SCIENCE AND TECHNOLOGY BRIEFINGS
PARLIAMENTARY OFFICE FOR SCIENTIFIC AND TECHNOLOGICAL ASSESSMENT

Briefing 13

Quantum Technologies: Introduction and Challenges

March 2019

© monsitj/ Adobe Stock

Summary

- *Many everyday technologies are based on the principles of quantum physics: lasers, transistors, satellite positioning systems (GPS), etc.*
- *Over the past few years, quantum technologies in the broad sense have been the focus of marked interest from both businesses and governments, in parallel to technical breakthroughs.*
- *New quantum technologies concern applications such as sensors, calculation or communications. These fields rely on the principles of quantum physics, particularly entanglement and state superposition.*
- *In Europe, a major "flagship" programme was launched in 2018 to support European projects in the global quantum technology race, the main countries in the running being China and the United States.*

Mr. Cédric Villani, MP (National Assembly), Vice-Chairman

Investments in the field of quantum technologies have grown considerably over the last few years. Special attention should be paid to these projects, which focus both on fundamental research and breakthrough innovations, and generate intense international scientific and technological competition.

Quantum physics and historical applications

On the atomic scale, the laws of traditional physics struggle to describe the behaviour of particles such as atoms, electrons and photons. In the 1920s, Niels Bohr, Louis de Broglie, Erwin Schrödinger, Werner Heisenberg and many other scientists developed a theory, complete with its own mathematical formalism, to better understand the phenomena at work at the scale of these particles. This work marked the birth of quantum physics.

In traditional physics, a physical object – for instance, an atom – has a continuously-changing energy level and can be modelled by a point located in a precise position at a given time. Physical objects are clearly different from waves, which are the propagation of a disruption in space.

In quantum physics, energy is exchanged discretely, or discontinuously, in packets called "quanta".[1] This principle of quantification, imagined back in 1900 by Max Planck, set down the initial foundations of quantum physics, in which the concepts of wave and point object are combined to account for the behaviour of objects on the atomic scale. In this wave-particle duality, the exact position of a particle at a given time can no longer be predicted, but only the probability of finding it in a given place at that time. These somewhat counter-intuitive phenomena are behind the two main concepts used by the majority of technologies based on quantum physics: state superposition and entanglement.

With the principle of superposition, the overall state of a quantum system at a given time becomes a linear combination of all its possible states at that moment in time. Only the probability of the presence of a particle in a given position can be predicted.

In parallel, anyone attempting to accurately measure the state of the particle comes up against Heisenberg's uncertainty principle.[2] According to this fundamental relationship, it is impossible to know the position and speed of a quantum particle simultaneously. More generally, acquisition of information on one quantum measurement inevitably involves a loss of information on others. In other terms, in quantum physics, it is impossible to take a measurement without disrupting the state of the object being measured.

Entanglement is the connection between two or more quantum objects and between their information. Modifying the state of one of them instantaneously causes a change in the other. The pair must then be considered as a single, inseparable and global system: the pair's properties are not simply the sum of the properties of the two bodies.

Nowadays, everyday devices already rely on quantum physics, such as **GPS** (*Global Positioning System*): our position is determined with an accuracy of one metre (or even one centimetre) using the **atomic clocks** created back in the 1960s and installed onboard orbiting satellites. These clocks, which are based on the unchanging state transition frequencies of certain atoms,[3] characteristic of quantum physics, enable the corrections that are essential for GPS satellite positioning systems[4] to function properly and accurately. **Laser**[5] technology

was also made possible by advances in the quantum field, particularly optics and electronics. Now used in a very wide range of applications, they were developed during the same period as atomic clocks. Finally, **transistors and integrated electronic circuits**, which today form the basis of communication and information technologies, are also among the first applications that retrospectively marked the **first quantum revolution**.

It was not until the 1980s that the first ideas for potential applications of quantum physics in computing and IT popped up, particularly in the work of Richard Feynman[6] on the potential power of a computer with the ability to simulate quantum phenomena. The concept of the quantum computer emerged gradually between the late 1980s and the early 1990s, via the work of the physicist David Deutsch and the mathematician Richard Jozsa, which led to the creation of the first quantum algorithm,[7] i.e. a sequence of logical operations using the principles of superposition and entanglement, solving a problem more quickly than all known traditional algorithms. In a higher theoretical manner, they demonstrated that **certain calculations would be significantly accelerated if the principles of quantum physics could be applied to computers.** In 1994, the development of Shor's algorithm renewed interest in the subject once again. This algorithm, which was designed to work on a quantum computer, **could decode** the **data encryption protocols**[8] used by governments and for civil purposes **in record time**. Back then, the threat was still only theoretical, however, as the technologies required to design quantum computers did not yet exist. However, this episode did open the way for scientists to attempt to develop quantum algorithms that were more powerful than standard traditional algorithms.

Scientific and technical progress was continuing, meanwhile: in the 1960s, major work was started by John Bell before being pushed further, in the early 1980s, with the "EPR" experiments of Alain Aspect[9], which irrefutably proved the phenomenon of quantum entanglement, despite scepticism among the contemporary scientific community. These rather complex experiments allowed **individual preparation and handling of quantum objects (atoms, ions, photons), which opened up a whole new range of possibilities** to make progress on the theoretical principles of quantum physics, as well as on potential applications using the principles of quantum superposition and entanglement.

Quantum technologies based on quantum properties

Superposition would make it possible to greatly increase the power of current computers. In traditional IT, information is stored and handled using a bit, i.e. a physical medium with a value of 0 (locked) or 1 (unlocked). In a quantum state, due to the principle of superposition, the state (or value) of the medium becomes a linear combination of 0 and 1 states. **For N quantum bits, the system's computing power grows exponentially because there are then 2^N possible states.**[10] This means that a few quantum bits would be sufficient to achieve considerable computing capacities.

At the same time, **entanglement allows secure, remote communication, i.e. exchange of information.** The most recent experiments have demonstrated that a pair of quantum objects remains entangled even hundreds of kilometres from each other. This allows detection of "intrusions" (disruptions), for instance on a sensitive communication line, which is why cryptography has become one of the main fields of application of entanglement.

As in the example of atomic clocks, **quantum sensors** rely on the reproducibility of a quantum system but also on its sensitivity on the scale of the unique quantum system. In practical terms, for instance, this means **handling isolated atoms almost individually**[11] **in order to make high-precision measurements** (electrical, magnetic, gravity, etc. fields). This is notably the case of magnetic resonance systems, and particularly their application to medical imaging - MRI[12] - which allows non-invasive observation inside the human body with unrivalled contrast and accuracy. Quantum sensors have been developed over a number of decades, particularly thanks to technical progress making it possible to improve their sensitivity and also extend their field of applications.

IT: new needs and the second quantum revolution

Over the last few years, **demand for computing power has grown non-stop**, particularly with the recent explosion of big data[13] and the need for increasingly-accurate digital simulations. Until now, one of the solutions to meet this demand was to use parallel **supercomputing**, but this was both expensive and increasingly energy-hungry[14].Growth in demand could also be due to the **exponential increase in computer transistor density, according to Moore's law**[15] (see insert). **These paradigms are now reaching their limits, making a technological breakthrough necessary.**

Moore's law:
In 1965, Gordon E. Moore (one of Intel's three founders) set out what is now known as **Moore's law**, i.e. that transistor density (number of transistors per unit of surface) – the source of traditional computers' computing power – **could double every two years**.
This prediction turned out to be astonishingly accurate, and over the last few years, process technology has continuously improved, hitting 10 nm (1 nm = 10^{-9}m) in 2017. However, this progress has hit its physical limits as we near the dimensions of an atom, and **the trend is expected to stall in around 2020-2022**.

This is why the quantum technology race has now been launched. In terms of technology, quantum sensors, which are already considered mature, are seeing their range of applications extended and their accuracy hitting new highs; major industrialists in the US (IBM, Microsoft, Google), France (Atos) or Asia (Alibaba) are showing interest in quantum computing, whether for new quantum physical data media or to develop an innovative algorithm using quantum principles. Finally, quantum computing could have knock-on effects in the field of data cryptography and security, by challenging current encryption methods, which need to be rethought as a precaution. These avant-garde technologies require massive investment, also in fundamental research. Even if major areas for application have already been identified (computing, communications), unexpected advances or discoveries could emerge as a result of this recent enthusiasm for this complex issue, for which different paths are being explored.(16)

Together, IT developments made since the early 2000s form the **second quantum revolution,** i.e. a "*turning point, the switch from theoretical fundamental research to an engineering and development phase*", as confirmed by economic stakeholders.(17)

Global investment programmes

Governments have followed these developments closely and are investing massively in the market to strengthen their international influence. In 2018, the **European Union** decided to allocate €1 billion over a 10-year period to quantum technologies, via a FET flagship(18) programme, which follows in the footsteps of the Quantum Manifesto(19) submitted to the European Commission in 2016 by 3,000 members of the scientific community. It is funded by the Horizon 2020 programme, but also by national schemes. Interest is such that non-EU countries have also signed up to the programme(20).The programme aims to include all aspects of quantum technologies and is divided into **four fields of interest, based on a common core of fundamental science:**

- quantum computing, which becomes exponentially faster and more powerful based on the principle of superposition;

- quantum simulation to simply reproduce quantum interactions between atoms within molecules or crystals;

- communications to exchange information via ultra-secure quantum protocols and media;

- quantum sensors, which are so accurate that they make industrial and fundamental research applications possible.

The results of the first flagship call for proposals were released at the end of October 2018: among the twenty projects selected, thirteen include CNRS laboratories, two with the participation of Atos (Pasquans and Aqtion), and two coordinated by French organisations, Sorbonne University (PhoQuS project) and Thales (ASTERIQS project). France is ranked among the five countries with the best success rates(21).

In addition to their good ranking, certain countries, such as **Germany** or the **United Kingdom**, have set up national programmes with budgets of several hundred million euros,(22) for instance €650m for the German initiative and more than €500m for its UK equivalent. Some of these national plans aim to have academic institutions and US businesses join forces.

In the **Netherlands**, the *QuTech*(23) initiative, a quantum computing and internet research centre on the campus of *TU Delft (Technische Universiteit Delft)*, has a 10-year budget of approximately €150m, which is publicly-funded but also backed by industrial partnerships with Intel and Microsoft.

In 2016, in the international race, **China** established the first quantum communication line from the QUESS (*Quantum Experiments at Space Scale*) programme's Micius geostationary satellite. This launch was a key part of the 2015-2020 five-year plan for China, which plans to use this satellite to secure its communications, both military and commercial. According to physicist Jian-Wei Pan, who is heading up the project, China plans to develop "*a global quantum communications network by 2030*".(24) The Chinese quantum programme is also working on quantum computing and sensors and a large number of patents have been filed since 2015, rising constantly since 2010. The budgets allocated to these two areas are estimated, with a high level of inaccuracy, to be €1 billion each.

Quantum communication lines:
Recent progress allow exchanging of information between two distant users using entangled photons.
It is now possible to send entangled pairs via two optical fibres heading off in different directions to establish a terrestrial communication line.
The Chinese QUESS experiment established a "satellite" communication line between an orbiting satellite, emitting entangled photons, and two ground receiving stations, 1,200km apart.
Though terrestrial quantum links are still limited to around a hundred kilometres, satellite links open the way for intercontinental and larger-scale quantum exchanges.

In the **United States**, even though the private sector is already in the race with investments by tech giants (Google, IBM, Microsoft, Intel), public policy has only recently caught up. The US Congress just adopted, in December 2018, the National Quantum Initiative Act:[25] this programme, also lasting 10 years, will start with a first five-year plan worth more than €1 billion. It will particularly focus **on quickly training quantum engineers and developers, who are still few and far between faced with the expected strong growth in the sector's needs.** The United Kingdom is also focusing heavily on this area, setting aside nearly €200m from its national programme for quantum technology thesis programmes and a little under €15m to train young researchers.[26]

The French ecosystem

In France, since 2017, the ANR (French National Research Agency) has set up a Scientific Assessment Board (CES 47) dedicated to quantum technologies and with a budget of some €10m. In Grenoble, three laboratories (CEA-Leti, INAC and Institut Néel) have joined forces to work on the QuCube project to develop a quantum processor using semiconducting silicon.[27] Their project was awarded the European Research Council's Synergy Grant and will receive €14m over a 6-year period. The Île-de-France region has recognised quantum technologies as a "Major Field of Interest" and is backing the SIRTEQ[28] project, which has a budget of approximately €10m over a 4-year period.

A few **private initiatives are being set up in anticipation of a large-scale national initiative**, such as the Quantonation[29] fund, created in September 2018. This scheme aims to raise a total of €40m for investment over 4 years to support start-ups from day 1.[30] Atos, meanwhile, has invested and is marketing its QLM (Quantum Learning Machine), the only quantum simulation platform on the market, with customers in both the US and Europe. Elsewhere, IBM inaugurated its seventh global centre of excellence, IBM Q Hub, which specialises in quantum computing, on December 2018 in Montpellier.[31]

Efforts are also being made to transfer technology and identify commercial applications in the French quantum physics research sector. The start-up Muquans[32] is specialised in quantum gravimeters[33] and very-high-accuracy atomic clocks (i.e. which lose less than 1 second over 30 million years). Likewise, the Quandela company,[34] which started out in the academic world (CNRS - *Comité National de la Recherche Scientifique* / French National Scientific Research Centre - and Paris Saclay University), manufactures indiscernible photon sources[35] that can be used as a data medium for an "optical" quantum computer.

Conclusions and prospects

With the start of the second quantum revolution, both governments and businesses in many countries are launching ambitious plans to anticipate upcoming changes and opportunities. As demonstrated by the European flagship programme, and without ruling out identification of currently-unknown possible uses, by serendipity, this revolution is strategically important for France and Europe and will have an impact on a wide range of fields, at the crossroads between fundamental research and engineering, which will be the focus of upcoming scientific papers, particularly on quantum IT and computers, as well as quantum and post-quantum cryptography.

OPECST websites:
http://www.assemblee-nationale.fr/commissions/opecst-index.asp
http://www.senat.fr/opecst/

Experts and scientists consulted

Mr. Alain Aspect, physicist at Institut d'Optique, member of the OPECST Scientific Board.

*Mrs. Astrid Lambrecht, Director of Research at the CNRS (*Comité National de la Recherche Scientifique - *French National Committee for Scientific Research), Director of the CNRS Institute of Physics (INP/CNRS), member of the OPECST Scientific Board.*

Mrs. Fanny Bouton, journalist specialised in new technologies.

Mr. Antoine Browaeys, Director of Research at Institut d'Optique.

Mrs. Anne Canteaut, Director of Research at INRIA (French National Research Institute for the Digital Sciences), SECRET group.

Philippe Chomaz, Executive Director of Scientific Affairs at the CEA Fundamental Research Department.

Mr. Thierry Debuisschert, research engineer, Thalès.

Mr. Bruno Desruelle, Chairman & CEO of the start-up Muquans.

Mrs. Eleni Diamanti, Research Manager at the Paris 6 IT Laboratory (LIP6).

Mr. Philippe Duluc, Atos Big Data & Security Technical Director.

Mr. Daniel Estève, Director of Research and Head of the Quantronics group at CEA.

Mr. Olivier Ezratty, consultant specialised in new technologies and author of the "Opinions libres" blog.

Mr. Adrien Facon, RISQ Programme lead manager, Innovation Group Director at Secure IC.

Mr. Philippe Grangier, CNRS Director of Research and Quantum Optics Group Manager at Institut d'Optique.

Mr. Serge Haroche, professor emeritus (Collège de France), 2012 Nobel prize in physics.

Mr. Christophe Jurczak, CEO of the Quantonation investment fund.

Mr. Anthony Leverrier, Research Manager at INRIA, in the SECRET group.

Mr. Grégoire Ribordy, co-founder and Chairman & CEO of the start-up ID Quantique.

Mrs. Pascale Senellart, Director of Research at the CNRS Photonics & Nanostructures Laboratory. Co-founder of the start-up Quandela.

Mr. Sébastien Tanzilli, Director of Research and project manager at CNRS specialising in quantum technologies.

Mr. Georges Uzbelger, AI/Advanced Analytics Solution at IBM France.

Benoit Wintrebert, Innovation Advisor to the French Armies Ministry.

Scientific coordination by Mrs. Sarah Tigrine, scientific advisor (with the participation of Mr. Gaëtan Douéneau).

Reference works consulted:

- "Comprendre l'informatique quantique", O. Ezratty, November 2018 (e-book)

- US academic report: National Academies of Sciences, Engineering, and Medicine. 2018. Quantum Computing: Progress and Prospects. The National Academies Press, Washington, DC. DOI: https ://doi.org/10.17226/25196.

- "Clefs CEA" N° 66- June 2018 "Quantum Revolutions"

N.B.: as agreed with the French National Assembly's ethics officer, Cédric Villani took a step back from his role on ATOS's Science Board (non-decision-making body) for the duration of his work for the Office on quantum technologies.

Endnotes

(1) Its singular form is "quantum", which is Latin for "how many". In physics, refers to an indivisible quantity (of energy, mass, etc.).

(2) Heisenberg was the winner of the 1932 Nobel Prize in Physics for his contribution to the creation of quantum mechanics.

(3) Atomic clocks are based on the unchanging energy level transition frequency of Caesium 133. Since 1967, this frequency has been used as a reference to set the second, which then becomes the amount of time during which 9,192,631,770 oscillations at the frequency of this transition occur.

(4) By comparison, a traditional quartz watch loses 1 second per day, but an atomic clock loses 10 ns per day (two billionths of a second). Desynchronization by 1 second causes a GPS positioning error of 300,000km.

(5) The word "laser" is an acronym: "*light amplification by stimulated emission of radiation*". The basic principle of the laser relies on de-excitation of an atom, stimulated by an input of (light) energy equivalent to the transition energy between two electronic states. Quantum mechanics posits that these levels are discrete and perfectly defined. The photon emitted by de-excitation is added to the incident light field, which creates the phenomenon of amplification.

(6) Richard Feynman, "*Simulating Physics with Computers*", International Journal of Theoretical Physics, vol. 21, nos 6–7, 1982, p. 467–488

(7) Deutsch-Jozsa's algorithm, which is used to solve a classification problem and is of no real practical interest, is nevertheless the first example of a practically-implemented "useful" quantum algorithm.

(8) Shor's algorithm is used to factorise a number, i.e. writing it as a product of prime numbers (e.g. 15 = 3×5), in an exponentially faster time than traditional algorithms. If this algorithm were to be implemented on a powerful quantum machine, current encryption protocols, which are based on the difficulty of the factorisation problem, would be very quickly cracked.

(9) The experiments conducted by Alain Aspect at the start of the 1980 are often called "EPR experiments" because they were in response to the Einstein-Podolsky-Rosen (EPR) paradox, published in 1935. They concern the quantum entanglement phenomenon, theoretically advanced by Niels Bohr. Einstein and his colleagues thought that entanglement violated the laws of physics, and more specifically locality, and that the formalism of quantum mechanics was incomplete. The debate wasn't settled until 1964, when John Bell, a theorist at CERN in Geneva, published a theorem, known as "Bell's theorem", making it possible to experimentally verify this concept. This is what Alain Aspect did in 1981 by violating Bell's theorem and providing irrefutable evidence of entanglement between a pair of photons.

(10) For instance, for N=10 quantum bits, $2^{10}=10^{24}$ possible states exist simultaneously and for N=50, there are $2^{50}\approx10^{15}$ superposed states, i.e. one million billion.

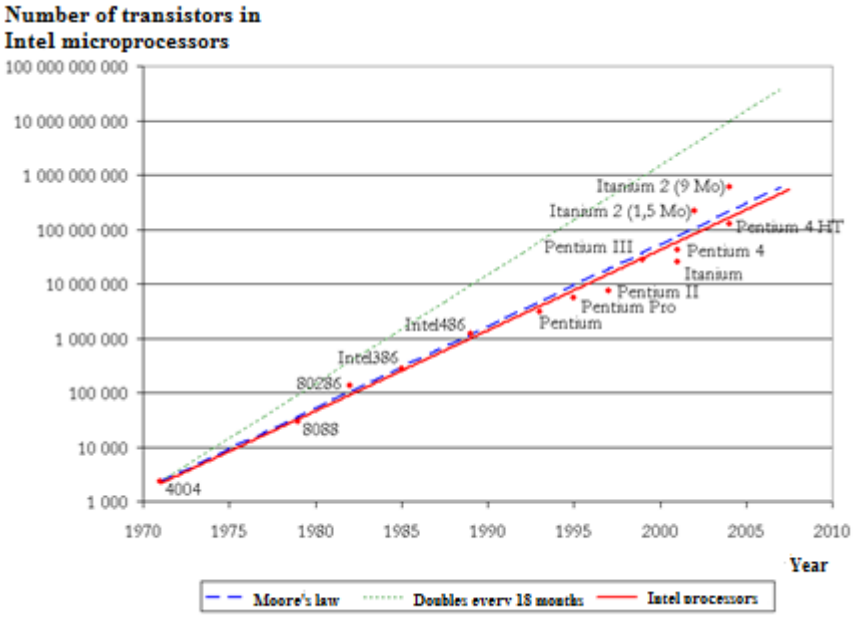
(*11*) There are two techniques to isolate atoms: cooling (using liquid helium at a temperature approaching -273K, i.e. absolute zero) or trapping the atom in a crystal matrix (principle of "NV centres", where a nitrogen atom N is trapped in a diamond matrix).

(*12*) Using a powerful magnetic field, produced by a superconducting magnet, human tissue is magnetised by aligning their magnetic spins. Combined with a less intense and oscillating magnetic field, the spins then adopt a precession movement, which produces a measurable electromagnetic signal. Used on humans for the first time in the 1970s, the principle of MRI won its inventors, Paul Lauterbur and Peter Mansfield, the Nobel Prize in Physiology or Medicine in 2003.

(*13*) It is estimated that, by 2020, 1.7 megabytes (Mb) of data will be created per second, per person. This is the size of a file in MP3 compressed format containing a song lasting approximately 2 minutes.

(*14*) Even if the United States and Asia clearly remain the leaders on the supercomputer market, France, with its BullSequana machine created by ATOS and operated by CEA (French Alternative Energies and Atomic Energy Commission), is ranked 16th worldwide (data from November 2018). Its (optimised) electrical consumption is 4MW, which is equivalent to the maximum power of an offshore wind turbine. The Chinese Taihulight machine consumes 15MW, which makes for an annual electricity bill of approximately €22 million (2017 data).

(*15*) Comparison between actual development of transistor density in computer processors (red line) and Moore's law's predictions since the 1970s (blue line: the green line shows the initial predictions, which have since been readjusted):



Adapted from: By Original uploaded by QcRef87 to French Wikipedia. — Transferred from fr.wikipedia to Commons by Bloody-libu using CommonsHelper., CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=16066564

(*16*) For instance, Microsoft is betting on quantum computing using the "Majorana fermion", an approach known as "topological quantum computing" and described by the team led by Michael Freedman (winner of the 1986 Fields Medal). The existence of this particle, thought to be its own antiparticle, was posited by the physicist E. Majorana, but has not yet been definitely detected. However, if it were to be discovered, it would allow the development of the most reliable and powerful quantum computer on the market today. https://experiences.microsoft.fr/technique/intelligence-artificielle-ia-technique/informatique-quantique-pari-fou/

(17) https://www.morganstanley.com/ideas/quantum-computing

(*18*) FET: Future and emerging technologies - http://www.horizon2020.gouv.fr/cid123504/1er-appel-du-fet-flagship-sur-les-technologies-quantiques.html

(19) http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf

(20) Turkey, Israel, and Switzerland.

(21) With, unsurprisingly, Germany, the United Kingdom, Italy, and Spain.
http://www.cnrs.fr/fr/premiers-laureats-pour-linitiative-europeenne-sur-les-technologies-quantiques

(22)

Country (EU)	Amount (millions of euros)	Country (Non-EU)	Amount (millions of euros)
Germany	650	China	~2,000
United Kingdom	450	United States	1,000
Netherlands	150		

National plans for public financing of quantum technologies in Europe and worldwide

(23) https://qutech.nl/

(24) https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-scientifique/veille-scientifique-et-technologique/chine/article/lancement-du-premier-satellite-a-communication-quantique-quess

(25) https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-scientifique/veille-scientifique-et-technologique/etats-unis/article/national-quantum-initiative-act-le-retour-des-etats-unis-dans-la-course-aux

(26) https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-scientifique/veille-scientifique-et-technologique/royaume-uni/article/financement-de-la-recherche-en-technologie-quantique

(27) http://www.cea.fr/presse/Pages/actualites-communiques/sciences-de-la-matiere/Un-ERC-Synergy-Grant-pour-la-recherche-grenobloise-sur-les-technologies-quantiques-.aspx

(28) http://www.sirteq.org

(29) https://www.quantonation.com/fr/

(30) Quantonation has already invested in France, particularly in LightOn and Pasqal, the very first national start-up focused on creating a quantum computer, based on cutting-edge French laser-based atom cooling technology.

(31) https://www-03.ibm.com/press/fr/fr/pressrelease/54572.wss This project aims to create a network of businesses, public organisations, and both research and higher education institutes using IBM quantum resources available in the cloud.

(32) https://www.muquans.com/

(33) A gravimeter is a measuring instrument designed to quantify the Earth's gravitational field.

(34) http://quandela.com/

(35) Photons are said to be "indiscernible" when they are considered identical from all points of view.