QUANTUM COMPUTING: READY FOR THE HUGE LEAP?

FRANCE DIGITALE

WAVESTONE

FRANCE DIGITALE

www.francedigitale.org

Founded in 2012, France Digitale is the largest startup association in Europe. France Digitale brings together the champions of digital entrepreneurship: it gathers 1400 digital startups with strong growth plans and more than 100 investors (venture capitalists and business angels).

The association (non-governmental organization) has a specific DNA, it associates entrepreneurs and investors to make the ecosystem more conducive to the emergence of new champions.

The Positive Way

WAVESTONE

www.wavestone.com

Today, knowing how to adapt and drive transformation are the keys to success. At Wavestone, we believe that a shared sense of enthusiasm is at the core of successful change. That's what we call "The Positive Way". "The Positive Way" is how we drive change in our clients, it's who we are and it's our commitment to creating a positive impact for all our stakeholders.

Wavestone has more than 3,000 employees in 8 countries. It is one of the leading independent consulting firms in Europe and the leading independent consulting firm in France.

Wavestone is listed on Euronext in Paris and is a Great Place To Work® listed company.

Quantum: the next frontier for startups?

What is going to be the next "buzzword" doing the rounds in our tech ecosystem? 2015 saw "big data", 2016 was flooded with mentions of "artificial intelligence", and in 2017 everybody was talking about "blockchain." Each of these breaking waves shared a key feature: to draw the attention of the general public and institutional investors to major technological advances.

Yet of all these tech waves, quantum computing might just prove to be the most powerful. At present, this breakthrough technology remains a relative unknown, concentrated in the hands of several big tech players, despite its apparently massive potential for application.

By increasing and accelerating computing capacity, quantum computers have the potential to transform many parts of tomorrow's economy—with banks, pharmaceuticals, and transport the first to be affected. Cryptography, artificial intelligence, and even the modeling of life forms will experience a technological acceleration.

Faced with the progress of American and Chinese giants, Europe needs a comprehensive "quantum strategy" to engage research institutes, scaleups, large groups, investors, and public authorities.

Quantum computing is too important a subject to be left just to engineers. It's time the life forces of the digital ecosystem seized it. This is the main mission of France Digitale, the leading association for startups in Europe. We hope this work will provide the foundations of a common framework.

Nicolas BRIEN
CEO France Digitale

SUMMARY

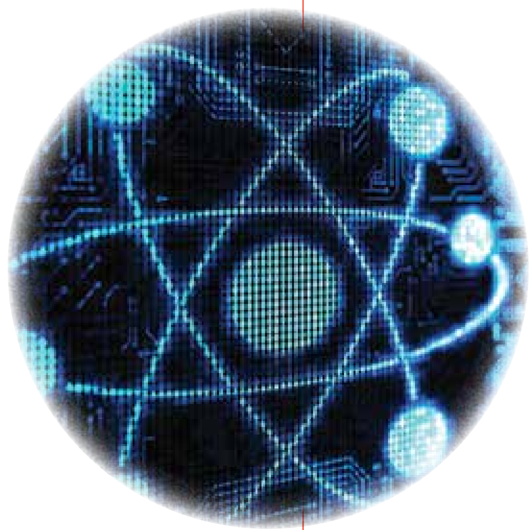
Our convictions on quantum

1

Quantum computing will be a source of progress in all sectors both finance and industry, it will then be a catalyst for research discoveries.

2

It poses a major risk to **cybersecurity**, threatening to render current encryption systems ineffective. But it is also a source of solutions to overcome this risk. It is also a source of solutions for securing our communications.



3

Europe has every interest in developing quantum technology in order to remain in the race, maintain its leadership, and mitigate critical risks (such as the outsourcing of R&D to the US or China, falling behind on productivity, and the inability to protect sensitive information such as classified documents or economic intelligence).

4

Europe needs a significant boost from **Member States** if it's to become a major global player: it needs to put in place a large-scale plan to stimulate investment, pursue training initiatives, and coordinate all its stakeholders more effectively.

5

France now occupies a prominent place (2nd) in the European quantum ecosystem: French **startups and manufacturers** must transform quantum technology into uses and immediately seize its opportunities; **investment funds** have a key role to play in seeing the emerging technologies take off.

What will the impact be on business sectors?

Quantum computing: ready for the huge leap?

Google announcing its quantum supremacy... IBM marketing its first quantum computer: this time, the big players are making big moves!

Since the middle of the last century, the race has been on to increase computing power. Computing problems are becoming increasingly complex: there are ever-greater volumes of data to exploit and organizations need to move faster to remain competitive.

Quantum computing promises to drive real progress in the area: Google claims it can reduce calculations that would take 10,000 years with a standard computer to a processing time of a few minutes.

But does it offer a miracle solution? And does quantum alone represent the future of computing? To better understand the coming revolution, and help you prepare for it effectively, in this document, we'll shed light on the issues, quantum's current and projected uses, its ecosystem, and the actions you need to take.

Quantum computers aren't just more powerful versions of conventional computers!

Before setting out on our analysis of this upcoming revolution, it's essential to be clear about the fundamental characteristic of a quantum computer: **its ability to process certain types of calculation in parallel and simultaneously**.

Quantum computers represent an entirely new model of computing, based on principles quite far removed from their traditional cousins—just as light bulbs and candles are only distant relations. In both cases, the overall objective is the same (to give light or perform calculations), but the technologies used, and the associated potential, have very little in common.

To summarize for now, the quantum properties used enable the same processor to calculate different problem "histories", whereas a traditional computer calculates them sequentially (or in parallel, but on multiple processors).

The time savings can be considerable... but only in certain cases: when the problem involves working through a large number of possible combinations!

Given this, there are **three major types of problem** that will benefit fully from advances in quantum computing: the simulation of complex systems, the optimization of large systems, and cybersecurity. These problems are found **in almost every sector of activity**, something that merits a rapid overview of the use cases envisaged, or even in use today.

> "The overall objective is the same, but the technologies used, and the associated potential, have very little in common"

The simulation of complex systems

By applying its powers to the infinitely small, the quantum computer is **an excellent tool to simulate how matter and life function**, as things that play out at precisely this scale; chemistry, physics, and biology, then, are prime areas to exploit the quantum's scope.

The facilitation of discoveries in these fields holds considerable promise—and rich rewards for humanity and certain industries:

/ Chemistry – Pharmaceuticals – Health

The computational power needed to design new molecules today is too large for current technology to cope with: quantum computing will make it possible to simulate complex structures and offer a concrete tool to design molecules with targeted properties (such as drugs, catalysts, proteins, enzymes, etc.) in a much more focused way than today.

In a similar way, it should also improve our understanding of parts of living organisms, such as the functioning of the brain.

/ Physics

Research laboratories in France and Europe spent billions of hours using supercomputers to solve complex equations—such as predictions about particle collisions and nuclear reactions. In the future, quantum computing will reduce calculation times and enable work on reactions that remain undiscovered today.

For example, it should provide a better understanding of the keys to creating superconductors that can operate at room temperature, something that could drastically reduce losses from national power grids, or increase the performance (and/or reduce the costs) of magnetic levitation trains (such as **Japan's Maglev**, which is scheduled to enter service in 2027).

Quantum computing alone can't make these applications a reality, but it will undoubtedly be an important catalyst. To date, the simulations possible with quantum computers have been limited to very simple systems (comprising a few atoms); much more powerful quantum computers will be needed to exploit the full potential.

The optimization of large systems

Leaving the atomic level, **large systems, composed of thousands or even millions of interacting parts**, are also good candidates for quantum computing: its ability to simultaneously process all possible "stories", and therefore avoid traditional "combinatorial explosions" in these types of areas, makes perfect sense—if the aim is **to rapidly identify optimal situations**. This concept can be applied to a wide range of areas:

/ Transport – Energy – Logistics

Logistics experts, such as energy specialists and transport operators, face a daily challenge to optimize numerous systems, without the option of being able to calculate the effects of all the possibilities (at least in an acceptable time). Examples are route planning, the management of fleets of vehicles or aircraft, the arrangement of containers in ports or on ships, the optimization of supply chains, the management of distribution networks (water, energy, etc.), and weather forecasting. Quantum computing should greatly improve and facilitate these optimization calculations.

For example, **Airbus launched its Quantum Computing Challenge** in early 2019, calling on the quantum community to help solve some of its strategic problems, the majority of which are optimization issues (wing shapes, aircraft loading, etc.).

/ Finance

Financial institutions also consume large amounts of computing power, especially to assess the risk exposure of their portfolios. This results in hundreds of thousands of daily transactions. By drastically reducing the calculation time for risk levels, quantum computing should further improve the performance of the algorithms that drive a growing proportion of today's transactions.

The financial sector, which combines a mature need and significant resources to invest, will almost certainly be at the forefront of quantum computing.

/ Marketing

Marketing departments face complex challenges, such as optimizing their marketing mix, advertising placements, or even predictive marketing. Quantum computing could accelerate the resolution of all these problems.

Cybersecurity

So far, we've been mostly talking about the opportunities offered by quantum computing: the areas where it could become a major lever of performance. But **quantum computing's power is not without its issues**: cybersecurity, vital to safeguarding the internet traffic that has become essential for modern societies, provides the best illustration.

/ Quantum computing as a major cyber risk...

One of the primary applications of a quantum computer is the decryption of the keys used to encrypt information: in doing so, it generates risk for communications, payment systems, the validation of financial transactions, and all blockchain applications—like bitcoin.

These keys are based on the fact that factorizing very large numbers as prime numbers is difficult, a problem that lies exactly within the core capabilities of a quantum computer; Shor's algorithm (1994) was specifically designed for this purpose.

However, it's not time to panic yet: this application won't be feasible for a good ten years given the complexity of current keys. It is, however, time to move to find solutions that could withstand this type of attack once it becomes trivial: research to define such post-quantum cryptography is underway, but as ever, the transition from theory to practice, with an acceptable level of standardization, will probably prove complicated.

/...but also as the ultimate solution!

But quantum physics also offers the definitive solution to securing exchanges: the sensitivity of particles to any observation makes it possible to detect, with absolute certainty, if information has been intercepted on the path between its transmitter and its receiver.

And the road to this solution may not be that long: China in particular has made strong progress in the area, having put in place a ground-space, quantum-communication link for its **satellite, Micius**, back in 2017.

These technologies will undoubtedly constitute one of the security bricks of tomorrow's internet and will strongly impact the telecommunications sector. The beginnings of this are already visible, via, for example, the Quantum ID solution, which, since early 2019, has played a part in 5G-network security for a South Korean mobile phone market leader (**SK Telecom**).

Artificial intelligence and quantum computing: a happy marriage?

Artificial intelligence (IA) has been the star of the computing world in recent years, thanks to the impressive nature of machine learning (or deep learning), but can it reach a new milestone using quantum computing?

A catalyst for acceleration

At first glance, and without a doubt, **AI is hungry for computing power. It often aims to solve optimization problems, making it an obvious candidate for quantum computing.**

Thanks to its combinatorial power, quantum computers should enable reduced learning and processing times for many AI applications. Some examples are:

/ Finance – Public Sector

One of AI's major applications today is detecting fraud and abnormal behaviors, a real weak spot for the financial sector and public-sector security departments: quantum computing should help to better and more quickly identify fraud-related patterns.

/ Automotive – Mobility

A combination of AI—to make vehicles autonomous, and quantum computing—to centrally optimize systems with thousands of parts, has huge potential here.

Some significant initiatives have been widely publicized: in 2017, **Volkswagen and D-Wave** demonstrated the benefits of the technology to optimize the use of 10,000 taxis in Beijing, and, in 2018, **Ford and NASA (again working with D-Wave)** used it to develop autonomous vehicles.

The impacts are sometimes less direct... but more quickly seen!

Quantum computing also means fundamentally revising the way algorithms are designed. This can be viewed negatively (because it forces us to learn new ways of doing things) but sometimes there can be benefits too.

For example, in 2018, Ewin Tang, a student at the University of Texas, improved a traditional machine learning algorithm to bring it up to the same level of performance as the quantum algorithm published in 2017. Compared with previous methods, this resulted in an exponential change in the efficiency of the calculations that make movie, book, and meeting recommendations.

Without calling into question quantum's potential, this anecdote highlights an interesting edge effect: current quantum algorithmic research can have positive short-term benefits.

A catalyst—certainly. But not a magic wand

Quantum computing is already driving the discovery of new algorithms and can contribute significantly to reducing the energy consumed in long-term AI learning. It will help to facilitate access to these technologies, and give a second wind to AI, by unlocking a new wave of development: intelligences based on quantum power.

Yet quantum computing is not a panacea, and it won't be able to address AI's current key weaknesses:

- / **Explaining** algorithms: the ability to explain AI decision-making is currently limited—and a source of mistrust for users.
- / Algorithmic **bias**: the systematic errors made by algorithms as a result of the data on which they were trained; and, more generally, the sensitivity of the algorithms to the data used to train them.

In short: quantum computing will affect almost all sectors

This brief overview demonstrates the **considerable potential for progress across a whole range of sectors:** today, who can honestly say that they're not facing any challenges related to resource optimization? For some sectors, the impacts are even greater. To name but one, pharmaceutical R&D could be completely transformed, resulting in large players making major strategic shifts that will gear them more toward organic growth based on in-house discoveries—and less focused on the targeted acquisitions that have become the norm in recent years.

The "big tent" of quantum technology also covers other innovations. To highlight just one, think about quantum metrology, which promises to create measuring devices (using time, position, gravity, underground soundings, etc.) that will be capable of unparalleled precision.

But this overview also raises undeniable risks, which need to be carefully monitored, especially when it comes to information security issues—a topic high on the agenda for today's organizations. On this point, major private-sector players can reasonably expect the market to offer them solutions that will address this new risk.

By now, we hope we've convinced you that it's worth understanding the subject in more depth... time to focus on quantum physics, the research labs that produce the qubits, and the trails being blazed in the race to quantum supremacy.

The fundamentals of quantum computing

A brief history of quantum computing

Moore's law, which empirically predicted a doubling of the computing processor power every 18 months, came into being in 1965. Up to this point, it had proved true, mostly as a result of the efforts to miniaturize the transistors used to build the processors. But, as a result of this need to miniaturize, by definition, physical limitations came into play: at very small scale (broadly the atomic level), quantum effects can no longer be ignored, something that completely disrupts operability.

Even though we're not there yet, the concept of the quantum computer originates from this observation, and especially the genius of physicist, Richard Feynman. In 1981, he explained he was convinced that there was **no need to give in to quantum effects: instead we should take advantage of them to move beyond the limits of conventional computers**.

From then on, research in the field has been increasing across all areas: hardware components, algorithms, languages, etc. In recent years, we've seen an acceleration in this technological revolution: quantum computers are being marketed and/or are accessible in the cloud (for example, those of D-Wave, Rigetti, and IBM); development environments are being used by communities (for example, LIQUi|> and Qiskit); and algorithms are being optimized for quantum computation (for example, the factorization of large integers into prime numbers, Shor; and the research algorithm, Grover).

The main milestones in quantum computing's development

- **1981** — **First basic model** of a quantum computer. "Traditional computers can't simulate the development of quantum systems in an efficient way." *R. Feynman*
- **1985** — **Theoretical description** of the functioning of a quantum computer and quantum gates. *D. Deutsch*
- **1994** — **Development of a quantum algorithm** to factorize large numbers. This exponentially outperforms the best traditional algorithms. *P. Shor*
- **1998** — **First experimental demonstration of a quantum algorithm** by a 2-Qbit quantum computer using Nuclear Magnetic Resonance (NMR). *Oxford University*
- **2000** — **First 5-Qbit NMR computer.** *Technical University of Munich*. Followed soon after by a **7-Qbit** machine. *Los Alamos National Laboratory*
- **2001** — **First demonstration of Shor's Algorithm** (factorization of the number 15). *IBM's Almaden research center*
- **2006** — **An operating standard** that allows the control of a **12-Qbit** machine. *Institute for Quantum Computing with input from the Institute for Theoretical Physics*
- **2011** — D-Wave One, **the first quantum computer available to purchase**. *D-Wave Systems*
- **2015** — Arrival of D-Wave's 2X, rated at **1,152-Qbits**. *D-Wave Systems*
- **2017**
  - Arrival of the D-Wave 2000Q, with **2048-Qbits**. Temporal Defense Systems is the first company to buy one. *D-Wave Systems*.
  - IBM unveils its 17-Qbit quantum computer.
  - Intel confirms the development of a 17-Qbit processor.
  - Google announces the creation of a 72-Qbit-processor, Bristlecone.
- **2019**
  - IBM unveils its **first commercial quantum computer**. *IBM Q System One*
  - Google announces that it has achieved **quantum supremacy**.

The fundamental principles: qubits and superposition

The basic building block: the qubit

As everyone knows, the basic building block of a conventional computer is the bit: with a value of 0 or 1 (depending on whether current is "passing" or not); by intelligently combining enough bits any information can be represented.

But in a quantum computer, there's a fundamental change: information is now stored in a qubit (a quantum bit), which has the astonishing property (a quantum property, obviously) of being able to take the values 0 or 1 (at the time when we measure it), with a certain probability. But as long as you don't measure it, its value is both 0 and 1: it exists in **several "superposed" states**.

We'll see later that a number of options are being studied to physically create qubits: atoms, electrons, and others. All sort of things become possible when you switch to the scale of quantum particles!

A key property: the superposition of states

The real "magic" of quantum computing comes into play when operations are performed on a qubit: because each operation is performed on the qubit's (two) different states.

But it's when we combine several qubits into a system that this concept gets interesting: the number of these superimposed states then increases very quickly. With 2 qubits we can operate on 4 states, with 10 on 1024 states, and over a million states are possible with 20 qubits: enough to consider a vast degree of parallelization.

The exponential (in its proper sense) capacity of a quantum computer is in play here, and this is how we can explain, in a few words and a necessarily simplified way, how a quantum computer calculates, in parallel and simultaneously, the different "histories" that we've discussed above.

Measuring a quantum computer's power

Reading press releases from the major players, **the measure of quantum computing power seems obvious: it's the number of qubits that counts**. **Google** was making announcements about 72 qubits in 2018, **IBM** about 53 qubits in 2019, while **D-Wave** is already marketing a computer rated at 2,048 qubits and is promising 5,000 soon.

But qubits alone aren't enough

The reality is more complex, because the **headline number of qubits is actually a poor representation of the power of a quantum computer**. That also depends on:

- / **Whether its nature is "universal"** or not: some quantum computers are designed to deal with certain types of problems only, so it's difficult to compare them with universal quantum machines (which are more complex to develop but have a broader scope of application);
- / **Its topology,** which describes how qubits are linked together.
- / **The number and variety of available operators** (the "quantum gates"), which offer unit operations (the equivalent of "and," "or," or "exclusive or," in traditional logic).

These last two characteristics, when cleverly combined, reduce the number of operations needed to perform a calculation.

The technology still needs to progress

Having said that, at present, the underlying technologies are still maturing, and so some of the intrinsic performance characteristics need to be considered; in particular:

- / **The error rate,** which measures the reliability of calculations: the lower it is, the greater the scope to link operations together and therefore perform complex calculations. The use of error-correcting codes can compensate for errors, but at the cost of reduced performance (as in conventional computing).
- / **The coherence time,** which defines the period when the qubit remains "coherent" or, to put it more simply, "exploitable": the longer this time is, the more operations, and therefore complex calculations, can be performed.

Two types of computers

	UNIVERSAL QUANTUM COMPUTER	QUANTUM ANNEALER
Description	With an ability to carry out any type of calculation, it can be used in all the areas mentioned above	Limited to certain types of computation, and slower than a universal quantum computer, it nevertheless works well for some AI-related applications (for example, autonomous vehicles)
The main players	Rigetti, IBM, IonQ, Alibaba, Google, Microsoft	D-Wave
Scale (number of qubits in 2019)	20-53	2,048

A key indicator: Quantum Volume

Announcements in the market are difficult to compare in the absence of all, or some of, the measures above, which makes it difficult to mark out the leaders in quantum technology.

However, IBM has been promoting an interesting measurement of power since 2017: Quantum Volume, which provides a single, aggregate measurement of the various characteristics mentioned. In homage to Moore and his famous law, IBM also aims to double the Quantum Volume of its computer every year.

The problem of technological standards

As with any maturing technology, there is the associated problem of standardization.

	STANDARDIZATION LEVEL
Qubit types	There is no consensus to date on how to physically create qubits. Each player is focusing on the topology it considers the most powerful and hoping it won't hit a glass ceiling. The most promising technologies seem to be those based on CMOS qubits (Intel), superconductors (Rigetti), trapped ions (IonQ), or cooled atoms (PasQal); and, so far, none of the routes has been abandoned.
Programming languages	Each manufacturer is developing its own programming language, compilers, machine languages, and development platforms. While quantum algorithms are widely shared, thanks to the Quantum Zoo initiative, which lists the algorithms developed for quantum computing, developers are faced with multiple choices when it comes to implementing them—all of which are related to the decisions made by manufacturers.

While there's a debate among researchers about quantum hardware, the software discussion is taking place in a different setting: here it's the developer teams that will have to understand this raft of languages and bring the applications to life. At this stage, it's hard to predict which framework will dominate, but don't doubt developers' ability to master a range of languages (just as they can master, today, a large number of conventional languages, provided they're based on common principles).

Will quantum computing replace traditional computing?

Quantum computers are not about to replace personal workstations. There are two reasons: their large size and their frequent need to be cooled to temperatures close to absolute zero (but who knows, new types of qubits might ease this constraint in the future).

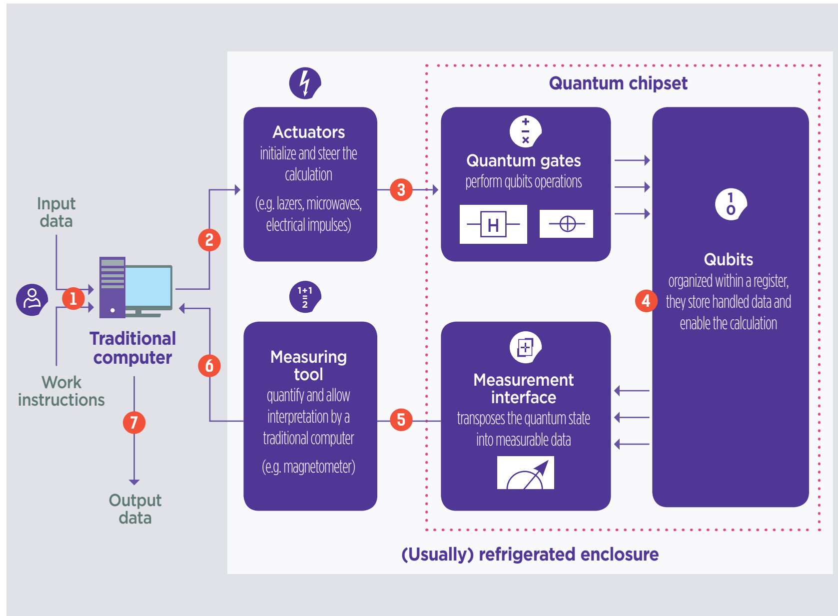
On the other hand, quantum computers are likely to be integrated with supercomputer manufacturers' datacenters. We anticipate that HPC (High Performance Computing) market players will gradually gear up to enable their customers to carry out complex calculations through combining the power of traditional computers with that of quantum computing—and reducing calculation times.

In the summer of 2019, **Accenture** filed a patent related to directing calculations toward the appropriate type of computer. Similarly, **Atos** already offers a powerful quantum algorithm emulator alongside its supercomputer offer. This should not be confused with a quantum computer proper, but the emulator none the less helps grow familiarity with the characteristics of quantum programming.

Moreover, as we've seen, the power offered by quantum computers is only valuable for certain types of problem: it's useless, for example, to try to harness it for the wide world of transactional processing (like booking train tickets or sending emails) or graphics processing (like video games or TV).

Finally, one last, decisive point: quantum computers won't replace all traditional machines because **conventional computers will still be needed to program and control their quantum cousins**, as the schematic below illustrates.

Understanding quantum computing



Source: schema inspired by "Understanding quantum computing" – O.Ezratty

An ecosystem that's rich... but still young

Like most recent technologies, quantum computing needs a rich and diverse ecosystem: from research, through financing, to marketing—all players need to be active to bring about operational solutions that will have an overall impact.

Research institutes as key partners

As the technology is still in its R&D phase, **institutes and universities are key players in the quantum ecosystem**. The majority of them collaborate with other research units or private companies.

At European level, many research projects involving international collaboration are in progress, such as the **OpenSuperQ**[1] project which brings together collaborators from Germany, Spain, Sweden, Switzerland, and Finland. Collaboration between institutions from at least three countries is also a condition for accessing funding from the European Quantum **Flagship program**[2].

On the French side, research is both ongoing and high quality. An example is the Quantum Silicon research project in Grenoble, which brings together researchers from three French institutes (CEA-IRIG, CNRS-Institut Néel, and CEA-Leti) to help develop silicon-based quantum processors.

Digital giants in the vanguard

Several major groups, with the US majors at the forefront, have developed in-house programs dedicated to quantum technology, in order to use it themselves, market it, or fund research programs. Chief among these are Google, Microsoft, IBM and Intel.

Since 2014, **Google** has been building its own quantum computer via its Quantum Artificial Intelligence Lab (QuAIL), which is hosted by NASA. Its investment has enabled it to become one of quantum computing's most important players. Google's research team claims to have reached quantum supremacy, the point where quantum computing overtakes the capabilities of conventional computers. However, Google has not yet officially confirmed this, and Sycamore, the quantum computer it used, has limited real applications.

Microsoft launched its efforts in 2005 by funding the Station Q research program at the University of California, Santa Barbara. In 2017, the company launched the Quantum Development Kit, a program that used its programming language (Q#) to develop quantum algorithms. The kit, available in open source, has been downloaded more than 100,000 times.

1- http://opensuperq.eu/partners

2- https://ec.europa.eu/digital-single-market/en/policies/quantum-technologies

IBM, which has traditionally been very active in basic research, does not want to be left behind. It has developed an in-house research group focused on the end-to-end build of its own quantum computer; and this has recently materialized in an announcement about the 53-bit system that became available in the cloud in October 2019. **The company aims to commercialize its quantum computer in the next five years and position itself as the ecosystem leader. IBM's global hub for these technologies is Montpellier, France.**

Intel's focus is on the production of quantum computer chips. Its aim is to be able to mass produce quantum processors, quickly and cheaply.

D-Wave and Rigetti, two North American startups, are key players in the quantum technology market.

D-Wave is a Canadian company often seen as a pioneer in quantum computing, since it was the first to market annealing quantum computers. It should be noted that this type of "simulated" computing only works for some, quite particular, types of calculations, and therefore isn't destined for the anticipated uses of a general quantum computer.

Rigetti Computing is a Californian company that aims to develop an entire quantum computer: manufacturing the chips, and developing the architecture and algorithms that will make them work. At this stage, it provides a cloud-based platform to develop algorithms using 36 qubits (although it's not clear whether this is an emulation or a 36-qubit machine).

Chinese companies are also competing in the technology race. In 2015, the Chinese e-commerce giant, **Alibaba**, created the Alibaba Quantum Computing Laboratory. Its team is working on a number of quantum projects, including, since March 2018, the manufacturing of 11-qubit processors, the emulation of a cloud-based quantum computer, and the development of quantum algorithms. In 2018, another Chinese giant, the search engine, **Baidu**, created an institute dedicated to quantum computers.

In France, Atos is the leading French player in quantum computing development. Launched in 2016, the Atos Quantum program is the largest industrial program in Europe. In July 2018, the company released the Atos Quantum Learning Machine (QLM) emulator, the first large-scale, ready-to-use system, capable of emulating up to 41 qubits on traditional Intel processors.

Industry players: the vital catalysts

Large industrial groups also play a role in quantum's development. Many have set up their own research teams or funded applied-quantum-research projects working with research institutes or startups. **Some economic sectors, especially transport, aviation, telecommunications and energy, are more aware of quantum's potential than others.**

In 2015, **Airbus** commissioned a dedicated team to work within its Defence & Space Unit. The aerospace giant is collaborating with QC Ware (founded in the US in 2014), a quantum software startup. The goal is to use quantum computing for optimization, and quantum simulation to create ultra-durable materials. **Volkswagen**, already mentioned above, for its work on optimizing Beijing taxi routes[3], is working in concrete fashion on quantum's possibilities thanks to its partnership with D-Wave.

In energy, **Total** is working with Atos (QLM) to, among other things, simulate and understand particle behavior, as well as optimize the logistics of industrial tools. In 2018, **EDF** too launched a dedicated project.

The **PASQuanS** project, which aims to develop a quantum simulator (covering both hardware and software), and is one of the projects supported by the European Flagship initiative, ensures the concrete application of the technology developed through a committee of end users that includes Airbus, Bosch, EDF, Siemens, and Total.

3- https://www.frontiersin.org/articles/10.3389/fict.2017.00029/full

Investment funds are essential allies

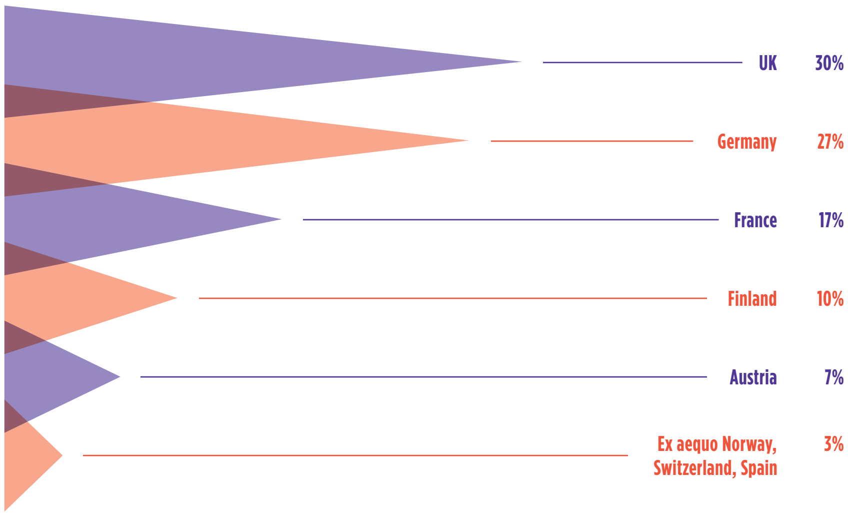
To date, about 150 venture capital firms have invested in quantum startups. However, the number of investment funds that specialize in quantum only is very low: no more than half a dozen in the world; **quantum technology is seen as a risky** investment because of the technology's complexity and the lack of visible returns on offer.

Current investments are mainly made by specialized funds focusing on research or those dedicated to one or more quantum technologies. Their number is still low, compared with artificial intelligence or blockchain.

In France, Quantonation, the fund created by Charles Beigbeder and Christophe Jurczak is an exception. Other French funds, such as the XAnge fund, however, have recently invested in quantum projects.

The number of investment transactions, and the total sums invested, have grown strongly in recent years. In 2012, three startups had raised funds, amounting to a total of US$34m. In 2018, 24 startups raised US$128m.

Distribution of European investment funds (2019)



Source: Wavestone

Countries as strategic players—and their funding programs

Quantum computers have become **a strategic issue for sovereignty and security**. Many countries have put in place national R&D strategies, with levels of state funding ranging from €140m to €1bn.

Looking worldwide

The **US** and **China** are the two countries that have invested the most[4]. In 2019, the US government passed the National Quantum Initiative Act. This $1.3bn state program aims to encourage both R&D and education in quantum technology.

China is the country that has invested the most in communications and quantum cryptography. In 2017, the country began the construction of its "National Laboratory for Quantum Innovation", which is expected to begin activity in 2019, at an estimated cost of $10bn. Since 2006, the total level of Chinese public investment has amounted to almost €2bn.

The European Union

In 1999, the European Union invested €550m in the Future and Emerging Technologies (FET) program. Following the "Quantum Manifesto" signed in May 2016 by more than 3400 players from the academy and industry, the EU translated its desire to increase its investment in quantum technology into action. **Quantum Flagship, launched in 2018, is a 10-year, European Commission project that invests €1bn** to support 20 projects in its first phase, and mobilizes a European academic community of more than 5,000 researchers.

In 2013, the UK was the first European country to launch its national quantum program with an investment of €370m over five years, which explains the many university programs and (relatively) large number of startups seen in Britain today.

France recently put quantum computing on its agenda with a parliamentary mission on quantum technologies. Led by deputy, Paula Forteza, it was launched in April 2019; and should result in the executive announcing a national plan by the end of the year.

4 https://www.ida.org/-/media/feature/publications/a/as/assessment-of-the-future-economic-impact-of-quantum-information-science/p-8567.ashx

The ecosystem in France and Europe: many projects... but few startups

To monitor the European market's development, Wavestone is launching its Quantum Ecosystem Radar this year (see the graph below). Some initial observations:

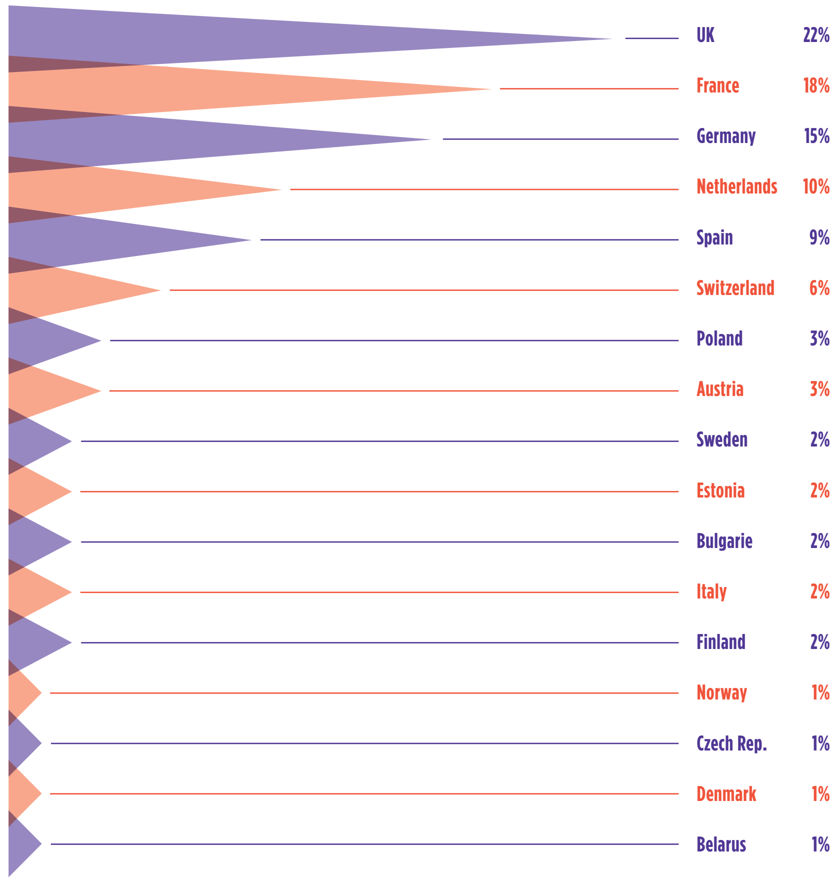
- **At European level, the ecosystem has about 90 players.** The UK is in first place with 20 startups, and behind are France, with 16, and Germany, with 14.
- The number of projects or startups focused on hardware and component development (which also includes the set of startups in the European Quantum Flagship initiative) reflects the **current state of the market well: creating sufficiently powerful and stable quantum computers is still the priority**. This probably means that opportunities in other areas (software development, for example) are still to be seized.

European startups in this field are still scarce and often recent: most were created in 2018 and 2019. Usually spin-offs from research projects, and still largely focused on R&D, most haven't yet gained clarity on their business model (which is, of course, to be expected for a startup).

> "With 18% of startups and 17% of venture capital firms in the quantum computing ecosystem, France is positioned as leader in Europe*"

NB: As the quantum market continues to evolve, we encourage the reader to adopt a certain degree of caution regarding the accuracy of these figures, which are mainly intended to provide an overview of the current ecosystem.

Distribution of European startups (2019)



Source: Wavestone

2019 Panorama of the European quantum ecosystem

Hardware

Computer
- OQC
- PASQAL
- PHASECRAFT
- Quantum Factory
- QuantumX
- NextGenQ
- BraneCell
- AQT
- IQM

Software

Algo
- Optalysys
- QILIMANJARO
- CQC
- HQS Quantum Simulations
- QuBalt
- NQCG
- VeriQloud
- QuantFi
- ⟨b| e

Machine Learning
- rahko
- APEXQUBIT
- Applied Qubit
- GTN LTD
- RIVERLANE
- Prevision.io

Interface, Error Correction
- QUANTASTICA
- Qu&Co
- Shyn
- Q-LION
- |Ketita⟩
- PHASECRAFT

Components

Photonic
- QuiX
- Lytid
- LIGENTEC
- Quandela
- Single Quantum
- Sparrow Quantum
- PicoQuant
- TUNDRA SYSTEMS GLOBAL LTD

Cryogenic
- Oxford Instruments
- CryoConcept
- Low Noise Factory
- kiutra
- Leiden Cryogenics
- BLUEFORS
- MyCryoFirm

Sensors
- Quantum Motion
- Phase Space Computing
- Aquarius
- Qnami
- SeeQC
- QBLOX
- Cryo Tech

Flagship

European Projects
- OpenSuperQ
- PhoQuS
- PhoQ
- QMiCS
- Qombs
- QRANGE
- S2QUIP
- UNIQORN
- QIA Quantum Internet Alliance
- Metabolics
- MicroQC
- CiViQ
- AQTION
- macQsimal
- 2D-SIPC
- SQUARE

Security
- QuantiCor
- Quantum Impenetrable
- QUSIDE
- SECURE-IC
- (InfiniQuant)
- IDQ
- Crypto Labs
- CRYPTONEXT Security
- |KETS⟩
- nu quantum

Consulting

Service
- bqb
- Entanglement Partners
- ⟨Φ|Quantum.Phi
- Quantiko

Investors

Capital Ventures
- PARKWALK Advisors
- QUANTONATION
- Q Ventures
- Seier Capital
- TESI
- UCL Technology Fund
- P|V⟩
- VITO VENTURES
- ipgroup
- WILCO
- XAnge
- MERCK VENTURES
- OpenOcean
- London Co-Investment Fund
- octopus ventures
- MAKI.VC
- BASF We create chemistry
- BOSCH
- MIG Fonds
- Global Founders Capital
- ASTERIONS
- High-Tech Gründerfonds
- Aster Capital
- Amadeus Capital Partners
- Cambridge Innovation Capital
- FLUXUS VENTURES

Hubs
- PCQC
- QUANTERA
- Quantum Communications Hub
- QUANTIC
- Qubiz
- QuSoft
- IQST
- IBM Q
- UK National Quantum Technologies Hub
- NQIT
- main

Wavestone figures from the following sources:

Investment fund XAnge - xange.fr

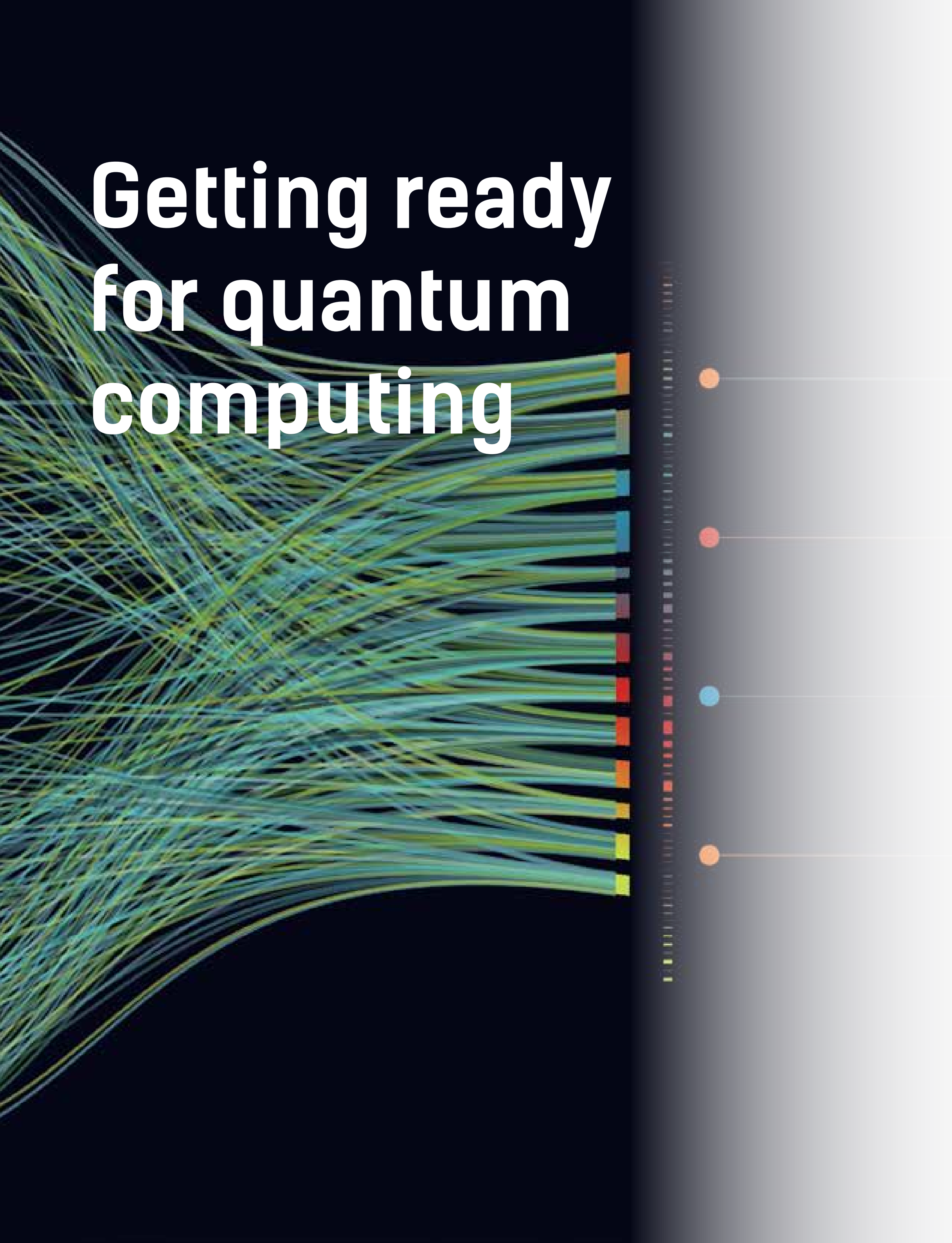
BPI QCB Conference (June 2019)

Data base Dealroom

Ezratty, O. (2019) - Understanding quantum computing

Quantum computing report - https://quantumcomputingreport.com

Press kit Flagship (2018) - https://www.iqclock.eu/uploads/1/2/0/6/120640577/press_dossier_final_embargoed_1.pdf



Getting ready for quantum computing

A computer revolution is imminent: it's difficult to put an exact timescale on it, but most announcements suggest we'll see the first concrete results in the next three to ten years, depending on how optimistic or skeptical their writers are.

However things develop, there's still time to prepare, and the following recommendations should help both public and private players take up the challenge of the quantum revolution, and the many opportunities it will bring.

For public decision-makers

1) Focus on European "quantum sovereignty"

Quantum technologies will be key in the defense and security sectors. And the mastery of quantum computers and communications will be major resources in building secure infrastructures and being able to draw on unprecedented computing power. This will mean getting the entire value chain right: materials, producing components, applications, etc.

The challenge is to avoid missing the boat on the next great technological wave, something now leading many decision-makers to **lament US hegemony**, which is driven by the current strength of the GAFA companies.

2) Encourage collaboration at European level

"Quantum sovereignty", like "digital sovereignty" can and must be thought through at European level—by strengthening cooperation. Due to the cost and complexity of the research involved, most quantum computer projects are collaborations between several public (and often international) institutions. Although already prioritized in actions being taken by the European Commission, this collaboration could be further strengthened even under the current framework.

Without any contradiction, creating national bodies, with the responsibility for coordinating research projects, linking the country's different players together, and steering relevant strategies, could also facilitate this transnational coordination.

3) Boost investment

Quantum technologies are still heavily in the R&D phase, and their development requires significant funding.

Beyond the funding of institutions engaged in basic research, there's a case for launching public-sector calls for quantum projects. In the short term, the defense and intelligence sector could be a major sponsor. Investments by major public or private players could also be encouraged through a dedicated taxation policy.

4) Develop skills

To enable quantum technologies to develop, new skills will have to be deployed: this requires the **training of engineers, doctoral students, professors, and researchers**—something that will need to be organized and financed at the right scale.

All facets need to be considered, because the creation of high-performance qubits isn't the only race taking place: beyond research in physics, research into software also needs to be boosted to pave the way for the emergence of future developers and algorithms—both essential in harnessing this new source of power.

5) Increase quantum's visibility

Finally, and more broadly, it's essential to raise awareness among the public in general, and public and private decision-makers in particular. All the more so because even the use of the term "quantum" is often enough to provoke negative reactions, like "completely incomprehensible," "complex" "impossible to describe or imagine),".

This sheds real light on the need for the quantum ecosystem to be clearly visible to both business and the general public. **National plans can be exceptional tools to bring these technologies to the fore, demonstrate educational excellence, and position a country as a recognized leader in the field.**

For the private sector

1) Evaluate the impact of quantum computing on strategic priorities

As we briefly explained in the first part of this Insight, the opportunities are vast, but only in certain areas: in short, the simulation and optimization of large systems.

It's up to the leaders and their strategists to integrate this new potential into their strategic thinking by asking questions like: "which of my products and services could benefit from this increased computing power?" or "Could it be a source of new offerings or significant competitive advantage?"

2) Evaluate the scope to reduce costs

The mirror image to considering quantum's potential to help companies grow is the equally important one of its application in reducing costs: "are there any cost-related areas we haven't addressed due to lack of computing power, but which could be tackled in a quantum era?"

We've seen previously that many optimization questions could benefit from this revolution: for example, decisions on allocating resources, something close to all business leaders' hearts, might be illuminated by new algorithms.

3) Begin to experiment—and understand

There are several routes to supporting this type of analysis and the resulting action plans: straightforward technology watching, training decision makers, or a one-off partnership with a quantum community player (a manufacturer, publisher, university, startup, VC firm, consulting firm, etc.)—to define or prototype a use case specific to the business's needs.

Businesses can draw on all the classic tactics used to engage with an ecosystem: calls for projects, co-development of solutions, financing teaching chairs, competitions (like Airbus's challenge, discussed above). Once the potential has been confirmed, then a dedicated team needs to be put in place, working in "commando" fashion to act quickly and precisely.

4) Send out development teams as scouts

In parallel, encouraging development teams to become familiar with quantum computing's new paradigms seems a promising way forward: they'll already be operational when the time comes, and can also help decision-makers identify where within the business quantum's power could be harnessed.

There's no need to plan to purchase and install a quantum computer to do this: the QCaaS (Quantum Computer as a Service) marketing model, which uses cloud-based resources, means progress can be made with limited initial investment.

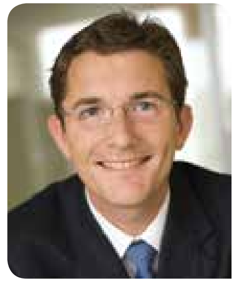
Conclusion

At the beginning of the 20th century, the advent of quantum physics turned models of the world upside down, at least for some of the period's greatest minds. But the subject, which was dry, complex, and often counterintuitive, remained obscure for mere mortals.

Yet we all use products, every day, that would not have been possible without this new science. And these have a considerable impact on our lives: semiconductors (transistors, microprocessors, and therefore traditional computing); photocells (photocopiers, digital cameras, solar panels, etc.); lasers (the key to the digitization of audio and video, but also extensively used in industry); etc.

Our firm conviction is that **quantum computing carries the seeds of a similar revolution**: by the huge leap it promises in addressing problems at the heart of our societies, it will **open up vast pathways of analysis and optimization that are closed today due to a lack of computing power**.

Its potential applications are legion and affect all sectors: for example, the creation of new molecules that enable the treatment of even more diseases; the simulation of complex, multi-million-component systems to manage smart cities effectively; or the arrival of impenetrable systems to secure communications.



Benoit DARDE, Partner Wavestone

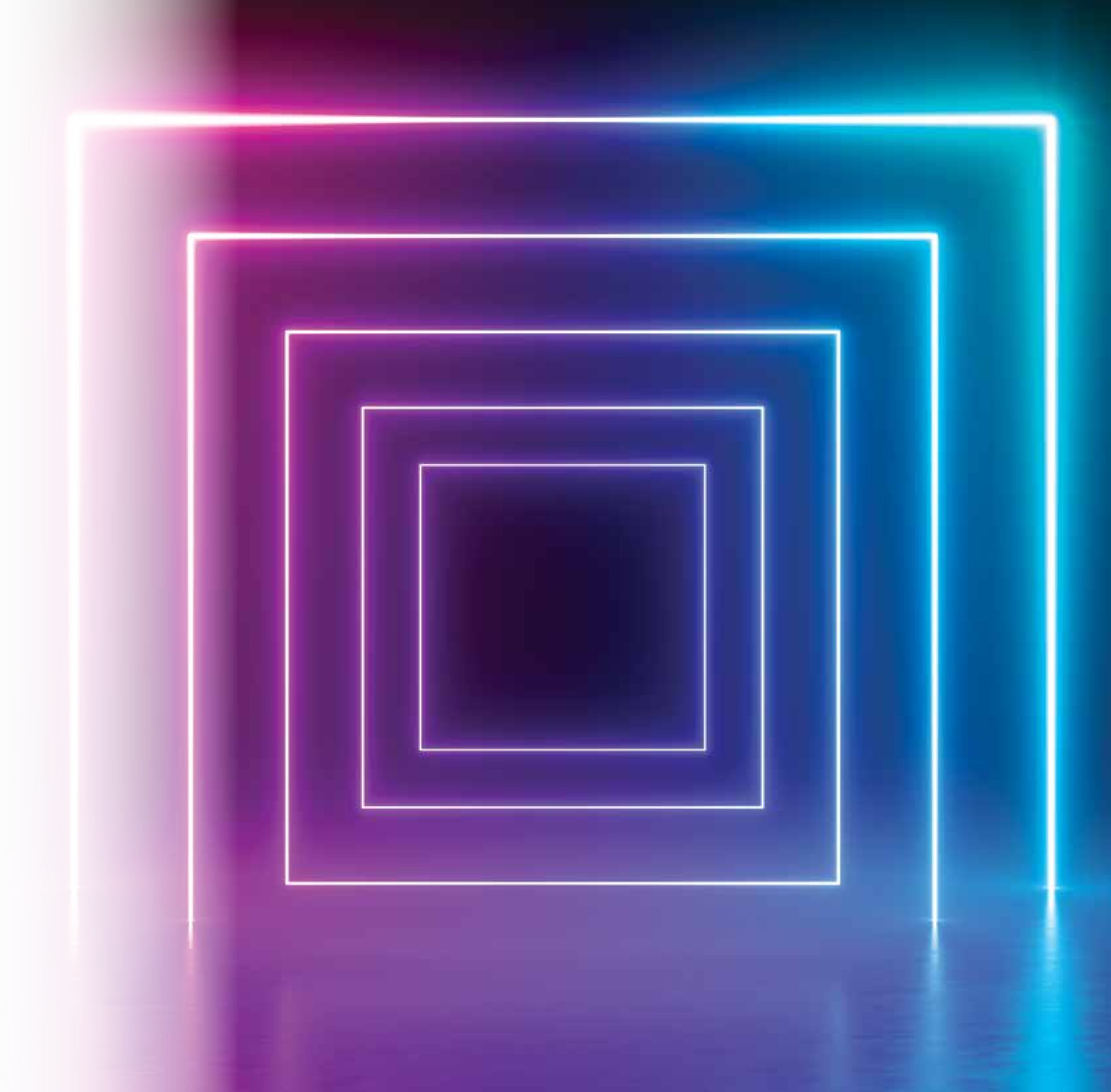
Today, the race to develop and perfect quantum technology is global; and Europe, despite being in the running, may struggle to stay the course, especially faced with the colossal investments being made by the US and China. But **the stakes are very high: they involve critical issues such as European leadership in areas like R&D, securing sensitive communications, or simply maintaining competitive levels of productivity**.

Beyond the remaining technical challenges, which shouldn't be underestimated, but, none the less, will be gradually resolved in the years to come, we observe two serious obstacles that need urgent attention.

The first is the challenge of **growing European ecosystems that are competitive compared** with their US or Chinese counterparts. The keys to this are well known: the creation of centers of excellence, the development of partnerships between basic research and industry, training people for tomorrow's skills, unlocking financing, and a willingness to take risks. Here, public authorities have a vital role as a catalyst.

The second is the problem of a **sluggish digital ecosystem, something probably linked to the technology's maturity**. Yet, as soon as this becomes accessible, and it doesn't seem far off, Europe will need all the richness and creativity that its start-ups can offer to translate the technology into everyday uses.

But we already have all the cards in hand to **make Europe a leader in quantum computing**. So, let's take courage; let's seize the opportunity right now, experiment, and build the future, "quantum" world!

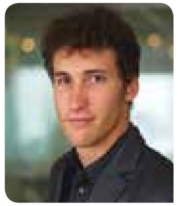


AUTHORS

Florian CARRIERE - Senior Manager

Florian is a Senior Manager in the Digital and Emerging Technologies practice. For 20 years he has been supporting IT Departments and Business Divisions in their major transformations related to the deployment of digital technologies. In recent years, he has led major projects on digital workplace and smart territories, mobilizing innovative technologies (platform, RPA, chatbots, AR/VR, etc.) using modern approaches (agile, UX design, lean startup).

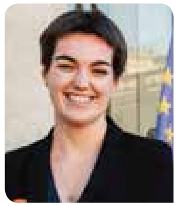
florian.carriere@wavestone.com



Robin GAYRARD - Manager

Robin is a Manager in the Emerging Technologies practice, specializing in Cloud and Digital Workplace topics. A graduate of École Centrale Paris, he began his career in Paris in Cloud transformations and IT organization at Wavestone. He then joined the Lyon office, where he has been working for the past 3 years with the major players in the Auvergne-Rhône-Alpes region on their IT strategy.

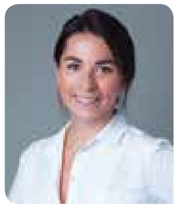
robin.gayrard@wavestone.com



Agathe RABAYROL - Policy Analyst France Digitale

Agathe Rabayrol is Policy Analyst at France Digitale, in the Public Affairs division. She specializes in deep techs and data. She collaborated with transport.data.gouv.fr within the public policy incubator of Sciences Po for the opening of transport data at the local level, and is particularly interested in issues of inclusiveness and legitimacy of digital public policies.

agathe@francedigitale.org



Marianne TORDEUX - Director of Public and European Affairs

Marianne is Director of Public and European Affairs at France Digitale. She represents the interests of France Digitale's 1500 startups and 150 VCs members, on all aspects (duch as tax, financing, platform workers status, IA, Blockchain, etc.). Marianne is also a tax lawyer and participated in the creation of the Blockchain reglementation in France.

marianne@francedigitale.org

CONTRIBUTORS

This publication was produced with the contribution of Jules Jaunay (jules.jaunay@wavestone.com), consultant, and Mélodie Lauque (melodie.lauque@wavestone.com), Wavestone Communication Department.

Acknowledgements

Interviews:

Cyril Allouche, Atos

Marianne Billard, Parliamentary Employee

Oscar Diez, European Commission

Alexis Du Peloux, XAnge

Olivier Ezratty, consultant and author,

Paula Forteza, French Parliament Deputy

Jean-Christophe Gougeon, BPI

Olivier Hess, IBM

Elham Kashefi, CNRS and VeriQloud

Pascal Maillot, European Commission

Bernard Ourghanlian, Microsoft

Georges-Olivier Reymond, Pasqal

Kristjan Sigurdson, Creative Destruction Lab

Olivier Tonneau, Quantonation

Christian Trefzger, European Commission

Our thanks to Olivier Ezratty and Olivier Tonneau for their thorough proofreadings.

To find out more:

IMT (2019) - "L'avantage quantique : enjeux industriels et de formation"

CNRS (2019) - Les promesses de l'aube quantique

Ezratty, O. (2019) - Comprendre l'informatique quantique.

University of Maryland (2019) - Machine Learning meets quantum physics

CEA (2018) - L'ordinateur quantique, graal du numérique

BCG (2018) - The Next Decade in Quantum Computing

D-Wave (2018) - Introduction to Quantum Computing

University of Innsbruck (2017) - Machine learning & artificial intelligence in the quantum domain

UE (2016) – Quantum Manifesto

FRANCE DIGITALE

WAVESTONE