FEBRUARY 2020

Cigref
SUCCEED
WITH DIGITAL

Quantum Computing

Understanding quantum computing to prepare for the unexpected

Editorial

Just a few years ago, quantum computing was a utopian dream. Today, however, it is beginning to take root in people's minds. It promises to replace the law of Gordon Moore, a cofounder of Intel who predicted that computing capacity would double every year...up to the physical limit of the atom.

Atoms are the starting point of quantum computing, which uses nanometric (10^{-9}) resources to solve problems that current computers cannot tackle.

The fields of application for quantum computing range from encryption, metrology, optimisation, simulation, data analysis and artificial intelligence, using a future 'universal quantum computer'. Led by several key players like Google, IBM, Microsoft and Atos, the emerging quantum computing ecosystem also includes many start-ups (primarily in North America but in France as well) and is growing.

While companies are currently undergoing profound transformations to prepare for and adapt to unexpected technological developments, they cannot ignore the quantum revolution that will undoubtedly shake up IT: first sequential, then parallel, computing will become 'co-occurrent'[1] and impact programming, algorithms, applications and computer security, resulting in new use cases.

Companies must prepare for this major technological breakthrough, the first tangible effects of which are expected within 5 to 10 years.[2]

This breakthrough will translate into new ways of thinking, new ways of working and new tools and skills that remain unknown at present. The use cases waiting to be invented will certainly change companies' business models and organisations which must be transformed, once again, to adapt.

Jean-Michel ANDRÉ
CIO of Groupe SEB, Leader of the Cigref working group

[1] If a co-occurrence is the simultaneous appearance of two or more elements or classes of elements linked together, generally in a speech. It is then possible to imagine a stack of two or more instructions or classes of functions linked together, derived from a quantum programming language and whose simultaneous execution would result in a 'quantum' program.

[2] This is a short span of time in terms of perception: remember that Gmail, the first cloud-based email system, was launched in 2005, 15 years ago.

Acknowledgements

We would like to thank Jean-Michel ANDRÉ, CIO of Groupe SEB, who steered this study, as well as all those who participated and contributed to this Cigref working group:

Nicolas BOUVIER – EIFFAGE
Blaise BRIGAUD – AIR FRANCE KLM
Eric GOUNOT – DASSAULT AVIATION
Samuel HOLLER – RENAULT
Paul LAJOIE-MAZENC – EDF
Bernard LOISEAU – GROUPE SEB
Mohamed MARFOUK – LVMH
Emmanuel MONZIES – GROUPE PSA
Nicolas PERRIN – BANQUE DE FRANCE
Marc PORCHERON – EDF
Sophie POURCHET – FONDATION DE FRANCE

We would also like to thank the speakers whose input guided our thinking:

- Mehdi BOZZO-REY – Global Offering Manager, IBM Q startups
- Philippe DULUC – Technical Director, Big Data & Security, Atos
- Olivier EZRATTY – Consultant, author and speaker
- Olivier HESS – IBM Q Hub France Leader, IBM Q Ambassador
- Sarah LAMOUDI – Technology Strategist and Advisor (AI, blockchain, Quantum and Fintech)
- Alain SARLETTE – Senior Researcher at INRIA's QUANTIC Lab
- Sébastien TANZILLI – Research Director at CNRS, Head of the Quantum Photonics and Information team at INPHYNI (*Institut de Physique de Nice*)

This document was written by Frédéric LAU, Cigref Mission Director, with help from Jean-Michel ANDRÉ, CIO of Groupe SEB, and other work participants.

Table of contents

Table of figures

1. Why be interested now?

Innovation is often based on existing technologies, or technologies whose foundations are, if not mastered, at least understandable.

Quantum computing is not one of these technologies.

It is hard to understand and calls into question existing principles of logic and computing. The technologies it uses are still in the research stage and do not come from electronics, an engineering science, but from principles of quantum mechanics, a physical science, applied to information theory.[3] These technologies are still in the research and development stage, and none has really proven its superiority over the others.

Their rapid evolution allows us to do things that were impossible just a few years ago. Even though real progress is difficult to measure, the number of quantum projects is increasing, and the levels of performance are progressing. One of the first revolutions allowed us to apply quantum properties to everyday objects like lasers or electronic structures. For example, these technologies have allowed components to be miniaturized to the nanometric level (10^{-9}). Today, we are at the dawn of a new revolution in quantum particle measurements and control.

Quantum computing will not replace classical computing. It will supplement it in a certain number of fields: encryption, metrology, simulation and computation. Also, the fulfilment of the promises of quantum computing will have a certain impact on companies' information systems and, beyond that, on their business models. We are going from a utopia into the real world, and this will not happen without disruptions:

- Technology: the tools used will be very different from those of classical computing.
- Business: the promises (power, algorithms, security) will certainly change many companies' business models and processes.
- Human resources: the skills required of quantum computer scientists will not be those currently taught.
- Cultural: we don't think about quantum like we think about computing.

Thus, we perceive that quantum computing will transform the company's culture, companies' information systems and how they are used, and the skills of IT teams. Companies need to be ready to transform themselves (in terms of understanding, skills and culture) the day when quantum computing will finally become effective and operational.

[3] Shannon's information theory: https://en.wikipedia.org/wiki/Information_theory

Access to cloud-hosted quantum computers allows us to experiment with hybrid algorithms that mix classical and quantum computing. Thus, it will be important to identify the cases where quantum computing can be applied in a useful way.

Quantum computing is a continuation of the virtualization of IT infrastructure that is currently developing. The global information architecture may not be changed, but the problems that IT can solve will be on a very different level. For example, we could run optimisation algorithms through a quantum cloud. And, in 10-15 years, complex problems should be able to be solved by occasionally calling on online quantum machines.

The organisation of internal processes could also be disrupted: for example, the computing time of statistical elements related to big data could be reduced, requiring companies to react much faster. This would result in a remodelling of business processes that could be made shorter, with an impact on the teams concerned.

In the same way as with artificial intelligence or big data, technologies that developed very quickly and which required swift proficiency, quantum computing will require new skills that will certainly be less computational than scientific, but still closer to those of an engineer than a physicist. However, given the field's complexity, it is also possible that high level languages will be developed to "smooth" this complexity (but this will not happen immediately), or that the truly quantum part will be outsourced to cloud-based providers, thus avoiding the need for the company to develop extremely specialized and hard-to-acquire skills.

As for artificial intelligence and big data, we will also need to raise awareness of quantum computing among audiences who, while not being experts in the field, will have to use quantum applications. So, not only will we need to raise awareness among, inform, and/or train technical audiences, but also business audiences so that they are aware of what it is possible, or impossible, to do and where the added value can be found, especially business value. We need to help them understand the quantum philosophy more than how it works or how powerful it is.

Quantum computing will not allow us to solve anything and everything in any which way. Above all, it will require us to think differently!

We need to demystify this expected major change right now so that executives can understand it. And so, to help companies prepare for the unexpected aspects of quantum computing, Cigref created a working group on the issue.

The studies of this working group, led by Jean-Michel André, CIO of Groupe SEB, seek to raise awareness and popularise the principles of quantum computing so that we can understand the reach of its promises, stakes and opportunities. And allow companies to anticipate, project themselves, and invest without delay for the future.

2. An accelerating movement

Here, we are not going to detail the history of quantum computing.[4] But if we want to move out of a utopian dream, it nevertheless seems necessary to demonstrate the historical bases that underlie quantum technologies and the moments that helped them to progress and to be aware of the acceleration that has occurred in the last 10 years.

Quantum computing began at the start of the 20th century with the initial work on the quantas theory began by German physicist Max Plank in 1900. This theory made the connection between classical physics and quantum physics. In 1925, the principles of quantum mechanics were developed by Albert Einstein, Niels Bohr, Louis de Broglie, Werner Heisenberg and many other scientists.

1935

In 1935, Albert Einstein and two other physicists, Boris Podolsky and Nathan Rosen, published an article that described a 'thought experiment' to demonstrate that quantum mechanics as defined at the time was incomplete. In summary, the theory explained that if we produced an electron and a positron[5] entangled in an experiment, the measurement of one of the electron's properties is immediately transferred to the positron, which 'knows it immediately', even if it is millions of kilometres away. Einstein speculated that, given that this quantum principle violated the principles of locality[6] and reality[7] and that nature should, hypothetically, be realistic and local, quantum mechanics must be incomplete. This is the EPR[8] (Einstein-Podolsky-Rosen) paradox.

For Einstein, this 'faster-than-light' transmission of information was unacceptable: there must be hidden variables that 'gave the impression' of immediate communication.

1964

In 1964, Northern Irish physicist John Bell proposed the principle of an experiment that would solve this problem. It formalises the question through so-called Bell inequalities[9] which are evaluated during the experiment. If the inequality is not respected, then the result of the experiment cannot be explained by the existence of hidden variables, and we must admit the non-local quality of nature that Einstein refused. The state of the technologies at the time only allowed this experiment to be

[4] For this, read the entire report from Olivier Ezratty (in French): https://www.oezratty.net/wordpress/2018/ebook-pour-comprendre-informatique-quantique/

[5] Positron: an antiparticle with a positive electrical charge associated with the electron, which has negative electrical charge.

[6] Locality: the principle according to which distant objects cannot have a direct influence on each other.

[7] Reality: for a physical property to be real, it only must be possible to predict it with certainty without disturbing the system.

[8] https://en.wikipedia.org/wiki/EPR_paradox

[9] Bell inequalities are the relationships that measurements of entangled states must respect assuming a local deterministic theory with hidden variables.

conducted in the 1980s. French scientist Alain Aspect[10] performed it and showed that Bell's inequalities are indeed violated, confirming the non-local quality of quantum physics, that quantum mechanics were indeed complete and that, consequently, one of Einstein's base hypotheses was false. With this experiment, Alain Aspect demonstrated that the entanglement phenomenon that Albert Einstein theorised, but did not believe, was valid. Later in this document[11], we will see that entanglement is one of the basic elements of quantum computing.

1981

The 1980s were important in the world of quantum computing. In 1981, the first MIT (Massachusetts Institute of Technology) conference was held on this subject. This conference assembled many renowned scientists and physicists and gave birth to the idea of encoding information in the quantum states of matter.

1 Freeman Dyson
2 Gregory Chaitin
3 James Crutchfield
4 Norman Packard
5 Panos Ligomenides
6 Jerome Rothstein
7 Carl Hewitt
8 Norman Hardy
9 Edward Fredkin
10 Tom Toffoli
11 Rolf Landauer
12 John Wheeler
13 Frederick Kantor
14 David Leinweber
15 Konrad Zuse
16 Bernard Zeigler
17 Carl Adam Petri
18 Anatol Holt
19 Roland Vollmar
20 Hans Bremerman
21 Donald Greenspan
22 Markus Buettiker
23 Otto Floberth
24 Robert Lewis
25 Robert Suaya
26 Stan Kugell
27 Bill Gosper
28 Lutz Priese
39 Madhu Gupta
30 Paul Benioff
31 Hans Moravec
32 Ian Richards
33 Marian Pour-El
34 Danny Hillis
35 Arthur Burks
36 John Cocke
37 George Michaels
38 Richard Feynman
39 Laurie Lingham
40 Thiagarajan
41 ?
42 Gerard Vichniac
43 Leonid Levin
44 Lev Levitin
45 Peter Gacs
46 Dan Greenberger

Figure 1: Physics of Computation Conference - Endicott House MIT - May 6-8, 1981

During the conference, American physicist Richard Feynman (winner of the 1965 Nobel prize in physics) was the first to see the potential of quantum computers. Since classical computers (Turing machines) were not powerful enough to simulate quantum phenomena, he suggested, in a quote that became famous, using quantum simulators, which were simpler and easier to control, to study other quantum systems.

It was the first time that someone had imagined a quantum computer, or at least a simulation of it! From then on, work sped up.

> *"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"*
>
> Richard Feynman - 1981

[10] http://www.cnrs.fr/fr/personne/alain-aspect (in French)
[11] See chapter 5.1.Three basic quantum principles

1984

In 1984, Charles H. Bennett of IBM Research, who had helped to develop quantum computing theory in the 70s, and Gilles Brassard of the University of Montreal, proposed the first quantum encryption protocol: BB84, a mechanism for exchanging quantum keys.

1993

In 1993, an international group of six scientists including Charles H. Bennet confirmed the intuitions of a majority of science fiction authors by demonstrating that perfect teleportation is possible *in principle*, but only if the original is destroyed (which could be a problem!).

1995

In 1995, Peter Shor, an applied mathematics researcher at MIT, demonstrated that quantum computing with qubits allows for an algorithm able to factor any integer into two prime numbers in record time (a few dozen seconds).[12] In theory—in practice is another matter—it is possible to break the secret codes not only of banks, but governments and armies, using Shor's algorithm.[13]

Quantum computing then began to interest people beyond the scientific world, since we understood that information system security could be under threat. Very soon, we started to see new actors get involved from outside the science field.

1996

In 1996, David DiVicenzo, a researcher at IBM, identified the first criteria of a quantum processor:

- the qubits must be integrable and feasible in great numbers,
- it must have universal quantum gates able to perform any kind of algorithm,
- it must be reliably readable in one go,
- each qubit must be able to be initialised to 0 efficiently.

The same year, IBM presented the first 2-qubit quantum computer.

1997

However, quantum computers are extremely fragile because many errors appear in the computations due to 'quantum decoherence'.[14] An error-correction mechanism is essential. In 1997 Alexei Kitaev, a Russian-American physics professor at the California Institute of Technology and researcher at Microsoft, had the idea of taking inspiration from topology, a branch of mathematics that studies objects and their properties when they are subjected to deformations, to suggest a solution to this problem.

[12] In comparison, in 2012, an algorithm running for a year on 425 classical 4-core computers factored a number coded with 768 bits (a record that has yet to be beaten!).
[13] https://interstices.info/lalgorithme-quantique-de-shor/ (in French)
[14] See chapter 5.2. Qubits: the basic unit of quantum computing

2001

In 2001, IBM researchers factored the number 15 using Shor's algorithm on their quantum machine.

2011

In 2011, new players came onto the scene, mainly from the digital technology sector, accelerating everything once again. In 2011, California company D-Wave presented the first 128-qubit quantum computer.

2012

In 2012, two physicists, David Wineland and Serge Haroche, received the Nobel prize in physics for their work on controlling and measuring atoms. The former successfully controlled the quantum state of ions using photons, and the latter studied the quantum decoherence phenomenon by successfully measuring the information of a quantum system without destroying it.

The quantum decoherence phenomenon was a problem: the longer this time is, the greater the number of quantum logic gates that can be executed.[15] But if this time is not long enough to execute all of an algorithm's operations, there is no point. This barrier fell the same year (2012) when IBM successfully executed quantum algorithms in a complete manner.

2015

In 2015, it was demonstrated that error-correction algorithms are functional and can be used.

2016

In 2016, Microsoft announced that quantum computing had become a strategic priority. IBM made the first quantum computer available on a public cloud. To date, more than 100,000 people have used it, and over 140 articles have been published using work done on this machine.

2017

In 2017, ATOS brought the ATOS QLM (Quantum Learning Machine) to the market, simulating 30 qubits. Rigetti began producing silicon wafers for quantum computing, and Intel announced the manufacture of a 17-qubit quantum computing circuit. IBM successfully simulated the molecular structure of beryllium hydride (BeH_2) and reached the theoretical threshold of quantum supremacy with a 50-qubit computer.

2018

In 2018, Intel revealed its 49-qubit computer, then Google unveiled Bristlecone, a 72-qubit quantum processor, while Atos showcased a 41-qubit version of ATOS QLM.

[15] A logic gate, whether quantum or electronic, is the basic component of an elementary electronic or quantum circuit. In electronics, these gates are built using several suitably connected transistors; in quantum technology, they operate on a small number of qubits.

2019

In 2019 at the CES in Las Vegas, IBM revealed the first 'compact' 20-qubit computer called IBM Q System One. In October 2019, Google announced having achieved quantum supremacy, although the results were controversial.

2020

At the 2020 CES, IBM announced that a new machine with 28 qubits called 'Raleigh' was online.

The utopian dream period is over: the real world is taking over, and all the key players in digital technology who see their ecosystem threatened by quantum computing are entering the ring.

3. The challenges of quantum computing

3.1. Technological challenges

Today, there are no companies that are not setting up computers or means of computing and communication based on technologies that use computing algorithms. These technologies, now referred to as digital, follow a sequential computing logic with increasing parallelism, which has helped to considerably reduce computation and processing time over the last fifty years. The increased computing power and miniaturisation of components also contributed heavily.

Nevertheless, despite new algorithms and technologies such as artificial intelligence, it is becoming increasingly complex to go faster. The technology is reaching physical limits that, it seems, cannot be circumvented.

INCREASING COMPUTING POWER

Quantum computing promises to break through this limit: instead of 'unfurling' instructions and processes to reach a solution, even if it requires exploring all the possibilities, we can envision simultaneously processing all the instructions, exploring all the facets of a problem at the same time and give the solution all at once in the end. This is the key promise of quantum computing: provide a result in record time where a classical computer would take several days, months, or years.

> In 1997, IBM's computer Deep Blue, the computer that beat a chess grandmaster, Garry Kasparov, for the first time, examined 200 million possible moves per second. With a quantum machine, it could have been capable of calculating several billion moves in one second.

A comparison of the number of bits and qubits[16] for modelling molecules:

- A water molecule (H_2O): 10^4 bits, but just 14 qubits.
- A caffeine molecule ($C_8H_{10}NO_2$): 10^{48} bits, but just 160 qubits.
- A penicillin molecule ($C_{16}H_{18}N_2NaO_4S$): 10^{86} bits, but just 286 qubits.

Source: IBM Q

Quantum computers can solve problems that would be impossible with classical computers. Of course, they will not replace classical computers, which are better at common tasks (office processing, emails, etc.), but they will be perfect for solving problems that require significant computing power. For example, optimising the journey time for transporters or scheduling flights, encryption and decryption, searching among big data sources, or modelling various materials or molecules.

APPLICATION APPROACHES

Today, important research programmes are studying what it is possible to do in terms of applications by exploiting the properties of entanglement, non-locality and superposition[17] that are specific to quantum systems. These works target four major fields: metrology, communication, simulation, and universal computers.

In **metrology**, the science of measurement, this is a true revolution in having results that are statistically reliable. Even though the information carried by a qubit is very sensitive to environmental disturbances, the work being carried out allows us to build very sensitive sensors. Today, several concrete projects are under development for very specialised applications like the LIGO gravitational wave detector, inertial measurement unit, etc. The key players in this field are Thalès, the Paris Observatory, the NIST[18] as well as many start-ups.

In **communications**, the quantum correlations between entangled particles allow a message to be encrypted, guaranteeing it will not be intercepted during transmission. One key player today is ID Quantic (in Geneva, Switzerland) which offers to send information protected by quantum keys over distances of around 100 km. China, the University of Delft, and the Experimental Physics Institute at the University of Innsbruck are working on reliable quantum node networks, including by satellite. Paris Saclay University is also working on 'quantum repeaters' to counter losses over the line.

Today, we can use classical computers to imitate a part of a quantum system that we know how it works. We call this a quantum **simulator**.[19] This type of tool does not allow us to simulate the entirety of quantum logic; we have to finely target what we want to simulate ('we have to ask the right question

[16] See chapter 5.2. Qubits: the basic unit of quantum computing
[17] See chapter 5.1.Three basic quantum principles
[18] NIST: National Institute of Standards and Technology
[19] See chapter 5.3. The main types of quantum computers

that the simulation will answer'). For example, a simulation can help us imagine improvements to optimisation algorithms. Some simulation methods are now considered mature (such as the Quantic Monte Carlo method[20]) and could represent a path that combines precision, error control and computing power as a function of the system's size. But, despite some interesting successes, the limits of these solutions mean they are still marginal. The players present in this field today are D-Wave, Google in electronic circuits, Atos, and Bull for classical simulations as well as major corporations and many academic researchers.

The last field of application concerns **universal quantum computers**.[21] This is the equivalent of a Turing machine[22], but quantum. It operates as a classical computer with discrete error correction strategies, and the result is probabilistic. It is an approach that allows us to focus only on certain aspects: the basic operations. The more we increase the number of basic operations, the more we increase precision. The increase in computation speed compared to classical computers is proven for certain computations such as integer factorisation, searching for NP[23] solutions or solving sparse linear systems (big data and machine learning). But the switch from classical computing to quantum computing will not systematically result in improvements. Furthermore, we will need extremely powerful electronics since problems multiply as we multiply the number of qubits. Currently, we see 99%[24] precision in small systems (from 5 to 10 qubits), and to reach an efficient scale, research is focusing on scalable error correction strategies, efficient control architectures for large systems and 'quantum compilation' optimization. The players are IBM, Microsoft, Intel, Google, and all the major universities in the world as well as a few big start-ups (for example, Rigetti[25]).

[20] Http://www.lcpq.ups-tlse.fr/spip.php?article591 (in French)
[21] See chapter 5.3. The main types of quantum computers
[22] https://en.wikipedia.org/wiki/Turing_machine
[23] https://en.wikipedia.org/wiki/Computational_complexity_theory)
[24] Remember, classical systems (computations based on bits) are 100% precise: they do not make errors.
[25] Https://www.itforbusiness.fr/thematiques/cloud-computing/item/10668-un-cloud-quantique-a-destination-des-entreprises (in French)

REACHING THE 'QUANTUM ADVANTAGE'

Quantum computers are still very fragile: the qubits that perform these feats are not yet stable enough, whatever the technologies used.[26] These same technologies are very diverse and have yet to demonstrate a clear competitive advantage that would allow us to choose one over another. This leads to the second technological challenge: once a technology will be able to produce a sufficient number of stable qubits without error (we estimate that a thousand qubits are needed for a tool to be useful) and an algorithm can be executed completely and repeatedly in a variety of contexts, speed will increase. So, while Moore's law, in its commonly-held meaning[27], predicted growth that was 'just' exponential (power increases by a factor of 2; it doubles each time: 2, 4, 8, 16, etc.), Neven's law[28] predicts 'doubly' exponential growth (the power increases by a power of a power of 2 each time: 2, 16, 256, 65536, etc.).

It is this very fast acceleration that allows the scientific community to say that, in 5 years, a team will emerge with a specific algorithm and use case that will demonstrate what we call a 'quantum advantage'.[29]

> *'By 2023, 20% of organisations will be budgeting for quantum computing projects compared to less than 1% today'*
>
> Brian Burke,
> Chief of research, Gartner
> Sept 2019 - Gartner Symposium/ITxpo

Right now, we are entering the phase that IBM calls 'quantum advantage'. In 2017, IBM already successfully simulated the molecular structure of beryllium hydride (BeH_2) and reached the theoretical threshold of quantum supremacy with a 50-qubit computer. More recently in October 2019, Google announced in an article in the journal Nature[30] having reached quantum supremacy with a quantum computer of its own design that successfully performed a computation in 3 minutes and 20 seconds that would have taken the largest computers currently in existence 10,000 years. IBM put this achievement into perspective by demonstrating that it was possible to arrive at the same result in 2.5 days by using an alternative technique on a classical computer. Nevertheless, it is a quantum achievement.

[26] See chapter 5.4. Mature technologies and those still in the research stage

[27] Initially, Moore's law predicted that the number of transistors on a chip would double (miniaturisation) every 18 months. More recently, this law has been commonly taken to mean that a computer's processing power would double over the same period.

[28] Harmut Neven is the director of the Quantum Artificial Intelligence lab, a joint initiative of NASA, the Universities Space Research Association and Google Research. QAILab's objective is to advance research into the way in which quantum computing could help machine learning.

[29] Some people talk about 'quantum supremacy', which is the supposed capability of a quantum computer to perform computations that a classical (super)computer cannot do. Achieving this would shift us into a whole other dimension that is currently inaccessible.

[30] *Quantum supremacy using a programmable superconducting processor* – Nature, 23 October 2019 https://www.nature.com/articles/s41586-019-1666-5

WHAT ALGORITHMS FOR QUANTUM COMPUTING?

This last example on Google's achievement and IBM's reaction is very interesting because it raises the issue of knowing which algorithms will be used on quantum machines. There is no reason to replace classical computing if the gains are not sufficient or if we can obtain the same results in an 'acceptable' timeframe using a classical method.

In public and private research labs right now, we know how to create quantum systems that are capable of making computations, but the issue that arises is knowing which type of computations are pertinent to quantum computers, because you cannot take a classical algorithm and transform it into quantum.

Given that there is no technology that is really operational and stable, the complex algorithms that could be applied to quantum computing have not yet been implemented. Nevertheless, there are several waiting to be experimented. We can classify them into four major families of algorithms[31]:

- **Search algorithms** to look for information in complex or large data sources or structures,
- **Algorithms based on quantum Fourier transforms**, which are considerably important in mathematics and encryption,
- **Algorithms related to complex systems** such as neural network training, optimal pathfinding in networks, or process optimisation,
- **Algorithms for simulating physical quantum systems** used to simulate interactions between atoms in various organic and inorganic molecular structures.

Encryption meets quantum

Shor's algorithm is the most spectacular illustration of quantum computing: its purpose is to solve the problem of factoring large numbers into its prime factors. Public-key encryption is based on this factoring problem to generate RSA encryption keys. With today's algorithms and supercomputers, we are capable of factoring numbers with around 250 digits, but beyond 500 digits, it becomes impossible. On the other hand, the more digits a key has, the longer it takes to crack by breaking it down into prime numbers. So, while several hundreds of classical computers working in tandem would take one billion years to decompose a 2048-bit key, a quantum computer would just need a hundred seconds.

[31] Olivier Ezratty's classification (in French) - https://www.oezratty.net/wordpress/2018/comprendre-informatique-quantique-algorithmes-et-applications/

3.2. Strategic challenges

According to the report 'Quantum Computing Market & Technologies - 2018-2024'[32] published by Industry 4.0 Market Research[33], which produced reports on the economic impact of existing or emerging technologies, the global market for quantum computing will grow by 24.6% per year. During the 2019 World Government Summit[34], a forum for discussions among executives, government officials and experts, it was announced[35] that the global market for quantum computing will quadruple between 2023 and 2027, with investment in software and services related to quantum computing growing from 2 to 8 billion dollars.

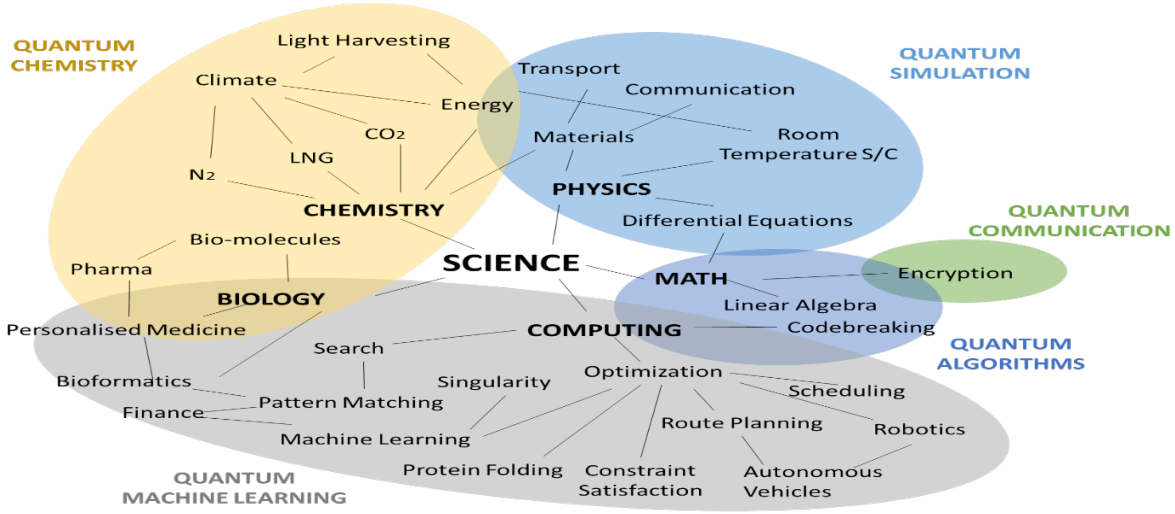

Figure 2: *Quantum Computing will transform almost every aspect of our technology, science, economy & life*
Source – World Economic Forum, HSRC[36]

Beyond industry, quantum computing has the potential to change the balance of power in intelligence, military affairs, and strategic balances. Companies and governments are preparing, because, given the assumption that the first applications will arrive within 5 to 10 years, it's practically tomorrow!

The key question is no longer whether there will be a quantum computer, but who will build it and who will profit from it. And the key challenge concerns the control of this technology, because it places communications and data storage security in danger. It has become a challenge to sovereignty.

FRANCE

In April 2019 in France, the Prime Minister tasked MP Paula Forteza with a mission on quantum technologies. Based on this report, the objective is to develop a French strategy on quantum

[32] https://industry40marketresearch.com/product/quantum-computing-market-technologies/
[33] https://industry40marketresearch.com/
[34] https://www.worldgovernmentsummit.org/
[35] https://www.pwc.com/m1/en/world-government-summit/documents/wgs-quantum-leap.pdf
[36] HSRC: Human Sciences Research Council

computing. This report,[37] 'Quantum: the technological revolution that France will not miss - 37 proposals for an ambitious national strategy' presented on 9 January 2020, proposes investing 1.4 billion euros over five years in this field, creating training courses with a quantum specialisation, and developing three clusters of excellence in Paris, Saclay and Grenoble with multi-disciplinary institutes in quantum computing.

Today, France is a leader in quantum technologies in Europe, with 18% of its start-ups and 17% of investment funding.[38] To build off this position, Paula Forteza proposes in her report to strengthen it by supporting, with Bpifrance, around fifty start-ups until 2024 and creating an investment fund of 300 to 500 million euros dedicated to quantum start-ups. Currently, there is Quantonation[39], which invests in all the components of quantum computing, and *Génération DeepTech*[40], supported by Bpifrance, which tackles the great challenges of the 21st century.

ANSSI[41] which reports to the Prime Minister, has also started to work on these questions. In its 2018 annual report, ANSSI highlighted that 'technologies such as artificial intelligence, connected health and quantum computing will change how security is done'. According to Paula Forteza, 'ANSSI has started to work on these issues, for example announcing that, starting in 2020, it will no longer certify encryption technologies that are not "quantic resistant".'[42]

EUROPE

In Europe, the Quantum Manifesto, signed by more than 3,000 players in the field, including 156 European companies and 20 research institutes, drove the creation of the European Quantum Technology scheme in 2016, taking inspiration from the FET (Future and Emerging Technology) Flagships[43]. Currently, within this framework several Member States and national financing agencies have launched the QuantERA FET Flagship project to support European research in the field of quantum technologies and invest one billion euros in hundreds of projects over 10 years.

UNITED STATES

In the United States, quantum computing has become a strategic asset. In 2018, the National Science & Technology Council produced a report[44] on the economic, scientific, strategic and military stakes. A

[37] https://forteza.fr/wp-content/uploads/2020/01/A5_Rapport-quantique-public-BD.pdf (in French)
[38] Source Wavestone: https://www.wavestone.com/app/uploads/2019/10/Quantum-Computing-WavestoneFrance-Digitale-EN-web-2019.pdf
[39] https://www.quantonation.com/
[40] https://www.bpifrance.fr/A-la-une/Dossiers/Generation-Deeptech-le-futur-de-l-innovation (in French)
[41] ANSSI: The French National Agency for Information System Security
[42] Le Monde Informatique, 10 June 2019: https://www.lemondeinformatique.fr/actualites/lire-paula-forteza-deputee-des-francais-de-l-etranger--en-termes-de-souverainete-c-est-une-necessite-de-maitriser-le-quantique-75546.html (in French)
[43] The FET Flagships are projects of more than one billion euros that bring together public and/or private players. https://qt.eu/
[44] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf

few months later, the National Quantum Initiative Act[45] came into force, allocating 1.2 billion dollars to research into quantum information systems. This law asked the DOE[46], the NSF[47] and the NIST[48] to support research and training in quantum technologies and to expand and facilitate projects of collaboration or consortia with other public- or private-sector players, including industry, universities and federal laboratories. This initiative is steered by a committee of the NSCT[49] dedicated to quantum computing that includes representatives from the NIST, the NSF, the DOE as well as NASA, the Department of Defense, the ODNI[50] and the White House Office of Management and Budget and the Office of Science and Technology Policy.

To protect the electronic and information systems that American federal organisations use from future quantum tools that can crack encryption, the NIST also launched a project in 2016 to evaluate the algorithms in use. The objective is to have the entire US administration using post-quantum, or quantic resistant, algorithms in 2024. By 2018, 69 algorithms had already been evaluated.

CHINA

China is also investing heavily in quantum computing. On 3 May 2017, Xinhua, the official news agency of the People's Republic of China, announced that Chinese scientists had built the first quantum computer, and they set a record in 2018 for entanglement with an 18-qubit quantum system.[51] Several experiments have also been announced, including one about transmission by satellite using quantum encryption as protection. China is also implementing a widescale quantum communication network.

RUSSIA

There is one last international player who communicates little today: Russia. Nevertheless, an article[52] published on 16 October 2019 on the website IOPScience[53] by a group of Russian scientists gave a detailed description of the players and state of Russian research into quantum technologies.

Quantum technologies are strategic and part of a national scheme to develop the Russian digital economy, the Digital Economy National Program, with an overall amount of 25 billion euros and in which the budget dedicated to quantum technologies should reach one billion euros. Work is supported by government organisations and Russian businesses (Rosatom, Rostech, Bank of Russia, Rostelecom, Gazprombank, Sberbank, etc.).

[45] https://www.aip.org/fyi/2019/national-quantum-initiative-signed-law
[46] DOE: Department of Energy
[47] NSF: National Science Foundation
[48] NIST: National Institute of Standards and Technology
[49] NSTC: National Science and Technology Council
[50] ODNI: Office of the Director of National Intelligence
[51] Scientific American: https://www.scientificamerican.com/article/chinese-researchers-achieve-stunning-quantum-entanglement-record/
[52] https://iopscience.iop.org/article/10.1088/2058-9565/ab4472/pdf
[53] https://iopscience.iop.org

In addition to the existing renowned scientific centres, several research centres were created recently between 2010 and 2018: the Russian Quantum Center (2010), The Kazan Quantum Center (2014), theNTI[54] Quantum Technologies Centre[55] (2017) et NTI Center for Quantum Communications[56] (2018).

The main objective of the Russian roadmap is to build a complete range of technologies for quantum computing. Among the work, we can cite the demonstration of operations of quantum logic gates at one and two qubits with a demonstrated reliability of 95% and the demonstration of a quantum computing and simulation platform with 50 qubits. In encryption, a Quantum Key Distribution system was tested on 32-km optical lines in urban conditions, demonstrating the functional applicability. Russian expertise has also heavily contributed to the work on the LIGO gravitational-wave detector.

3.3. Business challenges

In October 2018[57], an article published by IBM demonstrated that, with the quantum processors available and in spite of their imperfections (noise, low precision, etc.), a quantum advantage was possible. Which meant that it was possible to imagine what we could do once quantum computers became sufficiently powerful and precise. This excited not only the scientific community, but the business community as well!

The business and manufacturing sectors' fast-growing interest in quantum computing is real. Three or four years ago, there was not much in terms of achievements. But we are starting to see that, over the past two years, there is a real, growing appetite from manufacturers and start-ups who are working very seriously on it. On the one hand, we can explain this acceleration because an increasing number of major companies is taking up algorithms. Another reason is that the slightest innovation, improvement or optimisation (be it technical, software, physical, etc.) causes a jump in performance, and some players, in Canada especially where a consequential ecosystem of start-ups in this field has developed, are specialising in a particular issue to improve it by developing a few lines of code, algorithms, etc. Finally, companies have an increasing ability to work on complex issues in partnership with research organisations, as was the case with artificial intelligence (AI).

Even though they are still in the experimental stage, many companies are actively looking for what quantum computing can bring to their R&D, designing and operating their future products and related services and, *in fine*, their net profits.

The applications of quantum computing that seem possible concern molecular modelling (or quantum chemistry), financial optimisation and modelling, securing communications with Quantum Key Distribution (encryption) and activities related to AI and deep learning. Here are some examples.

[54] NTI: National Technological Initiative
[55] At the M.V. Lomonosov Moscow State University (QTC MSU)
[56] At the National University of Science and Technology MISiS
[57] https://www.ibm.com/blogs/research/2018/10/quantum-advantage-2/

OPTIMISATION

Daimler is working IBM and Google, similar to how Volkswagen is working with Google and D-Wave Systems, to see how quantum computers could help to solve problems in optimising vehicles' delivery itineraries or the flow of parts in factories.

Both carmakers are also studying what quantum computing can bring to the development of better batteries by simulating the structures and chemical reactions inside batteries to help improve electric vehicles.

In 2011, aerospace giant Lockheed Martin was the first to buy a quantum computer manufactured by D-Wave systems and continued to study how this technology could be used for applications related to air traffic management and optimisation and systems verification. Also in aeronautics, Airbus is also studying how quantum computing could contribute to and speed up its research activities. For this, Airbus has invested in the quantum computing software company QC Ware.[58]

In the financial sector, JPMorgan is working with IBM to explore how quantum computers can contribute to trading strategies, stock portfolio optimisation, asset evaluation and risk analysis. Similarly, Barclays is participating in the IBM Q network to determine if quantum computers could be used to optimise payment for big batches of financial transactions.

MOLECULAR STRUCTURE MODELLING

Simulating, *in silico* and in an exact way, how big molecules are structured and function has definite benefits for the pharmaceutical industry or agricultural science. In this field, Accenture Labs, biotech innovator Biogen, and the quantum software company 1QBit[59] are studying ways to speed up the discovery of medicines by using quantum computers to make molecular comparisons. In September 2017, IBM simulated the structure of a beryllium hydride molecule with three atoms. In October 2017, Google and Rigetti also announced OpenFermion, a chemical simulation software, on a quantum computer.

COMMUNICATIONS

Securing communications is a major concern not only for governments but also for businesses. All sectors are concerned since data is at the heart of most organisations. Quantum encryption is among the most mature fields (France is even very well-placed concerning theories and experiments).

As early as 2006, a quantum encryption experiment was conducted to transmit information about the football World Cup. The same year, several Japanese manufacturers, Mitsubishi Electric Corporation, NEC Corporation, the Institute of Industrial Science and the University of Tokyo set up quantum encryption to interconnect with each other. In 2007, the Swiss canton of Geneva partnered with the University of Geneva (UNIGE) to experiment with securing the link between ballot counting locations

[58] https://qcware.com/
[59] https://1qbit.com/

and the data centre with quantum encryption. In 2008, SECOQC[60] demonstrated the very first computer network using a functional Quantum Key Distribution (QKD) technology.

In May 2019, an experiment[61] in cooperation with Orange was launched in the Nice Côte d'Azur region to secure communications by exchanging quantum keys between the Nice Institute of Physics, based on the Valrose campus and the INRIA Sophia Antipolis centre (30 km away), and with IMREDD[62] in the Plaine du Var area as a source of data entanglement.

For communications, the real challenge is to be able to use quantum encryption over very long distances. On this topic, Toshiba's Cambridge Research Laboratory explained in a publication[63] in May 2018 that is possible to extend the reach of communications encrypted in such a way to 500 kilometres over standard fibres. For example, this could securely connect cities such as London, Paris, Dublin, Manchester and Amsterdam.

MACHINE LEARNING

In mid-2018, TERATEC[64] and a group of manufacturers launched a special initiative on quantum, with a focus on France and Europe, TQCI (Teratec Quantum Computing Initiative). The starting core brought together TERATEC, Total, EDF, Dassault Aviation, ATOS, the CEA and CERFACS[65], and was quickly expanded.

In this context, work is conducted on participants' feedback on the use of quantum technologies for machine learning applications. A project is being developed to design algorithms specific to quantum computing in the major fields of application, to identify and experiment with industrial use cases, and to train and guide the user community.

HIGH PERFORMANCE COMPUTING (HPC)

France has a strong position in both the technology and use cases. Remarkable progress has been made recently in the technologies and the emulation techniques. Quantum technology is a very important theme for high performance computing and for security technologies, making it one of the key strategic fields of the future. Now is the time to advance! Manufacturers, users, and technology suppliers are ready to participate in an ambitious program of actions in which TERATEC and its partners will play a key role.

[60] Development of a Global Network for Secure Communication based on Quantum Cryptography: http://www.secoqc.net/

[61] https://inphyni.cnrs.fr/contenus-riches/actualites/fr/universite-cote-d2019azur-et-orange-collaborent-pour-la-mise-en-place-d2019une-experimentation-en-matiere-de-cryptographie-quantique/@@highlight_view (in French)

[62] IMREDD: *Institut Méditerranéen du Risque de l'Environnement et du Développement Durable*: https://imredd.fr/

[63] https://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Press/Toshiba-Redefines-the-Limit-of-Intercity-Secure-Communications/

[64] http://www.teratec.eu

[65] CERFACS: *Centre Européen de Recherche et de Formation Avancée en Calcul Scientifique*: https://cerfacs.fr/

Quantum will also be included in 2020 in the major European programme EuroHPC[66], in which TERATEC is a participant.

3.4. Training challenges

During the meetings held by the Cigref working group, several participants drew our attention to the weakness of the training in quantum computing in France.

As we wrote before, quantum computing is more a science of physicists than engineers. But engineers are essential to designing and manufacturing products.

If we assume that the first industrial applications will appear in 5 to 10 years, that means that by 2030 we will need to train many students, or at least raise their awareness, in quantum technology, because we cannot think about 'quantum' as we do about 'computer science'. It is less about training future quantum physicists than it is about future quantum computer scientists.

Many universities, led by academic research into quantum physics, have implemented a variety of initiatives. Côte d'Azur University, the first French university to experiment with a quantum network, is training and raising awareness among students. The University of Montpellier, with support from the Occitanie/Pyrénées-Méditerranée region, has partnered with IBM to create training modules on quantum computing. Paris Saclay University also offers master's degrees and PhDs in quantum physics and, interestingly, is a partner of an engineering course at Centrale Supélec. ISAE-Sup Aero offers training in quantum engineering and ultimate miniaturisation. Paul Sabatier University and Toulouse INSA are also developing their courses in quantum technology using the University School of Research (EUR) Some applied computer science programmes, MIAGE, particularly in Evry, are also looking into it. There are also manufacturing chairs, such as those from Atos and CEA[67], which was founded in May 2018.

But most other higher education institutions, particularly computer engineering schools, have not included quantum technologies in their courses, even though it is a field that will impact, even transform, companies' future information systems as digital technologies have done today. We can, however, point out Télécom Paris, which has developed a three-year course in the basic elements of quantum mechanics, from encryption to quantum communications, computing and algorithms. As well as Ecole Polytechnique, which also offers a specialised master's degree in 'Physics and Applications' in quantum systems.

There is a lack of training in the subject, with the risk that companies will not have control over the technologies used or not understand their reach due to a lack of skills.

[66] https://eurohpc-ju.europa.eu/

[67] http://www.cea.fr/presse/Pages/actualites-communiques/sciences-de-la-matiere/atos-cea-anr-chaire-industrielle-informatique-quantique.aspx (in French)

Nevertheless in general, while the US government is asking various national agencies and players to support and invest in research AND training with the National Quantum Initiative Act, we can only hope that the future French quantum plan will follow the proposals in Paula Forteza's report and take this problem into consideration by organising the development of training courses for the future quantum computer scientists that we will need.

4. Excitement in the quantum ecosystem

Despite a technology readiness level (TLR) that is still low, many companies are showing a certain interest for and investing in quantum research.

And, while it seemed difficult just a few years ago, quantum physics researchers are now partnering with technology giants and big companies. Start-up ecosystems are also developing very quickly (in France, Canada, etc.).

All of these players have the ambition, of course, of successfully transferring research from the laboratory to manufacturing in business.

4.1. The key players

Given the business interest, the world's biggest companies and many government agencies are working on quantum technologies and software. The main players are Alibaba, Atos, D-Wave, Google, IBM, Intel, IonQ, Microsoft, Quantum Circuits, and Rigetti. Many of these companies also work in collaboration with large university research teams, and all of them continue to see significant progress.

ALIBABA

In July 2015, Alibaba, the Chinese web giant, partnered with the Chinese Academy of Sciences to found the 'Alibaba Quantum Computing Laboratory'[68] whose mission is to undertake cutting-edge research into the most promising systems to create practical applications in quantum computing.

Alibaba, like IBM, has made an experimental quantum computer available online. More specifically, in March 2018 the Chinese e-commerce giant opened up an 11-qubit quantum computer on the Chinese cloud, developed in collaboration with the Chinese Academy of Sciences, which allows users to run quantum programs and download the results.

[68] https://damo.alibaba.com/labs/quantum

ATOS

Atos is one of Europe's leaders in the quantum ecosystem. Atos launched Atos Quantum[69], an industrial quantum computing programme, in 2016 with a scientific council made up of many great quantum physicists[70]. Their approach differs from that of other players: working on the premise that it is not the hardware but the software and applications developed that make digital technology successful today, Atos developed a platform for programming quantum algorithms, Atos QLM, in 2017.[71] It is a monofunctional server (*Appliance*) that simulates any kind of quantum computer (30 to 40 qubits) and is equipped with a development environment (Atos myQLM). Today, Atos QLM's users include the US Department of Energy as well as Total and Zapata Computing Inc.[72]

Atos also has an R&D programme with multiple partners involved in multiple European projects such as the AQTION project[73] to provide a 50- to 100-qubit trapped-ion quantum accelerator by 2023 and the PASQuans[74] project to create quantum simulation platforms of up to 500 qubits.

D-WAVE

D-Wave[75] is a Canadian-based pure-play quantum computing pioneer that demonstrated a 16-qubit quantum machine in 2007. In 2011, D-Wave sold D-Wave One, a 128-qubit quantum system, to Lockheed Martin. Then, in 2013, Nasa and Google acquired a 512-qubit machine (the D-Wave Two). In 2015, D-Wave supposedly passed the threshold of 1,000 qubits with the D-Wave 2X and sold the D-Wave 2000Q (2,000 qubits) in 2017 to cybersecurity company Temporal Defense Systems. In September 2019, D-Wave announced a 5,000-qubit quantum computer.[76]

D-Wave is currently the only company to have sold a quantum computer system. However, machines from D-Wave, which communicates very little, are controversial in part due to the technology chosen (quantum annealing[77]) and in part because they seem to only do what they were designed to do, more like quantum 'automata' than quantum 'computers'. Nevertheless, Google's announcement in October 2019 that they had reached quantum supremacy is based on a D-Wave machine and is a demonstration of their know-how.

D-Wave markets the D-Wave Ocean Software suite, a set of tools for developing applications.

[69] https://atos.net/en/insights-and-innovation/quantum-computing/atos-quantum
[70] https://atos.net/en/2017/press-release/general-press-releases_2017_11_23/atos-quantum-programme-scientific-council-celebrates-major-developments-achieved-last-year
[71] Atos QLM: Atos Quantum Learning Machine
[72] An American company specialised in quantum algorithms
[73] AQTION: Advanced Quantum computing with Trapped IONs
[74] PASQuanS: Programmable Atomic Large-Scale Quantum Simulation
[75] https://www.dwavesys.com/
[76] https://siliconangle.com/2019/09/24/d-wave-debuts-new-5000-qubit-quantum-computer/
[77] https://www.frenchweb.fr/comprendre-linformatique-quantique-adiabatique/335616 (in French)

D-Wave, like Alibaba and IBM, also set up a cloud-based quantum application development environment called Leap in 2018. Leap allows users to access a quantum computer like the D-Wave 2000Q in real time.

GOOGLE

Google is working flat out to make quantum computing a reality through its AI Quantum Laboratory[78]. Google began its adventures in quantum computing using D-Wave machines. But Google quickly developed its own hardware and announced a 72-qubit quantum processor called 'Bristlecone' in March 2018.

In June 2019, Hartmut Neven, Director of Google's Quantum Artificial Intelligence Lab, stated 'Neven's law' which suggested that Google could reach the point of supremacy by the end of 2019. Indeed, in October 2019, an article in Nature[79] stated that it may just have been reached. The achievement was nevertheless contested by several players, including IBM.[80]

Google, like IBM, thinks that it is possible to see the first tangible, marketable results in the coming five years.

IBM

IBM has been working on quantum computers for more than 35 years now. In 2016, IBM made a 5-qubit and then a 16-qubit quantum computer available to the public on the cloud. Meanwhile, to help those wanting to learn and develop, IBM offers the open-source Qiskit framework.

In 2017, IBM created IBM Q Network[81] which brings together a global community of companies, start-ups, academic institutions and leading national research laboratories to drive quantum computing and explore use cases.

In January 2019, IBM unveiled IBM Q System One, an offer for businesses based on a compact, modular quantum computer intended for use outside research laboratories.

INTEL

As the world's leading producer of microprocessors, Intel is, of course, working to develop quantum computing processors.[82] Intel has decided to follow two separate research approaches. The first, in collaboration with the Dutch quantum computing pioneer QuTech[83], led to the creation of a 17-qubit trial chip. In January 2018 at the Las Vegas CES, Intel announced the delivery of a 49-qubit trial quantum processer called 'Tangle Lake'.

[78] https://ai.google/research/teams/applied-science/quantum/
[79] https://www.nature.com/articles/s41586-019-1666-5
[80] To understand Google's achievement (in French): https://www.youtube.com/watch?v=KaRd_eB2qOA
[81] https://www.ibm.com/quantum-computing/
[82] Https://www.intel.fr/content/www/fr/fr/research/quantum-computing.html (in French)
[83] https://qutech.nl/

Intel's second research approach is internal to the company. It seeks to create processors based on 'spin qubit' technology using Intel's tried-and-true traditional methods for making silicon chips. In June 2018, Intel stated that tests for a 26-spin-qubit chip had started. The quest for mastering the miniaturisation of qubits (spin qubits are 50 nanometres in diameter) allows Intel to envision the manufacture of minuscule quantum processors with thousands or millions of qubits within the next 10 years. Nevertheless, this technology raises doubts over its short-term feasibility, and Intel does not expect a market launch to be possible before 2025.

IONQ

IonQ[84] is also a pure player in quantum computing. The technology it uses is based on 'trapped ions'. Its objective is a scalable quantum computer that can support a variety of applications in many industrial sectors.

In November 2019, IonQ announced the creation of Azure Quantum in partnership with Microsoft. Its purpose it to make IonQ's computers available on Microsoft's cloud computing network.

MICROSOFT

Microsoft has been working on quantum computing[85] since 1997 with Alexei Kitaev, a Russian-American professor of physics at the California Institute of Technology and researcher at Microsoft, who takes inspiration from topology to design a solution to correct qubit errors.

Microsoft's strategy is to develop quantum computers based on topological qubits whose commercial applications seem easier to envision given that they are less subject to errors. According to an article published in Computer Weekly in May 2018[86], Todd Holmdahl, Microsoft's Corporate Vice President for Quantum, estimated that we could see commercial quantum computers on Azure in just five years.

Microsoft also works with several universities around the world where 'Q station'[87] laboratories have been created. In February 2019, Microsoft also announced the Microsoft Quantum Network to bring together many players to develop a 'quantum economy'.

Microsoft, like IBM and Atos, is interested in coding and made available a free online quantum computing development kit in December 2017. This kit includes a programming language called Q#[88] as well as a quantum computing simulator.

[84] https://ionq.com/
[85] https://www.microsoft.com/en-us/quantum/
[86] https://www.computerweekly.com/news/252440763/Microsoft-predicts-five-year-wait-for-quantum-computing-in-Azure
[87] https://news.microsoft.com/stories/stationq/
[88] https://docs.microsoft.com/en-us/quantum/language/?view=qsharp-preview

QUANTUM CIRCUITS

Quantum Circuits[89] is a start-up founded by Robert Schoelkopf, a professor in quantum computing, and his colleagues at Yale University. The company raised 18 million dollars with the ambition of overtaking computing giants in the race to manufacture an operational quantum computer.

RIGETTI

Start-up Rigetti is another pure player in quantum computing. This manufacturer of quantum chips brought a 19-qubit quantum processor (the 19Q) online in its development environment called Forest. In 2017, Rigetti demonstrated with its 19Q that it was possible to significantly advance artificial intelligence by being capable of performing an unsupervised machine learning task.

In 2018, Rigetti, like several of its competitors, put its hybrid quantum computing platform QCS in the cloud.[90] It also launched a million-dollar contest to demonstrate quantum advantage on its QCS platform.

Rigetti is currently working on developing a new 128-qubit chip planned for 2020.

TERATEC

TERATEC[91] is a European skills centre created by CEA and industry users to harness and promote digital technologies (supercomputers, simulation, data analytics, machine learning, AI, etc.) in association with scientific research and technology suppliers, large and small, in co-design mode.

Today, TERATEC represents 80 members with a campus in the Essonne area where more than 250 people work and has a major recognized position in Europe.

4.2. Public players in France

Many public players and French universities are involved in the race towards quantum expertise. In terms of location, these players are mainly located in 4 regions: Ile-de-France, Occitanie, Provence-Alpes-Côte d'Azur and Auvergne-Rhône-Alpes.

In the Ile-de-France region, the **Paris Saclay Quantum Cluster**[92] (led by Pascale Senellart[93] of CNRS), together with the **Paris Saclay University**, brings together some forty research teams working on quantum technologies. The university has also set up several partnerships with **Thalès**, **Atos**, **EDF**, **IBM** and **Air Liquide**.

[89] https://quantumcircuits.com/
[90] QCS: Quantum Cloud Services
[91] http://www.teratec.eu/
[92] https://www.universite-paris-saclay.fr/en/research/spotlights/quantum-centre-en-sciences-et-technologies-quantiques/nanotechnologies-and
[93] https://www.universite-paris-saclay.fr/en/news/pascale-senellart-mardon-cutting-edge-second-quantum-revolution

INRIA[94] is also a major player in quantum computing in Ile-de-France. With its **QUANTIC** team[95], INRIA seeks to develop methods and experimental systems that ensure robust processing of quantum information. This work is carried out in collaboration with the **Kastler-Brossel Laboratory** of **ENS** (École Normale Supérieure), **Yale University**, **CEA**, etc.

In the Occitanie region, the quantum field involves a dozen or so **laboratories in Montpellier and Toulouse** working with **CNRS**. Research here is essentially focused on quantum sensors and communications. **IBM** created the first Q Hub in France in cooperation with the **University of Montpellier**.

In Provence-Alpes-Côte d'Azur, with **CNRS**, the **Nice Institute of Physics** (INPHYNI) of **Côte d'Azur University** has developed a research centre on quantum and wave physics. The university is working with **Orange** to set up an experiment in quantum cryptography.

In Auvergne-Rhône-Alpes, **CEA** and **CNRS** are also leading quantum research through several laboratories such as **LETI**[96], **IRIG**[97] and **Institut Néel**.[98]

5. An explanation to help understand quantum

Without going into mathematical formulas that are hard to understand for the uninitiated, here are some elements that will help you to at least be aware of the spirit of quantum physics.

5.1. Three basic quantum principles

Quantum mechanics is based on several rather counter-intuitive principles which, put together, allow it to solve problems much faster than a classical algorithm: the principle of uncertainty (or indeterminacy), the quantum superposition of states and the entanglement phenomenon.

THE UNCERTAINTY (OR INDETERMINACY) PRINCIPLE

At a human scale, nature is deterministic: at a moment **T1**, we can determine an object's position and speed in nature and be able to calculate what its state will be at a moment **T2**.

A quantum system, on the other hand, is nondeterministic. Particles can be represented by either a wave or a wave packet. However, we cannot determine both a particle's speed and its position: if we

[94] *Institut national de recherche en informatique et en automatique*
[95] https://team.inria.fr/quantic/
[96] LETI: *Laboratoire d'électronique et de technologie de l'information*: http://www.leti-cea.com/cea-tech/leti/english
[97] IRIG: *Institut de Recherche Interdisciplinaire de Grenoble*: http://www.cea.fr/drf/irig/english
[98] http://neel.cnrs.fr/?lang=en

represent it as a wave, we can know its speed, but not its position. If we represent it as a wave packet, we can identify the packet's position, but not its speed.

Since its position and speed cannot be measured at the same time in a quantum system, we consider that an object can be 'in several places at the same time' or that it has no location as long as the position is not measured. This is the uncertainty, or indeterminacy principle.

> To understand this principle, let's imagine that there is an object that is travelling very fast in a chamber that is completely dark, and we need to take a photo of the object with a flash. Since we don't know where it is, we shoot at random. However, on the photos, either the image is sharp and we can see where the object is, but not its speed, or the image is blurry, and we can no longer see where the object is, but we can calculate its speed by following the length of the object's trail. Thus, it is not possible to know both where the object is and the speed at which it is travelling at the same time. We only have partial information.

THE QUANTUM SUPERPOSITION OF STATES

Classical physics is equipped with a whole set of mathematical equations which allow us to determine an object's state: its position, its speed, its weight, etc. In relation to a given moment, we can measure the characteristics of this object precisely without disturbing it. Observation does not modify its state. Thus, if you know the mass of an object and the force of gravity, you can easily calculate its weight at a given moment.

In the quantum world, we cannot determine these values for particles. But we can approach them probabilistically. For example, a particle can be at X% in a particular state, Y% in another, and Z% in a third, and the number of states can be infinite. In a certain way, a particle can be *more or less* in an 'infinity' of different states 'at the same time'. Describing a quantum system shows several states that coexist at the same time. This is the principle of the superposition of states.

When we take a measurement, we get a probabilistic result. And if we take the same measurement over n identical particles, it is the convergence of each of their probabilistic results that give us an acceptable result.

> To understand this principle, let's imagine a carpenter[99] who wants to take a piece of wood and craft a guitar, a chair, or any other object they might imagine. The possibilities are infinite. They exist, but as potentialities: there is a probability, according to various factors (the market, customers,

[99] An example inspired by the article (in French) https://www.gbnews.ch/ordinateur-quantique-2-le-principe-de-superposition/

humidity, type of wood, etc.), that the carpenter will make one object, or another, or a yet another. The piece of wood itself superposes all of these possibilities. But once the piece of wood has been worked, only one object is created, and all the other possibilities of creation disappear.
If we repeat the process n times, the convergence of objects made can allow us to say that this carpenter is specialised in making guitars, chairs, or some other object.

THE ENTANGLEMENT PHENOMENON

This third principle of quantum mechanics indicates that it is possible to create a linked system composed of several particles whose states depend on each other, regardless of the distance between them (this is what Albert Einstein did not want to believe).

In this linked system, each particle's behaviour is not individual: they behave collectively. Measuring data on one of the system's particles immediately affects the others, wherever they are. We say that these particles are entangled; this is the principle of entanglement.

Once the information carried by one of the system's particles is known (measured), it is set on (or passed to) all the other particles in the system, and we can no longer change it.

To understand this principle, let's imagine that we cut a shirt into two halves (left and right). We blindly place each half of the shirt into one of two different boxes. These two boxes are sent to two different places, New York and Tokyo, for example. Once it arrives in Tokyo, the box is opened, containing the left half of the shirt. We instantly know that the right half is in New York, even without opening the box in New York. The information about New York is 'instantly propagated' to Tokyo. Similarly, our contact in Tokyo, without opening their box, could call their contact in New York and ask them to open their box: the New York contact, by observing the content within, can immediately transfer the information about the box in Tokyo without Tokyo having to open it. So, there is a sort of immediate link between the two boxes concerning the information about their content, a sort of implicit collaboration between the two boxes.

5.2. Qubits: the basic unit of quantum computing

BITS VS. QUBITS / DETERMINISM VS. PROBABILISM

As everyone knows, bits are the basic unit for storing data in classical computing. Generally, this corresponds to creating an electric charge that expresses the flow of current, either possible or not. If the current flows, the bit is 1; if the current does not, the bit is 0. So when reading a bit, there can be

one of two values: 0 or 1. This reading is deterministic: if we repeat it several times, we will always obtain the same result.

In quantum computing, the basic unit of data storage is the qubit. We can represent a qubit's state by a point on a sphere (which we call the Bloch sphere[93]). This sphere covers the states that a particle can have: base or excited. Let's imagine that the sphere's 'north pole' is its base state (written|0>), and its 'south pole' is its excited state (written|1>). Between the two, there is an infinite number of possible points: a qubit can therefore have as many quantum states as there are points on a sphere. It can be 'more or less' 0 AND 'more or less' 1; in other words, it can be both in state 0 and in state 1 but in proportions that are variable. Reading it is probabilistic.

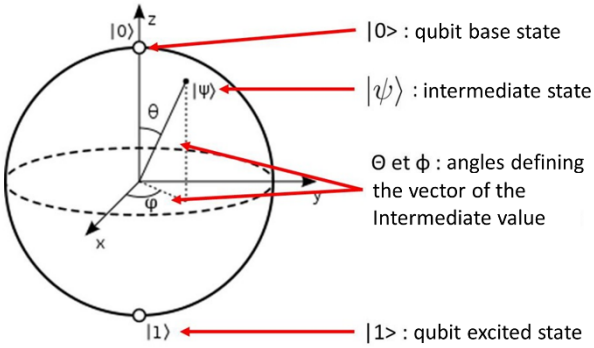

Figure 3: A Bloch sphere

All these intermediary states are represented by what we call vectors.[100] Between the moment when the qubit is initialised at 0 and the final moment when we read its output value (0 or 1), the information can be handled through what can take an infinity of superposed states. In the end, when we read the qubit's value, we get either a 0 or a 1 but with a probabilistic feedback that depends on the parameters of the qubit state's vector. Therefore, the qubit's mathematical value comes into play during, and only during, processing. Not at the start nor at the end of processing

So, while a classical computer will run N combinations or instructions sequentially and will only provide a result at the end of the chain of instructions, a qubit's superposition of states gives us a system with 2^N simultaneous combinations that will produce an immediate solution when it is measured, providing unleashed computing power.

The entanglement principle allows several qubits to be synchronised in two different places or to make copies. And if we take a measurement on one, such as reading the information it carries, all the entangled qubits are affected immediately.

ERRORS, NOISE, AND QUANTUM DECOHERENCE

The technologies implemented in classical computers are currently sufficiently powerful to create data, send it, copy it, regenerate it, store it, etc. Of course, classical electronic components produce errors, but today, with very few resources (memory, CPU), it is possible to correct them to achieve a 100% reliability rate.

We are not there yet with quantum technologies. They are extremely sensitive to interactions with their environment (what we call 'noise'), and qubits tend to lose their quantum states very quickly

[100] https://www.frenchweb.fr/comprendre-linformatique-quantique-qubits/330991 (in French)

(superposition of states, entanglement, etc.). This is what we call decoherence. And, if decoherence intervenes before the end of a quantum algorithm's run, this makes it essentially unusable.

There are several strategies to try to solve this problem:

- Either execute error correction codes. But these themselves require qubits to run. In the end, this implies being able to create and maintain coherence among a significant number of qubits (those that run the algorithm and those that correct errors), and it is currently difficult to generate a consequential number of qubits (several hundred). This entails only being able to execute short algorithms that require little code.
- Or adjust the computers to the algorithms (depending on the technology used, the qubits are more or less sensitive to certain types of noise). But, in this case, the computer becomes dedicated to a type of algorithm which must nevertheless be optimised. Teams are currently working to implement a learning-based approach to translate a quantum circuit into an algorithmic equivalent that is extremely short and suitable for a specific quantum computer.

5.3. The main types of quantum computers

QUANTUM-INSPIRED ANALOGUE COMPUTERS

There are 'classical' systems that can use quantum effects to solve or emulate a specific problem. They have 'limited' programmability but are faster than computers that use conventional algorithms. However, one question remains: do these software simulations on non-quantum computers obtain the same results?

NOISY INTERMEDIATE-SCALE QUANTUM (NISQ) COMPUTERS

These are quantum systems that are not fault-tolerant. They are not precise enough, but they do demonstrate that it works, that the algorithms are valid. They are built to demonstrate useful applications by interacting with a classical information system, for example in chemistry or to perform optimisation. Today, many start-ups are working on this concept, in particular with hybrid quantum/classical algorithms. To be truly effective, they should have between 1,000 and 5,000 qubits.

FAULT-TOLERANT UNIVERSAL QUANTUM COMPUTERS

These computers are the holy grail in quantum computer science. They should be able to execute useful quantum algorithms and exponentially increase computing speed over classical algorithms. However, to implement a quantum error correction rate that is effective, these computers would need between 1 and 5 million qubits.

5.4. Mature technologies and those still in the research stage

Producing stable qubits is essential to being able to carry out operations and run algorithms in a complete manner. While the theory of quantum mechanics has been there since the early 20th century, the quantum technologies that produce the qubits that could be the basic building blocks of quantum computers are very recent and, above all, diverse. But, while these technologies can produce qubits in different ways, the approaches do not all have the same maturity, or involve constraints that impact their effectiveness or narrow their possible use cases.

SUPERCONDUCTING CIRCUITS

Technologies based on superconducting circuits seem to be the most advanced. They can create extremely fast qubits, and assembling them is just as fast. Nevertheless, the low coherence time and the significant qubit error rate are their main flaws. Furthermore, miniaturising a system is not easy, at least for the moment.

Among the pioneers, we can count the French researchers at the CEA who created the first superconducting qubit in 2002. To date, IBM, Intel, Google, Rigetti, D-Wave, INRIA and other players are working on superconducting circuits.

TRAPPED IONS

Technologies based on trapped ions (kept under vacuum and suspended by electrostatic suspension) are also extremely interesting for other reasons: the qubits they produce are of very good quality. Even if they are rather slow and exceeding one hundred qubits is complicated, they are significantly isolated from their environment, so the noise (which generates errors) is very low. Furthermore, they can be entangled in an effective way. Finally, using lasers, it is easy to prepare and measure entangled quantum superpositions made with a small number of ions. But the system is still hard to miniaturise.

There are no teams in France working on trapped ions. In the USA, the start-up IonQ from the University of Maryland is the key player working on this subject with the University of Innsbruck in Austria and its spin-off AQT. IonQ recently created 80 qubits stored in trapped ions and demonstrated quantum advantage.[101]

[101] See the paragraph 'Reaching the quantum advantage' in chapter 3.1. Technological challenges

ELECTRON SPIN SILICON QUBITS (OR QUANTUM DOTS OR CMOS, DEPENDING ON THE NAME)

This is the path chosen by Intel and CEA at Leti and in collaboration with CNRS. Several other players are following suit: Princeton University, UNSW in Australia, CEA-Leti and CNRS in France, and Quantum Motion Technologies in the UK.

NV CENTRES

This technology uses defects in diamond crystals. Qubits are difficult to manufacture in a reproducible way, and entanglement is difficult to implement. This is the path chosen by Quantum Diamond Technologies. The universities of Delft, Stuttgart, Harvard, Chicago and Hefi are working on this technology.

MAJORANA FERMIONS

These are topological qubits that use a singular type of particle, the Majorana fermion, both a particle and an antiparticle that possesses a quantum state intrinsically. While currently uncertain since the existence of Majorana particles has not yet been proven, this technology would have the benefit of being able to create very stable, resistant qubits, two key criteria for effective quantum computers. This is the path chosen by Microsoft and Bell Labs. The Universities of Delft, Maryland, California (Santa Barbara) and the Niels Bohr Institute are also working on this technology.

QUANTUM PHOTONICS

In the 1980s, Alain Aspect and his team demonstrated the reality of non-local quantum correlations using pairs of photons. This technology relies on the entanglement of photons, the keys to securing communications over long distances.

Quantum photonics is a very promising technology for quantum computing that allows us to overcome the problems of decoherence, perform computations at room temperature, and rely on techniques of classical optical technologies to create processors on a wide scale. Paris Saclay University as well as Côte d'Azur University with the INPHYNI are working on these optical quantum technologies.

Achieving digital success to help promote the economic growth and competitiveness of its members, who are major French companies and public administrations, and users of digital solutions and services

Cigref is a network of major French corporations and public administrations set up in order to develop its members' ability to acquire and master digital technology. It is a unifying player in the digital society, thanks to its high-quality thinking and the extent to which it represents its members. Cigref is a not-for-profit body in accordance with the French law of 1901, created in 1970.

To achieve its mission, Cigref counts on three business units, which make it unique.

1/ Belonging:
Cigref speaks with one voice on behalf of major French companies and public administrations on the subject of digital technology. Its members share their experiences of the use of technology in working groups in order to elicit best practices.

2/ Intelligence:
Cigref takes part in group discussions of the economic and societal issues raised by information technologies. Founded nearly 50 years ago, making it one of the oldest digital associations in France, it draws its legitimacy from both its history and its understanding of technical topics, giving it a solid platform of skills and know-how, the foundation stones of digital technology.

3/ Influence:
Cigref publicised, promotes and champions its member organisations' collective positions on digital technology issues. As an independent organisation in which digital technology practitioners and actors can discuss and create content, Cigref is a benchmark recognised by its ecosystem.

www.cigref.fr

21 av. de Messine, 75008 Paris
+33 1 56 59 70 00
cigref@cigref.fr