparatus and a huge constraint to develop more complex magnetic potentials to manipulate atoms. But many potential applications of ultracold atoms required to generate more complex potentials with magnetic field, that coils couldn't easily produce. It was also a strong limitation for scability, required for the development of quantum calculation. A milestone has been reach when several research group [5] have proposed to generate those magnetic fields with microwires on a chip fabricated with standard clean room microfabrication technics. They are cold *atomchips*. With current of maximum values of few Amps, they have demonstrated the possibility to trap ultracold atoms, produce Bose-Einstein condensates, and coherently manipulate them. This technology is very efficient and has been developed further in academic labs. Moreover, it has permit an important reduction of the size of ultracold atoms devices, small enough to be realistic for industrial application. A compact system for

4. *Bridging the technological "valley of death"*, Alessandro Rossini, November 6th, 2018, `https://blogg.pwc.no/digital-transformasjon/bridging-the-technological-valley-of-death`

5. such as Jakob Reichel or Jörg Schmiedmayer.

production of ultracold atoms, based on atomchips, has been developed and patented by Dana Anderson and Jakob Reichel in 2004 (US patent #US20050199871, *Cold atom system with atom chip wall*). A startup company, Cold Quanta Inc., now sales such systems, which are used by companies to develop quantum technologies (`https://www.coldquanta.com`. Their products ranges from complete ultra-cold atom systems, cold atoms systems, ion trap systems, vacuum cells to electronics associated. The concept of atomchips has been used also to trap ions and manipulate them in a compact device. The startup IonQ proposes a quantum computer based on trapped ion with an atomchip technology (`https://ionq.com/`), while previous academic labs experimental setups were very bulky systems.

Microfabrication technologies have permit to miniaturize cold atoms and trapped ion systems, but they also have permit to develop solid-state solutions for quantum technologies, such as semiconductor base single photon emitters, with for instance solutions provided by the startup Quandela (`http://quandela.com`), which technology is issued from academic research. Solid-state qubits have also been developed, either based on quantum dots or superconducting josephson junctions. Such qubit implementation is very attractive since it is scalable on a chip in the cm range. Currently, superconducting qubits is the most common technology used by end-to-end industrial players such as IBM, Google, D-waves, Intel or Rigetti. For programmable quantum computers, from 50 to 100 qubits chips have been demonstrated, on a chip in the cm range. For quantum annealing computers, D-wave company has reported in February 2019 a 5,640 qubits device (Pegasus P16), on a chip in the cm range.

Most of quantum technologies basic elements have been miniaturized, making them ready for integration to develop commercial devices. A constraint remains for superconducting qubits which requires subKelvin temperature, and the use of a diluation helium cryostat. But most of industrial players have chosen this technology anyways. The business model consists not in selling the computer but selling the quantum calculation. The client has a cloud access to the quantum computer which physically remains the property of the company (like IBM or Rigetti). It is the most common business model for the moment, even if D-wave has sold quantum annealing computers.

Chapter III

Quantum sensors: atomic interferometry

1. Atoms and sensing

1.1. Atom as a probe

Atomic structure

Without spin-orbit interaction, eigenstates of hydrogen-like atoms can be expressed in basis of mutually commuting operators: $\hat{H}_0$, $\hat{\mathbf{L}}^2$, $\hat{L}_z^2$, $\hat{\mathbf{S}}^2$ and $\hat{S}_z^2$, where $\hat{H}_0$ is the hamiltonian associated to the electron motion (spatial degrees of freedom). In this case, electrons are fully described with four quantum number n, l, m_l and m_s. The principal quantum number n is associated to the electron energy, typically in the eV range (**optical transitions**). **Within a given n value, without spin-orbit coupling, all states are energy degenerated.** The azimuthal quantum number l is associated to the eigenvectors of $\hat{\mathbf{L}}^2$ such that

$$\hat{\mathbf{L}}^2|n,l,m_l,m_s\rangle = \hbar^2 l(l+1)|n,l,m_l,m_s\rangle, \;\; l \in [\![0, n-1]\!].$$

In chemistry and spectroscopy, $l=0$ is called an s orbital, $l=1$ a p orbital, $l=2$ a d orbital, and $l=3$ an f orbital. The projection of the orbital momentum along z axis provides m_l quantum number, such that

$$\hat{L}_z|n,l,m_l,m_s\rangle = \hbar m_l|n,l,m_l,m_s\rangle, \;\; l \in [\![-l, l]\!].$$

Similarly, m_s is the spin quantum number, taking into account that an electron is a spin half particle, $S = 1/2$ and $m_S \in \{-1/2, +1/2\}$.

In atoms, the fine structure originates from the coupling between $\hat{\mathbf{L}}$ is the angular momentum of the electron and $\hat{\mathbf{S}}$ the spin of the electrons. For a general potential of interaction with the nucleus $V(r)$, it is possible to show that this coupling is described by the following hamiltonian

$$\hat{H}_{\mathrm{f}} = \frac{1}{2m^2c^2}\frac{1}{r}\left(\frac{\partial V}{\partial r}\right)\hat{\mathbf{L}}\cdot\hat{\mathbf{S}}.$$

For a hydrogen-like atom,

$$V(r) = -\frac{1}{4\pi\varepsilon_0}\frac{Ze^2}{r},$$

so that the spin-orbit coupling hamiltonian as the following expression

$$\hat{H}_{\mathrm{f}} = \frac{1}{2m^2c^2}\frac{1}{4\pi\varepsilon_0}\frac{Ze^2}{r^3}\hat{\mathbf{L}}\cdot\hat{\mathbf{S}}.$$

With spin-orbit, total Hamiltonian no longer commutes with $\hat{L}_z$ or $\hat{S}_z$. One needs to exploit degeneracy of $\hat{H}_0$ and found a new basis in which $\hat{\mathbf{L}}\cdot\hat{\mathbf{S}}$ is diagonal. In that goal, one introduces the total orbital momentum $\hat{\mathbf{J}} = \hat{\mathbf{L}} + \hat{\mathbf{S}}$. It is straightforward that

$$\hat{\mathbf{L}}\cdot\hat{\mathbf{S}} = \frac{1}{2}\left(\hat{\mathbf{J}}^2 - \hat{\mathbf{L}}^2 - \hat{\mathbf{S}}^2\right).$$

Combining a spin 1/2 with angular momentum l, the total angular momentum $\hat{J}$ can take values

$$J = l \pm 1/2, \text{ and } m_J \in [\![-J, J]\!].$$

For a hydrogen-like atom, the energy shift induced by spin-orbit coupling depends on n and J as follow

$$\Delta E_{n,J=1\pm l,m_J,l,m_S} = \frac{1}{2}mc^2\left(\frac{\alpha E}{n}\right)^4\left(\frac{3}{4}-\frac{n}{J+1/2}\right),$$

where

$$\alpha = \frac{e^2}{4\pi\varepsilon_0\hbar c},$$

is the *fine structure constant*. The fine structure of energy levels of atoms is also corrected for some relativistic effects such as the Lamb shift. Fine structure results in level splitting of the gross initial structure with energy shift in the 10^{-5} to 10^{-4} eV range.

In spectroscopy, for a state with principal quantum number n, total spin S, orbital angular momentum l and total angular momentum J, one may define the state by the spectroscopic notation

$$n^{2S+1}L_J,$$

with $L \in \{S,P,D,F\}$. For hydrogen-like atom, with a single electron, $2S+1=2$. In this case, the factor $2S+1$ is just dropped for brevity. Example: $2P_{3/2}$ level.

The atomic hyperfine structure results from the interaction between the nuclear spin $\hat{\mathbf{I}}$ and the total angular momentum $\hat{\mathbf{J}} = \hat{\mathbf{L}} + \hat{\mathbf{S}}$, where $\hat{\mathbf{L}}$ is the angular momentum and $\hat{\mathbf{S}}$ the spin.

The appropriate quantum observable is $\hat{\mathbf{F}} = \hat{\mathbf{I}} + \hat{\mathbf{J}}$, the total orbital momentum. The hamiltonian associated to the nuclear spin - orbital spin coupling is commonly written as

$$\hat{H}_{\text{hf}} = A\hat{\mathbf{I}}\cdot\hat{\mathbf{J}}.$$

The operator $\hat{\mathbf{I}}\cdot\hat{\mathbf{J}}$ might be rewritten as follow

$$\hat{\mathbf{I}}\cdot\hat{\mathbf{J}} = \frac{1}{2}\left(\hat{\mathbf{F}}^2 - \hat{\mathbf{I}}^2 - \hat{\mathbf{J}}^2\right)$$

In the appropriate basis (eigenvectors of $\hat{F}$, $\hat{J}$ and $\hat{I}$), the energy shift due to nuclear spin - electronic orbital momentum coupling is

$$\Delta E_{F,J,I} = \frac{\hbar^2}{2}A\left(F(F+1) - I(I+1) - J(J+1)\right),$$

with $F \in [\![|J-I|, J+I]\!]$. Hyperfine structure results in level splitting of the initial fine structure with energy shift in the 10^{-6} to 10^{-5} eV range. In spectroscopy, levels are design with both the fine structure notation but adding the information on the F quantum number, for example the ${}^2S_{1/2}$, $F=0$ state.

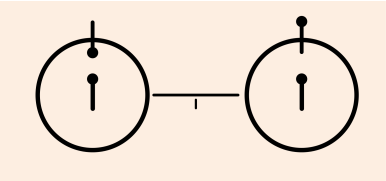


Fig. III.1. The hyperfine transition as depicted on the Pioneer plaque. Extracted from `https://en.wikipedia.org/wiki/Hyperfine_structure`

The hyperfine transition of hydrogen ($\lambda = 21$ cm) is considered to be a sufficiently universal phenomenon so as to be used as a base unit of time and length on the Pioneer plaque and later Voyager Golden Record. The Voyager Golden Records are two phonograph records that were included aboard both Voyager spacecraft launched in 1977. The records contain sounds and images selected to portray the diversity of life and culture on Earth, and are intended for any intelligent extraterrestrial life form who may find them. The records are a sort of time capsule.

Atom	D_1 line	wavelength	D_2 line	wavelength
Cs	$6^2S_{1/2} \longrightarrow 6^2P_{1/2}$	894.592,959,86(10) nm	$6^2S_{1/2} \longrightarrow 6^2P_{3/2}$	852.347,275,82(27) nm
Na	$3^2S_{1/2} \longrightarrow 3^2P_{1/2}$	589.755,814,7(15) nm	$3^2S_{1/2} \longrightarrow 3^2P_{3/2}$	589.158,326,4(15) nm
^{87}Rb	$5^2S_{1/2} \longrightarrow 5^2P_{1/2}$	794.978,851,156(23) nm	$5^2S_{1/2} \longrightarrow 5^2P_{3/2}$	780.241,209,686(13) nm
^{85}Rb	$5^2S_{1/2} \longrightarrow 5^2P_{1/2}$	794.979,014,933(96) nm	$5^2S_{1/2} \longrightarrow 5^2P_{3/2}$	780.241,368,271(27) nm

Atom	Hyperfine splitting (ground state)	frequency
Cs	$6^2S_{1/2}, F = 3 \longrightarrow F = 4$	9.192,631,770 GHz (exact)
Na	$3^2S_{1/2}, F = 1 \longrightarrow F = 2$	1.771,626,128,8(10) GHz
^{87}Rb	$5^2S_{1/2}, F = 1 \longrightarrow F = 2$	6.834,682,610,904,290(90) GHz
^{85}Rb	$5^2S_{1/2}, F = 1 \longrightarrow F = 2$	3.035,732,439,0(60) GHz

Table III.1 – D_1 and D_2 lines of alkali atoms, and hyperfine splitting of the ground state. Values are extracted from `https://steck.us/alkalidata/`.

Alkali atoms

An isolated atom is a very sensitive system to external perturbations. Let's consider the case of ^{133}Cs atom. It's an alkali atom, well-known in metrology. Indeed, since 1968, the International System of Units (SI) has defined the second as the duration of 9,192,631,770 cycles of radiation corresponding to the transition between two hyperfine levels of the ground state of the ^{133}Cs atom. Beyond Cs, alkali atoms have energy level structures well-adapted for laser cooling, and commonly used in ultracold atoms experiments or for production of atomic Bose-Einstein condensates. In such atoms, the hyperfine splitting of the ground state typically lies in the GHz range (see Tab. III.1).

In an alkali atom, the fundamental state is split into two hyperfine states, and might be seen as a two-level system. With a hyperfine splitting in the GHz range, the lifetime is rather long and spontaneous emission can be neglected. Indeed, the spontaneous emission rate of an two level system $\Gamma_{\text{rad}}(\omega)$, with an energy difference $\hbar\omega$, coupled to free space electromagnetic modes is

$$\Gamma_{\text{rad}}(\omega) = \frac{\omega^3 n \left|\langle 0|\hat{\mathbf{d}}|1\rangle\right|^2}{3\pi\varepsilon_0\hbar c^3},$$

where n is the index of refraction, $\hat{\mathbf{d}}$ the electric dipolar coupling matrix of the transition, $|0\rangle$ and $|1\rangle$ the two levels considered. This result is obtained from the application of Fermi's golden rule. This spontaneous emission rate scales as ω^3, so that it is low enough in the GHz range but high enough.

Atoms as sensors

The energy level structure of a atom might be affected both by a magnetic field or an electrical field. A field changes transitions frequency. Thus, measuring a frequency shift of a transition permit to calculate the corresponding field. Recently, atomic magnetometer with microfabricated cell of Cs vapor has been reported, with sensitivity below 100 fT/$\sqrt{\text{Hz}}$ range, a bandwidth close to 1 kHz for scalar field measurement below the pT range [58]. Moreover, this experimental setup is suited for portable devices. Another research team has reported 0.54 fT/$\sqrt{\text{Hz}}$ sensitivity but with a lab setup [48]. Such a magnetometer based on laser measurements of atomic energy levels can detect a magnetic field one hundred billion times smaller than the Earth's.

Atoms are massive particles, and can be used to measure gravity. Atomic gravimeters are based on free fall of an atomic cloud

Fig. III.2. Absolute atomic gravimeter proposed by Muquans (`https://www.muquans.com`).

combined to an atomic interferometry scheme. Gravimeter have many applications such as oil prospection. Rotations might be measured also thanks to atomic interferometer, based on Sagnac's effect, and are used as precision gyrometers. Muquans is a supplier of integrated quantum solutions, more specifically absolute atomic gravimeters and atomic clocks (`https://www.muquans.com`). This company has developed quantum inertial sensors (gravimeters), high performance time and frequency applications, and advanced laser solutions, as a spinoff company from research labs (Observatoire de Paris (LNE-SYRTE) and Institut d'Optique (LP2N) in France). The absolute gravimeter of Muquans reach the 50 μGal/$\sqrt{\text{Hz}}$ range [1] in a quiet place, with 2 Hz measurement frequency and a long-term stability better than 1 μGal.

Finally, atoms are used for time measurement, as a frequency etalon. The hyperfine transition $F = 3 \longrightarrow F = 4$ of the $6^2S_{1/2}$ ground state of Cs is fixed at $9.192,631,770$ GHz as a consequence of the SI unit definition of the second. The technical challenge for time measurement consists in measurement this transition frequency without energy shift due to external electrical or magnetic field, or due to interactions between atoms in the cloud probed. Time metrology is an important research activity of atomic physics. Precise and transportable clocks are of importance for geopositioning systems such as GPS or Galileo.

1.2. Light matter interaction

Rabi oscillations and state preparation

Let consider an atom, modeled by a two level system $\{|0\rangle, |1\rangle\}$. It is equivalent to an effective spin, an is well-suited to Bloch sphere formalism. These two levels might be the two hyperfine states of the ground state of the atom and might be manipulation with microwaves radiation. Without radiation, in the $\{|0\rangle, |1\rangle\}$ basis, the Hamiltonian of the atom is

$$\hat{H}_0 = \hbar\omega_0 |1\rangle\langle 1| = \begin{pmatrix} \hbar\omega_0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Each pure state can be written in the following form

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\varphi}|1\rangle.$$

The corresponding point on the Bloch's sphere is the point on the unit sphere in $\mathbb{R}^3$ which has the same polar angles (θ, φ). Free evolution of an atom is the following

$$|\psi(t)\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\varphi - i\omega_0 t}|1\rangle,$$

which is geometrically interpreted on the Bloch's sphere as a rotation at ω_0 along the axis Oz.

Now one considers that the atom interacts with a radiation at ω, $E(t) = E_0\cos(\omega t + \phi)$. The interaction Hamiltonian $\hat{H}_I$ is a dipolar coupling such that

$$\hat{H}_I = \hat{d}E(t) = \frac{\hbar\Omega}{2}\cos(\omega t + \phi)\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

with

$$\Omega = \frac{2dE_0}{\hbar}, \quad d = \langle 1|\hat{d}|0\rangle.$$

Ω is the Rabi frequency, quantifying the coupling between the atom and the radiation. Now let's move to the rotating frame at ω along Oz, applying the following unitary operation

$$\hat{U}(t) = \exp\left(i\omega t|1\rangle\langle 1|\right).$$

1. 1 μGal$= 10^{-8}$ m$\cdot$s^{-2}.

In the interaction representation, $|\psi\rangle_{\text{int}} = \hat{U}(t)|\psi\rangle$, the interaction Hamiltonian of the light-atom coupling is then

$$\hat{H}_{I,\text{int}} = \hat{U}(t)\hat{H}_I\hat{U}^\dagger(t) = \frac{\hbar\Omega}{2}\begin{pmatrix} e^{i\phi}+e^{i(2\omega t+\phi)} & 0 \\ 0 & e^{-i\phi}+e^{-i(2\omega t+\phi)} \end{pmatrix}.$$

In the limit $\Omega, \delta \ll \omega_0$, with $\delta = \omega_0 - \omega$, one may use the widely used rotating wave approximation (RWA) in which one will neglect the terms $e^{\pm i(2\omega t+\phi)}$. In this approximation, the full Hamiltonian in the rotating frame becomes

$$\hat{H} = \hbar\delta|1\rangle\langle 1| + \frac{\hbar\Omega}{2}\left(e^{i\phi}|1\rangle\langle 0| + e^{-i\phi}|0\rangle\langle 1|\right) = \hbar\begin{pmatrix} \delta & e^{i\phi} \\ e^{-i\phi} & 0 \end{pmatrix}.$$

This is an effective spin-1/2 Hamiltonian. Adding a total energy of $-\hbar\delta/2$, it can be rewritten using the Pauli matrices $\hat{\vec{\sigma}} = \hat{\sigma}_x\vec{u}_x + \hat{\sigma}_y\vec{u}_y + \hat{\sigma}_z\vec{u}_z$

$$\hat{H} = \frac{\hbar}{2}\vec{\Omega}\cdot\hat{\vec{\sigma}}, \text{ with } \vec{\Omega} = \begin{pmatrix} \Omega\cos\theta \\ \Omega\sin\theta \\ \delta \end{pmatrix}.$$

For a radiation of constant amplitude, it corresponds to a rotation of the initial state $|\psi(0)\rangle$ at the angular rotation vector $\vec{\Omega}$

$$|\psi(t)\rangle = \exp\left(-i\vec{\Omega}\cdot\hat{\vec{\sigma}}t/2\right)|\psi(0)\rangle.$$

In the case of a state initially in the ground state, $|\psi(0)\rangle = |0\rangle$, and a phase $\phi = 0$, this rotation results in so-called **Rabi oscillation**: the probability $P_{0\to1}(t)$ to detect the atom in the state $|1\rangle$ after an interaction time t is

$$P_{0\to1}(t) = \frac{\Omega^2}{\delta^2+\Omega^2}\sin^2\left(\frac{\sqrt{\delta^2+\Omega^2}}{2}t\right).$$

At resonance, the transition probability is simplified to

$$P_{0\to1}(t) = \sin^2\left(\frac{\Omega t}{2}\right),$$

with maximal amplitude of oscillation. This permits to manipulate the state of an atom and prepare it is a given state. For instance, going from $|0\rangle$ to $|1\rangle$, one just has to adjust the interaction time t_π with the radiation so that

$$\frac{\Omega t_\pi}{2} = \frac{\pi}{2} \Leftrightarrow t_\pi = \frac{\pi}{\Omega}.$$

This operation is called a π pulse, corresponding to a rotation on the Bloch sphere of an angle π. For an intermediate time between 0 and t_π, one obtains a superposition of states. In the particular case of $t_{\pi/2} = \frac{t_\pi}{2} = \frac{\pi}{2\Omega}$, a so-called $\frac{\pi}{2}$ pulse, providing the following state

$$|0\rangle \longrightarrow \frac{|0\rangle + i|1\rangle}{\sqrt{2}}.$$

Ramsey interrogation

A Ramsey interrogation of a two level system consists in the following sequence

Initialization Atoms are prepared in the ground state $|0\rangle$.

$\pi/2$ pulse Preparation of atoms in a superposition of states, on the equator of the Bloch's sphere.

Free evolution during a time T Atoms evolves free without any radiation, and rotates on the equator at Larmor frequency.

$\pi/2$ pulse State is rotated on the Bloch sphere.

Measurement of the $\hat{\sigma}_z$ observable.

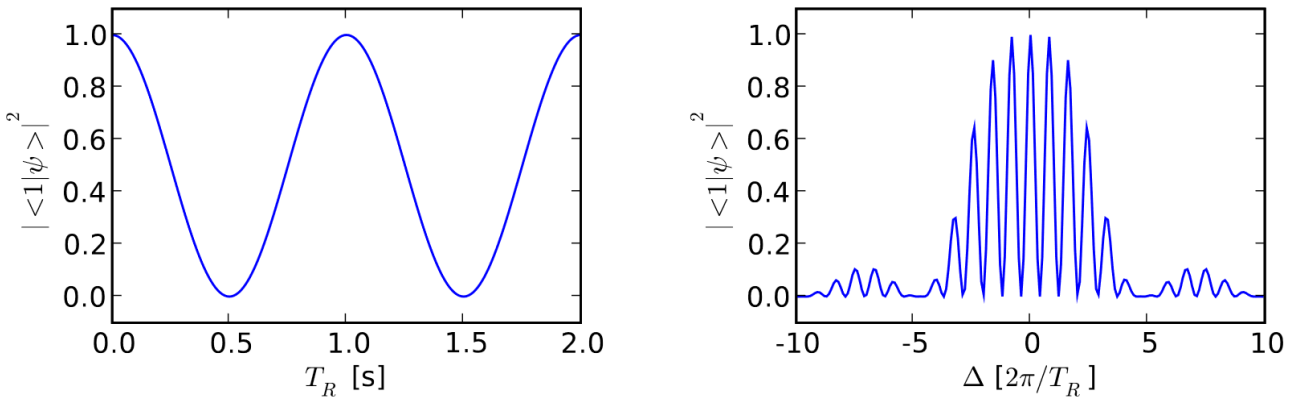


Fig. III.3. Ramsey fringes in the time domain (left, for $\delta = 2\pi \times 1$ Hz) and the frequency domain (right). In the frequency domain, the fringes have a period of $2\pi/T$ and are modulated by an envelope function (the "Rabi pedestal") stemming from the finite Rabi frequency Ω of the $\pi/2$ pulse. For large detuning ($\delta \gg \Omega$), the excitation pulsees are not resonant any more and $|\langle 1|\psi\rangle|^2 \to 0$. Figure extracted from `https://tel.archives-ouvertes.fr/tel-00414386/document`

Assuming $\phi = 0$, the action of the Ramsey interrogation can be expressed by the following operator

$$\hat{R} = \exp\left(-i\frac{\pi}{2}\frac{\hat{\sigma}_x}{2} - i\delta t_{\pi/2}\right)\exp\left(i\varphi\frac{\hat{\sigma}_z}{2}\right)\exp\left(-i\frac{\pi}{2}\frac{\hat{\sigma}_x}{2} - i\delta t_{\pi/2}\right),$$

where $t_{\pi/2}$ is the $\pi/2$ pulse duration, and $\varphi = -\delta T$ with T the duration of interrogation. Usually, such sequence is realized near resonance such that $|\delta| \ll \Omega$ then

$$\hat{R} \approx \exp\left(-i\frac{\pi}{2}\frac{\hat{\sigma}_x}{2}\right)\exp\left(i\varphi\frac{\hat{\sigma}_z}{2}\right)\exp\left(-i\frac{\pi}{2}\frac{\hat{\sigma}_x}{2}\right).$$

The first $\pi/2$ pulse places atoms in the superposition of states

$$|0\rangle \xrightarrow{\pi/2 \text{ pulse}} \frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right).$$

During the period of free evolution T, the system rotates around the z-axis with the angular velocity δ. The superposition thus picks up a phase $\varphi = -\delta T$, ending up in the state

$$\frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right) \xrightarrow{\text{free evolution during } T} \frac{1}{\sqrt{2}}\left(|0\rangle + ie^{i\varphi}|1\rangle\right).$$

The second $\pi/2$ pulse rotates the atoms by $\pi/2$ around the x-axis on the Bloch's sphere. The resulting final state is then

$$\frac{1}{\sqrt{2}}\left(|0\rangle + ie^{i\varphi}|1\rangle\right) \xrightarrow{\pi/2 \text{ pulse}} -\sin\left(\frac{\varphi}{2}\right)|0\rangle + \cos\left(\frac{\varphi}{2}\right)|1\rangle.$$

The measurable result of a Ramsey sequence is an excitation probability of the excited atomic state *i.e.* , experimentally, a population imbalance of the atomic state states. This imbalance is an oscillating function of $\varphi = -\delta T$. For a fixed detuning δ, it is a measure of T. For a fixed interrogation time T, it is a measurement of the detuning δ. Experimentally, either version can be realized and the result is refered to as Ramsey fringes in the time and frequency domain, respectively. In an atomic clock, T is always kept fixed, so that Ramsey interrogation yields a measurement of the detuning δ. To maximize the sensitivity to δ, the clock is operated on the slope of the central Ramsey fringe. The maximum slope that can be obtained is

$$\left.\frac{\mathrm{d}p}{\mathrm{d}\delta}\right|_{\max} = \frac{T}{2} = \frac{\pi}{2}\frac{Q_{\text{at}}}{\omega_0},$$

where Q_{at} is the quality factor of the clock,

$$Q_{at} = \frac{\omega_0 T}{\pi} = \frac{\omega_0}{\Delta},$$

with $\Delta = \pi/T$ the half width of the central Ramsey fringe.

To measure δ, one has to keep T fixed. Since φ scales linearly with T and δ, any error on T will translate into an equally larger error on δ. At first sight, the seems impossible: how can we fix a time without having a precisse clock, which is the very goal of this endeavour? The paradox is resolved by considering that the error of one interrogation is

$$\frac{\sigma_{\omega_0}}{\omega_0} = \frac{\sigma_\delta}{\delta}\frac{\delta}{\omega_0},$$

with σ_{ω_0} denoting the error bar on the clock interrogation. Therefore σ_δ is suppressed by the factor $\frac{\delta}{\omega_0}$, typically of the order of 10^{-10}. Therefore it is possible to reach a relative error bar

$$\frac{\sigma_{\omega_0}}{\omega_0} = 10^{-13},$$

with a moderate timing precision of

$$\frac{\sigma_T}{T} = 10^{-3}.$$

T can therefore be controlled from a clock having a performance largely inferior to the atomic clock.

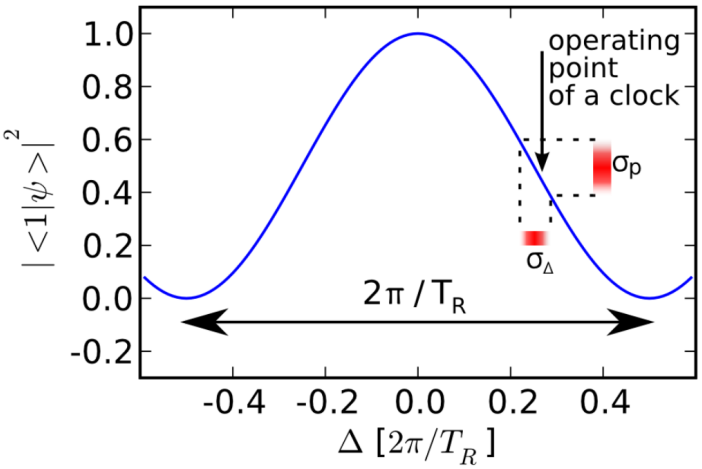


Fig. III.4. The central frequency–domain Ramsey fringe. Clocks are operated at the point of highest slope, where the transisition probability is the most sensitive to δ. Here, a given error σ_p on the measurement of the transition probability translates into a minimal error σ_δ on the frequency measurement. Figure extracted from `https://tel.archives-ouvertes.fr/tel-00414386/document`

Naively, one might argue by the time-frequency uncertainty principle that the error bar on a frequency measurement taking a mesurement time T cannot be lower than $1/T$. For typical values, $T = 1$ s and $\omega_0 = 2\pi \times 10^{10}$ Hz. This would correspond to a relative error bar of

$$\frac{\sigma_{\omega_0}}{\omega_0} = 10^{-10}.$$

However, the relative error bar of today's benchmark atomic clock after a $T = 1$ s integration time is only

$$\frac{\sigma_{\omega_0}}{\omega_0} = 10^{-14}!$$

Indeed, the width of the central Ramsey fring is $2\pi/T$, but clocks are measurement the probability over multiple atoms. Thus, the precision is directly related to the uncertainty of the probability measurement of the slope of the sine rather than the half-width of the Ramsey signal. This uncertainty is related to the number of atoms used, with a fundamental limit so-called *quantum standard limit* or *shot noise*.

2. Concept of squeezed states in spin systems

In this section, we will introduce the notion of squeezed state for $1/2$ spin systems, as well as their potential applications. Formally, any two-level system can be described by a $1/2$ spin, and thus the reasoning presented is generalizable to a wide variety of physical systems. We will use an essentially geometrical approach, based on the representation of the state of a set of two-level systems using the Bloch sphere formalism, supposedly known. A more detailed approach is described in the literature [53, 52, 32, 35, 34].

Squeezing of a quantum state consists in the redistribution of quantum fluctuations between two observables that do not commute, while minimizing Heisenberg's uncertainty relationship [32]. The quantum fluctuations of the two observables $\hat{A}$ and $\hat{B}$ verify Heisenberg's inequality according to

$$\Delta\hat{A}\Delta\hat{B} \geq \frac{1}{2}\left|\left\langle\left[\hat{A},\hat{B}\right]\right\rangle\right|.$$

In the case of a spin, or an angular momentum, one obtains

$$\Delta\hat{J}_i\Delta\hat{J}_j \geq \frac{1}{2}\left|\left\langle\hat{J}_k\right\rangle\right|,$$

where $(i,j,k) \in \{x,y,z\}$, as well as all circular permutations.

The coherent spin state (denoted CSS) is defined as the eigenvector of the spin component in the direction (θ,φ),

$$\hat{J}_{\theta,\varphi} = \hat{J}_x \sin\theta\cos\varphi + \hat{J}_y \sin\theta\sin\varphi + \hat{J}_z\cos\theta,$$

with eigenvalue [2] J, where θ and φ are the polar and azimuthal angles. The CSS state $|\theta,\varphi\rangle$ minimizes the Heisenberg relation with standard deviations $\sqrt{\frac{J}{2}}$ equally distributed over any components orthogonal to the (θ,φ) direction.

The squeezed spin state (denoted SSS) is the state for which the variance of one spin component orthogonal to the mean direction is smaller than the standard quantum limit, i.e. $\frac{J}{2}$. If we consider a system of $2J$ spins, with $J = N/2$, and if all the spins initially point in the x direction, *i.e.* $\langle\hat{J}_x\rangle = N/2$, so $\Delta\hat{J}_z^2 = \left\langle\hat{J}_z^2\right\rangle - \left\langle\hat{J}_z\right\rangle^2 = \left\langle\hat{J}_z^2\right\rangle$. Moreover,

$$\left\langle\hat{J}_z^2\right\rangle = \sum_{j,l}\left\langle\hat{s}_{z,j}\hat{s}_{z,l}\right\rangle = \sum_j\left\langle\hat{s}_{z,j}^2\right\rangle + \sum_{j\neq l}\left\langle\hat{s}_{z,j}\hat{s}_{s,l}\right\rangle,$$

and if there are no correlations between the individual spins, the variance of J_z is simply the sum of the individual variances, *i.e.*

$$\Delta\hat{J}_z^2 = \sum_j\left\langle\hat{s}_{z,j}^2\right\rangle = \frac{N}{4}.$$

It is the case of a CSS state, with

$$\Delta\hat{J}_z = \Delta\hat{J}_y = \sqrt{\frac{\left\langle\hat{J}_x\right\rangle}{2}}.$$

These variances, from a system of uncorrelated N spins, then have a characteristic value called *quantum standard limit*. This is the "reference" variance for a given number of particles, the variance of the reference state that is the coherent state, made of N uncorrelated spins. To introduce correlations between the spins, a non-linear interaction must be used [3]. If we consider the simplest non-linear interaction, the Hamiltonian can be put in the following form

$$\hat{H} = \hbar\chi J_z^2.$$

Such hamiltonian is called "Kerr hamiltonian". Let consider a CSS as initial state $\left|\frac{\pi}{2},0\right\rangle$ in the direction $\theta = \frac{\pi}{2}$ and $\varphi = 0$ on the Bloch sphere. This state might be decomposed on the $|J,J-k\rangle$ basis such that

$$\left|\frac{\pi}{2},0\right\rangle = \frac{1}{2^J}\sum_{k=0}^{2J}\sqrt{\begin{pmatrix}2J\\k\end{pmatrix}}\left|J,J-k\right\rangle,$$

and $\left\langle\hat{\mathbf{J}}\right\rangle \simeq J\mathbf{u}_x$. The system will evolve according to a unitary transformation of evolution operator

$$\hat{U}(t) = \exp\left(-i\chi t\hat{J}_z^2\right).$$

As a result of this non-linear evolution, we still have $\left\langle\hat{\mathbf{J}}\right\rangle \propto \mathbf{u}_x$, but the coherent state has been "distorted" to give an ellipse on the Bloch sphere, of squeezed axis $\mathbf{u}_\perp$ (see Fig. III.5) for times shorter than $1/\left(|\chi|\sqrt{2J}\right)$.

2. for a system containing N spin particles $1/2$, $J = N/2$.
3. a linear Hamiltonian simply rotates the individual spins without introducing correlations between them

This axis is then said *squeezed* in the sense that the variance of the operator $\hat{J}_\perp = \hat{\mathbf{J}}\cdot\mathbf{u}_\perp$ associated is below the standard quantum limit $J/2$. The conjugate axis has a variance greater than the standard quantum limit in order to satisfy the Heisenberg inequality. It is possible to transfer the squeezed property of the $\mathbf{u}_\perp$ component to any component perpendicular to $\mathbf{u}_x$. To do this, a pulse is applied to generate a rotation of the state around the x axis, and align the compressed quasiprobability with this axis. The final state can be written as

$$|\psi(t)\rangle = \exp(-i\nu\hat{J}_x)\exp(-i\chi t\hat{J}_z^2)\left|\frac{\pi}{2},0\right\rangle. \tag{III.1}$$

From the equation (III.1), one obtains the mean values and standard deviations of the different components of spin

$$\begin{aligned}
\langle\hat{J}_x\rangle &= J\cos^{2J-1}(\chi t),\ \langle\hat{J}_y\rangle = 0,\ \langle\hat{J}_z\rangle = 0,\\
\langle\Delta\hat{J}_x^2\rangle &= \frac{J}{2}\left(2J\left(1-\cos^{2(2J-1)}(\chi t)\right)-\left(J-\frac{1}{2}\right)A\right),\\
\langle\Delta\hat{J}_y^2\rangle &= \frac{J}{2}\left(1+\frac{1}{2}\left(J-\frac{1}{2}\right)\left(A+\sqrt{A^2+B^2}\cos(2\nu+2\delta)\right)\right),\\
\langle\Delta\hat{J}_z^2\rangle &= \frac{J}{2}\left(1+\frac{1}{2}\left(J-\frac{1}{2}\right)\left(A-\sqrt{A^2+B^2}\cos(2\nu+2\delta)\right)\right),
\end{aligned}$$

where one defines $A = 1-\cos^{2J-2}(2\chi t)$, $B = 4\sin(\chi t)\cos^{2J-2}(\chi t)$, and $\delta = \frac{1}{2}\arctan\left(\frac{B}{A}\right)$, the angle between the ellipse and the equator. Note in particular that, after squeezing, the average spin norm $\langle\hat{J}_x\rangle$ has decreased.

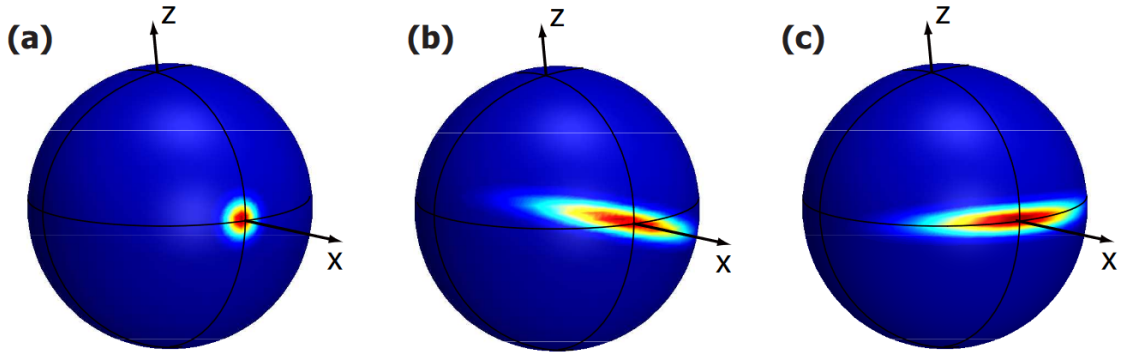


Fig. III.5. Evolution of a coherent state under the action of a Hamiltonian of the Kerr effect type. (a) Initial coherent state (CSS). (b) "Elliptical" deformation of the state under the action of the non-linear hamiltonian. The state is said to be compressed because the minor axis of this ellipse corresponds to a variance below the standard quantum limit. (c) A rotation around Ox aligns the compressed axis with Oz for example. The report is then said to be compressed in number. If the compressed axis is aligned with the equator, then the report is said to be compressed in phase.

The $\hat{J}_x$ operator can be seen as describing the relative phase between two different spins along the $\mathbf{u}_z$ axis. By expanding the second order cosine in t, we obtain

$$\cos^{2J-1}(\chi t) = e^{(2J-1)\ln\cos(\chi t)} \approx e^{-(2J-1)(\chi t)^2/2}.$$

One can see that the average value of $\hat{J}_x$ of the state (III.1) is a gaussian decay, indicating that the phase blurs according to the following time scale

$$t_c \sim \frac{1}{|\chi|\sqrt{2J}}.$$

One can also observe the resurgence of phase coherence at the t_q times defined according to

$$t_q = \frac{q\pi}{|\chi|},\ \ q\in\mathbb{N},$$

when the cosine takes the values ± 1 in the evolution equation of the spin components and their variance. Moreover, at particular times $t_m = t_{1/2}$, the equation (III.1) can be rewritten as

$$|\psi(t_m)\rangle = \frac{e^{-i(\nu J+\frac{\pi}{4})}}{\sqrt{2}}\left|\frac{\pi}{2},0\right\rangle + \frac{e^{-i((\nu+\pi)J+\frac{\pi}{4})}}{\sqrt{2}}\left|-\frac{\pi}{2},0\right\rangle,$$

corresponding to a Schrödinger cat state in phase [56]. For $\nu = \frac{\pi}{2} - \delta$, the term $\left\langle \Delta \hat{J}_y^2 \right\rangle$ is minimized and $\left\langle \Delta \hat{J}_z^2 \right\rangle$ maximized, and when $\nu = -\delta$, $\left\langle \Delta \hat{J}_z^2 \right\rangle$ is minimized while $\left\langle \Delta \hat{J}_y^2 \right\rangle$ is maximized. The increase ($+$ sign) and reduction of the variance ($-$ sign) are

$$V_\pm = \frac{J}{2}\left(\left(1+\frac{1}{2}\left(J-\frac{1}{2}\right)A\right) \pm \frac{1}{2}\left(J-\frac{1}{2}\right)\sqrt{A^2+B^2}\right).$$

For $J \gg 1$ and $|2\chi t| \ll 1$, the reduced variance V_- reaches its minimum

$$V_{\min} \approx \frac{1}{2}\left(\frac{J}{3}\right)^{1/3},$$

at the following time

$$t_{\min} = t_0 \approx \left(\frac{3}{8}\right)^{1/6} \frac{J^{-2/3}}{|\chi|}.$$

The normalized uncertainty product is

$$U_{yz} = \frac{4\left\langle \Delta J_y^2 \right\rangle \left\langle \Delta J_z^2 \right\rangle}{|\langle J_x \rangle|^2},$$

which can be calculated according to [32]

$$U_{yz} \approx 1 + \left(\frac{t}{t_0}\right)^6.$$

Then the state remains in a state minimizing Heisenberg's inequality for $t < t_0$. The non-linear interaction will therefore tend to increase the product of uncertainty of the conjugated observables for long times, producing a state that does not saturate the Heisenberg inequality [32].

3. Entanglement for enhanced interferometry

In the previous section, we introduced the notion of squeezed states from a formal point of view, under the action of a non-linear Hamiltonian. In this section, we will show how these non classical states are potentially interesting for interferometry [3, 42].

3.1. Case of a NOON state

One considers the case of a Ramsey interferometer, without loss of generality, the reasoning being generalizable to any atomic interferometer. Each particle can then be described by a two-level system $|0\rangle$ and $|1\rangle$ as well as their possible superpositions. We then consider N atoms initially in the state $|0\rangle$ and after a $\pi/2$ pulse, each atom is then in the superposition of state $|0\rangle$ and $|1\rangle$.

$$|\Psi_i\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right).$$

After the free evolution during an interrogation time T, a relative phase φ is accumulated between states

$$\left|\Psi_f\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\varphi}|1\rangle\right).$$

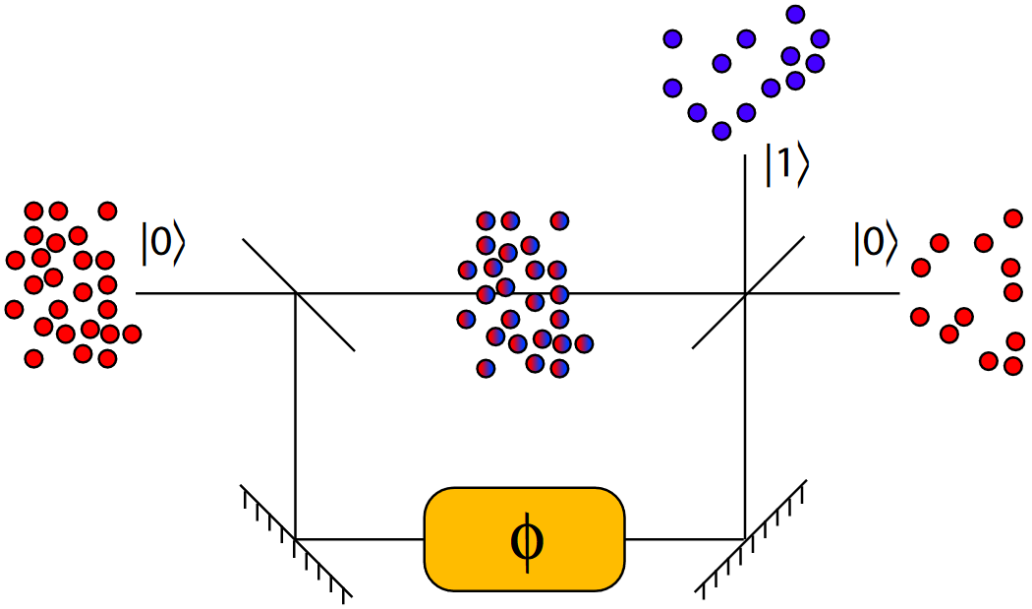


Fig. III.6. Atomic interferometry: we consider the case of a Mach-Zehnder interferometer in order to keep the generality of the reasoning. Most interferometers can be formally reduced to the case of a Mach-Zehnder, such as Ramsey interferometry. The first beam-splitter corresponds then to a $\pi/2$ pulse, and the atoms initially in the state $|0\rangle$ evolve then in the state superposition $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. If the two states are of different energies, a relative phase φ is accumulated between the two states, thus corresponding to the two arms of the equivalent Mach-Zehnder, to obtain a state $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\varphi}|1\rangle\right)$. The second beam-splitter corresponds to a second $\pi/2$ pulse, and the population of the two states (*i.e.* the two output modes of the Mach-Zehnder) will depend on φ.

The probability $p(\varphi)$ that the final state Ψ_f is equal to the initial state Ψ_i makes it possible to evaluate φ according to

$$p(\varphi) = \left|\langle \Psi_i | \Psi_f \rangle\right|^2 = \cos^2\left(\frac{\varphi}{2}\right).$$

If we consider any observable $\hat{O}$ depending on a ζ parameter, measurements of $\hat{O}(\zeta)$ can traced back to ζ. The uncertainty in determining ζ for a single measurement is then

$$\delta\zeta = \frac{\Delta\hat{O}}{\left|\partial\langle\hat{O}\rangle/\partial\zeta\right|},$$

where $\left(\Delta\hat{O}\right)^2 \overset{\text{def.}}{=} \langle\hat{O}^2\rangle - \langle\hat{O}\rangle^2$ is the variance of the observable $\hat{O}$. In the case considered, the uncertainty associated with the phase measurement is then

$$\Delta\varphi = \frac{\Delta p(\varphi)}{\left|\partial p(\varphi)/\partial\varphi\right|},$$

which in the case of a single achievement is $\Delta\varphi = \phi_0$. To improve this measure, the simplest way is to repeat the measure N times, in practice using a cloud of N atoms queried at the same time. If one performs N measurements $\{x_i\}$, then one obtains a good estimator of X with the mean value of x_i

$$X = \sum_{i=1}^{N} \frac{x_i}{N},$$

and an associated uncertainty, in the case of uncorrelated measurements

$$\Delta X = \sqrt{\sum_{i=1}^{N} \frac{\left(\Delta x_i\right)^2}{N}} = \frac{\Delta x}{\sqrt{N}},$$

where the uncertainties of each measurement are assumed to be the same and equal to Δx. Thus a phase measurement with a cloud of uncorrelated N atoms will give an error of

$$\Delta\varphi = \frac{\phi_0}{\sqrt{N}},$$

also known as *standard quantum limit*, by analogy with the corresponding optical case (Mach-Zehnder interferometer), or *quantum projection noise*. Cold atomic clocks have recently reached this limit [13].

We will now focus on the case where the states used in such an interferometer show quantum correlations. First, to illustrate the effect of correlations, we will consider the case of a Schrödinger cat-like state at N atoms. We thus consider the initial NOON-type state

$$|\Psi_i\rangle = \frac{1}{\sqrt{2}}\left(|N,0\rangle + |0,N\rangle\right),$$

which evolves, after interrogation, to the following state

$$\left|\Psi_f\right\rangle = \frac{1}{\sqrt{2}}\left(|N,0\rangle + e^{iN\varphi}\,|0,N\rangle\right).$$

The probability $q(\varphi)$ that $\left|\Psi_f\right\rangle$ is equal to $|\Psi_i\rangle$ is then

$$q(\varphi) = \cos^2\left(N\frac{\varphi}{2}\right),$$

such that one may extract the value of the phase with an uncertainty given by

$$\Delta\varphi = \frac{\Delta q(\varphi)}{|\partial q(\varphi)/\partial\varphi|} = \frac{\phi_0}{N}.$$

The use of a maximally entangled state improves the accuracy of phase measurement by a factor of $\sqrt{N}$ over the standard quantum limit. The limit reached is then fundamental, and it is not possible to obtain a smaller error. This limit is then called *Heisenberg limit*, studied experimentally for a two-ion system of $^9Be^+$ [38], as well as for three ions in a GHZ state [33].

From this simple example, we can see that the introduction of correlations between the different particles reduces the noise of the measurement below the standard quantum limit. From this observation, we deduce that compressed states, in which the different particles are correlated, will also allow measurements to be made below the standard quantum limit. In the next section, we will briefly present the improvement of a measurement using a compressed state in the case of a Ramsey type interferometer. This approach was first performed by D.J. Wineland [53, 52].

3.2. Squeezed states and quantum projection noise

Any two-level system is like an effective spin $1/2$, possibly immersed in a homogeneous magnetic field. Without loss of generality, we will therefore consider a spin $1/2$ in the following, and a Ramsey type interferometer.

During a measurement by Ramsey interferometry, one uses a set of N spin $1/2$ initially in a given state noted $|0\rangle$. An initial $\pi/2$ pulse prepares the set of particles in the state

$$|\Psi_i\rangle = \left(\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\right)^{\otimes N},$$

which after a time of free evolution becomes

$$\left|\Psi_f\right\rangle = \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\varphi}\,|1\rangle\right)\right)^{\otimes N}.$$

In order to measure the relative phase φ accumulated, a second $\pi/2$ pulse is applied to obtain a superposition of the form

$$|\Psi_m\rangle = (\alpha(\varphi)|0\rangle + \beta(\varphi)|1\rangle)^{\otimes N},$$

where $(\alpha, \beta) \in \mathbb{C}$ only depends on the relative phase φ. Excepted of the trivial cases where $\alpha = 1$ or 0, the measurement of the number of atoms in the state $|0\rangle$ is obtained with a statistical error given by the projection noise according to

$$\Delta N_0 = \sqrt{N|\alpha|^2\left(1-|\alpha|^2\right)}.$$

To interpret this Ramsey sequence geometrically, one places oneself within the framework of the formalism of Bloch's sphere. Each particle is a spin $1/2$, $\hat{\mathbf{s}}_i$, the set forming a collective spin $\hat{\mathbf{J}}$ defined as the vectorial sum of the individual spins

$$\hat{\mathbf{J}} = \sum_{i=1}^{N} \hat{\mathbf{s}}_i.$$

This is the direction of the mean effective spin $\mathbf{u} = \langle\hat{\mathbf{J}}\rangle / \left|\langle\hat{\mathbf{J}}\rangle\right|$ which is represented on the Bloch sphere, and the associated uncertainty. Geometrically, a measurement of the populations of the two states corresponds to a projection on the $\mathbf{u}_z$ axis, while a $\pi/2$ pulse is a rotation of $\pi/2$ around the Oy axis. The relative phase φ corresponds to the azimuthal angle with respect to the direction Ox. In the case of a coherent state, the projection noise is the projection of the uncertainty circle on the Oz axis (see Fig. III.7). One now considers

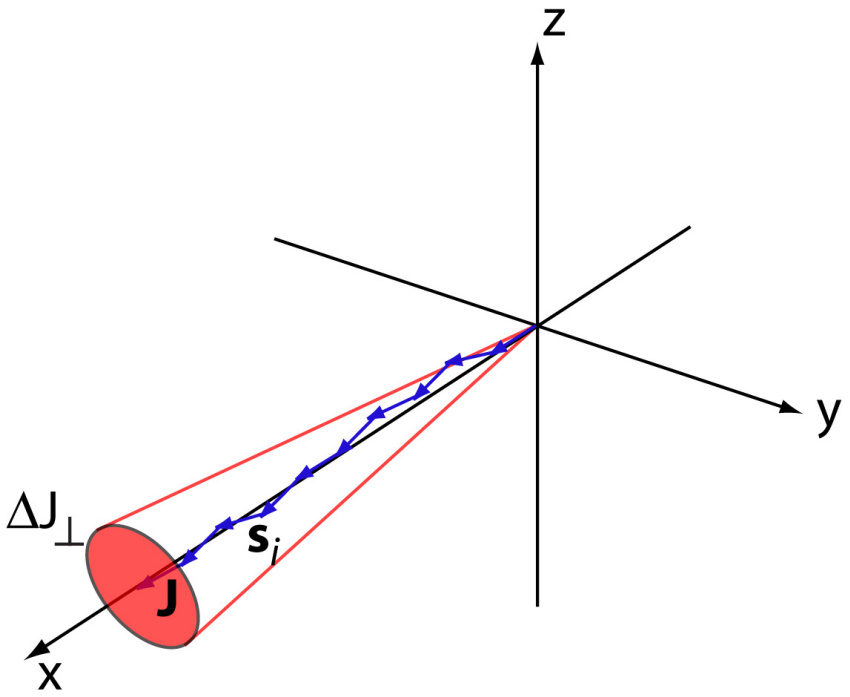


Fig. III.7. Geometric representation of a coherent state in the Bloch sphere. The measurement of populations is geometrically interpreted as the projection of a collective spin on the Oz axis. The circle of uncertainty is represented in red. The variance of the population measurement is related to the variance of the $\hat{J}_z$ operator, geometrically represented in green as the projection of the uncertainty circle on Oz.

a clock based on a Ramsey interferometer where the population measurement N_0 of the state $|0\rangle$ allows to estimate the phase $\varphi = (\omega - \omega_0)T$, where ω is the frequency of the wave coupling the two levels, ω_0 the Larmor frequency associated with the two-level system under consideration and T the interrogation time. One

then obtains an rms error $\delta\omega$ on the measurement of the angular frequency of

$$\delta\omega = \frac{\Delta N_0}{\left|\partial \langle N_0 \rangle / \partial\omega\right|}.$$

By introducing the vector operators associated with the collective spin, we can rewrite this expression according to

$$\delta\omega = \frac{\Delta \hat{J}_z}{\left|\partial \langle \hat{J}_z \rangle / \partial\omega\right|}.$$

Thus, the projection noise $\Delta\hat{J}_z$ has a direct impact on the accuracy of the frequency measurement. In the absolute, this variance $\Delta\hat{J}_z$ is not necessarily equal to $\Delta J_{\perp i}$, the variances of the two axes orthogonal to the direction of the mean spin $\mathbf{u}$. Nevertheless, in practice, a clock works at maximum sensitivity, ie a point of operation where $\left|\partial \langle \hat{J}_z \rangle / \partial\omega\right|$ is maximum. This point corresponds to a collective spin aligned with the Oy axis after interrogation. During the rotation of the second interrogation pulse, the average collective spin will therefore not be affected, only the fluctuations will eventually be modified during the rotation. In this case, the Oz axis is then orthogonal to $\mathbf{u}$ and thus the projection noise corresponds to a variance of a $\mathbf{v}$ component orthogonal to the direction of the mean collective spin.

In the case of a coherent state (CSS), this variance is independent of the $\mathbf{v}$ direction used, and is determined only in respect to the number of particles used. On the other hand, if one considers now the case of an SSS compressed spin state in the sense of the previous section, then there are two axes $\mathbf{v}_1$ and $\mathbf{v}_2$ of minimum and maximum variances respectively. If $\mathbf{v}_1$ is contained in the Oyz plane, then the variance ΔJ_z^2 will be reduced compared to the case of a coherent state. *The use of a compressed spin state reduces the statistical uncertainty due to projection noise in the case of a Ramsey interferometer*. This situation is geometrically illustrated in the formalism of the Bloch sphere in the Fig. III.8. On the other hand, if $\mathbf{v}_2$ is contained in the Oyz plane, the

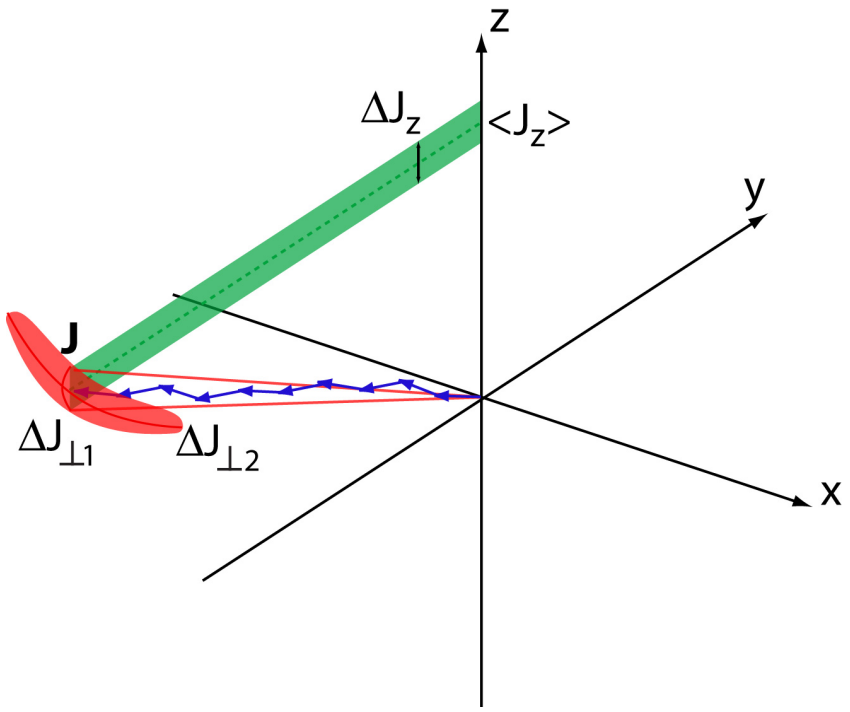


Fig. III.8. Geometrical representation of a squeezed state in the Bloch sphere. The unsqueezed axis is orthogonal to the projection direction $\mathbf{u}_z$. Thus the reduction of the variance $\Delta J_{\perp 1}^2$ reduces the variance of the measured observable ΔJ_z^2. If the state is highly squeezed, the norm of the mean value of the collective spin is reduced compared to a coherent state.

variance ΔJ_z^2 will this time be higher than that of a coherent state, and thus the accuracy of the measurement will be degraded. In the other cases, we obtain a variance value between the two previous extremes.

The use of compressed states will thus make possible to reduce the statistical error of a Ramsey interferometer, as well as any other formally assimilated device. On the other hand, the symmetry of the orthogonal fluctuations of the effective spin is broken, requiring additional precautions for the initial preparation: geometrically one has an ellipse instead of a disc. During a Ramsey interrogation, it is the observable phase that allows to go back to the angular frequency difference $\omega - \omega_0$ in the rotating frame. It is thus the fluctuations of the observable phase which will limit the measurement, i.e. the variance of the collective spin according to the orthogonal direction contained in the plane of the equator. It will thus be necessary to initially generate a compressed state *in phase* to improve a Ramsey interferometer. The projection noise comes from the fluctuations of the observable *number* ($\hat{J}_z$), but this is a direct consequence of the method used to measure the phase, based on a population measurement. Indeed, it is the second $\pi/2$ pulse that causes the state to rotate around Oy. This operation somehow "converts" the phase information into number information. The fluctuations of the compressed state also undergo this rotation, becoming a number compressed state for the measurement (see Fig. III.9).

Finally, it should be noted that the reduction of measurement noise is not sufficient to increase the signal-to-noise ratio. When a state is squeezed, if the angular dispersion of an orthogonal component decreases, the counterpart is that the orthogonal dispersion increases relative to a coherent state. Therefore, for a squeezed state, the mean value of the collective spin $\left\langle \hat{\mathbf{J}} \right\rangle$ will decrease as a norm compared to the case of a coherent state (where $\left\langle \hat{\mathbf{J}} \right\rangle \approx J = N/2$ it the limit $N \gg 1$). This decrease in the mean collective spin norm translates in practice into a reduction in the contrast of the Ramsey fringes (see Fig. III.10 and Fig. III.11), and thus a decrease in the useful signal. Thus, if the state is too highly compressed, the signal reduction will outweigh the noise reduction and the signal-to-noise ratio will decrease. For a compressed state to be useful in the interferometric sense, it must be ensured that it retains sufficient coherence to provide a signal of sufficient amplitude.

3.3. Squeezing factor and Wineland's criterium

In this section, we try to define a compression factor ξ quantifying the fluctuations with respect to the standard quantum limit. Several types of summarization factors can be defined, depending on the context in which the summarized reports are used. In absolute terms, a squeezed state corresponds to the definition introduced previously, i.e. a redistribution of fluctuations in the plane orthogonal to the direction of the average collective spin.

Squeezing factor as a measurement of correlation

This notion was initially introduced by Kitagawa and Ueda [32]. They consider that a state is squeezed of it exists a component $\hat{J}_\perp$ perpendicular to the direction of the mean collectif spin $\left\langle \hat{\mathbf{J}} \right\rangle$, and which variance is below the one of a coherent state (*i.e.* the standard quantum limit $J/2$) [32]. One defines then the spin squeezing factor ξ_S such that

$$\xi_S = \frac{\Delta J_\perp}{\sqrt{J/2}}.$$

In this approach, it is possible to rotate the collective spin to align it with Oz, *i.e.* $\left\langle \hat{\mathbf{J}} \right\rangle = \left\langle \hat{J}_z \right\rangle \mathbf{u}_z$ and such that $\Delta \hat{J}_\perp = \Delta \hat{J}_y$.

Number squeezing factor

Let's now put oneself in the context of interferometers. The relevant observables of the problem are then the relative phase and the number of atoms in a state (or the relative population). In the collective spin formalism, the observable corresponding to the relative populations is $\hat{J}_z$. One will thus be interested only in the reduction of fluctuations of this observable and define the number squeezing factor ξ_N

$$\xi_N = \frac{\Delta \hat{J}_z}{\sqrt{J/2}},$$

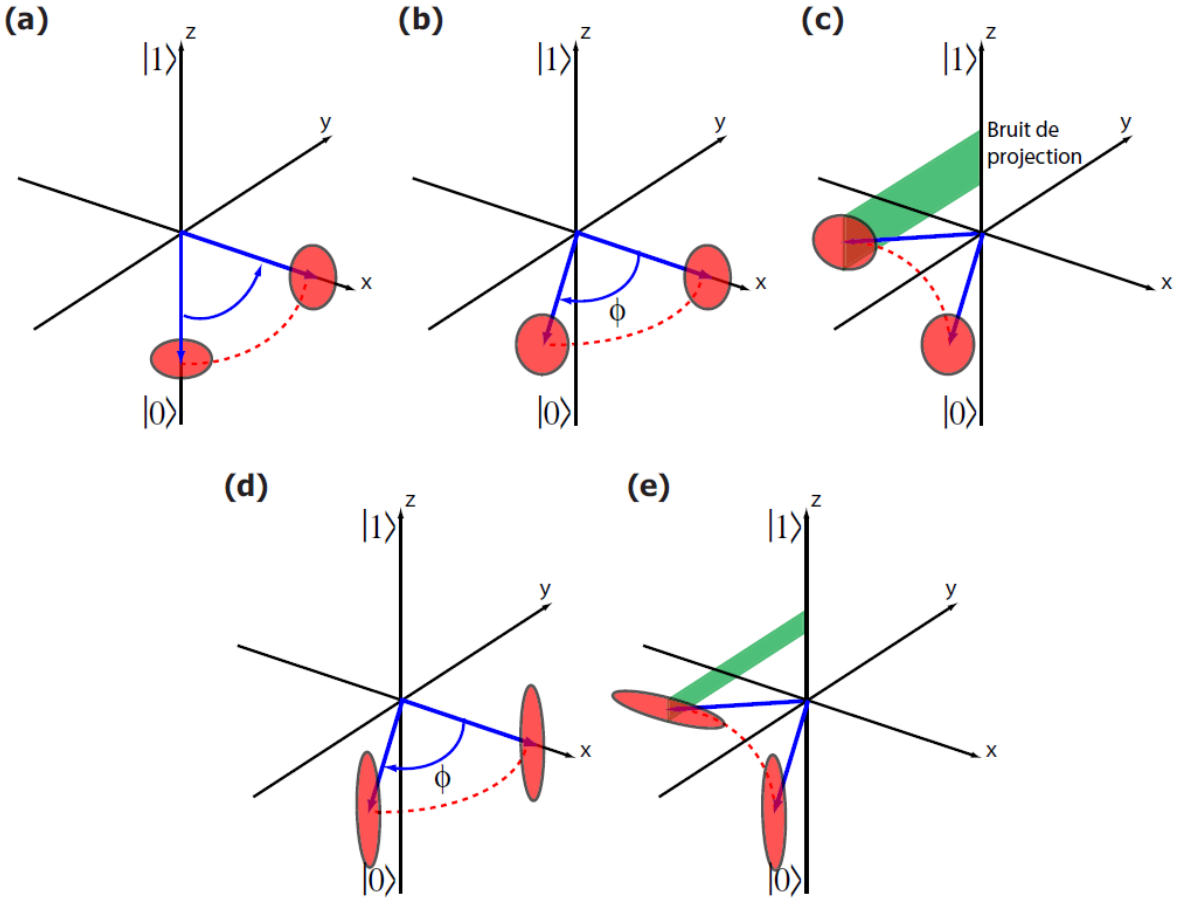


Fig. III.9. Ramsey interferometry with a coherent state (a-b-c) and a compressed state (d-e). Case of a coherent state. (a) Initially, all the spins are in the state $|0\rangle$. A $\pi/2$ pulse prepares them in the superposition $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$. (b) During free evolution, the state precesses around Oz on the Bloch sphere, accumulating a relative φ phase. (c) After interrogation, a second $\pi/2$ pulse allows access to the phase by a population measurement. The projection noise is interpreted geometrically as the projection of the uncertainty disc on the Oz axis. Case of a compressed state. (d) The set of spins is initially prepared in a compressed state, whose low variance axis is aligned with the equator of the Bloch sphere (phase-compressed state). This state accumulates a relative φ phase during the query. (e) A $\pi/2$ pulse is then applied, geometrically translating into a rotation of the state about the Oy axis. The compressed axis of the state is then contained in the yOz plane (number compressed state). During measurement, the projection noise then corresponds to the projection of the compressed variance on the Oz axis. This significantly reduces the measurement noise.

i.e. it compares the fluctuations of the observable $\hat{J}_z$ to the standard quantum limit obtained for a coherent state aligned with the equator of Bloch's sphere. This criterion does not allow a complete estimation of the metrological gain obtained, as it does not include the decrease in contrast, which is due to the fact that $\left|\langle\hat{\mathbf{J}}\rangle\right| < J/2$ for highly squeezed states.

Squeezing factor for metrology

To quantify the gain obtained on the signal-to-noise ratio by using a compressed state instead of a coherent state, a quantization of this gain is introduced using the compression factor for Ramsey interferometry ξ_R [52]

$$\xi_R^2 = \frac{N\Delta J_z^2}{\langle J_x\rangle^2 + \langle J_z\rangle^2}.$$

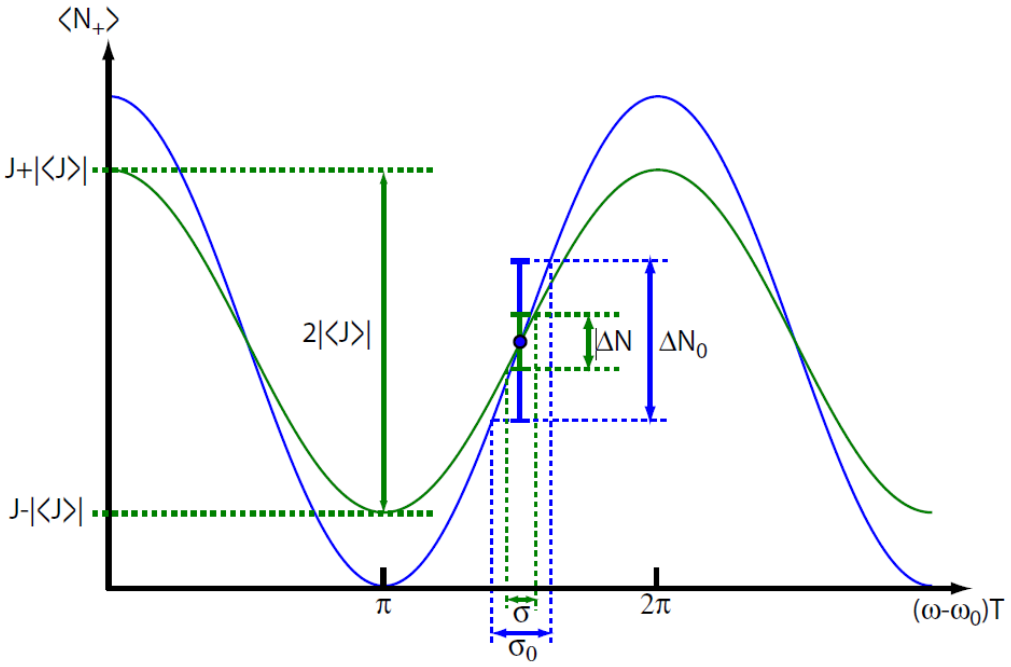


Fig. III.10. Illustration of projection noise reduction on a Ramsey interference signal. The blue curve corresponds to the case of a coherent state while the green curve corresponds to a compressed state. Using a compressed state reduces the projection noise ΔN below its value for a coherent state ΔN_0. On the other hand, the compression of the state decreases the norm of the average collective spin, resulting in practice in a decrease of the amplitude of the interference fringes. These two effects are contradictory, and therefore a compressed state will not necessarily improve the signal-to-noise ratio if the amplitude of the fringes is not sufficient.

If we consider a phase measurement with a Ramsey interferometer, we get a statistical error on the measurement with a compressed state $\delta\varphi$ such that [52]

$$\delta\varphi = \xi_R \delta\varphi_{\text{CSS}},$$

where $\delta\varphi_{\text{CSS}}$ is the statistical error obtained in the case of a consistent report. So we'll have a metrological gain if $\xi_R < 1$. We will notice that in the case of a state pointing the equator of the Bloch sphere, ξ_R is the ratio between the compression angle of the considered state and that of a coherent state.

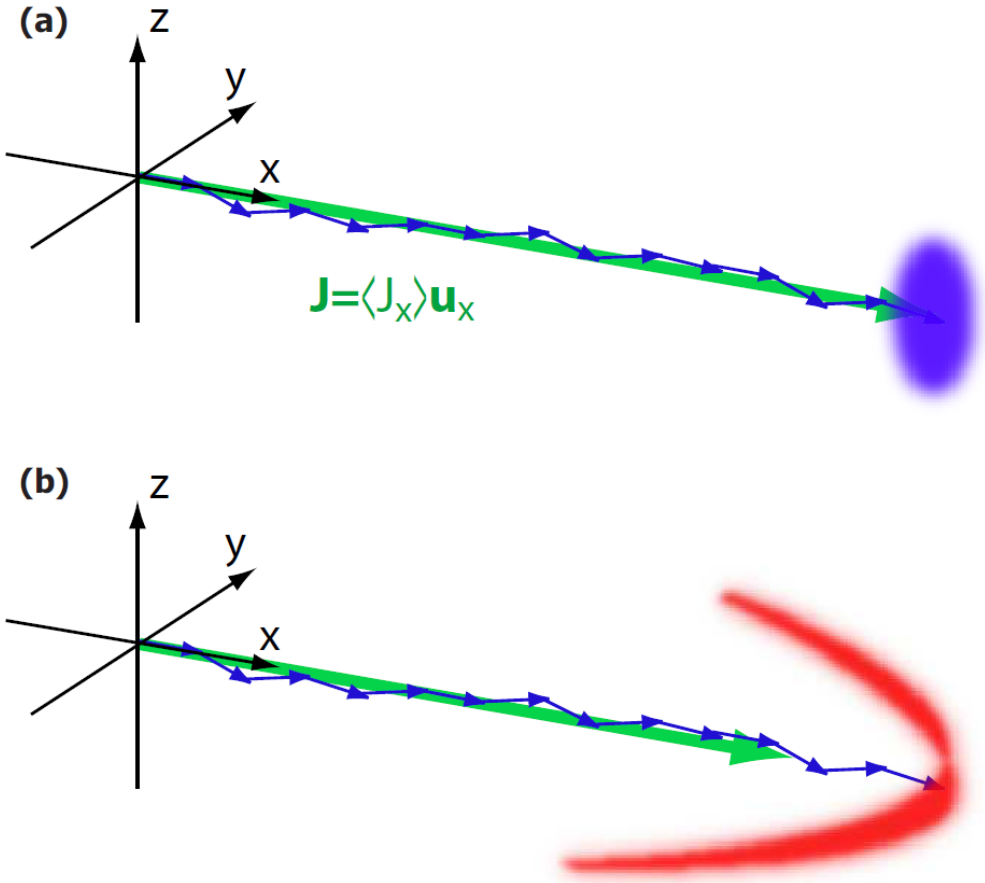


Fig. III.11. Illustration of the contrast reduction of a compressed state. (a) Coherent state of N spins $1/2$. The average total spin is then $\langle \mathbf{J} \rangle \approx N/2\mathbf{u}_x$, with variances $\Delta \left(\mathbf{J} \cdot \mathbf{u}_\perp \right)^2 = N/4$, $\forall \mathbf{u}_\perp$ orthogonal à $\langle \mathbf{J} \rangle$. (b) In the case of a compressed state, the average total spin norm $\langle \mathbf{J} \rangle$ is decreased due to squeezing, *i.e.* the "spreading" of the state over the Bloch sphere. The contrast of the interference fringes is directly proportional to $|\langle \mathbf{J} \rangle|$, so the squeezed quadrature of variance $\Delta J_\perp^2$ will be useful if the signal-to-noise ratio is improved compared to a coherent state, ìe $\Delta J_\perp / |\langle \mathbf{J} \rangle| < 1/\sqrt{N}$.

Chapter IV

Quantum communications: exploiting entanglement

Foundations of quantum physics can be demonstrated with different types of microscopic objects, such as electrons, neutrons, atoms, molecules and Bose-Einstein-condensates. Photons are also quantum objects and they are easy to handle. In the field of experimental quantum physics, many effects are first shown with photons and then extended to more advanced techniques. Photon based systems for quantum cryptography are now commercially available (for example ID Quantique, `http://www.idquantique.com/`).

1. Einstein-Podolsky-Rosen paradox (EPR paradox)

1.1. EPR paradox and the construction of quantum mechanics

In quantum mechanics, the measurement of a superposition of states is inherently random. Let's consider the following state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right).$$

The measurement of the state while give 0 with a probability $P_{|0\rangle} = 1/2$ and 1 with a probability $P_{|1\rangle} = 1/2$. So, in quantum mechanics, the results of a measurement in fundamentally not deterministic: one has only a probability to obtain a given result. At the beginning of quantum mechanics theory, it was difficult for people to admit this lose of deterministic result for measurement (even though the wavefunction is deterministic). Albert Einstein, Boris Podolsky and Nathan Rosen (EPR) argued that the description of physical reality provided by quantum mechanics was incomplete, and there was hidden variables that are missing in the description. Such variables are not accessible to the observer of a given system. In a 1935 paper entitled "Can Quantum-Mechanical Description of Physical Reality be Considered Complete?", they argued for the existence of "elements of reality" that were not part of quantum theory, and speculated that it should be possible to construct a theory containing them. Resolutions of the paradox have important implications for the interpretation of quantum mechanics. Their argumentation was based on a though experiment.

1.2. EPR though experiment

In this though experiment, one considers an entangled state of two particles. Einstein, Podolsky and Rosen pointed out that, in this state, if the position (for example) of the first particle were measured, the result of measuring the position of the second particle could be predicted. They argued that no action taken on the first particle could instantaneously affect the other, since this would involve information being transmitted faster than light, which is forbidden by the theory of relativity. From this, they inferred that the second particle must have a definite value of position and of momentum prior to either being measured. It's a hidden variable theory that could heal the non-locality of quantum mechanics theory.

1.3. Bell's theorem

In 1964, John Bell published a paper on the EPR paradox [4] to investigate whether it was indeed possible to solve the nonlocality problem with hidden variables. One considers then a entangled state made of two spins. Then, each spin is measured on a given axis, but not necessary the same axis. Bell showed that both models (quantum and hidden variables) can reproduce the correlations between the two measurements when they are

performed on the same axis or on perpendicular axes for both particles. As soon as other angles between their axes of measurement are allowed, local hidden-variable theories become unable of reproducing the quantum mechanical correlations. This difference, expressed using inequalities known as "Bell inequalities", is in principle experimentally testable. The experiment proposed by Bell has been experimentally realized for the first time in 1982 by Alain Aspect and his team at Orsay, Paris, conducted Bell tests using calcium cascade sources [2].

1.4. Bell's states and Bell's inequality

The Bell states are specific quantum states of two 2-level particles maximally entangled. Entanglement is a basis-independent result of superposition. Due to this superposition, measurement of the particle will collapse it into one of its basis states with a given probability. Because of the entanglement, measurement of one particle will assign one of two possible values to the other particle instantly, where the value assigned depends on which Bell state the two particles are in. Bell states can be generalized to represent specific quantum states of multi-particles systems, such as the GHZ state for three particles. Now one consider the case of two particles only, for example two photons which might be described by their polarization, equivalent to a two level system (two orthogonal polarizations). Let labels one particle A (for Alice) and the other one B (for Bob). Each observer, Alice and Bob, might measure their photon within two different directions (not necessarily orthogonal). Let note $\hat{A}_i$ (resp. $\hat{B}_i$) the two observables associated to the measurement with the photon A (resp. B). These observables are such that they outcomes ± 1 and $\left[\hat{A}_i, \hat{B}_j\right] = 0, \forall i, j$.

Then, one defines the Clauser-Horne-Shimony-Holt (CHSH) observable $\hat{\mathscr{O}}$ such as

$$\hat{\mathscr{O}} = \hat{A}_1\hat{B}_1 + \hat{A}_1\hat{B}_2 + \hat{A}_2\hat{B}_1 - \hat{A}_2\hat{B}_2.$$

Since $\hat{A}_i^2 = \hat{B}_i^2 = \hat{\mathbb{I}}$, one obtains

$$\hat{\mathscr{O}}^2 = 4\hat{\mathbb{I}} - [A_1, A_2]\,[B_2, B_2]\,.$$

If $[A_1, A_2] = [B_2, B_2] = 0$, then $\hat{\mathscr{O}}^2 = 4\hat{\mathbb{I}}$ such that immediately $\left\langle \hat{\mathscr{O}} \right\rangle \leq 2$. This upper bound of 2 is also the upper bound one obtains in the case of a classical hidden variable theory.

In the quantum case, since

$$\left|\left\langle \left[\hat{A}_1, \hat{A}_2\right] \right\rangle\right| \leq 2\left|\left\langle \hat{A}_1 \right\rangle\right| \cdot \left|\left\langle \hat{A}_2 \right\rangle\right| \leq 2.$$

Similarly,

$$\left|\left\langle \left[\hat{B}_1, \hat{B}_2\right] \right\rangle\right| \leq 2\left|\left\langle \hat{B}_1 \right\rangle\right| \cdot \left|\left\langle \hat{B}_2 \right\rangle\right| \leq 2.$$

Therefore

$$\left\langle \hat{\mathscr{O}}^2 \right\rangle \leq 4 + \left|\left\langle [A_1, A_2]\,[B_2, B_2] \right\rangle\right| \leq 4 + \left|\left\langle [A_1, A_2] \right\rangle\right| \cdot \left|\left\langle [B_1, B_2] \right\rangle\right| \leq 4 + 4.$$

So finally, in the quantum case, the Clauser-Horne-Shimony-Holt observable is upper-bounded by the so-called Tsirelson bound

$$\left\langle \hat{\mathscr{O}} \right\rangle \leq 2\sqrt{2}.$$

Then, if one realizes experimentally a situation such that

$$2 < \left\langle \hat{\mathscr{O}} \right\rangle \leq 2\sqrt{2},$$

Bell's inequalities are said to be violated: only quantum correlations may explain such inequality, not hidden variables theory.

The upper-bound is obtained for certain type of observables, for instance

$$\hat{A}_1 = \hat{\sigma}_{z,A},\ \ \hat{A}_2 = \hat{\sigma}_{x,A},\ \ \hat{B}_1 = -\frac{1}{\sqrt{2}}\left(\hat{\sigma}_{z,B} + \hat{\sigma}_{x,B}\right),\ \ \hat{B}_2 = \frac{1}{\sqrt{2}}\left(\hat{\sigma}_{z,B} - \hat{\sigma}_{x,B}\right),$$

then it is easy to demonstrate that

$$\left\langle \hat{\mathscr{O}} \right\rangle = 2\sqrt{2} > 2.$$

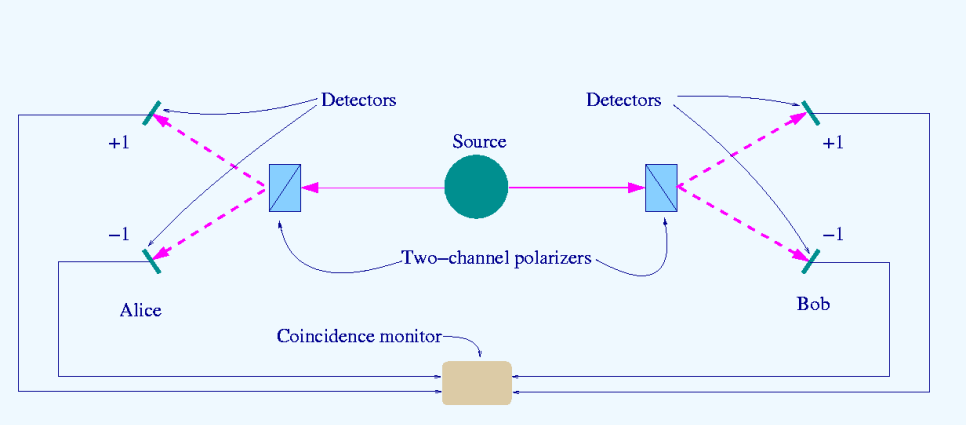


Fig. IV.1. Scheme of a "two-channel" Bell test The source S produces pairs of "photons", sent in opposite directions. Each photon encounters a two-channel polariser whose orientation (a or b) can be set by the experimenter. Emerging signals from each channel are detected and coincidences of four types (++, –, +- and -+) counted by the coincidence monitor. `https://en.wikipedia.org/wiki/Bell's_theorem`

A Bell test consists in testing such inequality to insure that two particle have quantum correlations (*i.e.* not explained classically) to insure they are entangled. Classical correlation can't explain such inequality. Four specific two-qubit states with the maximal value of $2\sqrt{2}$ are designated as "Bell states". They are known as the four maximally entangled two-qubit Bell states, and they form a maximally entangled basis, known as the Bell basis, of the four-dimensional Hilbert space for two qubits:

$$|\phi+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

$$|\phi-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$

$$|\psi+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$

$$|\psi-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

1.5. GHZ state

A Greenberger–Horne–Zeilinger state (GHZ state) is a certain type of entangled quantum state that involves $M > 2$ subsystems (particle states, or qubits). It was first studied by Daniel Greenberger, Michael Horne and Anton Zeilinger in 1989. If each subsystem has a dimension d, the local Hilbert space is isomorphic to $\mathbb{C}^d$, then the total Hilbert space is M subsystems is $\mathscr{H} = (\mathbb{C}^d)^{\otimes M}$.

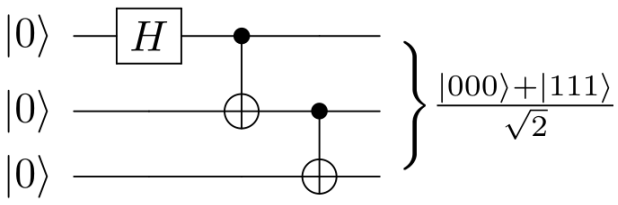


Fig. IV.2. Generation of a 3-qubits GHZ state with a quantum computer. Extract from `https://en.wikipedia.org/wiki/Greenberger-Horne-Zeilinger_state`

Then, the GHZ state is expressed as

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle\otimes\cdots\otimes|i\rangle = \frac{1}{\sqrt{d}}(|0\rangle\otimes\cdots\otimes|0\rangle + \cdots + |d-1\rangle\otimes\cdots\otimes|d-1\rangle).$$

In the case of qubits ($d = 2$),

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes M} + |1\rangle^{\otimes M}\right).$$

The GHZ state is a maximally entangled quantum state. The simplest one is the 3-qubit GHZ state:

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right).$$

GHZ states are used in several protocols in quantum communication and cryptography.

2. QRNG and QKD

2.1. Quantum Random Number Generators

Random numbers are essential for a number of applications: encrypted data transmission (secret keys) or numerical methods rely on them (such as Monte-Carlo) for example. The random numbers have to be unpredictable and uniformly distributed. Random Number Generators (RNG) produce sequences of random numbers. If in some application the random numbers may be known, it is clearly not the case for several such as encrypted communication based on secret keys. Unpredictability refers to the fact that it is impossible to predict the next random number, even if the previous ones are known. Insuring unpredictability of a random number sequence is actually very challenging. There are three distinct types of random number generators (RNG): Pseudo-RNGs, True RNGs, and Quantum RNGs.

Pseudo-RNGs are deterministic mathematical algorithms that basically “expand” a given random seed to a much longer sequence of random numbers. The random seed is supposed to be "real randomness". The advantage of pseudo-RNGs is that they are very cheap. But they are not suited for high-quality cryptography, as a result of lack of standardization of the original seed.

In the case of True RNGs (TRNGs) and Quantum RNGs (QRNGs), random numbers are produced from the results of physical processes. Random number sequences gained in this way always have a particular level of predictability, so that they are not ideal. But applying randomness extraction to a non-ideal random number sequence produces an ideal but shorter random number sequence. TRNGs take their random numbers from classical physical processes which are unpredictable, caused by many uncontrollable degrees of freedom (for example noise) or systems with chaotic behaviour. TRNGs based on noise in electronic circuits are very cheap and small, but the quality of the random numbers produced by TRNGs is difficult to assess. Realizing a quality TRNG is challenging and difficult to certify.

QRNGs produces random numbers from inherently indeterministic quantum processes. The inability to predict the numbers is not just based on complexity but from the fundamental probabilistic nature of a measurement of a quantum state, providing the later is not an eigenstate of the observable used. Consequently, it is impossible to predict random numbers that are produced by QRNGs. For instance, it could be a measurement of a qubit on the following state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$$

which results in 50% probability of 0 as result, and 50% probability of 1. Repeating the process, it is straightforward that one obtains a random binary number with a arbitrary number of bits. QRNGs have two major advantages: they exploit the randomness of nature which results from quantum mechanics and their implementation is relatively easy. However, it is still challenging to make a small and cheap or a really fast QRNG.

2.2. Quantum Key Distribution

Today’s digital society is highly dependent on the security of data, both during communication as well as in storage. With the progress of quantum computers that can potentially break this security, alternative encryption scheme have been developed to exploit quantum properties for higher level and long term security. The concept of quantum key distribution (QKD) was first proposed in the 1970s but it wasn’t until the 1990s

that physicists started to get really interested. Since then the progress has been remarkable and **it is the most mature quantum technology, being commercially available for over 15 years now.** Progress continues on making these systems more compact, cheaper, and capable of operating over longer distances. These are all critical steps for the uptake of these technologies by governments and industry. The main actual challenge of such QKD systems is their integration into the existing network infrastructure.

QKD provides a way of distributing and sharing secret keys that are necessary for cryptographic protocols. The security is insured from the projective nature of measurement. If a spy intercept the quantum communication, he will project the state. In other words, the observation modifies a quantum state. The key point of secured quantum communications is the ability to detect that a quantum state has been projected prior to its arrival (meaning there was a spy on the line). Typically, information is encoded on two orthogonal states of polarizations of single photons. The beauty that quantum physics is that if a spy tries to intercept the key generation, he will introduce detectable consequences from projective measurement and reveal themselves. Importantly, this happens at the secret key generation, and therefore before any information is encoded or communicated! First commercial systems of QKD appeared in the early 2000s. High rates (>Mbps) and long distances (>400km) have been demonstrated and both academic and commercial systems continue to get smaller and cheaper.

3. Cryptography and quantum physics

3.1. Benefits of quantum physics for cryptography

The principle of cryptography relies on encoding a message with a key. With a mathematical operation based on this key, the message might be revealed. Otherwise, an algorithm might be sued to "crack" the message. Cryptography consists in the use of a encoding procedure complex enough (mathematically) so it takes decades of years for an algorithm to crack it with a classical computer.

The most common algorithm used for secured transaction on internet and files encryption is the *RAS algorithm*. RSA algorithm has been described in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman. It has been patented by MIT in 1983. The patent is in the public domain since 2000. The RSA algorithm is asymmetric, based on the use of two *keys*. A key is an integer number of large value. The *public key* is used to encrypt and the *private* key is used to decrypt confidential data.

Let call *Alice* a person who wants to receive confidential data or files. She creates two keys : a public and a private key. Alice makes the public key accessible. Alice's correspondent, called *Bob*, uses this key to encrypt the data he wants to send to her. The private key is reserved for Alice, and allows her to decrypt theses data. The private key can also be sued by Alice to sign a file she sends: the public key allowing anybody to verify the signature.

A prerequisite is that it is "computationally" impossible to decrypt the file using only the public key and impossible to reconstruct the private key from the public key. RSA encryption is often used to communicate a symmetric encryption key, which then allows the exchange to continue in a confidential manner. Mathematically, RSA encryption is based on the difficulty for factorizing $n = p \times q$ a large integer number as a production of two prime numbers.

With a quantum computer, it is possible to crack a RSA key "easily" with Shor's algorithm. But in the context of cryptography, quantum *strangness* has two major advantages

— Quantum measurements are probabilistic. It is possible to generate real random number while it is not easy to have a random generator which is really random in classical computers. For example, with a state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, then the quantity $\langle\psi|\hat{Z}|\psi\rangle$ randomly produces -1 or $+1$ as result, and it is fundamentally random.

— In classical computers and classical communications, if the message is intercepted by a spy (let's call it *Eve*), then she can copy the message and transmit it to Alice or Bob. There is not way for Alice or Bob to know if the message has been intercepted or not. In quantum mechanics, if the spy intercept a quantum message, she will perform a measurement and the state will be affected (projective measurement). As we will see later, it is not possible to duplicate a quantum state (non-cloning theorem). Then, it is possible for Alice and Bob to know that a spy as intercept the message in the case of quantum communications.

3.2. Non-cloning theorem

It is impossible to physically duplicate an arbitrary quantum state $|\psi\rangle$ [54].

Remark: the non-cloning theorem considers an arbitrary state $|\psi\rangle$. Of course it is possible to duplicate pure states $|0\rangle$ or $|1\rangle$ for example with C-gates.

Demonstration: Let assume that we have a unitry operator $\hat{U}_{\text{cloning}}$ and two quantum states $|\phi\rangle$ and $|\psi\rangle$ which $\hat{U}_{\text{cloning}}$ duplicates, *i.e.*

$$|\phi\rangle \otimes |0\rangle \overset{\hat{U}_{\text{cloning}}}{\longrightarrow} |\phi\rangle \otimes |\phi\rangle,$$
$$|\psi\rangle \otimes |0\rangle \overset{\hat{U}_{\text{cloning}}}{\longrightarrow} |\psi\rangle \otimes |\psi\rangle.$$

Then,

$$\langle\phi|\psi\rangle = \left(\langle\phi|\langle 0|\right)\left(|\psi\rangle|0\rangle\right).$$

Or, $\hat{U}_{\text{cloning}}$ is unitary

$$\hat{U}^{\dagger}_{\text{cloning}}\hat{U}_{\text{cloning}} = \hat{U}_{\text{cloning}}\hat{U}^{\dagger}_{\text{cloning}} = \mathbb{I}$$

Then

$$\begin{aligned}\langle\phi|\psi\rangle &= \left(\langle\phi|\langle 0|\right)\hat{U}^{\dagger}_{\text{cloning}}\hat{U}_{\text{cloning}}\left(|\psi\rangle|0\rangle\right)\\ &= \left(\langle\phi|\langle\phi|\right)\left(|\psi\rangle|\psi\rangle\right)\\ &= \langle\phi|\psi\rangle^2,\end{aligned}$$

therefore

$$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2 \Rightarrow \langle\phi|\psi\rangle = 0 \text{ or } 1.$$

Suppose that $\hat{U}_{\text{cloning}}$ duplicates the following state

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

then

$$\begin{aligned}|\phi\rangle \otimes |0\rangle \overset{\hat{U}_{\text{cloning}}}{\longrightarrow} |\phi\rangle \otimes |\phi\rangle &= \left(\alpha|0\rangle + \beta|1\rangle\right)\left(\alpha|0\rangle + \beta|1\rangle\right),\\ &= \alpha^2|00\rangle + \alpha\beta\left(|10\rangle + |01\rangle\right) + \beta^2|11\rangle.\end{aligned}$$

But now if we use $\hat{U}_{\text{cloning}}$ to clone the expansion of $|\phi\rangle$, we arrive at a different state.

$$\left(\alpha|0\rangle + \beta|1\rangle\right)|0\rangle \overset{\hat{U}_{\text{cloning}}}{\longrightarrow} \alpha|00\rangle + \beta|11\rangle.$$

In the last expression, there is no crossed terms, thus we have a contradiction. Such an unitary operator $\hat{U}_{\text{cloning}}$ does not exist. Note that it is however possible to clone a known state such as $|0\rangle$ and $|1\rangle$.

3.3. Teleportation

If it is not possible to duplicate a state, it is possible to teleport a state. Quantum teleportation is a mean to replace the state of one qubit with another. The state is "transmitted" by setting an entangled state-space of three qubits and then removing two qubits from the entanglement (via measurement). Let consider a state

$$|\psi\rangle = a|0\rangle + b|1\rangle,$$

a state to teleport, and

$$|\phi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right),$$

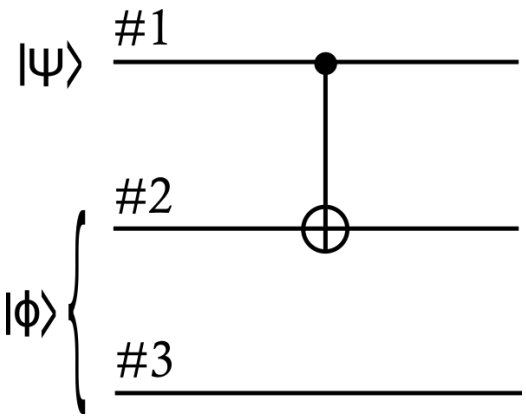


Fig. IV.3. Encoding $|\psi\rangle$ in $|\phi\rangle$ for quantum teleportation.

a so-called EPR state [1]. The state of the entire system is

$$|\psi\rangle|\phi\rangle = \frac{1}{\sqrt{2}}\left(a|0\rangle\left(|00\rangle+|11\rangle\right)+b|1\rangle\left(|00\rangle+|11\rangle\right)\right).$$

Then, applying a C-NOT control with $|\psi\rangle$ as a control qubit and the first qubit of $|\phi\rangle$ as a target qubit (see Fig. IV.3), one obtains the following state

$$\frac{1}{\sqrt{2}}\left(a|0\rangle\left(|00\rangle+|11\rangle\right)+b|1\rangle\left(|10\rangle+|01\rangle\right)\right).$$

Then, we apply a Hadamard gate on the qubit $|\psi\rangle$, to obtain the state $|\varphi\rangle$

$$|\varphi\rangle = \frac{1}{\sqrt{2}}\left(\frac{a}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\left(|00\rangle+|11\rangle\right)+\frac{b}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)\left(|10\rangle+|01\rangle\right)\right).$$

This state might be written as

$$|\varphi\rangle = \frac{1}{2}\left(|00\rangle\left(a|0\rangle+b|1\rangle\right)+|01\rangle\left(a|1\rangle+b|0\rangle\right)+|10\rangle\left(a|0\rangle-b|1\rangle\right)+|11\rangle\left(a|1\rangle-b|0\rangle\right)\right),$$

which we can shorten to

$$|\varphi\rangle = \frac{1}{2}\left(|00\rangle\begin{pmatrix}1&0\\0&1\end{pmatrix}|\psi\rangle+|01\rangle\begin{pmatrix}0&1\\1&0\end{pmatrix}|\psi\rangle+|10\rangle\begin{pmatrix}1&0\\0&-1\end{pmatrix}|\psi\rangle+i|11\rangle\begin{pmatrix}0&-i\\i&0\end{pmatrix}|\psi\rangle\right)$$

Introducing Pauli's matrix of qubit #3 ($\hat{\mathbb{I}}$,$\hat{X}$,$\hat{Y}$,$\hat{Z}$), then

$$|\varphi\rangle = \frac{1}{2}\left(|00\rangle\hat{\mathbb{I}}|\psi\rangle+|01\rangle\hat{X}|\psi\rangle+|10\rangle\hat{Z}|\psi\rangle+i|11\rangle\hat{Y}|\psi\rangle\right),$$

and alternatively

$$|\varphi\rangle = \frac{1}{2}\left(|00\rangle\hat{\mathbb{I}}|\psi\rangle+|01\rangle\hat{X}|\psi\rangle+|10\rangle\hat{Z}|\psi\rangle+|11\rangle\hat{X}\hat{Z}|\psi\rangle\right).$$

For each term, the two qubits state of qubits #1 and #2 is different in each term. This result implies that we can measure the first and second qubits to obtain two classical bits which tell us what unitary operation was applied on the third qubit. Then, we can subsequently "fix up" the third qubit once we know the classical outcome of the measurement of the first two qubits. This fix-up is fairly straightforward,either applying nothing, $\hat{X}$, $\hat{Z}$ or $\hat{Z}\hat{X}$ (reminder: $\hat{X}^2=\hat{Y}^2=\hat{Z}^2=\hat{\mathbb{I}}$), see Fig. IV.4.

Remark: if qubit #1 is measured in state $|1\rangle$, one should apply $\hat{Z}$, nothing otherwise. If qubit #2 is measured in state $|1\rangle$, one should apply $\hat{X}$, nothing otherwise.

It is then possible to implement quantum teleportation with the following circuit (double lines represent classical information), represented Fig. IV.5. First, one prepares the EPR state, then it is possible to have qubit #2 and qubit #3 at different locations.

1. An EPR state might be generated by an Hadamard gate followed by a C-NOT gate.

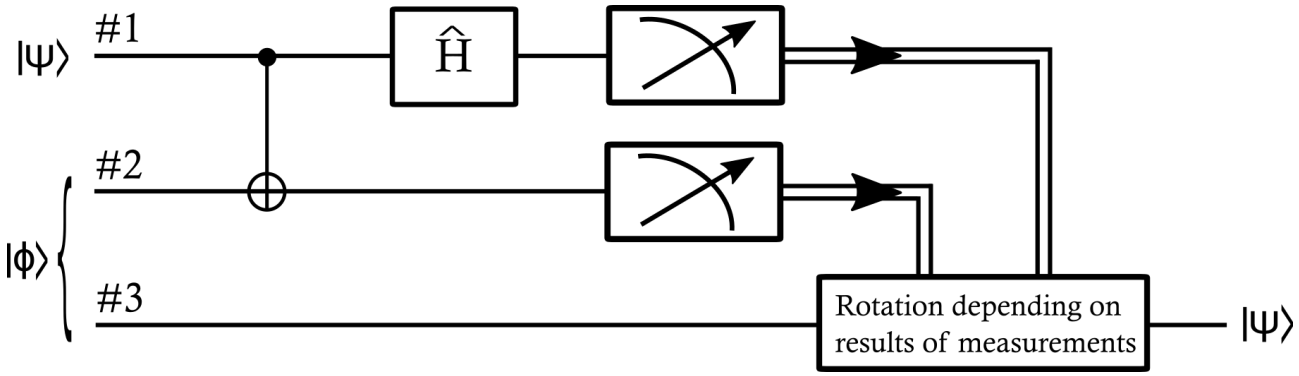


Fig. IV.4. Reconstruction of the initial state.

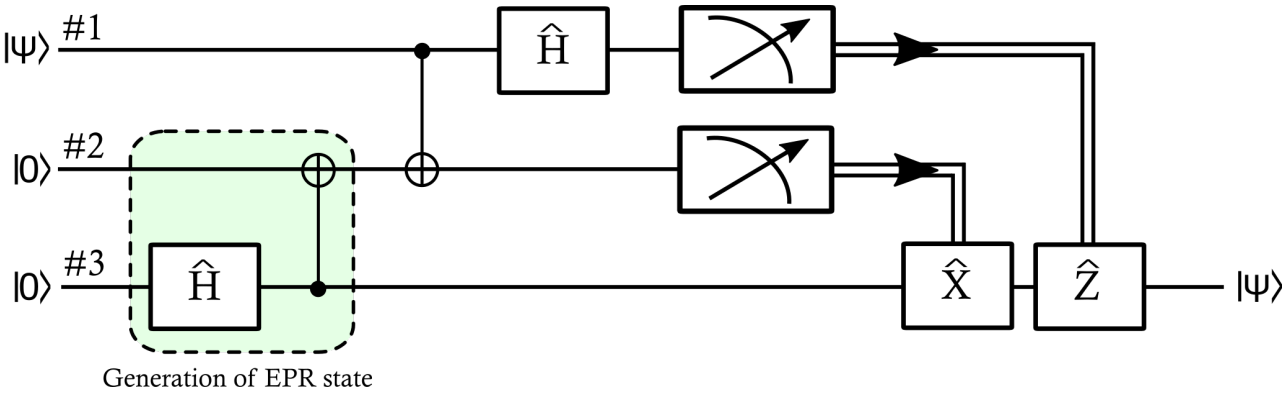


Fig. IV.5. Implementation of quantum teleportation: complet diagram.

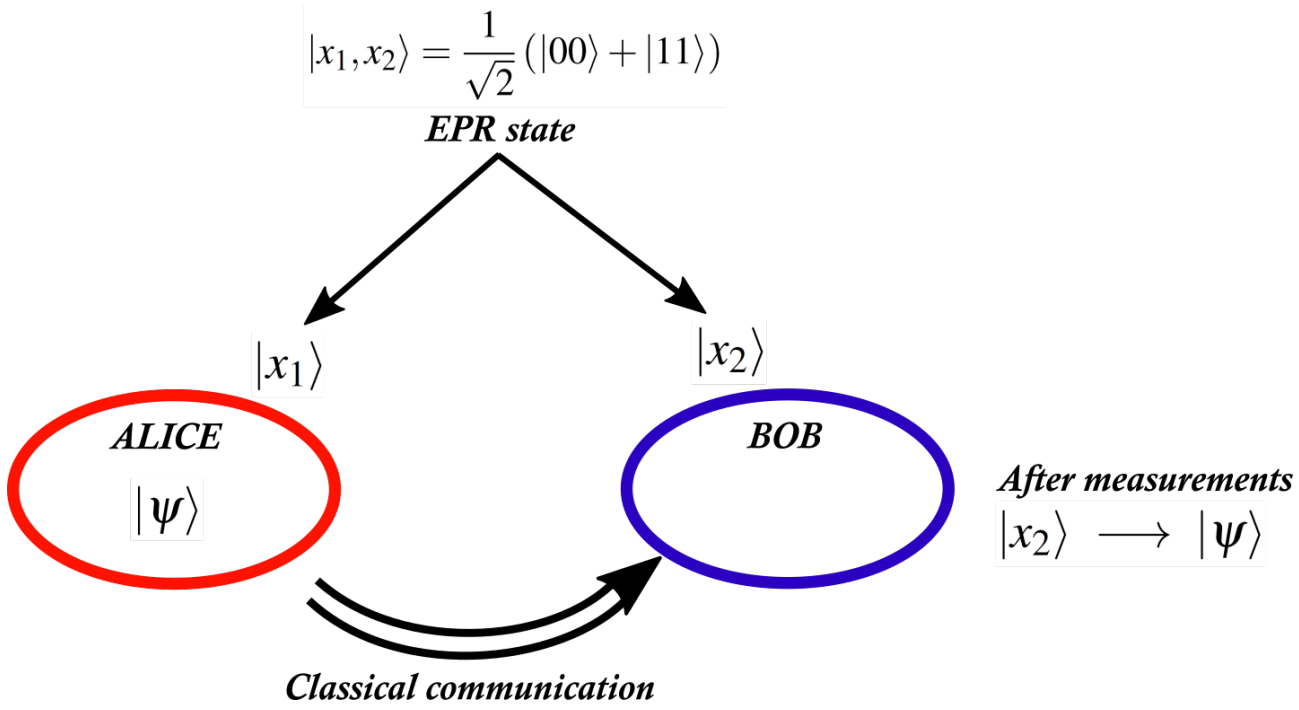


Fig. IV.6. General scheme of quantum teleportation

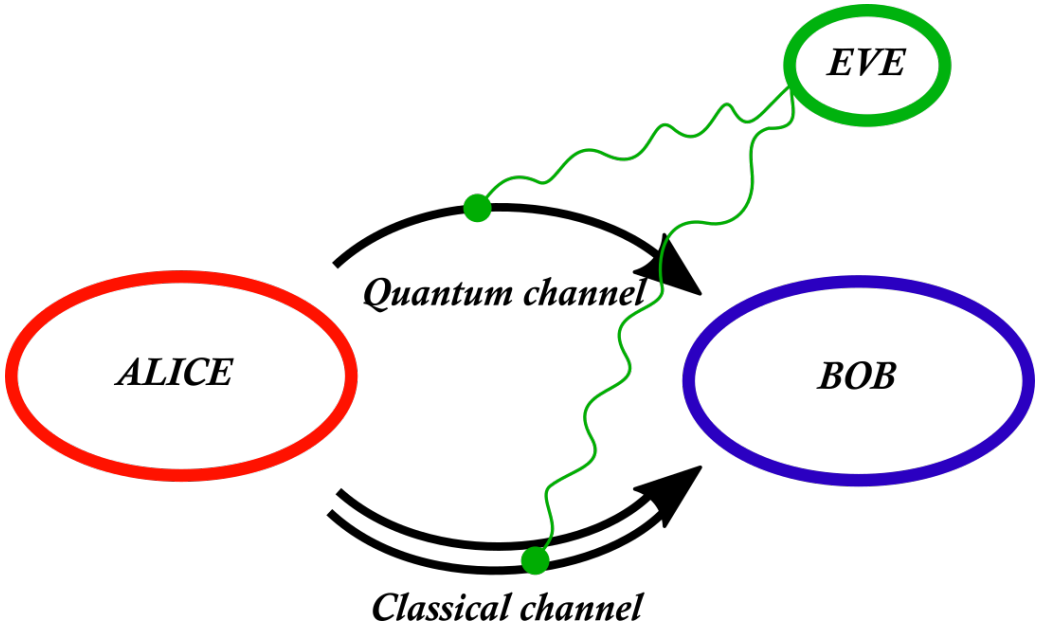


Fig. IV.7. General scheme of the BB84 protocol.

4. The BB84 protocol

In 1984, the first protocol for quantum cryptography was proposed by Charles H. Bennett and Gilles Brassard, name "BB84" [5]. The BB84 protocol uses pulses of polarized light, where each pulse contains a single photon. Alice and Bob are connected by a quantum channel, for example an optical fibre, and a classical public channel, such as a phone line or an Internet connexion [50].

In pratice, it is common to use the same link for both channels. In the case of polarized photons, this would be an optical fiber, differing only in the intensity of light pulses: while for the quantum channel it consists in one photon per qubit, the classical channel uses hundreds of photons per bits. In order to encrypte messages, Alice and Bob need to share a secret key: that is the aim of quantum cryptography. Alice has the message and the key, she can generate an encrypted message. The problem consists in transferring the key. In order to provide a secure communication, Alice can choose between four non-orthogonal states. She has two bases with polarized photons.

The horizontal-vertical basis (noted $\oplus$)
- Horizontally polarized photon $|\rightarrow\rangle$,
- Vertically polarized photon $|\uparrow\rangle$,

and the diagonal basis (noted $\otimes$)
- $+45°$ polarized photon $|\nearrow\rangle$,
- $-45°$ polarized photon $|\nwarrow\rangle$.

To transmit information, a coding system is required. In this case and the diagonal basis (noted $\otimes$)
- $|\uparrow\rangle$ and $|\nwarrow\rangle$ encode for 0,
- $|\rightarrow\rangle$ and $|\nearrow\rangle$ encode for 1.

Alice chooses randomly one of the polarization state ($\oplus$ or $\otimes$) for each photon and sends the corresponding state to Bob. Then, Bob measures the incoming state in one of the two bases. If Alice and Bob use the same basis, they will get perfectly correlated results. However, every time Bob chooses a different basis than Alice, he will not get any information about the state of the photon. For example, if Alice send $|\rightarrow\rangle$ and Bob measures in the diagonal basis $\otimes$, he will get 50% probability of measuring $+45°$ and 50% probability of measuring $-45°$. Even if he finds out afterwards that he has chosen the wrong basis, he will not be able to determine which polarization state Alice has sent.

BB84 protocol

1. Alice chooses randomly both the basis and polarization of each photon and sends the corresponding polarization state to Bob.
2. Independently and randomly for each photon, Bob chooses one of the two bases. He either measures in the same basis than Alice and gets a perfectly correlated result or the exact opposite. If he measures in a different basis than Alice, he gets uncorrelated results. Sometimes, it also happens that Bob does not register anything because of errors on the detection or in the transmission.
3. Bob obtains a string of all received bits, also called *raw key*.
4. For each bit, Bob announces via the public channel which bases was used and which photons were registered ($\oplus$ or $\otimes$) but of course **he does not reveal which result he obtained**.
5. After comparing the selected bases, Alice and Bob keep only the bits corresponding to the same basis. Because both have randomly chosen the basis, they get correlated and uncorrelated results with equal probability. Therefore, about 50% of raw key is discarded. The shorter key is called *sifted key*.
6. Alice and Bob choose randomly some of the remaining bits which they will discard later to check the error rate. There are two main reason why the error rate can differ from the expected value: technical imperfections in the setup and a potential **spy** on the transmission line. To ensure a secret key, Alice and Bob must correct the errors and they reduce Eve's knowledge of the key. The remaining string of bits is the secret key.
7. Eventually, the actual process encrypting a message can begin.

The role of the spy

Eve's goal is to obtain as much valuable information as possible. The easiest way is to intercept a qubit which is transmitted from Alice to Bob. But Eve must send a qubit to Bob. Otherwise, he will tell Alice to disregard this measurement, because he did not receive the expected qubit. Consequently, Eve would not gain any useful information. In the ideal case, Eve would send a qubit in its original state. But because of the non-cloning theorem which states that creating a copy of an unknown quantum state is impossible, Eve must find another spying strategy.

One of them is the intercept-resend strategy. In this case, Eve uses the same equipment than Bob, but just like him, she can't know in which basis Alice has measured the qubit ($\oplus$ or $\otimes$). She has no other choice but to choose the basis randomly. In 50% of the cases, Eve will guess the correct basis and resend a qubit in the correct state to Bob. Consequently, Eve's intervention will not be noticed by the legitimate users. However in the remaining cases, Eve will use the wrong basis as she has no information about Alice's choice. This intervention will be discovered, in half of the cases, by Alice and Bob as they get uncorrelated results. With the help of the intercept-resend strategy, Eve will get 50% information but Alice and Bob will obtain 25% error rate in their sifted key, which reveals the presence of Eve.

What if Eve applies this strategy to only a fraction of measurements?

For example, with only 10% of the measurements collected by Eve, only 2.5% error rate is expected, while Eve information will be 5%. In order to appeal against such an attack, Alice and Bob use classical algorithms, first to correct the errors, and then to reduce Eve's knowledge of the final key. This process is called **privacy amplification** [23].

Chapter V

Quantum computers: industrial applications and actual players

1. Development of a commercial computer: a technological challenge!

1.1. Which technology is appropriated?

The quantum race

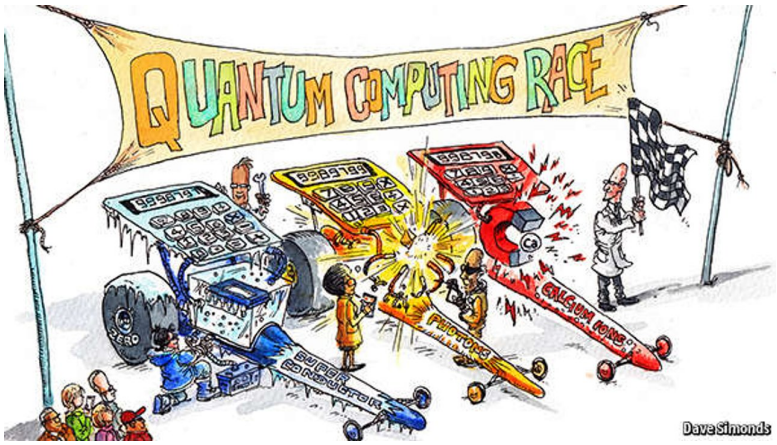


Fig. V.1. The quantum race for the most appropriate technology to develop a commercial quantum computer. Extracted from *A little bit, better*, The Economist, June 20th, 2015
`https://www.economist.com/science-and-technology/2015/06/20/a-little-bit-better`

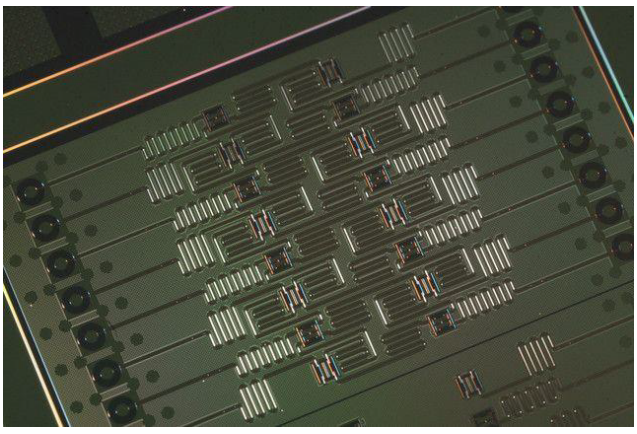


Fig. V.2. Photo of a chip with superconducting qubits (Picture credits: IBM research). Extracted from reference [41].

Building a quantum computer relies on the ability to develop a chip on which are integrated qubits, or an equivalent system. Hardware companies are pursuing a range of technologies with very different characteristics and properties. As of now, it is unclear which will ultimately form the underlying architecture for quantum computers, but the field has narrowed to a handful of potential candidates. Several systems might been proposed to achieve such a device:

— single photons (used in photonic computing);
— superconducting qubits (transmon's qubits);
— atoms (Rydberg atoms or neutral atoms);
— molecules (case of NRM quantum computing);
— ions (trapped with electrostatic potentials and manipulated with lasers);
— quantum dots;
— ...

Most of first industrial players which have developed industrial quantum computers have chosen a solution based on superconducting qubits. For instance, IBM, Google, Rigetti, D-waves have chosen such a technology.

Beyond superconducting qubits, the research landscape is more open, with a few promising candidate technologies in the race, all of which are still immature. Each approach has its attractive aspects and its challenges. Photons, for example, could have an advantage in terms of handling because they operate at room temperature and chip design can leverage known silicon technology. For instance, PsiQ, a Silicon Valley startup, wants to leapfrog the NISQ period with an ambition to develop a large-scale linear optical quantum computer, or LOQC, based on photons as qubits, with 1 million qubits as its first go-to-market product within about five years. This would be a major breakthrough if and when it becomes available. The challenges for photons lie in developing single photon sources and detectors as well as controlling multiphoton interactions, which are critical for two-qubit gates.

Topological approach is an unprecedented low error rate of 1 part per million (and not excluding even 1 part per billion). This would constitute a game changer. The underlying physical mechanism (the exotic Majorana quasiparticle) is now largely accepted, but the first topological qubit is still expected while it was initially announced by Microsoft to become reality in 2018. Two-qubit gates, however, are an entirely different ballgame, and even a truly ambitious roadmap would not produce a workable quantum computer for at least five years.

Superconductive qubits

The advantages of superconducting qubits is that they are easily scalable with a rather well-controlled clean room process well-adapted for on-chip integration. But they rely on a josephson junction circuit, which consists in a small insulating layer that couples two wavefunction of superconducting material. Such devices requires cryogenics temperatures, so that lithographically patterned superconducting circuits are kept at millikelvin temperatures in dilution refrigerators! But the advantage of such architecture is that qubits might be probed and manipulated with electronic tools such as microwave and RF waves. As a counterpart, the quantum computer is not really sold but the service is commercialised as a cloud quantum calculation which is most of provider business model currently: they do not sell the hardware but provide an access to the quantum computer for calculations. Coherence time of superconducting qubits are rather smaller but this time constant is relevant if it is compared to the typical manipulation time necessary to construct a quantum gate. With a rather short manipulation time compared to the coherence time, since this technology is the most commonly used currently, adapted for first generation quantum computers with a rather small number of qubits manipulations. Intel is also developing quantum chips based on superconducting qubits, but does not develop a quantum computer itself.

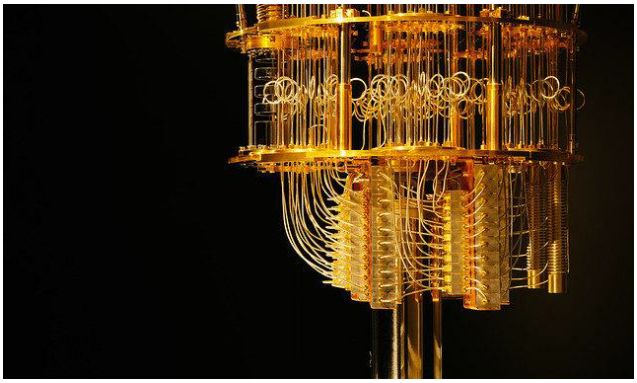


Fig. V.3. Photo of a IBM quantum computer with 53 cubits chip. Visibles cables are used to provide microwave and RF signals on the chip to probe and manipulate qubits. The overall system is mounted on a helium cryostat, open for the picture. (Picture credits: IBM research). Extracted from reference [41].

Ions

Several group, either academics or industrial, are working on alternative technology. The prospect of significant commercial revenues has now attracted the attention of large computing corporations. In principle, there are lots of ways to construct qubits. Some advanced prototypes use qubits made of a few dozen ions of rubidium or ytterbium, trapped in a vacuum chamber by time-varying electromagnetic fields. For instance,

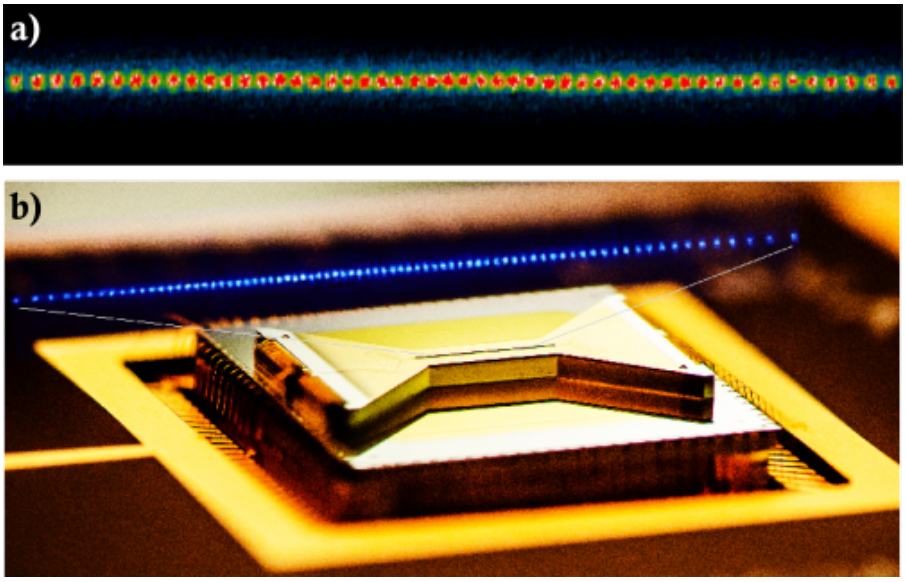


Fig. V.4. a) Optical image of a chain of ion trapped. Each ion might be observed individually. Picture extracted from Prof. Christopher Monroe's group website (`http://iontrap.umd.edu/`). University of Maryland, Department of Physics, Joint Quantum Institute, and Center for Quantum Information and Computer Science.
b) Integration of a ion trap on a chip. Electromagnetic trap is realised with a microfabricated chip for scalability and to reduce the size of the device. Chip is few cm large. K. Hudek & E. Edwards/Univ. of Maryland/IonQ, Inc./JQI. Extracted from [44].

the startup IonQ [1], founded in 2016, has proposed a quantum computer architecture based on individual ion (trapped electromagnetically) as a qubit. The big advantage of such a solution is that coherence time are very important in ions. However, as a counterpart, scalability is more challenging, and qubits are manipulated with lasers rather than electronic means. To date, IonQ has run single-qubit gates on a 79 ion chain, and complex algorithms on chains of up to 11 ions. While superconducting qubits permit a 2D topology to couple qubits, ion trap restrict topology to a linear chain. But the performances of this technology are promising, such that Samsung and a sovereign wealth fund of the United Arab Emirates are leading a new $55 million funding round for IonQ [26].

Silicon based technologies

Recently, however, experimental breakthroughs in silicon-based nanodevices have brought a third option to the fore, either from academics [39, 51] or industrial players as Hitatchi [24]. This option is, in effect, to manufacture quantum processors in the same way as conventional microprocessors, by leveraging widely deployed industrial complementary metal-oxide-semiconductor (CMOS) technology. This would provide a huge avantage for the architecture of the chip, with the benefice of all the technical knowhow of CMOS and silicon technologies and without the need of cryogenic temperatures.

Silicon-based CMOS technologies to build quantum computers was first proposed in 1998 by Bruce Kane [31], based on an arrays of individual phosphorus atoms in crystalline silicon. Each individual phosphorus atom possesses a nuclear spin that might be seen as a qubit (just like NMR but localised specially in each phosphorus atoms). These spin qubits could be read and manipulated using nuclear magnetic resonance techniques. Another reason for the focus on silicon stems from the properties of the material itself. Noise is one of the great bugbears of quantum information processing, because it can make qubits change state leading to computational errors. Most interactions with the surrounding environment, such as charge instabilities and thermal fluctuations. The major source of unwanted quantum bit errors in silicon transistor-based qubits comes from the nuclear spins of ^{29}Si, the naturally dominant isotope, while otherwise silicon offers a relatively noise-free

1. `https://ionq.com/`

environment. But ^{29}Si isotope is spin-free and offers long coherence times for phosphorus qubits in it. For this reason, electron spins in silicon are among the most robust solid-state qubits available, but requires highly purified ^{29}Si silicon wafer which is not a common material.

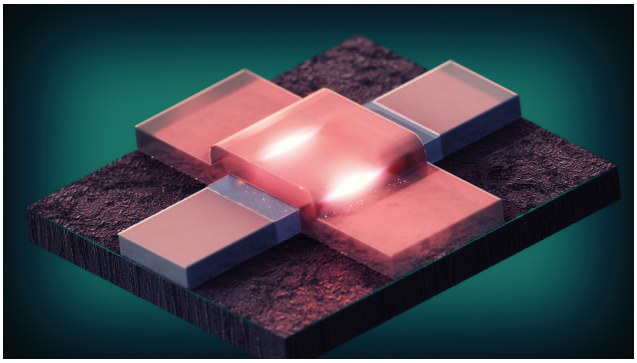


Fig. V.5. Silicon nanowire based transistor for realization of a spin qubit with CMOS technologies. Two quantum dots are formed in the top corners of the nanowire and trap individual spins. Qubit control is achieved via electron spin resonance techniques with microwave pulsing. (Picture credits: Hitachi). Extracted from reference [24].

The mean advantage of silicon-based quantum processors is that they use the same technology that the microchip industry has handled for decades. Manufacturers could still use previous multibillion-dollar infrastructure investments, and therefore reduce production costs. As an alternative approach, CEA-LETI in France has proposed a qubit device with an industry-standard fabrication process based on 300 mm silicon-on-insulator wafers. The project has been developed as part of the European research consortium MOSQUITO (`http://www.mos-quito.eu`). It consists in the development of a nanowire transistor with an undoped channel and wrap-around gate electrodes. At low temperatures, two QDs form in the upper corners of the nanowire in which individual spins can be trapped (see reference [37] and Fig. V.5). Under the effect of a magnetic field, the electron spins align parallel or antiparallel to the field direction, producing the necessary quantum binary states. The need for two QDs arises because one is used to host a qubit, while the other one is used as a sensor to readout the qubit state. If this technology has been demonstrated, it still requires cryogenics temperatures in milliKelvin range [47], while phosphorus nuclear spins in ^{29}Si have been demonstrated at room temperature.

The high-risk/high-gain way: topological qubits

Microsoft is supporting fundamental research on the development of a new kind of high-quality qubits, based on topological insulators. Such qubits are very interesting since they are expected to be highly unsensitive to external noise, exhibiting low decoherence and consequently low error rates. They are so-called *topologically protected*. However such qubits are purely conceptual for the moment, since they rely on the existence of a particle called *Majorana fermion*. But such a particle hasn't been observed yet! That is why it is a highly risky strategy from Microsoft. But if they are successful, these qubits will be of high quality and very low error rates, resulting in huge gain for Microsoft, in term of performances and technological advance. Recent technological progress have been reported toward the experimental observation of this particle, using indium phosphide nanowires in a hashtag shape [19], but it remains unobserved for the moment.

Other physical realizations

Optical lattices qubit implemented by internal states of neutral atoms trapped in an optical lattice.

Quantum dot spin-based (qubit given either by the spin states of trapped electrons or by electron position in double quantum dot [15]).

Coupled Quantum Wire qubit implemented by a pair of Quantum Wires coupled by a Quantum Point Contact [6].

Solid-state NMR Kane quantum computers qubit realized by the nuclear spin state of phosphorus donors in silicon.

Electrons-on-helium quantum computers qubit is the electron spin.

Cavity quantum electrodynamics (CQED) qubit provided by the internal state of trapped atoms coupled to high-finesse cavities.

Molecular magnet qubit given by spin states.

Linear optical quantum computer qubits are realized by processing states of different modes of light through linear elements (mirrors, beam splitters and phase shifters).

Diamond-based quantum computer qubit realized by the electronic or nuclear spin of nitrogen-vacancy centers in diamond.

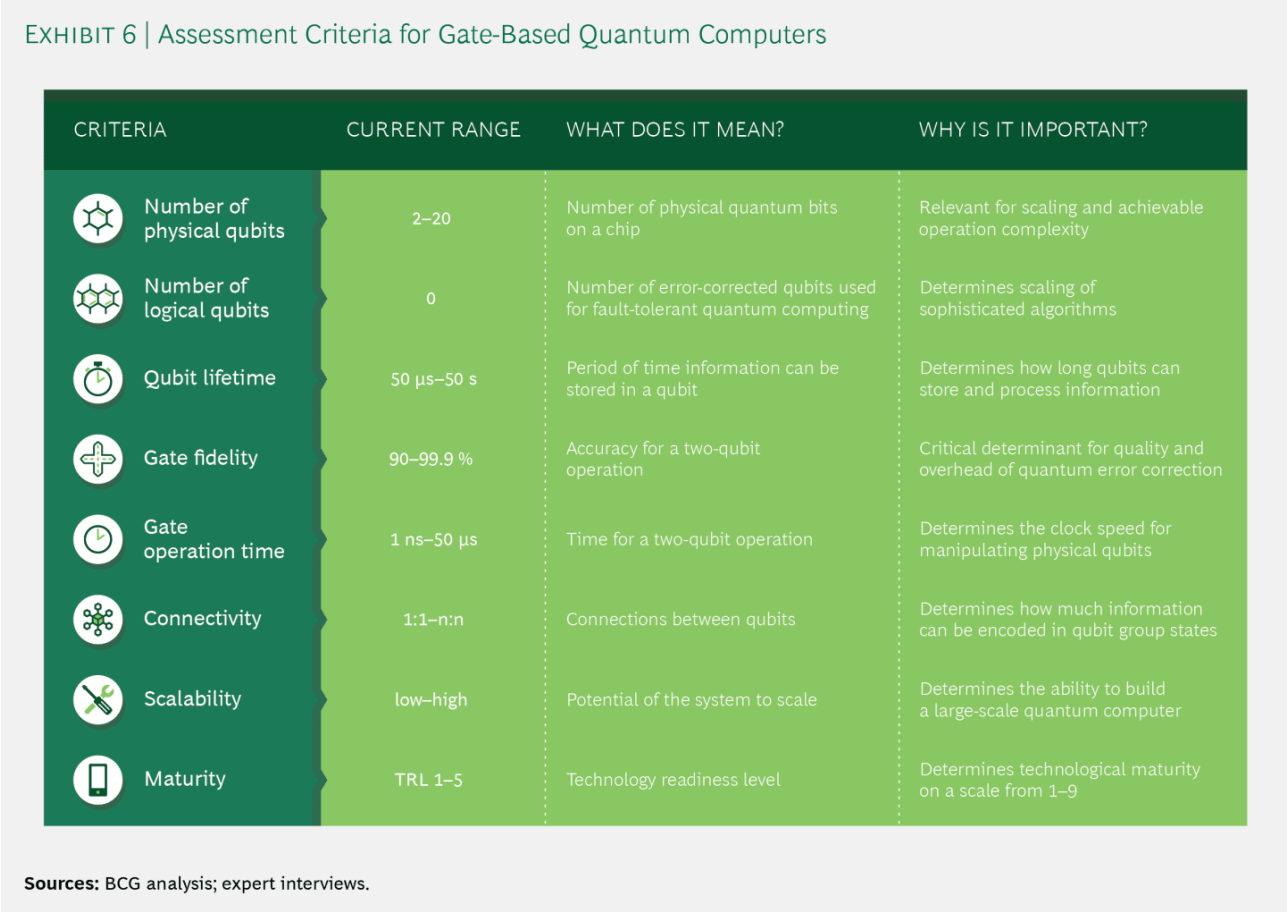


EXHIBIT 6 | Assessment Criteria for Gate-Based Quantum Computers

CRITERIA	CURRENT RANGE	WHAT DOES IT MEAN?	WHY IS IT IMPORTANT?
Number of physical qubits	2–20	Number of physical quantum bits on a chip	Relevant for scaling and achievable operation complexity
Number of logical qubits	0	Number of error-corrected qubits used for fault-tolerant quantum computing	Determines scaling of sophisticated algorithms
Qubit lifetime	50 µs–50 s	Period of time information can be stored in a qubit	Determines how long qubits can store and process information
Gate fidelity	90–99.9 %	Accuracy for a two-qubit operation	Critical determinant for quality and overhead of quantum error correction
Gate operation time	1 ns–50 µs	Time for a two-qubit operation	Determines the clock speed for manipulating physical qubits
Connectivity	1:1–n:n	Connections between qubits	Determines how much information can be encoded in qubit group states
Scalability	low–high	Potential of the system to scale	Determines the ability to build a large-scale quantum computer
Maturity	TRL 1–5	Technology readiness level	Determines technological maturity on a scale from 1–9

Sources: BCG analysis; expert interviews.

Fig. V.6. Extracted from `https://www.bcg.com/fr-fr/publications/2018/next-decade-quantum-computing-how-play.aspx`.

1.2. Open questions for the development of a commercial quantum computer

Number of qubits and quantum volume

The number of qubit is not necessarily relevant to quantify the potentiality of a quantum computer. Indeed, you may have a lot of qubits but to fully exploit quantum algorithm it requires quantum superpositions and qubit manipulations with quantum gates. Performances are then fundamentally related to coherence time and error rates of gates. In that spirit, IBM as develop in 2017 the notion of *quantum volume* in order to have a metric of the performances of a quantum computer. Quantum volume is a heuristic measure somewhat may be seen as the number of qubits times the number of gate operations that can be reliably performed until an error occurs. Quantum volume should be seen as a tool that allowed them to systematically measure and understand how incremental technology, configuration and design changes affected a quantum computer's overall power and performance. Scientists believe that computers with a few hundred physical qubits are within technological reach. A better standard for size and capability in the future would be the number of fully error-

corrected "logical qubits," but no one has yet developed a machine with logical qubits, so their number across all technologies is still zero (and will likely remain so for a while).

Unfortunately, the comparative performance of algorithms on different hardware technologies cannot be directly determined from these characteristics. The most common approach for performance assessments is a benchmarking on randomized algorithms by independent companies. End-to-end software and specialist players are offering services at different levels of sophistication both to assess the performance of specific algorithms on the available hardware and to help with developing the best quantum algorithm based on these assessments.

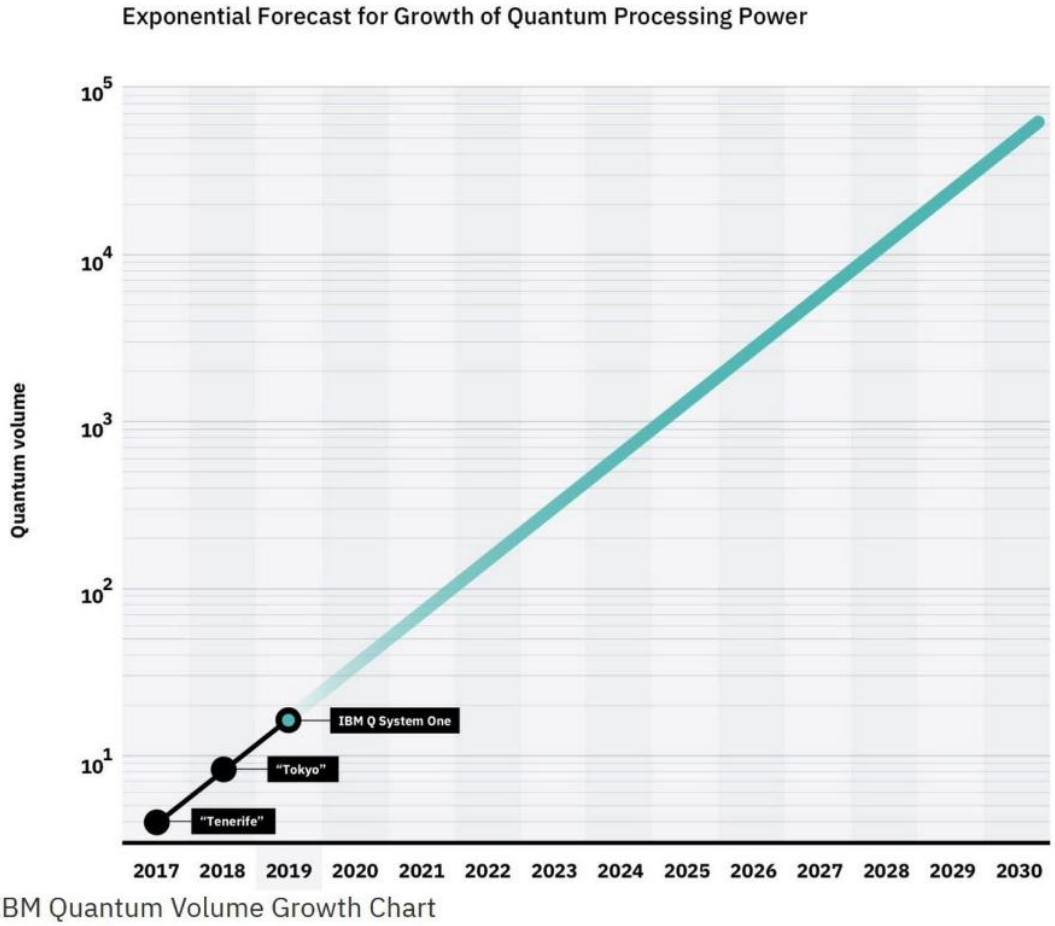


Fig. V.7. IBM Quantum Volume Growth Chart. `https://www.forbes.com/sites/moorinsights/2019/11/23/quantum-volume-a-yardstick-to-measure-the-power-of-quantum-computers/#4c82dd755bf4`

Complexity of accurate calculations

The factors that determine a computer's calculating capability include a number of factors which are

Qubit lifetime currently 50 μs to 50 s;

Operation accuracy in particular the most sensitive two-qubit gate fidelity (currently 90% to 99.9%, with 99.9% minimally required for reasonably effective scaling with error correction);

Gate operation time currently 1 ns to 50 μs;

Topology of the qubits connections currently from the worst (one-to-one) to the best (all-to-all). This is important, because entanglement is a distinguishing factor of quantum computing and requires qubits to be connected to one another so they can interact.

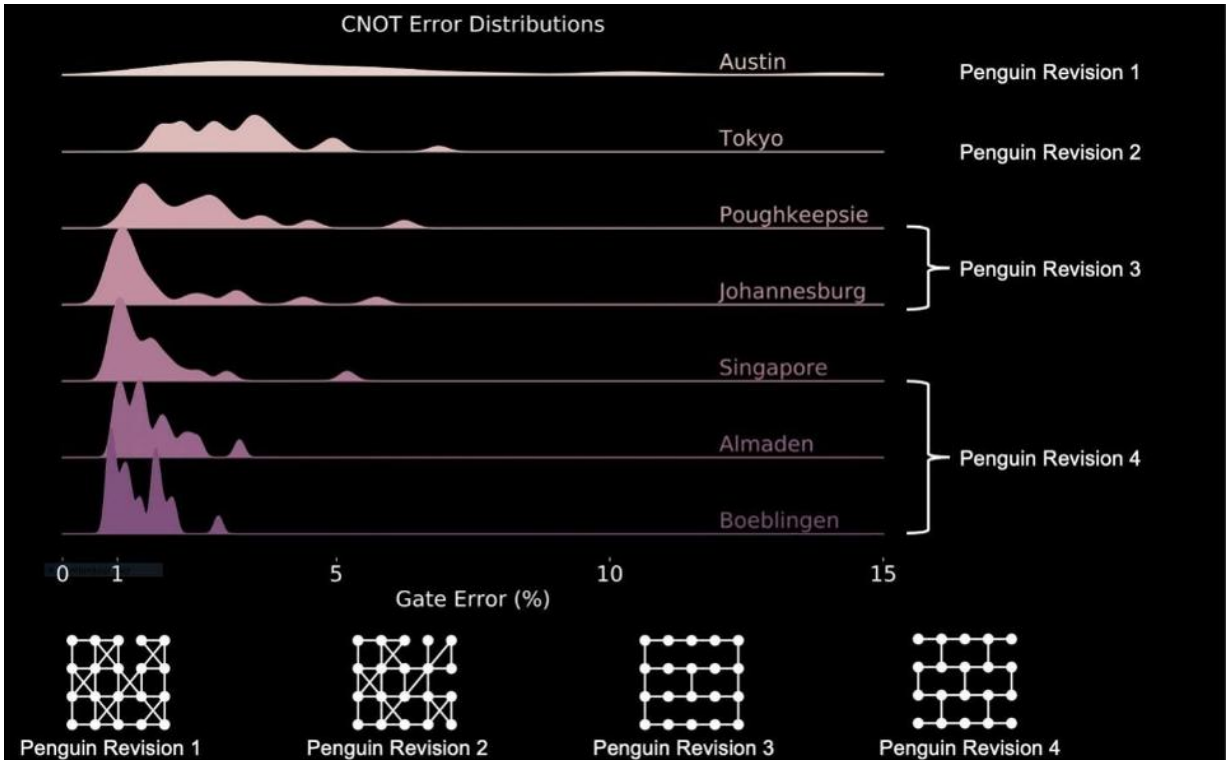


Fig. V.8. CNOT Error Distributions for different version of IBM's 20-qubits systems. `https://www.forbes.com/sites/moorinsights/2019/11/23/quantum-volume-a-yardstick-to-measure-the-power-of-quantum-computers/#4c82dd755bf4`

Remaining technological challenges

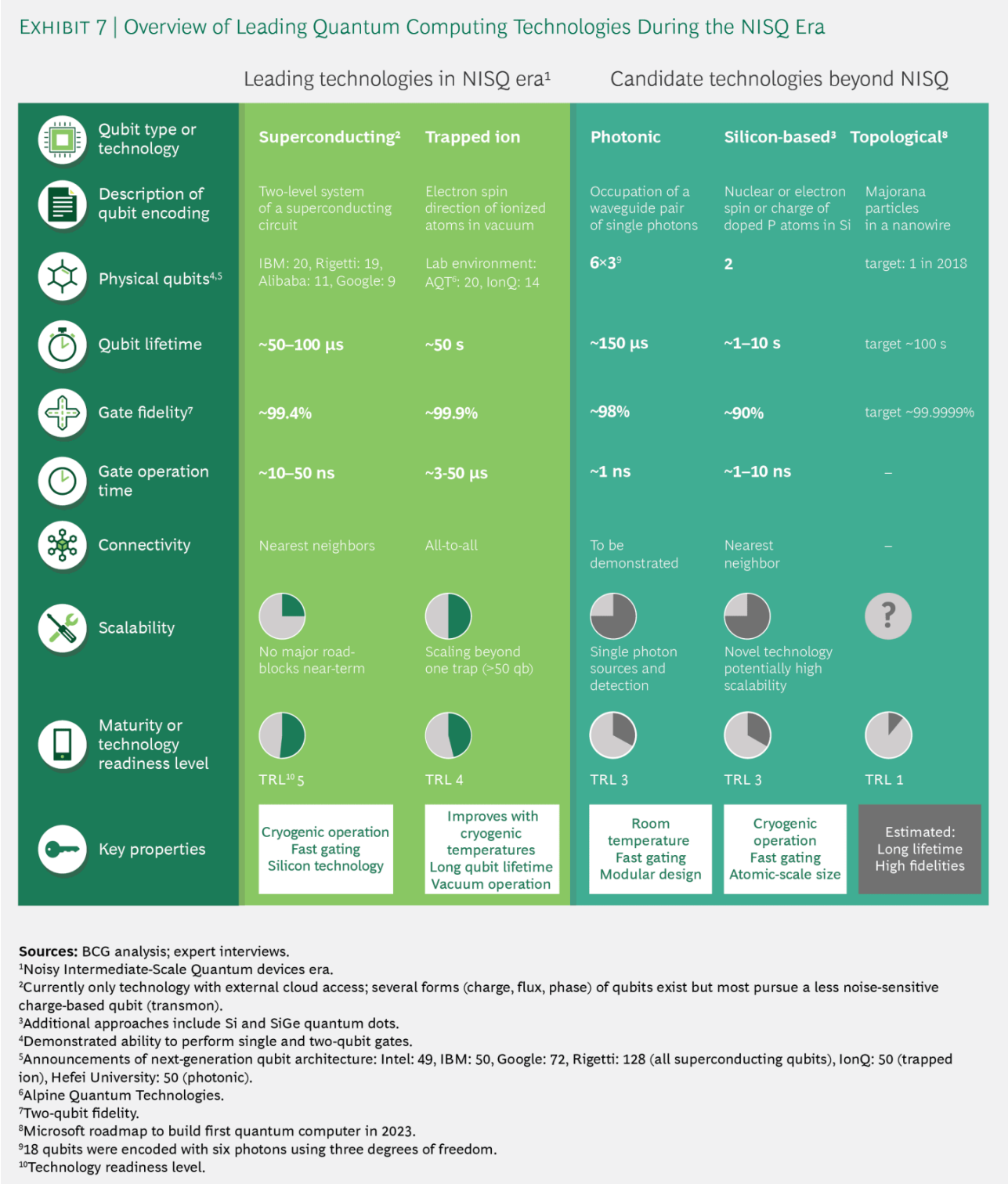
There are a number of technical challenges in building a large-scale quantum computer, David DiVincenzo listed the following requirements for a practical quantum computer [12]:

— scalable physically to increase the number of qubits;
— qubits that can be initialized to arbitrary values;
— quantum gates that are faster than decoherence time;
— universal gate set;
— qubits that can be read easily.

One of the greatest challenges is controlling or removing quantum decoherence. This usually means isolating the system from its environment as interactions with the external world cause the system to decohere. However, other sources of decoherence also exist. Examples include the quantum gates, and the lattice vibrations and background spin of the physical system used to implement the qubits. Decoherence is irreversible and is usually something that should be highly controlled, if not avoided. Decoherence times for candidate systems in particular, the transverse relaxation time T_2 (the dephasing time), typically range between nanoseconds and seconds at low temperature. Currently, quantum computers based on superconductive qubits require the quantum chip to be cooled to 20 millikelvins in order to prevent significant decoherence. To achieve such temperature, dilution helium fridge cooling systems are necessary. Such cooling systems are based on the use of ^{3}He, which is a nuclear research byproduct, very expensive with important price fluctuations (from \$500 to \$2000 per litre) [2]. The price of ^{3}He is so high that dilution fridge are design to work with closed ^{3}He circuit.

Due to decoherence, time-consuming tasks may render some quantum algorithms inoperable, as maintaining the state of qubits for a long enough duration will eventually corrupt the superpositions. Several strategies are proposed to pass through this difficulty, such as quantum error correction codes. If the error rate is small enough,

2. The Helium Stewardship Act of 2013 has been signed by President Barack Obama in 2013, to improve the economics of recovering helium in USA.



Sources: BCG analysis; expert interviews.
[1]Noisy Intermediate-Scale Quantum devices era.
[2]Currently only technology with external cloud access; several forms (charge, flux, phase) of qubits exist but most pursue a less noise-sensitive charge-based qubit (transmon).
[3]Additional approaches include Si and SiGe quantum dots.
[4]Demonstrated ability to perform single and two-qubit gates.
[5]Announcements of next-generation qubit architecture: Intel: 49, IBM: 50, Google: 72, Rigetti: 128 (all superconducting qubits), IonQ: 50 (trapped ion), Hefei University: 50 (photonic).
[6]Alpine Quantum Technologies.
[7]Two-qubit fidelity.
[8]Microsoft roadmap to build first quantum computer in 2023.
[9]18 qubits were encoded with six photons using three degrees of freedom.
[10]Technology readiness level.

Fig. V.9. Extracted from `https://www.bcg.com/fr-fr/publications/2018/next-decade-quantum-computing-how-play.aspx`.

it is thought to be possible to use quantum error correction to suppress errors and decoherence. This allows the total calculation time to be longer than the decoherence time if the error correction scheme can correct errors faster than decoherence introduces them. But numerical studies estimate that, assuming a depolarizing error probability of $p < 10^{-3}$ per elementary gate, a logical qubit needs to consist of between 1,000 and 10,000 physical qubits [10]. Building a large logical qubit with such a low error rate could be a second rest stop along the road to robust quantum computing.

Improving the fidelity of qubit operations is therefore key for being able to increase the number of gates and the usefulness of algorithms, as well as for implementing error correction schemes with reasonable qubit overhead. If error correction has been implemented, there is a price on clock speed that all gate-based technologies will have to pay for fault-tolerant quantum computing. Measurement times, required in known error-correction schemes, are in the range of μs. Thus, an upper limit on clock speed of about 1 MHz emerges for future fault-tolerant quantum computers. This in turn will be a hurdle for the execution speed-up potential of quantum algorithms.

The use of helium fridge for the development of quantum computers has been pointed out as a difficulty for mass production of such systems. Dilution fridge, which can cost between $500,000 and $1 million each, are custom-made usually, by only a few companies like BlueFors in Finland and Oxford Instruments in the UK, are producing high-quality ones. Such a fridge might requires up to $40,000 of ^{3}He. In addition to the use of ^{3}He, it requires the use of superconducting cables to control and measure qubits. These are specially designed to conduct very little heat so that they don't affects qubits states. Only one main manufacturer supplies them, a Japanese company called Coax Co [22]. Sourcing parts for quantum computers has been stressed out as a difficulty for their mass production deployment [3]. In fact, superconducting qubits scaling challenge may seem somewhat mundane: electric cabling and control electronics. The current way of addressing a qubit with two to four cables, while also maintaining cryogenic temperatures, triggers severe engineering challenges when the number of qubits runs into the hundreds. That being said, even superconducting qubit architectures have achieved only about 50 to 128 reliable qubits so far (IBM: 50qubits; Google: 72 qubits; Rigetti: 128 qubits; Intel: 49 qubits), compared with 10^{10} bits on a chip for classical computing, so there is still some ways to go. The roadmaps of all these players extend to about 1 million qubits! They have a strong grip on what needs to be resolved consecutively along the journey, even if they do not yet have workable solutions for them.

Why quantum?

The two biggest questions facing the emerging quantum computing industry are, *When will we have a large, reliable quantum computer*, and *What will be its architecture?* The main remaining question is the utility of quantum computing, even if one may achieve a perfect qubit with no errors. Is a universal quantum computer sufficient to efficiently simulate an arbitrary physical system ? that is still an open question. Even quantum supremacy, regardless usefulness of the algorithm, is still not demonstration until now. However, such a demonstration is deemed imminent, and Rigetti recently offered a $1 million prize to the first group that proves quantum advantage [4]. Several companies are proposing *quantum challenges* [5], such as Airbus or Zeiss, to investigate, in a open innovation scheme, to potential benefits of such technologies.

1.3. Growth of quantum technologies fundings

Public fundings

A regional race is also developing, involving large publicly funded programs that are devoted to quantum technologies more broadly, including quantum communication and sensing as well as computing. China leads

3. https://futurism.com/sourcing-parts-quantum-computers-difficult
4. BCG's publication *The Next Decade in Quantum Computing—and How to Play*, page 9
5. https://www.airbus.com/innovation/tech-challenges-and-competitions/airbus-quantum-computing-challenge.html
https://www.zeiss.com/corporate/int/careers/events/zeiss-quantum-challenge.html

the pack with a $10 billion quantum program spanning the next five years, of which $3 billion is reserved for quantum computing. In 2016, EU has announced a €1 billion investment for a large-scale EU-wide quantum technologies flagship [6]. Germany has allocated €650 million for quantum technology R&D [7]. UK has launched $381 million in the UK National Quantum Technologies Programm. The US just passed the National Quantum Initiative Act, a law that allocates $ 1.2 billion for quantum information science research [8] [45]. It passed unanimously by United States Senate and was signed by President Donald Trump in 2019. Many other countries, notably Australia, Canada, and Israel are also very active.

Private companies race for Quantum Computing Supremacy

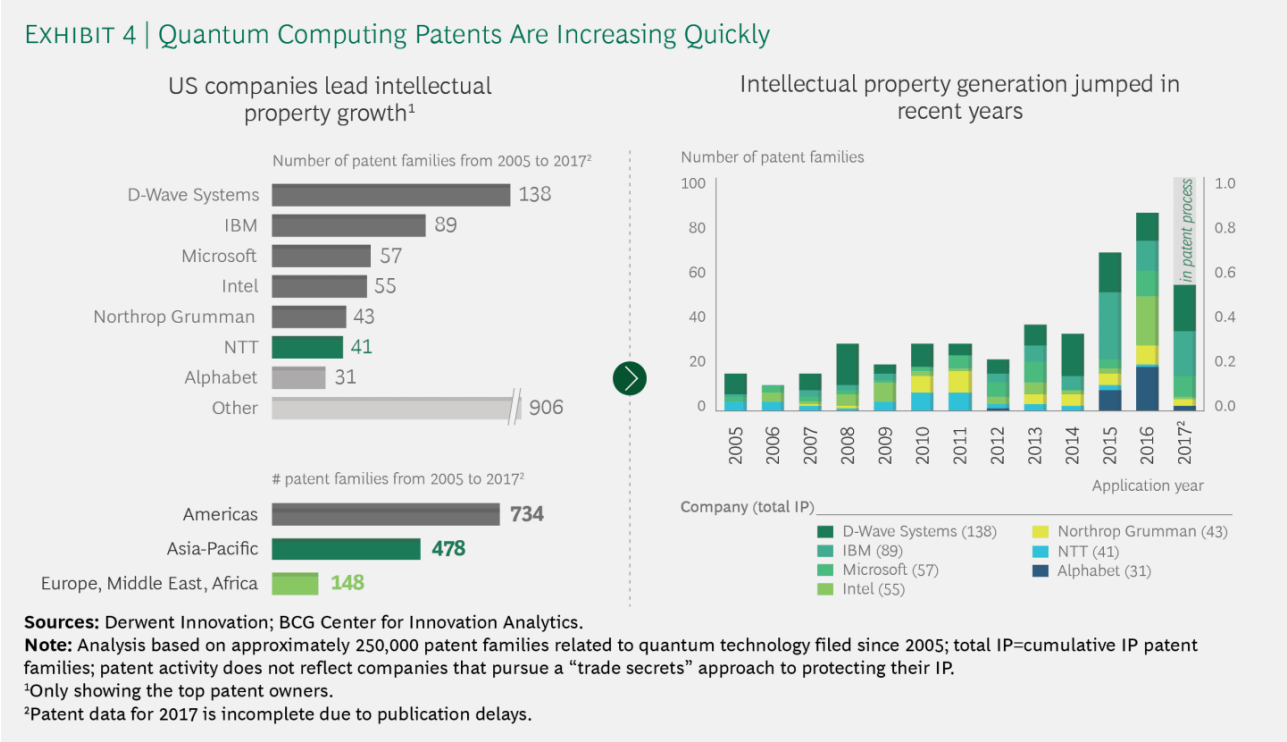


Fig. V.10. Extracted from `https://www.bcg.com/fr-fr/publications/2018/next-decade-quantum-computing-how-play.aspx`.

With more than 60 separate investments totaling more than $700 million since 2012, quantum computing has come to the attention of venture investors, even if is still dwarfed by more mature and market-ready technologies such as blockchain (1,500 deals, $12 billion, not including cryptocurrencies) and AI (9,800 deals, $110 billion). For instance, several private quantum computing companies have risen important funds in recent years (total risen amount)

— D-Wave (since 2012), $205 millions;
— Rigetti, $119 millions;
— PsiQ, $65 millions;
— Silicon Quantum Computing, $50 millions;
— 1QBit, $35 millions;
— IonQ, $22 millions;
— Quanyum Circuits, $18 millions.

6. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_1409
7. https://www.nextplatform.com/2019/01/16/germany-makes-massive-quantum-neuromorphic-investment/
8. https://en.wikipedia.org/wiki/National_Quantum_Initiative_Act

The money has been accompanied by a flurry of patents and publishing. North America and East Asia are clearly in the lead; these are also the regions with the most active commercial technology activity. Europe is a distant third (a number of leading European quantum experts joining US-based companies in recent years). Australia, a hotspot for quantum technologies for many years, is striking given its much smaller population. The country is determined to play in the quantum race; in fact, one of its leading quantum computing researchers, Michelle Simmons, was named Australian of the Year 2018.

EXHIBIT 3 | Funding for Startups Has Increased in Recent Years

Startup	Total [US$ millions]	Most recent funding	
D-Wave Systems	205	June 1, 2018	US$10.15 million of grant funding in a deal led by the Canadian Government
Rigetti Computing	119	March 28, 2017	Announced further US$40 million in its series B round of funding
PsiQ	65	Undisclosed	Undisclosed
Silicon Quantum Computing	60	August 2017	AU$83 million venture funded by: New South Wales Government (AU$9 million), University of New South Wales (AU$25 million), Commonwealth Bank of Australia (AU$14 million), Telstra (AU$10 million over two years), and the Australian Government (AU$25 million over five years)
Cambridge Quantum Computing	50	August 26, 2015	US$50 million of development capital
1QBit	35	November 28, 2017	CA$45 million of development capital in Series B funding
IonQ	22	February 24, 2017	US$20 million of Series B venture funding
Quantum Circuits	18	November 13, 2017	US$18 million of Series A venture funding
Alpine Quantum Computing	12	February 8, 2018	€10 million of grant funding
QC Ware	8	July 5, 2018	US$7 million of Series A venture funding
Optalysys	8	September 21, 2017	£3 million of seed funding from undisclosed investors
Nextremer	5	August 8, 2017	JP¥500 million of venture funding
Oxford Quantum Circuits	3	September 8, 2017	£2 million of venture funding

Sources: Crunchbase; Pitchbook; BCG analysis.

Fig. V.11. Extracted from `https://www.bcg.com/fr-fr/publications/2018/next-decade-quantum-computing-how-play.aspx`.

1.4. Scientific publishing

Two things are noteworthy about the volume of scientific publishing regarding quantum computing since 2013

— the rise of China, which has surpassed the US to become the leader in quantity of scientific articles published;

— the high degree of international collaboration (in which the US remains the primary hub).

The cooperation shows that quantum computing is not dominated by national security interests yet, owing in large part to consensus around the view that cryptographic applications are still further in the future and that effective remedies for such applications are in the making.

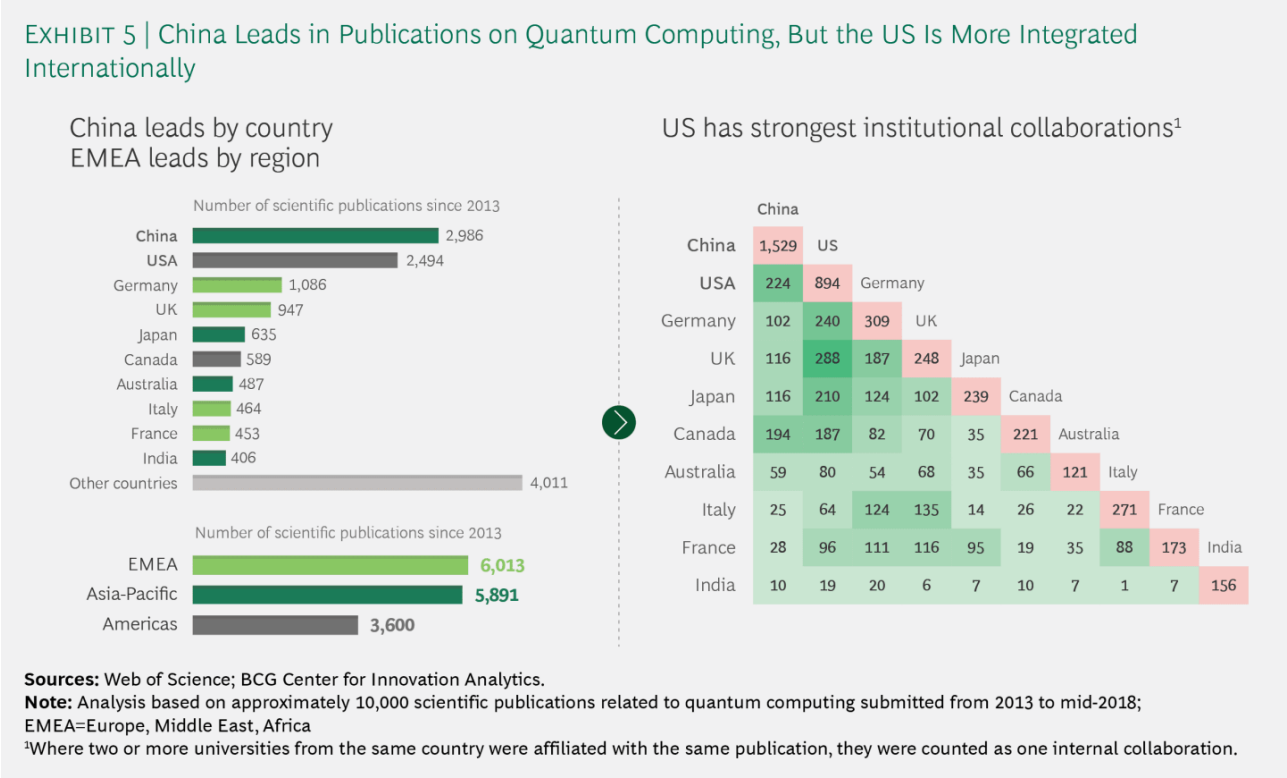


Fig. V.12. Extracted from `https://www.bcg.com/fr-fr/publications/2018/next-decade-quantum-computing-how-play.aspx`.

2. Applications of quantum computers

2.1. Boosting big data and AI

Supercomputer calculation power relies on the ability to process huge batches of data simultaneously and exchanging data between them quickly. Thus they are not based on a very powerful processor but rather on a architecture of many processors running in parallel. But there is still a number of problems that bring these supercomputers to their limits.

Quantum computers fully exploits quantum parallelism: they can prepare quantum registers in a way that explores a lot of inputs at the same time – all within a single processor, no need for many copies. Quantum computers are not equivalent to very powerful supercomputer since they require quantum algorithmic. But several problems have been demonstrated to be adapted to quantum computers: signals processing, unsorted databases search, molecular simulations, salesman problem,... But many of these algorithms are what drives the services we get from big data and artificial intelligence. Quantum algorithms use quantum physics to explore many possible test solutions at the same time and then slowly confirm to the best one. The business model proposed relies on a cloud accessible service (currently proposed by IBM and D-waves for the access to a real quantum computer). A good example is GPS navigation for cars. The optimum trajectory relies on artificial intelligence learning what traffic patterns predict – learning from these big data can be made faster by the parallel computing of a quantum computers (to retrieve the fastest way for example).

2.2. Quantum computers and chemistry: killer apps?

Impact on the materials and pharmaceutical industries

Designing new chemical processes or components is a crucial aspect of chemistry industry. The experimental development is slow and difficult; therefore it is assisted by computational chemistry, which aims at simulating

molecules and chemical reactions. But chemical bond, which is the key element of molecule stability, conformation and configuration, is inherently of quantum nature. To simulate it completely, one needs to store the complete quantum state in a computer memory, which often leads to memory problems. This memory issue is inextricable when molecule size is getting important (pharmaceutical components, proteins,...). But a quantum computer is well suited to simulate quantum systems, especially molecules. And since the quantum state is stored in a quantum qubits, memory is no longer a limitation in such systems. This has been performed on small molecules with the first generation of quantum computers. One of the most anticipated uses for quantum computers is as a tool for developing new drugs, catalysts, and materials.

First realizations

In 2017, IBM has demonstrated the calculation of the ground state of small molecules, up to three atoms with the molecule BeH_2 simulated. Those simulations have been realized with a 6 qubits quantum computer [30] (variational quantum eigen-solver), also computing potential energy surface and demonstrating the possiblity for magnetic properties prediction.

There is currently a lot of hope regarding the potential of quantum computers for computational chemistry. So big that the *Chemical and engineering news* journal has published an article entitled *Chemistry is quantum computing's killer app* [8]. Today's computational chemistry methods such as density functional theory (DFT) work well for many problems, in particular in organic chemistry. But those methods are less efficient when applied to inorganic systems, which are nevertheless of importance in term of applications. Indeed, computational chemistry requires approximations regarding the electronic structure, in order to simplify calculation so they might be handle by a classical computer. But it neglects important details of the electronic structure, which affects properties predictions. The more electrons there are in a system, the harder it is to describe on a classical computer; the strategy to simplify calculation consists in neglecting the behavior of some electrons. It's a rather good approximation in organic chemistry but less justified in inorganic chemistry. Today's computational chemistry modeling algorithms can provide usually good enough, but inexact, predictions. For example, metal are poorly described with such algorithms. On the contrary, the advantage of a quantum computer simulation is that no approximation would be introduced; so the exact solution would be provided and consequently reliable prediction on molecule or material properties.

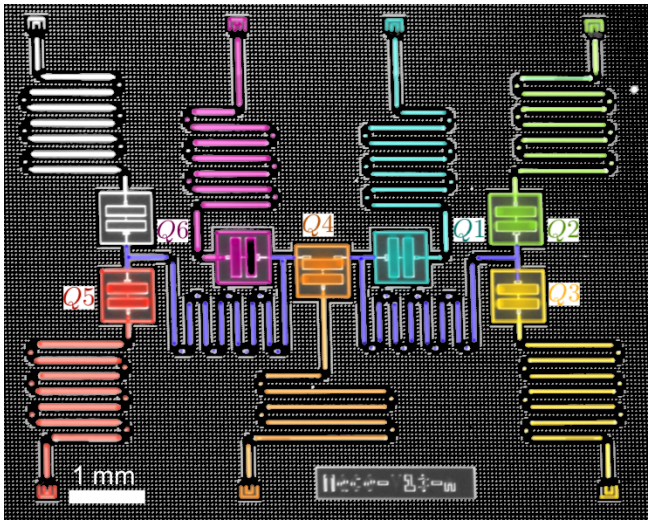


Fig. V.13. Photography of the chip used in IBM's quantum computer used for BeH_2 quantum chemistry simulation of reference [30]. The chip was made out of six superconducting qubits, labeled $Q1$,...,$Q6$. Strip lines attached to qubits are waveguides to address qubits with microwaves excitation in order to manipulate qubits.

Expectations

Consequently, quantum computers has a huge potential in computational chemistry. It could aid development of catalysts for clean energy and renewable chemical manufacturing, enable deeper understanding of the enzymes that underlie photosynthesis and the nitrogen cycle, power the discovery of high-temperature superconductors and new materials for solar cells, and much more. In all those applications, strong correlation between electrons are involved and these situations are poorly described with actual computational chemistry algorithms. "If you have 125 orbitals and you want to store all possible configurations, then you need more

memory in your classical computer than there are atoms in the universe," says Matthias Troyer (Microsoft Research, Zurich), but a quantum computer could model such a system with just 250 qubits [8].

Quantum computers could help in explaining the electronic structure of molecules but also their reactivity: it would be possible to compute all the possible transitional structures that a molecule could present during each phase of a chemical reaction and the associated energy. Once all these informations are obtained, it is possible to predict exactly what could happen, *i.e.* the reactivity of the molecules and the products obtained after chemical reaction. Progress in the development of quantum computers have been sufficient in the last decade so that researchers have decided to explore to possibility of simulating useful molecules with quantum computers, and more specifically molecules for which standard computational chemistry methods fails. Researchers at Microsoft and ETH Zurich have decided in 2014 to explore that possibility without waiting for a real quantum computer with enough qubits to exists [8]: they decided to simulate classically the quantum simulation of a quantum computer! Several industrial players have the same strategy (Total, Atos,...). It consists in developing appropriate quantum algorithms with classical supercomputers in order to test, to optimise then and explore their possibilities prior to the existence of a quantum computer with enough qubits to implement it. It also permits to evaluate the effect of noise and decoherence on the quantum calculation, and to estimate which qubits performances are required (error rate, number of qubits, topology of the chip [9]). In term of innovation strategy, it is a way of exploring the potentiality of the technology and its impact on the market for companies. It is also a method to established a specification chart of what is required for a given application in target and consequently guide potential investments in hardware. To sum up, companies want to know how many qubits with which error rate the quantum computer would need for their applications and whether it would truly solve a real, important problem in a reasonable amount of time.

In 2017, Google released an open-source software package called OpenFermion to help scientists translate existing quantum chemistry software into algorithms compatible with quantum hardware. Several start-up companies have emerged (like Zapata Computing), oriented toward the development of software for chemistry applications on quantum computers.

Top targets for industrial applications

Nitrogenase:

Nitrogenase is an enzyme which is used by bacteria to make ammonia from atmospheric nitrogen in ambient conditions. The mechanism by which nitrogenase performs that conversion is still unknown. Industrial actors would like to understand how nitrogenase performs this reaction in order to design industrial processes for synthesizing nitrogen-based fertilizers with less energy consumption. The current process used to produce nitrogen-based fertilizers from atmosphere nitrogen is the Haber-Bosch process, realized at high pressures and high temperatures. It consumes then a lot of energy and produces an important quantity of greenhouse gases. As a result, the carbon footprint of a loaf of bread - from growing and harvesting the wheat to the baking - is about 590 g. Nitrogen-based fertilizer for wheat growth represent 40% of the total emission of CO_2.

At nitrogenase's heart is on iron-molybdenum cofactor called FeMoco. Traditional supercomputers can't model the nitrogen fixation on FeMoco. Quantum computers are expected to provide information on that mechanism. In a paper published in 2017 [46], researchers from ETH Zurich have demonstrated that quantum comput-

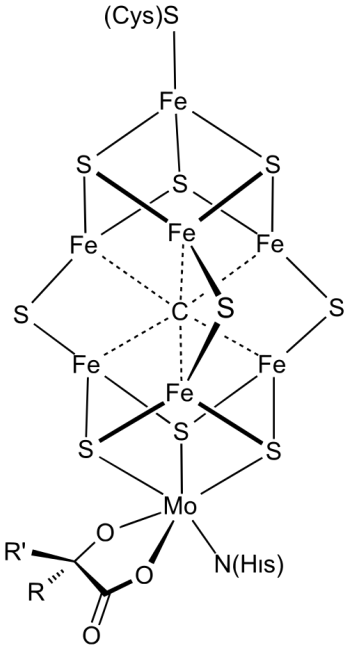


Fig. V.14. Structure of the FeMoco cofactor showing the sites of binding to nitrogenase (the amino acids cys and his). Extract from `https://en.wikipedia.org/wiki/Nitrogenase`

9. performances may be affected by the topology, requiring additional swap gates to achieve a C-gate between non-adjacent qubits. Then, if coherence time of ions are high, the overall performances may be affected by the linear topology of solutions based on a linear chain of ions.

ers with 100 qubits working perfectly [10] could solve the FeMoco mechanism within days or months [11]. The calculation is based on phase estimation algorithm, parallelised over 100 quantum computers in their estimation [46]. The required space and time resources for simulating FeMoco using the 54-orbital basis and nesting are comparable to that of Shor's factoring algorithm for 4,096-bit numbers [46]. But one has to keep in mind that if it would be a snap to develop a 100 qubits chip regarding recent developments in the hardware development, realizing multi-qubits gates over 100 qubits with low error rates remains an important challenge. With error rate required in [46], error correcting code would be necessary and involve far larger number of qubits, or a technological breakthrough to reduce severely error rates in current devices technology. Software development might also help, improving the algorithm itself. With current technologies, hundreds of thousands up to a million of physical qubits are expected to be necessary to achieve such a calculation that requires 100 logical qubits [8].

Photosystem II:
It is an enzymatic complex that has an important role in the firsts steps of photosynthesis, the mechanism occurring in vegetable such that absorbed light permits to oxidize water and harvest electrons (cellular breathing). Water oxidation occurs at a location of the macromolecule called *the manganese center*. Quantum computers should help to model the behavior of this manganese center during the photosynthesis process. A better understand of the reactivity of Photosystem II could enable chemists to design catalysts for artificial photosynthesis as a path toward renewable process for hydrogen or hydrocarbon fuel production.

High-T_c supraconductors:
These material are not yet understood dispite their discovery decades ago. Quantum computers could help in understanding the microscopic process at the origin of supraconductivity in such materials.

Solar-cell materials:
A current challenge in these materials consists in understanding the charge carriers dynamics from their photogeneration to their capture by electrodes as free-carriers for generation of electrical current. Better understanding of this dynamics would permit to predict and design new solar-cell materials with better performances or additional properties such as low cost or flexibility. Quantum computers are good candidates for simulation of carriers dynamics in solar-cells materials.

Computers for drugs discovery

Among the areas where quantum computers may have received the most hype is the multibillion-dollar industry of drug discovery. A 2018 report by the Boston Consulting Group [12] suggested that a massive $20-billion quantum pharmaceutical industry could emerge by 2030. Pharmaceutical drugs are typically small molecules of 50 to 80 atoms. But to be effective, drugs must interact with biological molecules such as proteins, which can contain thousands of atoms, far beyond what any quantum computer will be able to handle in the near future. Nowadays, such molecules are simulated with molecular dynamics and DFT methods. The number of atoms involved is high and the gap is important for quantum computers to be competitive. In previous section, lower number of atoms were considered, focusing on a given active center of a large molecule, which is not the case of a drug activity on proteins. But the potential market is so huge that it remains of interest.

Another application of quantum computers for drugs has been proposed by Marco de Vivo [44], a theoretical biochemist at the Italian Institute of Technology in Genova: rapidly screening large numbers of molecules to more efficiently pick out promising drug candidates for further study.

Hybrid approach

But the noisy quantum processors of the near future need not tackle an entire protein to have an impact. A classical method like DFT might be used to treat most of the system and then treat just the most quantum part of

10. 100 MHz gates with 10^{-6} error rates.
11. The model assumed multiple computers working in parallel.
12. `https://www.bcg.com/en-us/publications/2018/coming-quantum-leap-computing.aspx`

it, the calculation might be delegated to a quantum computer. It is an **hybrid approach**: a classical computer is combined to a quantum computer and only particular tasks are treated by the quantum computer where quantum algorithms offers performances benefits compared to classical ones. This hybrid approach is more and more common nowadays, and proposed by many players providing end-to-end solution such as Rigetti for example. IBM proposes a cloud access to its quantum computers, accessible with an API or a python script, particularly well adapted to such hybrid architecture. In the case of drug activity calculation on a protein, the quantum calculation would concerns the electrons involved in forming or breaking a bond between the protein and ligand. Other electrons dynamics could be calculated classically.

Software and quantum algorithm optimisation

Quantum computers are still far from performances required for useful applications. But another side of quantum computing has been developed recently and rapidly: quantum software development. Microsoft researchers, for example, used algorithm improvements to reduce by a factor of ten million the number of quantum logic operations needed to exactly solve FeMoco. Such software may help to reduce the number of quantum gates used for a calculation. And the lower the number of gates are, the higher will be the tolerance on the error rate of each gate. If a quantum computer's performances are not enough, software optimization of the quantum algorithm could help to deal with it. A quantum processor will be a part of a workflow in which a classical computer sets up the problem and feeds it to the quantum machine for specific computational steps.

Moreover, this software step is necessary to implement a given algorithm on a chip with a given topology of qubits which is a properties of the hardware. This step is called "transpilation" in the case of IBM Q experience's quantum computers. Besides topology, the implementation of the quantum algorithm (compilation) is also optimized, taking into account the calibration of qubits (measured error rates) on the hardware used.

2.3. Quantum computing is a marathon not a sprint

Christopher Monroe is Professor of Physics at the University of Maryland and co-founder and CEO of IonQ, a quantum computing startup. In a recent article on-line on `venturebeat.com`, he warned that quantum computing is a marathon not a sprint, and too much hype risks disillusionment that may slow the progress [40]. He predicted that 5 to 10 years of additional research and development will be needed before quantum computers start solving useful problems.

3. Quantum gold rush

France Digitale is an association gathering french digital's entrepreneur and investor. With the consulting company Wavestone, France Digitale has published a study on quantum computing and its impact on business and industry [13]. Almost simultanously, *Nature* pusblished a analysis on investment from venture capital to quantum technologies, quantum start-up and its global trends [20]. Companies are meanly involved in three main technology categories: quantum computing, quantum communication and quantum software. Besides, additional companies are involved in providing instruments and hardware component to quantum technologies actors. In 2018, the Boston Consulting Group has published an analysis of the impact of quantum computing on business entitled *The next decade in quantum computing*. In February 2020, CIGREF (a french association [14]) has published a report entitled *Informatique quantique : comprendre le quantum computing pour se préparer à l'inattendu* [15], in which they analyze the disruptive potentiality of quantum computing.

13. L'informatique quantique : prêts pour le grand saut ?, France Digitale - Wavestone (octobre 2019), `https://www.wavestone.com/fr/insight/informatique-quantique/`

14. Cigref is an association representing the largest French companies and public administrations, exclusively users of digital solutions and services, which accompanies its members in their collective reflections on digital issues.

15. `https://www.cigref.fr/quantum-computing-comprendre-informatique-quantique` `https://www.cigref.fr/wp/wp-content/uploads/2020/02/Cigref-Informatique-quantique-Comprendre-Quantum-computing-pou` `pdf`

All these reports and analyze result from the increasing interest of private companies on quantum computing. One is currently at the stage of development of quantum computers where the dream might becomes reality but there's still uncertainty regarding performances that could be obtained. Most of companies rather prefer investing in the technology as a technological prospects, in the case that quantum computers performances reach the required level for huge impact on their market. Consulting groups and professional association have analyzed the potential impact on different markets in ordre to guide companies in their innovation strategies, and avoid to miss the quantum computer revolution (just like Kodak did with the digital camera). This section aims at providing few elements on this market analysis, and is mainly inspired from BCG's analysis.

3.1. "The quantum computing era is here"

In Forbes, Matt Hunter has listed several applications of quantum computing
— hyper-accurate long term weather forecasting;
— drugs discovery through deep study of the behavior of complex molecules;
— new synthetic carbon capturing materials;
— stable, long lasting batteries.

In reference [27], he explained: *"One analyst predicted* **quantum will be as world altering in the 2020s as the smartphone was in the decade just ended**. *"*A beauty of quantum computers is that they will offer a more subtle way of thinking about problems that goes beyond binary - that goes beyond simple 0 or 1, Yes or No, True or False.*" says Dario Gil, the director of IBM research. While the quantum are may develop slowly, it's worth remembering that the Internet - or an early version of it - was around for decades before it was established as the truly revolutionary force it would become. But like Internet, the work researchers are doing on quantum computing lead to a world we can't now imagine."*

In reference [20], E. Gibney has analyze the development of start-ups and spin-off in quantum technologies.

Robert Schoelkopf spent more than 15 years studying the building blocks of quantum computers, until, in 2015, he decided it was time to start constructing one (Quantum Circuits Inc.). *Within 2 years, the team had secured* **US $ 18 million from venture capitalists**. *By the start of the year 2019, investors had funded at least 52 quantum technology compagnies globally since 2012,* **many of them spin-outs from university departments** *(Academics have founded many more start-ups that have yet to close deals).* **In 2017 and 2018, compagnies received at least $ 450 million in private funding - more than 4 times the $ 104 millions disclosed the previous 2 years**. *Hundreds of firms are rushing to invest in the field, by names such as IBM, Google, Alibaba, Hewlett-Packard, Tencent, Baidu and Huawei all doing their own research. From the perspective of investors, the cash pumped into the field annually represents a small outlay so far - on a par with VC (venture capital) investments in artificial intelligence (AI) firms before 2010, for instance. (By 2018, US VC investments in AI had boomed to $9.3 billion.) Despite this, some software firms are already marketing their work on quantum algorithms, which are written for hardware that does not yet exist. Some VC investors are betting on a breakthrough that brings general purpose quantum computers to fruition in five or ten years. Others are banking on making just enough progress for another firm to buy them out.* **Many also hope scientists can find applications for relatively small, imperfect quantum computers, which might emerge sooner.** *These would be limited to tackling specific questions, such as simulating a reaction in quantum chemistry or optimizing a financial model. They might not perform better than a classical that has unlimited computing resources, but they could still create marketable products. If these early quantum computers don't emerge soon with profitable uses, the field could face a "valley of death" in which investment falters, warned a December 2018 report from the US National Academics of Science, Engineering, and Medecine. Some researchers worry about a "quantum winter" similar to "AI winter".* From 2012 to 2018, $ 110 million have been raised in quantum software development, *"this seems like a small investment to get ready for another potentially disruptive force".*

Computing isn't the only quantum technology attracting funds. For example, the swiss startup Qnami in Basel has reveived $130,000 in 2018 to develop a quantum magnetic microscope using NV centers. The hottest quantum technologies field is quantum communication and quantum cryptography.

The boom in quantum startups means that there are already to supply the firms - and the industry, such as it is, risks draining academic talent away from universities, as it happened in AI, says Xanadu's Weedbrook: "*I think we are starting to hit a point where we are concerned about it. More training is needed: a major strand of the $1.2 billion US National Quantum Initiative, which President Donald Trump signed in December 2018, is to train a new generation in quantum related jobs*".

There are solid reasons to think that quantum technologies will create game changing advances. "*It is a question of the timeline, rather than if that will happen*" says Celia Merzbacher, Director of the Quantum Economic Development Consortium Associate.

3.2. Tech companies

End-to-end providers

End-to-end providers are mainly big tech companies and well-funded startups. IBM has been the pioneer in quantum computing and continues at the forefront of the field. More recently: Google and Alibaba have drawn a lot of attention. Microsoft is active but has get to unveil achievements toward actual hardware. Honeywell has just emerged as a new player. Rigetti is the most advanced among the startups. Each company offers its own cloud-based open-source software and varying levels of access to hardware, simulators, and partnerships. In 2016, IBM launched Q Experience, arguably still the most extensive platform to date. It has been followed in 2018 by Rigetti's Forest, Google's Cirq and Alibaba's Aliyun, which has launched a quantum cloud computing service in cooperation with the Chinese Academy of Sciences. Microsoft provides access to a quantum simulator on Azure using its Quantum Development kit. Finally, D-wave Systems, the first company ever to sell quantum computers, its own real-time cloud access to its quantum annealer hard-ware, in October 2018.

The end-to-end integrated companies continue to reside at the center of ecosystem for now. Indeed, vertical integration provides a performance advantage at the current maturity level of the industry. The biggest investments thus far have flowed into the stack's lower layers, but we have not yet seen a convergence on a single winning architecture. Several architectures may coexist over a longer period and even work hand-in-hand in a hybrid fashion to leverage the advantages of each technology.

Hardware and Systems Players

Other entities are focused on developing hardware only (since this is the core bottleneck today). Again, these include both technology giants (such as Intel) but also startups (IonQ, Quantum Circuits, QuTech). Quantum Circuits is a spinoff from Yale university (R. Schoelkopf). It intends to build a robust quantum computer based on a unique modular architecture, while QuTech - a joint effort between Delft University of Technology and TNO, the applied scientific research organization, in the Netherlands - offers a variety of partnering options for companies. Example of hardware and systems players extending into software and services: QuTech. QuTech launched Quantum Inspire, the first European quantum computing plateform, with supercomputing access to a quantum simulator. Quantum hardware access is planned to be available in the first half of 2019.

Software and Services Players

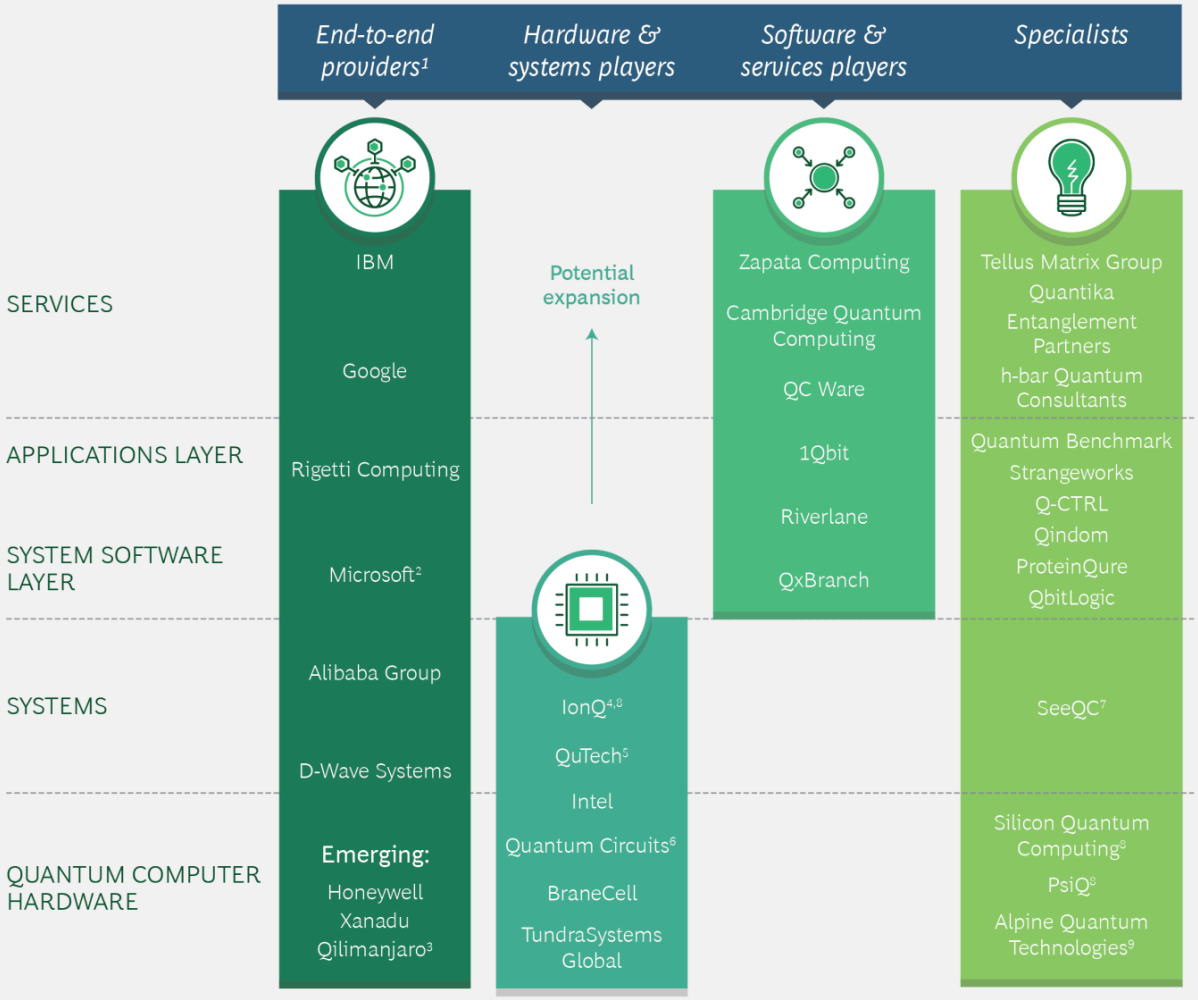
Another group of companies work on potential applications: translating real world problems into the quantum world. It consists in algorithmic and software development. Actual players are Zapata Computing, QC ware, QxBranch, Cambridge Quantum Computing,... which provide software and services to users. Such companies see themselves as an important interface between emerging users of quantum computing and the hardware stack. All are partners of one or more of the end-to-end or hardware players within their mini-ecosystems.

Specialists

Theses are mainly startups, often spinoffs from research institutions, that provide focused solutions to other quantum computing players or to enterprise users. For example, Q-CTRL works on solutions to provide better

systems control and gate operation; Quantum Benchmark asses and predicts errors of hardware and specific algorithms. Both serve hardware companies and users.

EXHIBIT 1 | Companies Assume Four Roles Across Layers of the Stack in the Quantum Computing Ecosystem



Sources: Quantum Computing Report (quantumcomputingreport.com); BCG analysis.
[1]Based on player's ambition with varying levels of maturity and service activities.
[2]Multiple technologies in the labs with focus on topological qubits.
[3]Qilimanjaro is a spinoff from the University of Barcelona.
[4]AWS is invested in IonQ.
[5]QuTech was founded by TU Delft and TNO, and has collaborations with Intel and Microsoft.
[6]Quantum Circuits (qci) is a spinoff from Yale University.
[7]SeeQC is a subsidiary of Hypres.
[8]Vision to become end-to-end provider.
[9]Alpine Quantum Technologies (AQT) is a spinoff from University of Innsbruck.

Fig. V.15. Extracted from `https://www.bcg.com/fr-fr/publications/2018/next-decade-quantum-computing-how-play.aspx`.

Applications end users

For many years, the biggest potential end users for quantum computing capability were national governments. They were particulary interested in their potentiality for security regarding Shor's algorithm and RSA encryption. In documents he released in Wikileaks, Edward Snowden has revealed the project *Penetrating Hard*

Targets, in which NSA has developed a quantum computer for cryptography. This development has cost NSA $79.7 million to develop the machine [16].

Significant government funds flowed fast into quantum computing research thereafter. Widespread consensus eventually formed that algorithms such as Shor's would remain beyond the realm of quantum computers for some years to come and even if current cryptographic methods are threatened, other solutions exist and are being assessed by standard-setting institutions. This has allowed the private sector to develop and pursue other applications of quantum computing. Quite a few industries outside the tech sector have taken notice of the developments in, and the potential of, quantum computing, and companies are joining forces with tech players to explore potential uses. The most common categories of use are for simulation, optimization, machine learning, and AI. Not surprisingly, there are plenty of potential applications.

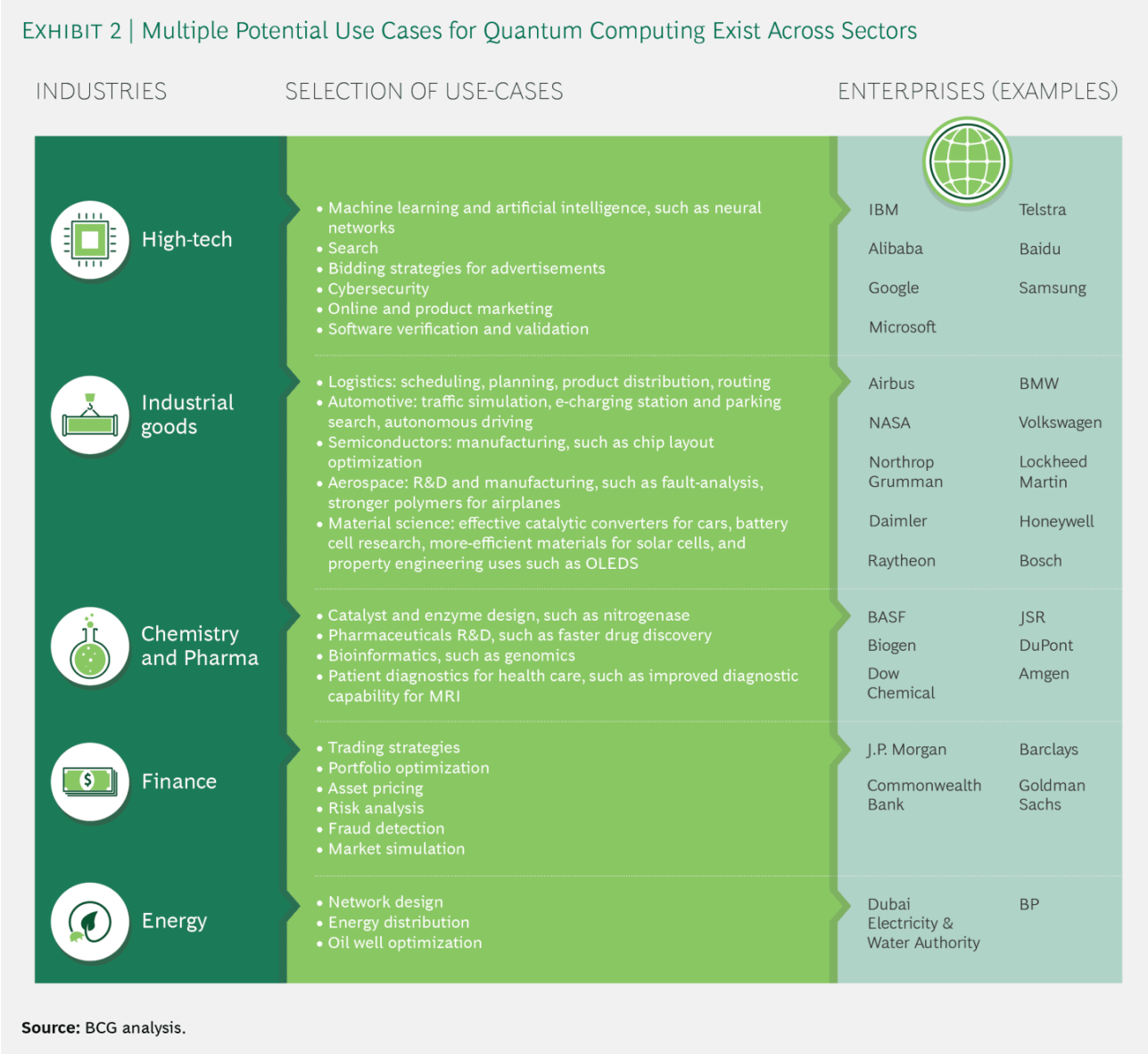


Fig. V.16. Extracted from `https://www.bcg.com/fr-fr/publications/2018/next-decade-quantum-computing-how-play.aspx`.

16. https://www.washingtonpost.com/apps/g/page/world/a-description-of-the-penetrating-hard-targets-project/691/

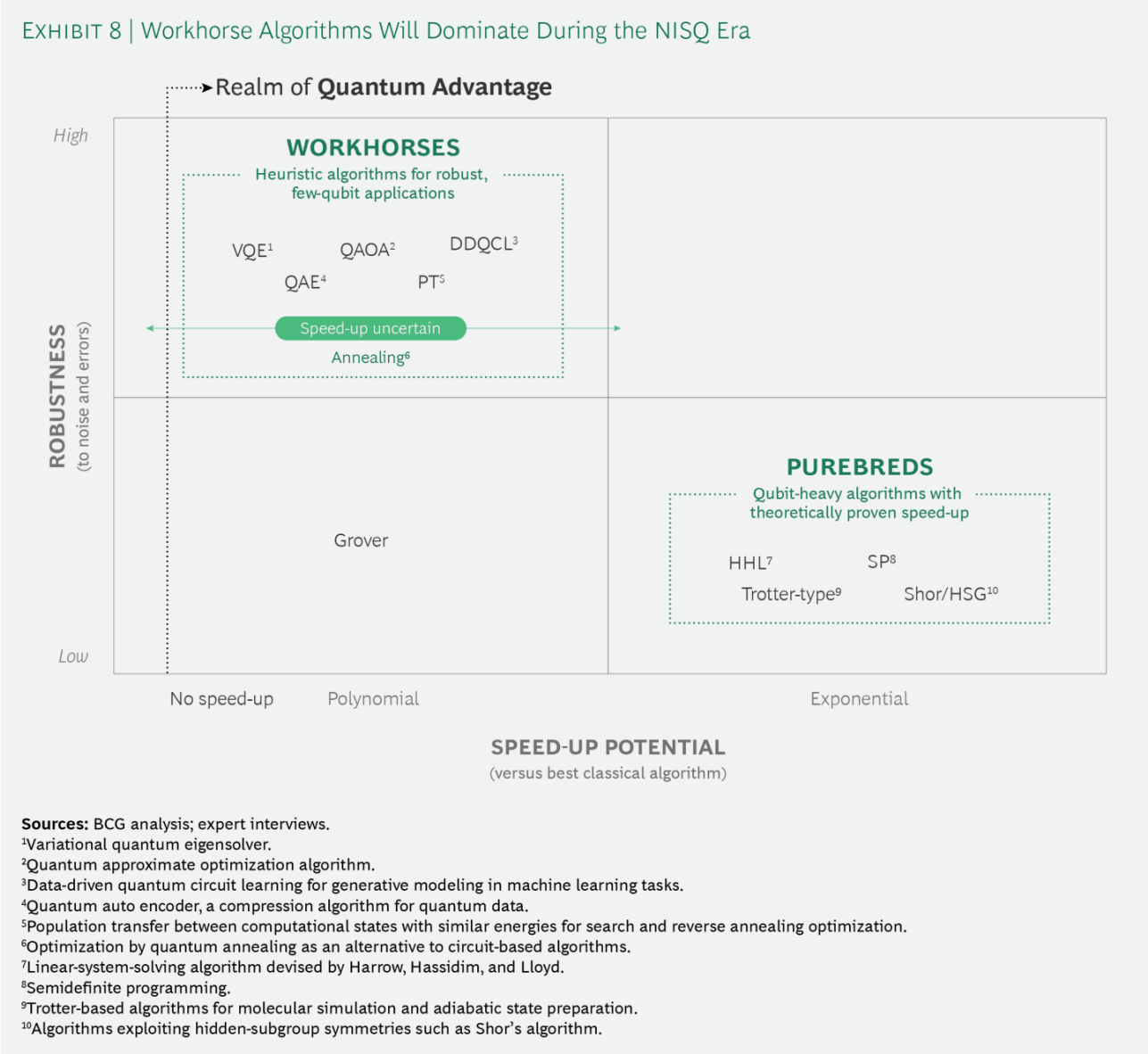


Fig. V.17. Extracted from `https://www.bcg.com/fr-fr/publications/2018/next-decade-quantum-computing-how-play.aspx`.

3.3. Simplifying the quantum algorithm zoo

The US National Institute for Standards and Technology (NIST) maintains a webpage entitled Quantum Algorithm Zoo that contains descriptions of more than 60 types of quantum algorithms. Two of their attributes are especially important in the near term:

Speed-Up How much faster can a quantum computer running the algorithm solve a particular class of problem than the best-known classical computing counterpart?

Robustness How resilient is the algorithm to the random "noise," or other errors, in quantum computing?

There are two classes of algorithm today, named *purebreds* and *workhorses* by BCG in their analysis.

— purebreds are built for speed in noiseless or error-corrected environments.

— workhorses are very sturdy algorithms, but they have a somewhat uncertain speed-up over classical algorithms.

Purebreds have theoretically proven exponential speed-up over conventional computers for specific problems, but require a long sequence of flawless execution, which in turn necessitate very low noise operations and

error correction. For example, one may mentions Shor's factorization algorithm for cracking cryptography and Trotter-type algorithms used for molecular simulation. Unfortunately, their susceptibility to noise puts them out of the realm of practical application for the next ten years and perhaps longer.

Workhorses are designed to be robust in the face of noise and errors. They might have built-in error mitigation, and the number of gate operations is kept low. Most of them are then integrated with classical algorithms. The workhorses should be able to run on anticipated machines in the 100 qubits range (the annealing approaches, although somewhat different, also fall into this category). The dilemma is that very little can be proven about their speed-up performance with respect to classical algorithms until they are put to experimental testing.

But remember that deep learning, which today dominates the fast-growing field of AI, was also once a purely experimental success. Indeed, almost nothing had been proven theoretically about the performance of deep neural networks by 2012 when they started to win every AI and ML competition. The real experiments in quantum computing of the coming years will be truly interesting.

Quantum computing companies are currently betting on the workhorses, which are likely to be the useful algorithms during the error-prone NISQ period of the next decade.

3.4. Within next five years

Industries and potential applications can be clustered on the basis of two factors:
— the expected timing of quantum advantage;
— the value of this advantage to business.
BCG's has grouped them into four categories of engagement: racing team members, riders, followers, and observers.

Racing team members They are at the forefront of immediate business benefits. Their expected time frame to quantum advantage is shortest and the potential business benefit is high. It consists mainly of companies experimenting with quantum chemistry, followed by AI, ML, or both.

Riders they will profit from similar developments, but for less critical value drivers, and are therefore less likely to fund core investments.

Followers They see high potential in the quantum computing technology but are aware of the long development time frames to quantum advantage. For observers, both a clear path to benefits and the development time are still unclear.

Observers Observers are looking at his technology but both a clear path to benefits and the development time are still unclear.

Quantum chemistry is particularly interesting because many important compounds, in particular the active centers of catalysts and inhibitors, can be described by a few hundred quantum states. A number of these compounds are important factors in the speed and cost of production of fertilizers, in the stability and other properties of materials, and potentially in the discovery of new drugs. For these companies and applications, quantum computing provides a highly valuable complementary lens and even outright quantum advantage could be within reach of the next generation of quantum computers. New advances and discoveries could have an incredible impact in agriculture, batteries, and energy systems (all critical in fighting climate change), and on new materials across a wider range of industries, as well as in health care and other areas. Next, speeding up AI and ML is one of the most active fields of research for quantum computing, and combined classical-quantum algorithms are arguably the most promising avenue in the short term. At the same time, AI-based learning models (assuming sufficient volumes of data) can address many of the same business needs as quantum computing, which leads to a certain level of competition between the approaches. Overall, quantum computing can help solve simulation and optimization problems across all industries. In many instances, quantum computers do not focus on replacing current high-performance computing methods, but rather on offering a new and complementary perspective, which in turn may open the door to novel solutions. Risk mitigation or investment strategies in finance are two such examples.

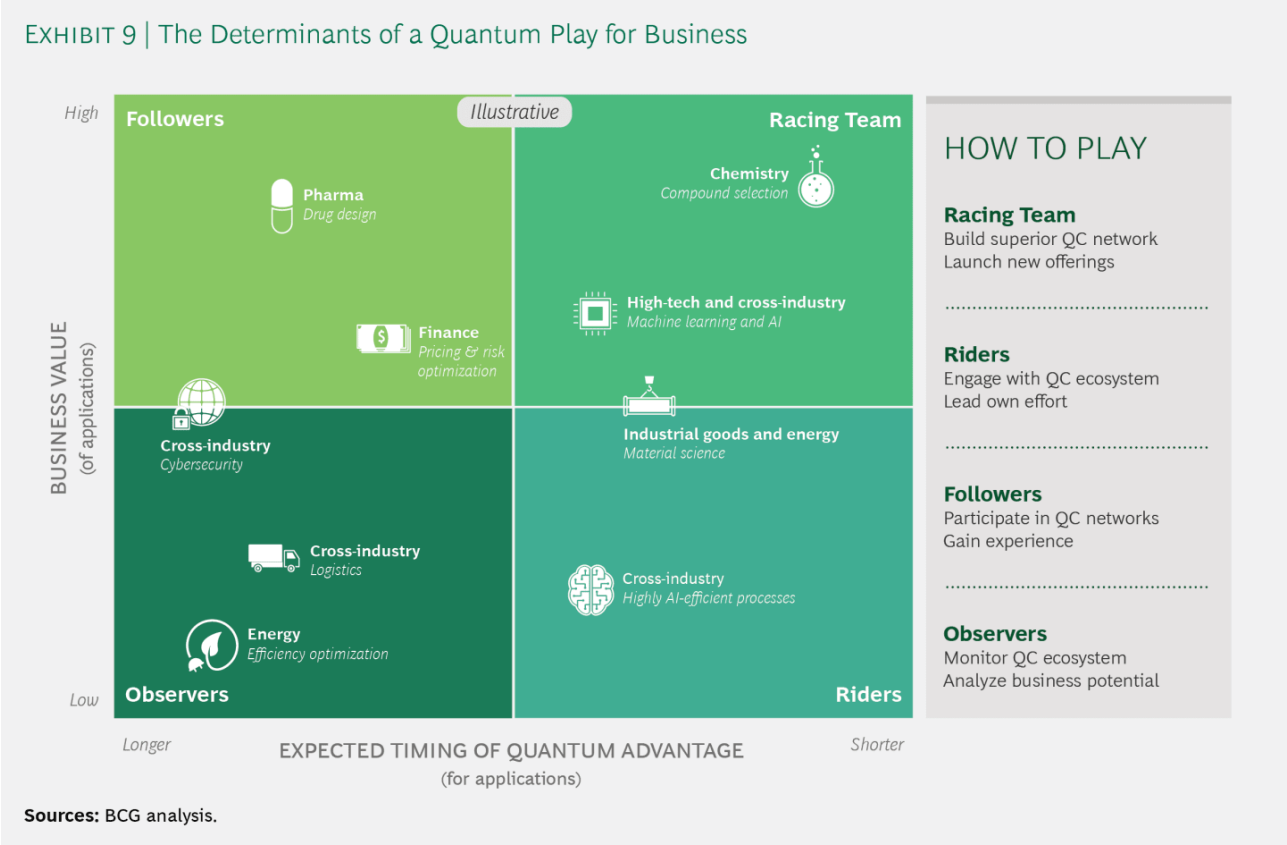


Fig. V.18. Extracted from `https://www.bcg.com/fr-fr/publications/2018/next-decade-quantum-computing-how-play.aspx`.

Businesses are already active at all levels of engagement. A few companies with a significant interest in the technology (Northrop Grumman, Lockheed Martin, or Honeywell), already own or are building their own quantum computing systems. Several partnerships are emerging between quantum computing players and other industries

— JP Morgan, Barclays, and Samsung are working with IBM;
— Volkswagen Group and Daimler are working with Google;
— Airbus, Goldman Sachs, and BMW prefer to work with software and services intermediaries;
— Commonwealth Bank and Telstra have co-invested in Sydney's Silicon Quantum Computing startup (spinoff of University of New South Wales);
— Intel and Microsoft have set up strong collaborations with QuTech;
— OTI Lumionics (startup specialized in customized OLEDs) has started integrating quantum algorithms to discover new materials, in collaboration with D-Wave, Rigetti, and others.
—

3.5. A potential quantum winter

Quantum computing has already been through cycles of excitement and disappointment. While the NISQ period undoubtedly has demonstrated few surprises and breakthroughs, the pathway toward a fault-tolerant quantum computer may well turn out to be the key to unearthing the full potential of quantum computing applications. Some experts thus warn of a potential "quantum winter", as a consequence of too much excitement which tends tend to overestimate the technology potential. As Christopher Monroe warned, **quantum computing is a marathon not a sprint**, and too much hype risks disillusionment that may slow the progress [40]

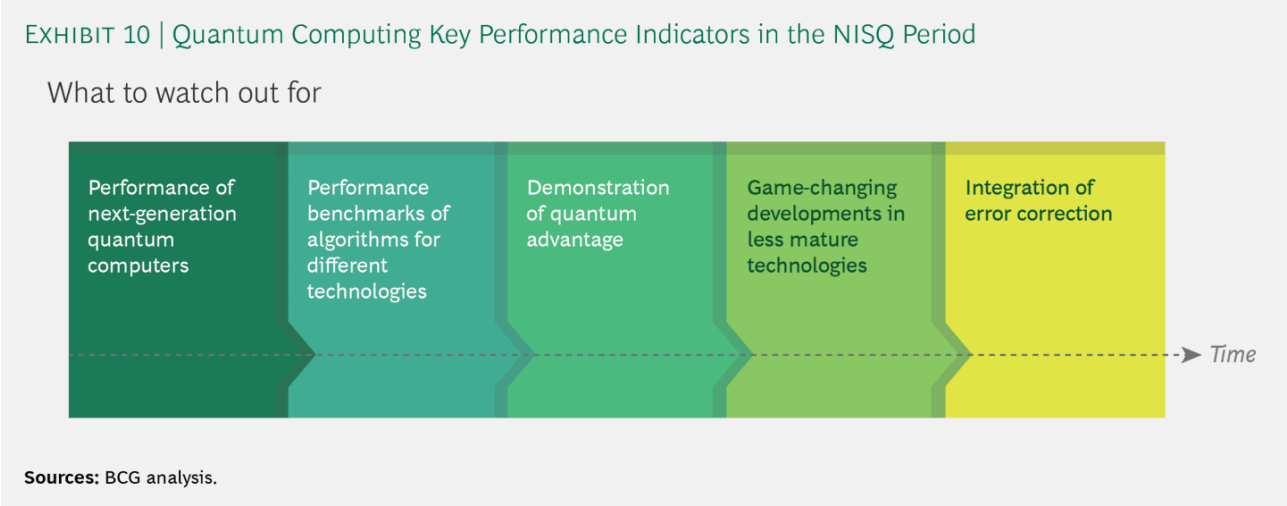


Fig. V.19. Extracted from `https://www.bcg.com/fr-fr/publications/2018/next-decade-quantum-computing-how-play.aspx`.

Bibliography

[1] David W. Allan, Neil Ashby, and Clifford C. Hodge. 1hthe science of timekeeping. *Hewlett-Packard - Application Note 1289*, 1997.

[2] Alain Aspect, Jean Dalibard, and Gérard Roger. Experimental test of bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49:1804–1807, Dec 1982.

[3] S.M. Barnett, C. Fabre, and A. Maître. Ultimate quantum limits for resolution of beam displacements. *Eur. Phys. J. D*, 22(3):513–519, Mar 2003.

[4] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1(3):195–200, November 1964.

[5] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984.

[6] A. Bertoni, P. Bordone, R. Brunetti, C. Jacoboni, and S. Reggiani. Quantum logic gates based on coherent electron transport in quantum wires. *Phys. Rev. Lett.*, 84:5912–5915, Jun 2000.

[7] Niels Bohr. On the constitution of atoms and molecules, part i. *Philosophical Magazine*, 26:1–25, 1913.

[8] Katherine Bourzac. Chemistry is quantum computing's killer app. *C&EN Global Enterprise*, 95, 10 2017.

[9] Joseph L. Bower and Clayton M. Christensen. Disruptive Technologies: Catching the Wave. *Harvard Business Review*, (January–February 1995), January 1995.

[10] Earl T. Campbell, Barbara M. Terhal, and Christophe Vuillot. Roads towards fault-tolerant universal quantum computation. *Nature*, 549(7671):172–179, September 2017. Number: 7671 Publisher: Nature Publishing Group.

[11] Davide Castelvecchi. China's quantum satellite clears major hurdle on way to ultrasecure communications. *Nature News*, 2017.

[12] David P. DiVincenzo. The physical implementation of quantum computation. *Fortschritte der Physik*, 48(9-11):771–783, Sep 2000.

[13] D. Döring, G. McDonald, J.E. Debs, C. Figl, P.A. Altin, H.-A. Bachor, N.P. Robins, and J.D. Close. Quantum projection noise limited interferometry with coherent atoms in a ramsey type setup. *quant-ph/arXiv:1002.3624*, 2010.

[14] Jonathan P. Dowling and Gerard J. Milburn. Quantum Technology: The Second Quantum Revolution. *arXiv:quant-ph/0206091*, June 2002. arXiv: quant-ph/0206091.

[15] L. Fedichkin, M. Yanchenko, and K. A. Valiev. Novel coherent quantum bit using spatial quantization levels in semiconductor quantum dot, 2000.

[16] Richard P. Feynman. There's Plenty of Room at the Bottom. *Engineering and Science*, 23(5):22–36, February 1960. Number: 5 Place: Pasadena, CA Publisher: California Institute of Technology.

[17] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6/7), 1982.

[18] forbes. Innovation Strategy: 4 Key Tactics of Top Growth Companies, January 2014.

[19] Sasa Gazibegovic, Diana Car, Hao Zhang, Stijn C. Balk, John A. Logan, Michiel W. A. de Moor, Maja C. Cassidy, Rudi Schmits, Di Xu, Guanzhong Wang, Peter Krogstrup, Roy L. M. Op het Veld, Kun Zuo, Yoram Vos, Jie Shen, Daniël Bouman, Borzoyeh Shojaei, Daniel Pennachio, Joon Sue Lee, Petrus J. van Veldhoven, Sebastian Koelling, Marcel A. Verheijen, Leo P. Kouwenhoven, Chris J. Palmstrøm, and Erik P. A. M. Bakkers. Epitaxy of advanced nanowire quantum devices. *Nature*, 548(7668):434–438, August 2017.

[20] Elizabeth Gibney. Quantum gold rush: the private funding pouring into quantum start-ups. *Nature*, 574:22–24, October 2019.

[21] Clark Gilbert and Joseph L. Bower. Disruptive Change: When Trying Harder Is Part of the Problem. *Harvard Business Review*, (May 2002), May 2002.

[22] Martin Giles. We'd have more quantum computers if it weren't so hard to find the damn cables. Library Catalog: www.technologyreview.com.

[23] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.

[24] Fernando Gonzales-Zalba, Tsung-Yeh Yang, and Alessandro Rossi. Manufacturing silicon qubits at scale, November 2019.

[25] I. Gross, W. Akhtar, V. Garcia, L. J. Martínez, S. Chouaieb, K. Garcia, C. Carrétéro, A. Barthélémy, P. Appel, P. Maletinsky, J.-V. Kim, J. Y. Chauleau, N. Jaouen, M. Viret, M. Bibes, S. Fusil, and V. Jacques. Real-space imaging of non-collinear antiferromagnetic order with a single-spin magnetometer. *Nature*, 549(7671):252–256, September 2017.

[26] Robert Hackett. Samsung joins google and amazon in backing 'trapped ion' quantum computer startup.

[27] Matt Hunter. IBM BrandVoice: The quantum Computing Era Is Here. Why It Matters—And How It May Change Our World. Library Catalog: www.forbes.com Section: Innovation.

[28] Ingmar Jakobi, Philipp Neumann, Ya Wang, Durga Bhaktavatsala Rao Dasari, Fadi El Hallak, Muhammad Asif Bashir, Matthew Markham, Andrew Edmonds, Daniel Twitchen, and Jörg Wrachtrup. Measuring broadband magnetic fields on the nanoscale using a hybrid quantum register. *Nature Nanotechnology*, 12(1):67–72, January 2017.

[29] E. A. Johnson. Touch display–a novel input/output device for computers. *Electronics Letters*, 1(8):219–220, October 1965.

[30] Abhinav Kandala, Antonio Mezzacapo, Kristan Temme, Maika Takita, Markus Brink, Jerry M. Chow, and Jay M. Gambetta. Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *Nature*, 549(7671):242–246, September 2017.

[31] B. E. Kane. A silicon-based nuclear spin quantum computer. *Nature*, 393(6681):133–137, May 1998.

[32] Masahiro Kitagawa and Masahito Ueda. Squeezed spin states. *Phys. Rev. A*, 47(6):5138–5143, Jun 1993.

[33] D. Leibfried, M. D. Barrett, T. Schaetz, J. Britton, J. Chiaverini, W. M. Itano, J. D. Jost, C. Langer, and D. J. Wineland. Toward Heisenberg-Limited Spectroscopy with Multiparticle Entangled States. *Science*, 304(5676):1476–1478, 2004.

[34] Yun Li. *États comprimés de spin dans un condensat de Bose-Einstein*. PhD thesis, Université Pierre et Marie Curie, 2010.

[35] Yun Li, Y. Castin, and A. Sinatra. Optimum spin squeezing in bose-einstein condensates with particle losses. *Phys. Rev. Lett.*, 100(21):210401, May 2008.

[36] I. Lovchinsky, A. O. Sushkov, E. Urbach, N. P. de Leon, S. Choi, K. De Greve, R. Evans, R. Gertner, E. Bersin, C. Müller, L. McGuinness, F. Jelezko, R. L. Walsworth, H. Park, and M. D. Lukin. Nuclear magnetic resonance detection and spectroscopy of single proteins using quantum logic. *Science*, 351(6275):836–841, 2016.

[37] R. Maurand, X. Jehl, D. Kotekar-Patil, A. Corna, H. Bohuslavskyi, R. Laviéville, L. Hutin, S. Barraud, M. Vinet, M. Sanquer, and S. De Franceschi. A CMOS silicon spin qubit. *Nature Communications*, 7(1):1–6, November 2016. Number: 1 Publisher: Nature Publishing Group.

[38] V. Meyer, M. A. Rowe, D. Kielpinski, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland. Experimental demonstration of entanglement-enhanced rotation angle estimation using trapped ions. *Phys. Rev. Lett.*, 86(26):5870–5873, Jun 2001.

[39] X. Mi, M. Benito, S. Putz, D. M. Zajac, J. M. Taylor, Guido Burkard, and J. R. Petta. A coherent spin–photon interface in silicon. *Nature*, 555(7698):599–603, March 2018.

[40] Christopher Monroe. Quantum computing is a marathon not a sprint, April 2019.

[41] Xavier Vasques Olivier Hess, Jean-Michel Torres. Une nouvelle ère de l'informatique. *Ingénierie cognitique*, 4(Numéro 1), 2020.

[42] K.I. Petsas, A. Gatti, L.A. Lugiato, and C. Fabre. Multimode squeezed states produced by a confocal parametric oscillator. *Eur. Phys. J. D*, 22(3):501–512, Mar 2003.

[43] Gary P. Pisano. You Need an Innovation Strategy. *Harvard Business Review*, (June 2015), June 2015.

[44] Gabriel Popkin. Waiting for the Quantum Simulation Revolution. *Physics*, 12, October 2019.

[45] Michael G. Raymer and Christopher Monroe. The US National Quantum Initiative. *Quantum Science and Technology*, 4(2):020504, February 2019.

[46] Markus Reiher, Nathan Wiebe, Krysta M. Svore, Dave Wecker, and Matthias Troyer. Elucidating reaction mechanisms on quantum computers. *Proceedings of the National Academy of Sciences*, 114(29):7555–7560, 2017.

[47] Simon Schaal, Alessandro Rossi, Virginia N. Ciriano-Tejel, Tsung-Yeh Yang, Sylvain Barraud, John J. L. Morton, and M. Fernando Gonzalez-Zalba. A CMOS dynamic random access architecture for radio-frequency readout of quantum devices. *Nature Electronics*, 2(6):236–242, June 2019.

[48] D. Sheng, S. Li, N. Dural, and M. V. Romalis. Subfemtotesla scalar atomic magnetometry using multipass cells. *Phys. Rev. Lett.*, 110:160802, Apr 2013.

[49] Christoph Stampfer, Heidrun Heinke, and Sebastian Staacks. A lab in the pocket. *Nature Reviews Materials*, pages 1–2, February 2020.

[50] Wolfgang Tittel, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography. *Physics World*, 11(3):41–46, mar 1998.

[51] T. F. Watson, S. G. J. Philips, E. Kawakami, D. R. Ward, P. Scarlino, M. Veldhorst, D. E. Savage, M. G. Lagally, Mark Friesen, S. N. Coppersmith, M. A. Eriksson, and L. M. K. Vandersypen. A programmable two-qubit quantum processor in silicon. *Nature*, 555(7698):633–637, March 2018.

[52] D. J. Wineland, J. J. Bollinger, W. M. Itano, and D. J. Heinzen. Squeezed atomic states and projection noise in spectroscopy. *Phys. Rev. A*, 50(1):67–88, Jul 1994.

[53] D. J. Wineland, J. J. Bollinger, W. M. Itano, F. L. Moore, and D. J. Heinzen. Spin squeezing and reduced quantum noise in spectroscopy. *Phys. Rev. A*, 46(11):R6797–R6800, Dec 1992.

[54] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, October 1982.

[55] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, Guang-Bing Li, Qi-Ming Lu, Yun-Hong Gong, Yu Xu, Shuang-Lin Li, Feng-Zhi Li, Ya-Yun Yin, Zi-Qing Jiang, Ming Li, Jian-Jun Jia, Ge Ren, Dong He, Yi-Lin Zhou, Xiao-Xiang Zhang, Na Wang, Xiang Chang, Zhen-Cai Zhu, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[56] B. Yurke and D. Stoler. Generating quantum mechanical superpositions of macroscopically distinguishable states via amplitude dispersion. *Phys. Rev. Lett.*, 57(1):13–16, Jul 1986.

[57] MILAN ZELENY. High technology and barriers to innovation: From globalization to relocalization. *International Journal of Information Technology & Decision Making*, 11(02):441–456, 2012.

[58] Rui Zhang, Terry Dyer, Nathan Brockie, Roozbeh Parsa, and Rahul Mhaskar. Subpicotesla scalar atomic magnetometer with a microfabricated cell. *Journal of Applied Physics*, 126(12):124503, 2019.