INTERBANK CONVENTION
FOR AUTOMATION
(CIPA)

Quantum technologies in the banking sector

May 2024

The Technical Secretariat of the Convention would like to thank the members of the working group, listed below, for their cooperation and contribution in carrying out the group's activities.

Elena	BUCCIOL	Banca d'Italia (Coordinator)
Katia	BORIA	Banca d'Italia - CIPA Technical Secretariat
Matteo	ELIA	Banca d'Italia - CIPA Technical Secretariat
Domenico	PETRUCCIANI	Banca d'Italia - CIPA Technical Secretariat
Mario	TRINCHERA	ABI Lab
Ivan Luciano	DANESI	UniCredit
Lorenzo	DEMELAS	UniCredit
Davide	CORBELLETTO	Intesa Sanpaolo
Dimitar	ANASTASOVSKI	Sella
Stefano	PRIOLA	Sella
Matteo	BALBONI	Banco BPM
Gloria	MASSERA	Banco BPM

We would also like to thank Cristina Andriani, Giuseppe Bruno, Angelo Germoni and Pietro Tiberi of the Banca d'Italia for their useful collaboration in deepening some of the aspects discussed, Marina Natalucci, of the "Quantum computing & communication" Observatory of the Politecnico di Milano, for her willingness to share the survey data, whose copyright © is held by the DIG - Department of Management Engineering of the Politecnico di Milano, whose references are given in the chapter 4.4.

Index

1 Foreword

Quantum technologies, i.e. the set of hardware and software components that exploit the laws of quantum mechanics to deal with objects on an atomic and subatomic scale, represent one of the most interesting emerging phenomena in the Information Technology (IT) landscape in recent years.

The objective of this document is to raise awareness in the banking and financial world of the opportunities and risks associated with their advent and to provide a common knowledge base for taking initiatives and launching strategies.

Unlike many aspects of IT, an in-depth understanding of these topics is inseparable from knowledge of the underlying physical theory that has successfully described the behaviour of phenomena at the microscopic level for more than a century. Furthermore, approaching some topics, such as algorithms that can be used with quantum computers or the principles behind cryptography, requires expertise in linear algebra and advanced mathematics. However, reading a paper with continuous references to specific details of the theory would be rather laborious. An effort of abstraction has therefore been made to capture the main aspects of this new and stimulating context, with a few references being included to delve into individual aspects.

This document, drafted in early 2024, does not claim to be exhaustive; it is the result of the authors' insights and discussions on the topics covered, as well as the experiences they have gained during their own professional practice.

For the purposes of the report, the working group made use of several sources: data and information made public by analysts and by specialized press, resources made freely available by the world of scientific research and industry, websites of technology and consulting providers.

The availability of the web pages, whose references are given in the text, has been verified at the date of drafting (May 2024).

The opinions expressed in this report describe the views of the authors and do not necessarily reflect those of the respective institutions they represent.

2 Introduction

The complex of insights, interpretations and mathematical models born since the early 1900s for the description of phenomena on an atomic scale, which goes by the name of quantum mechanics, represents, in the history of scientific progress, one of the most astonishing achievements in terms of prediction and practical implications. The digital technology with which we are familiar, with which we measure ourselves on a daily basis and which facilitates, for example, the writing and dissemination of documents such as this report, is based on devices created through the discovery of the laws of quantum mechanics. In particular, the introduction of semiconductor physics for the construction of components such as transistors, lasers and other electronic elements is considered part of what is known as the "first quantum revolution". The aspects that are the subject of this discussion (quantum computing, quantum cryptography, quantum sensing), on the other hand, are part of the so-called "second quantum revolution", in which features (such as superposition and entanglement of physical states) relating to the behaviour of individual subatomic particles are exploited.

The peculiarity of the behaviour of microscopic objects has made it first conceivable, starting in the 1980s, and then feasible, thanks to continuous technological advances, to design devices capable of enabling a new paradigm of computation that is completely different from those known from classical theoretical computer science, based on Boolean algebra (where the information unit, the bit, can assume the values "0" and "1"). Quantum computers exploit, in fact, the property of microscopic objects (qubits) of being able to take on different values (formally "0" and "1") "at the same time" and offer, in a certain way, a degree of parallelism that has different applications. In particular, it would result, once a certain technological maturity has been reached, in a substantial increase in computing capacity that would allow the resolution of certain problems considered intractable by classical computer science. From this point of view, like other technologies, quantum computing could become human heritage for the benefit of research and development in the fields of health, environment and artificial intelligence.

The practical realization of this computational paradigm, due to the complexity involved in handling microscopic particles[1], is, at the moment, far from being defined, despite huge investments by many large commercial enterprises. In particular, the current technological offer falls into the category of "Noise Intermediate Scale Quantum" (NISQ), with the presence of a limited number of qubits defined as "noisy" due to their instability and without a reliable error correction mechanism due to the difficulty of maintaining coherence between quantum states. In the long term, the goal is to have fault-tolerant devices (FTQC), also called "universal" quantum computers, that allow the full realization of the new computing model.

Meanwhile, several initiatives have been launched to identify different fields in which the introduction of this new approach could bring real benefits. Since the 1990s, even before large companies began designing these devices, quantum algorithms have been developed for the

[1] There is also an entire field of study, not mentioned in this report, dedicated to "enabling" technologies for quantum computing: cryogenics, electronics, lasers, photon sources and detectors, and the production of specific materials with quantum properties.

optimization of certain problems, known from computational complexity theory, such as the search of an element in an unstructured space or the integer factorisation.

However, the availability of sufficient quantum processing to ensure the execution of these algorithms on a large scale poses a serious threat[2] to the cryptographic systems at the basis of the security of the cyber universe in which sensitive data, economic transactions and military secrets circulate every day.

To deal with these threats, two main strategies have been identified. The first consists of using classical mathematical problems in encryption for which, at present, there is no quantum algorithm that allows their violation. The second exploits certain properties of quantum mechanics in the construction of optical devices (photon emitters and detectors) that allow information (in particular encryption keys) to be "exchanged" in a completely secure manner.

Even if the available quantum processors are not currently able to breach the mechanisms behind traditional cryptography, data that need to be kept confidential for a long period of time may already be at risk, as cyber criminals may have taken possession of them and store them until they have the tools to breach them ("harvest now, decrypt later"). In addition, the breach problem also concerns digital signatures and the compromise of the validity of already signed documents, for which the introduction of a guarantee system such as a public key infrastructure (PKI) that is also valid in the "post-quantum" era is necessary.

This context becomes particularly important when looking at the financial world due to its increasing digitisation and interconnection and the fact that it is an increasing target of cyber attacks[3]. Awaiting the "Q-day"[4], it is necessary to plan as soon as possible an assessment of the sensitive and critical data assets within each organization and their processing for the introduction of a quantum safe strategy[5].

The market already offers many opportunities both to experiment with the possibilities offered by quantum computing[6], and to introduce quantum safe elements into IT infrastructures. In the world of banking and finance, a large part of current experiments and applications are related to models

[2] In 1995, Bell Lab mathematician Peter Shor demonstrated that the integer factorisation problem, the complexity of which is one of the foundations of modern cryptography, is "solvable" with a sufficiently powerful quantum computer, using a quantum algorithm, in significantly less time (on the order of minutes) than that required by classical processing (comparable to the life-span of the universe).

[3] Data from the recent Clusit 2023 report show not only that in the last five years the financial and insurance sectors have been among the main targets in terms of the number of attacks (10,5%) and their impact (40% of attacks deemed critical), but also that this figure is constantly growing.

[4] The "Q-day" is defined as the time when a computer capable of compromising current public-key based encryption systems (e.g. RSA-2048) will be available.

[5] To give some examples: the migration from SHA-1 to SHA-2 took approximately 10 years. Blackberry took five years to migrate from 3DES to AES, while having control of all devices and servers. MD5, despite known vulnerabilities, is still used in some contexts (CARAF: Crypto Agility Risk Assessment Framework | Journal of Cybersecurity | Oxford Academic (oup.com) https://doi.org/10.1093/cybsec/tyab013).

[6] Quantum resources can be accessed in a similar way to traditional computing, i.e. via APIs to cloud systems, using software development kits that allow code to be compiled and "launched" on quantum platforms. According to some estimates, the market for quantum computing "as a service" could reach USD 26 billion in 2030 (https://thequantuminsider.com/about-us/).

for solving problems that are applied in this sector and represent its core business such as credit risk estimation and portfolio optimization.

Since the last decade, the field of quantum technologies has seen significant investments, including by national and supranational governments: China alone has announced the investment of more than $15 billion, but Europe is also the second geopolitical area for public investment[7]. The European Commission, in particular, has earmarked investments for a long-term plan to coordinate different activities between research institutes, industry and public bodies. In the national sphere, there are several initiatives, although the investment is limited (EUR 1.6 billion within the National Recovery and Resilience Plan - PNRR for critical technological topics, including quantum computing).

The nature of the issues related to quantum technology is extremely complex: on the one hand, the knowledge required for its development and sometimes even its use is related to the scientific field and requires academic research, and on the other hand, the costs involved in adopting these technologies are high and require planning for a long-term return on investment. There is a growth of innovative start-ups offering services of various kinds, an increase in the supply of training in these areas and the drafting of national strategy plans for the development of this sector. The interest in these technologies involves numerous players, from private to institutional ones, up to international bodies and organizations: there is a need for strong collaboration, which this document promotes, between these realities in order to identify a common strategy, particularly for data and communication security issues.

Some application areas, in particular those concerning security, may benefit more from quantum solutions. Other areas, such as machine learning, may benefit in the medium to long term; this depends on the maturity of scientific research and the availability of affordable technology. As a result of these considerations, this report takes a more in-depth look at security issues - such as the protection of communications and the safeguarding of data integrity, which are affected by the advent of quantum technologies in the short term - and deals in less detail with areas related to business or machine learning models, as these are still in the early stages of the quantum technology revolution.

This work is organized into thematic chapters to guide the reader to a general understanding of how quantum technology works, its implementations and possible adoption strategies. After an insight into quantum mechanics, the chapter 3 addresses the main applications, both in the area of security and possible business applications. Chapter 4 is dedicated to an in-depth examination of the peculiarities of the ecosystem around the technology: research, the involvement of institutions, associated investments, the market. It was decided to devote an entire chapter (chapter 5) to quantum safety strategies to emphasize the importance of the topic. In chapter 6 an in-depth study is proposed on the impacts and possibilities generated by quantum technologies with the focus on the needs of the banking sector. The paper ends with some thoughts, shared by the working group, on the topics covered and the indications that emerge to address this issue of global impact.

[7] https://www3.weforum.org/docs/WEF_Quantum_Economy_Blueprint_2024.pdf

3 Quantum mechanics and its applications in IT

3.1 Introduction to quantum mechanics

Classical physics is a model that describes a world in which "objects" possess macroscopic properties (position, velocity, etc.) that can be measured with arbitrary precision, a reference system having been fixed. The evolution of a given physical system, given the initial conditions, is thus uniquely determined by solving equations derived from physical laws.

When the size of objects is reduced to the subatomic scale, classical physics is no longer suitable for describing their behaviour and quantum mechanics is resorted to. The latter contemplates the existence of entities that do not possess defined values for physical properties (so-called "states").

The operation of measuring the state of these entities assumes a fundamental role: prior to measurement, they may be in a configuration in which they possess all their possible states "simultaneously" ("superposition of states"). The measurement makes only one of the possible states manifest with a defined probability. For example, the quantum of light, the photon, possesses a property (polarisation) that determines its behaviour in passing through an oriented polarising filter or not. A photon polarised at $90°$ (vertical) has a 100% probability of passing through a filter oriented along the same axis and a 0% probability of passing through a $0°$ (horizontal) filter. If, however, a differently polarised filter ($45°$ for example) is used, the same vertically polarised photon has a 50% chance of crossing the filter (and a 50% chance of not crossing it) and, surprisingly, acquiring the respective property ($45°$ polarisation) due to the measurement itself.

The quantum computer encodes information precisely in the properties of some of these subatomic objects, such as electrons or photons, which can be exploited to solve certain computational problems much faster than with conventional computers.

The classical computer has as its fundamental components bits ("0" or "1"), the quantum computer uses qubits, realized through objects that can be prepared in superposition of states (linked, for example, to certain features of elementary particles, such as the polarisation of photons) and which, therefore, only have a defined probability of being "0" or "1".

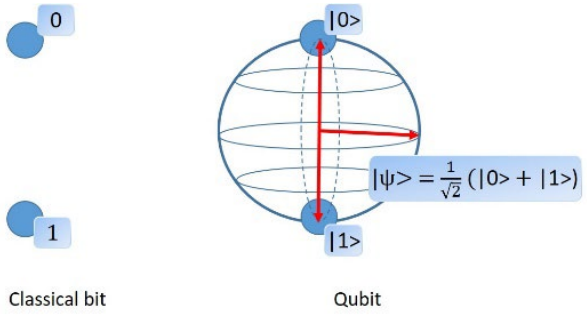


Figure 1: Classical bit and qubit[8] - In the classical description of phenomena, the value of a given physical property (e.g. position) can be uniquely identified (e.g. "0" for "up" and "1" for "down"). To realize qubits, on

[8] Taken from: https://w3.lnf.infn.it/computer-quantistici-verso-la-qubit-generation/. The Dirac notation |0> and |1> indicates the possible states of the particle, linked to the values associated with a certain physical property: for example |0> could correspond to a horizontally polarized photon and |1> to a vertically polarized one.

the other hand, one exploits the quantum properties of subatomic particles of being able to be prepared in such a way as to be in "coherent superposition of states", i.e. to be in a state (normally identified with Dirac's notation $|\psi>$) corresponding to the linear superposition of several basis states ($|0>$ and $|1>$) corresponding to the values "0" and "1". The coefficients of the linear composition of these states (in the example in the figure $1/\sqrt{2}$) are related to the probability (in this case ½) of finding the particle in the corresponding basis state at the moment a measurement operation is performed on it.

This property of being "0" and "1" at the same time implies the possibility of using a form of parallelism in the calculation, by combining several qubits, which, for certain problems, through the sequencing of a certain number of operations (algorithms), makes it possible to arrive at a solution more quickly. A system consisting of two qubits in superposition of states is, in fact, able to store the same information (using the possible combinations 00, 01, 10 and 11) as 4 classical bits: n qubits correspond to 2^n classical bits.

Quantum algorithms and quantum communication protocols used to exchange encrypted messages also exploit another phenomenon that has no analogue in classical physics, entanglement. Thanks to this, under certain conditions, the values of a property of two or more interacting systems cannot be described separately but are correlated in such a way that the measurement on one of the systems influences, even at an arbitrary distance, the outcome of the measurement on the other.

For example, it is possible to manipulate two photons to produce a physical state that results in the superposition of states in which the two photons are both horizontally polarised or both vertically polarised. In this case, not only do the photons no longer possess any defined polarisation value, but the measurement of the value of one would also cause the other to acquire a value without any direct interaction with it.

This property can be exploited and passed on by making it possible to perform algorithms that find no analogue in the classical world.

3.2 Quantum Computing

In 1982, Nobel Prize-winning physicist Richard Feynman hypothesized the possibility of exploiting the properties of quantum mechanics for the realization of computers, pointing out that a hypothetical quantum computer could be a true simulator of the theory, i.e. it could actually perform quantum experiments during its operation.

Starting in the 1980s, a long journey began, of which our times are a part, to identify the technology with which to build this type of computer. In parallel, studies focused on algorithms that were not based on the adaptation of what was used in classical computers, but took advantage of this new processing mode and the intrinsic features of quantum systems.

The requirements addressed by this new calculation paradigm can be summarized as follows:

- perform some calculations based on more complex problems, classically intractable[9], than the ones that can be done with conventional computers today;

[9] In computational complexity theory, an intractable problem is defined as a mathematical problem for which there is no "efficient" algorithm (with polynomial complexity) capable of solving it.

- for the same processing complexity, guarantee superior execution performance.

Although encouraging progress has been (and continues to be) made in the field of traditional high performance computing[10], traditional computing has technologically insuperable limitations[11].

In fact, some mathematical problems are intractable by classical computers for several reasons:

- it is not possible to process all the data required for execution at the same time (space complexity); for example, the representation of the possible energy configurations of the atoms[12] of a caffeine molecule, which are 10^{48} in number, cannot be tackled with conventional calculators while it requires 160 qubits of a quantum computer;
- the time required for execution is unreasonably long or in any case not compatible with operational requirements (time complexity); for example, the decomposition into prime factors of a natural number with a sufficiently large number of digits is an operation that would take up to hundreds of years of calculation time even if it employed the largest conventional computing capacity;
- the accuracy of the calculated solution does not prove to be satisfactory (inaccuracy): there are classes of problems, such as optimization problems, which admit more than one valid solution (e.g. maximizing the use of space within an aircraft hold for baggage transport). However, if in some cases it is easy to find sub-optimal solutions (local best), it may be extremely difficult to search for the absolute best solution (global best), especially in the presence of constraints that complicate the formulation of the problem.

Among the advantages offered by quantum computing, that of reducing environmental impact could also be of particular importance. On the one hand, quantum computers could be exploited precisely to analyse data, simulate behaviour (carbon-absorbing materials, catalysts behaviour) and create models to aid analysis and the identification of solutions (optimization of logistics or energy distribution) to limit or counteract the effects of climate change[13]. On the other hand, the energy consumption of these devices (access to which is likely to take the form of a cloud service) could be

[10] High Performance Computing is the technology that can provide very high performance by typically using parallel computing.

[11] The mechanism underlying the operation of traditional processors is based on semiconductors (transistors) which, by allowing or not allowing current to flow, enable the application of Boolean logic, the basis of today's classical computation. The number of these components within the microchip (in the order of billions) is directly proportional to the power of the processor itself. Over the years, microelectronics has succeeded in progressively decreasing the size of these objects, allowing the corresponding growth in computing power. However, the process of miniaturization of transistors seems to find a limit precisely in the quantum effects they suffer at sizes close to the nanometre.

[12] The single caffeine molecule $C_8H_{10}N_4O_2$ consists of 24 atoms each with different possible electron configurations in the available orbital levels (10^{48}). A 160-qubit system is capable of representing 2^{160} possible configurations.

[13] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/quantum-computing-climate-change-2023.pdf

limited[14] especially when compared to the energy-intensive use of High Performance Computing systems.

3.2.1 Quantum hardware

The two main emerging quantum computing technologies exploit two very different computing paradigms[15]:

1. "gate-based" (also called universal quantum computers): this is a quantum generalization of the traditional logic gate model used in classical computers in which the properties of individual qubits are manipulated and exploited through controlled pulses, magnetic fields, optical devices or other control mechanisms;
2. "adiabatic quantum computing" (also called quantum annealer): on the basis of a theorem known in quantum mechanics (adiabatic theorem), systems of qubits are manipulated by controlling their dynamic evolution, using special devices (annealers). The system is prepared in an initial state and then slowly evolved towards the state that represents the solution to maximum and minimum detection problems (minimum energy state).

3.2.1.1 Gate-based quantum computer

Gate-based quantum computers are based on the manipulation, via a finite series of “gates”, of individual qubits. The algorithms are realized through a series of gates that form so-called “circuits”.

With regard to the types of hardware available, i.e. the technology behind the physical realization of qubits and the manner of their interactions, it should be noted that there is still no dominant technology. Today's situation is even more complex than the one experienced by traditional computers in the 1950s and 1960s, when transistors had not yet established themselves over thermionic valves as the prevailing construction standard. In fact, there are multiple construction techniques, with different aspects in favour or disadvantage, based on different quantum physical properties.

Based on the different physical phenomena used, there are at least seven different approaches to the realization of qubits (see box “Quantum computer technology: qubit physics”).

Quantum computer technology: qubit physics

The different approaches to physically realizing a qubit are:

- Superconducting: thanks to the properties of superconducting materials, which below a critical temperature conduct electricity with zero resistance, it is possible to realize systems capable of

[14] Given that quantum computers do not appear to be destined to replace conventional computers and that a comparison of their energy consumption may not be particularly valuable, estimating this consumption is at present particularly complex, both because the final technology is not yet established (e.g. not all qubits require an energy-intensive cryogenic system) and because it is difficult to identify correct indicators to assess their impact. Reference is made to a project (https://quantum-energy-initiative.org/) that aims to scientifically address the environmental cost of the entire quantum technology landscape.

[15] There are also devices called “quantum simulators” that are designed to simulate specific physical systems and allow them to be controlled in order to experimentally study the behaviour of certain physical problems that are difficult to solve. Their use, of great interest for example in physics, chemistry and pharmaceuticals, is beyond the scope of this report.

exhibiting quantum behaviour at a macroscopic level that can be manipulated and assembled to scale. However, such devices in order to operate consistently require physically isolated environments with extremely low temperatures (< 20 thousandths of a degree Kelvin) that can only be achieved through the use of sophisticated cryostats. The technology is one of the most mature in which several large market players (IBM, D-Wave, Google, Rigetti Computing and IQM) have invested.

- Ion Traps: qubits are obtained with special electromagnetic ion traps (i.e. positively or negatively charged atoms). Although such devices are at least two orders of magnitude more stable in terms of coherence times, they are much more difficult to scale and considerably slower to perform calculations than qubits made with superconductors. Moreover, although the temperatures at which these devices are able to guarantee sufficient qubit coherence times for computation are higher than those required by quantum computers based on superconducting qubits, the practical realization of such qubits requires the use of special cooling techniques (laser cooling) that are particularly energy-intensive. The main market players in this segment are the Quantinuum consortium, the result of the merger of the large industrial group Honeywell and the start-up Cambridge Quantum Computing, IonQ and Alpine QT.
- Neutral Atom: This is a technology similar to Ion Traps that, instead of trapping ions, confines uncharged atoms - typically in a gaseous state - inside Ultra-High Vacuum (HUV) chambers, with pressures □ 10^{-7} Pa). This makes devices realized in this way more easily scalable, but, in addition to the problems of slowness in calculation, there is the added complexity of manipulating the qubits obtained in this way, making it easier to use these devices as analog rather than digital processors, effectively limiting their use to specific classes of problems, particularly in the area of simulations. The main market players in this segment are QuEra, Pasqal, Atom Computing and ColdQuanta.
- Photonic: in this case, the qubits correspond to photons travelling along circuits made of ordinary optical fiber. This is an extremely reliable technology in terms of computing coherence, since the way in which the channel where qubits of light interact is shielded is similar to the way in which current pulses are shielded for data transmission, and can be implemented at room temperature (with the exception of photon detection systems that operate at a temperature of ~4K). However, it is particularly complex, compared to other technologies, to manipulate photons in such a way as to obtain operable logic gates in accordance with quantum information theory. The main market players in this segment are PsiQuantum, Xanadu, Quandela and QuiX.
- Nitrogenvacancy: inspired by the impurities of natural diamonds, it is possible to make synthetic diamonds in which two carbon atoms are replaced - in the crystal structure - by a nitrogen atom and a lacuna (or lattice cavity). This nitrogen atom acts as a qubit within the lacuna (vacancy) and its operation does not require any kind of environmental prerequisite. However, systems of this type are not designed to be scalable and are in fact intended for a potential on-premise niche market in which the largest start-up in the segment, Quantum Brilliance, has invested. These devices, limited in size but with a small number of qubits, can be used for simulations and initial experiments of quantum algorithms in order to estimate the computing resources required for their large-scale implementation.
- Spin-based: qubits correspond to electrons confined in common cavities made of semiconductors (e.g. silicon) and their states to the spin (a particular form of angular momentum) that the electron can be induced to assume. The technology is not dissimilar to that used to make the so-called quantum dots used in the Q-LED TV already on the market - thus, easily scalable - and would require temperatures of 1 to 4 Kelvin to work consistently. Although this is a prototype solution whose

engineering realization remains to be validated in practice, many research centers around the world and Intel itself seem to have recently turned their attention to this technology.

- Topological: the idea is to build quantum logic gates using braided paths (braids) on which quasi-particles (systems of particles behaving as a single entity) such as anions can be addressed. To date, this would be the only solution without potential drawbacks. However, the technology is still highly experimental and there is no concrete evidence that it is actually feasible. Nevertheless, many technology companies, including Microsoft, are investing heavily in it.

There are, however, features common to all realizations: the possibility of initializing the state of a defined set of qubits, of manipulating one or more of them by means of gates that allow a linear transformation of their states (as are the laws of quantum mechanics) and, finally, of subjecting them to measurement after the application of the circuits provided by the specific algorithm.

It is also crucial that these processes take place while maintaining the coherence of the physical system and reducing errors as much as possible. Every element that interferes with the qubits (other particles, heat, noise) can represent a "measurement" of it. In this sense, qubits are said to be "noisy", i.e. they are subject to the loss of their quantum properties, such as superposition or entanglement. Dedicated qubit systems are used to identify possible errors: with the set of physical qubits, they contribute to the creation of "logical" qubits, with a reasonable error correction[16]. Clearly, this is one of the most complex elements to be taken into account for the scalability of these processors and constitutes a special area of study in its own right, involving notions of electronics, connectivity, cryogenics, etc.

3.2.1.2 Adiabatic quantum computer

Quantum annealers are generally considered to be less versatile than universal quantum computers as their use is mainly for solving optimization problems, whereas the logic gate model lends itself to the development of a more generic set of algorithms.

The operating principle of these devices is based on quantum mechanics' prediction that a system, if allowed to evolve slowly, tends to configure itself in a minimum energy state.

As things stand at present, annealers are far more effective than gate-based computers in solving the particular class of problems to which they are dedicated.

3.2.2 A new calculation paradigm

A first advantage of working with qubits configured in superposition of states is that the space of computation, and consequently the number of operations that can be performed, grows exponentially as their number increases, whereas in the classical world this ratio remains constant. In addition, quantum entanglement makes operations on multiple qubits possible by allowing the writing of computing algorithms that exploit their dependencies, without the need for them to be contiguous in the processor and - theoretically - regardless of the actual distance separating them.

[16] The number of physical qubits required for the realization of a logical qubit depends on the type of algorithm, the type of error the specific qubits are subject to, and their connection (the physical elements that enable one or more of them to be connected).

Compared to traditional computation, the distinguishing features of quantum computation are:

- the different approach to problem solving, which, instead of being deterministic in nature, is probabilistic;
- the current degree of reliability of the devices, which is still rather immature when compared to the excellent fault tolerance that classical computers have achieved over time;
- the lack of a predominant engineering standard for hardware construction, i.e. the equivalent of the transistor in the classical world.

It is important to note that even when the underlying technology is mature and completely stable (fault tolerant), quantum computing is not a candidate to replace ordinary computers. The quantum computer (QC) is to be thought of as an extremely powerful coprocessor that can be used to solve specific classes of problems that are - wholly or in part - not addressable today.

More than sixty quantum algorithms[17] produced in the last 25 years are known.

The main application classes are as follows:

- oracle function-based: mainly include search and counting algorithms, the best known of which is the algorithm proposed by Grover[18] and its generalization[19] (QAE – "Quantum Amplitude Estimation"), which allows the approximate counting of the number of objects that satisfy certain conditions within a set. They are frequently found as sub-problems of various use cases in the financial field, such as the estimation of statistical properties of a sample used in Monte Carlo methods (cf. 6.1.1.2);
- quantum physics and biology simulations: algorithms enabling simulations of interactions between atoms in molecules, useful for the study of materials physics and molecular biology (e.g. for research into new materials or drugs);
- optimization: algorithms that search for the best solution to particularly complex problems such as that of the "travelling salesman"[20]; they are used in a wide variety of scenarios (transport, logistics, power distribution, finance or the environment); in quantum annealers, it is possible

[17] For a complete and up-to-date overview of all algorithms, please refer to https://quantumalgorithmzoo.org/ containing details on the technology, where they can be applied and the speed benefits of each.

[18] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, ser. STOC '96, Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, pp. 212-219, ISBN: 0897917855. https://doi.org/10.1145/237814. 237866

[19] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, "Quantum amplitude amplification and estimation," AMS Contemporary Mathematics Series, vol. 305, 2000.

[20] This term refers to a class of graph theory problems, the most typical representation of which is to find the shortest route a travelling salesman should take to visit a number of cities with given distances between them and return home.

to use a class of special variational algorithms[21] that allow approximate solutions to different classes of optimization problems. (QAOA - Quantum Approximate Optimization Algorithms);

- classical mathematical problems known to be computationally intractable: problems for which there is no efficient classical algorithm (i.e. with polynomial resolution times[22]) such as integer factorisation or discrete logarithm calculation;
- Quantum Machine Learning (see box below): a set of classification and learning algorithms that, under certain conditions, may be more efficient than the corresponding classical algorithms currently used.

Quantum Machine Learning (QML)

Machine learning is that branch of artificial intelligence that studies correlations between data and, through the application of algorithms, creates models of reality. In particular, a software "learns" from a given experience if its ability to perform a series of tasks improves through the acquisition and analysis of data derived from that experience[23]. Algorithms are, therefore, "trained" iteratively to be used in different contexts: making predictions, identifying correlations, interpreting different languages and translating them.

Since this type of process requires both high computational resources and the processing of a large amount of data for learning, it is foreseeable that the availability of quantum processors could provide significant advantages for supplementing, improving or making more efficient traditional machine learning models as well as developing completely new ones based on the different computational paradigm.

The integration of quantum technologies in machine learning can translate[24] either into the use of data from quantum sources (e.g. from quantum sensors) in classical or quantum processing, or into the use of quantum algorithms for processing classical data. The latter scenario is currently the one most studies are focusing on[25].

Two areas of research should be mentioned by way of example:

- algorithms solving optimization problems that, in principle, could improve current learning mechanisms (currently estimated to be quadratic or polynomial improvement);

[21] The basic idea of a variational algorithm is to introduce solutions to a problem in parametric form. These parameters are modified in a series of successive iterations in order to achieve, through various techniques, the minimum of the "objective function", i.e. the solution to a given optimization problem. The main characteristic of a variational algorithm is the use of hybrid computational resources aimed at obtaining an approximate solution to the problem. The quantum component is aimed at measuring the state of a parametric circuit, while the classical component minimizes the expected value.

[22] For a problem of size *n,* the time or number of steps required to find the solution is a polynomial function of *n*.

[23] Mitchell, Tom M. "Machine learning". Vol. 1. , bk. 9. : McGraw-hill New York, 1997.

[24] "An Introduction to Quantum Machine Learning for Engineers" - Osvaldo Simeone - https://arxiv.org/abs/2205.09510

[25] Among others: Implementation of Quantum Support Vector Machine Algorithm Using a Benchmarking Dataset: https://inspirehep.net/files/33c812bc465883c2210ab4c4c7cd8a42 and Supervised learning with quantum enhanced feature spaces: https://arxiv.org/pdf/1804.11326.pdf

- the possibility of finding correlations between variables to divide them into classes: recent results show how, for example, certain parameters for clustering[26] data can be estimated more efficiently using quantum algorithms.

An example concerns one of the traditional methods for classification problems, SVM (Support Vector Machine), whose objective is to be able to identify the best boundary separating different classes of data. The best boundary is the one that maximizes the margin, i.e. the distance between the boundary and the nearest points in each class. This calculation is easier when the data is linearly separable. To handle situations where the separation is not linear, the SVM uses a technique called a kernel trick, which maps the data into a higher dimensional space where the separation can become linear. In essence, the kernel allows the data to be processed in an expanded variable space, simplifying the search for the optimal boundary. This mapping method has limitations when the space becomes very large. The application of quantum methods would make it possible to find solutions to optimal problems at dimensionalities otherwise precluded by classical methods.

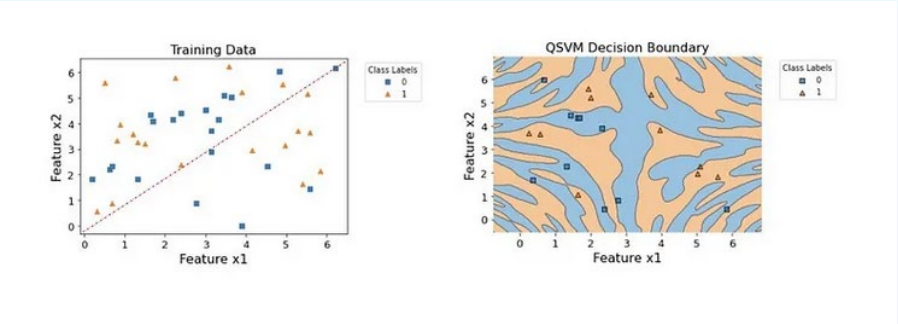


Figure 2 - Simplified example of two-dimensional mapping of two classes of data (squares and triangles) using a quantum algorithm[27]

Underlying the computational advantage offered by these quantum variants of algorithms, compared to their classical counterparts, are often quantum implementations of basic calculation operations (Fourier transforms, matrix multiplications and inversions) that are much more efficient than their classical counterparts[28].

3.3 Quantum Programming

A quantum computing system is characterized by the integration of several layers as described in Figure 3.

[26] An important ML process is to identify patterns and relationships in unclassified data. For this purpose, clustering techniques are used to identify homogeneous groups within a data set. One such clustering algorithm (K-means) works with the aim of minimizing the variance within each cluster. The quantum version would allow an exponential advantage in this calculation.

[27] https://medium.com/be-tech-with-santander/what-is-quantum-machine-learning-qml-1960c83425f4, its code is freely available: https://github.com/jjprietotorres/QuantumML/tree/master

[28] One of the best-known quantum algorithms is the integer factorisation (Schor) algorithm, which exploits a quantum implementation of the Fourier transform (QFT) to solve in polynomial time a problem that would “classically” be intractable.

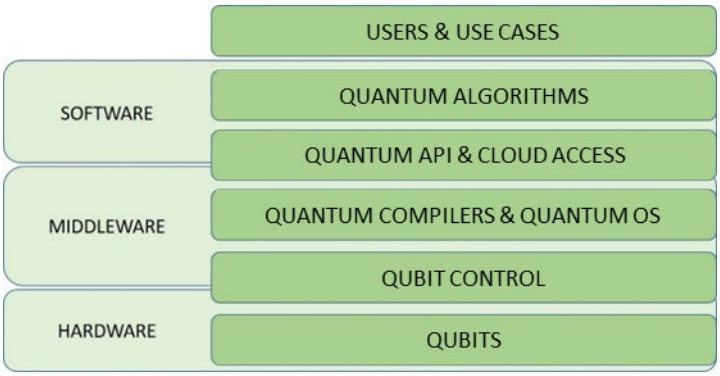


Figure 3 - Quantum computing stack - Strategic Research and Industry Agenda[29]

The qubits are embedded in circuits that provide for their manipulation, connection and control elements. These systems are accessible via basic software that enables the compilation of programs written by users and entered via access to resources usually available in the cloud.

Quantum programming obviously requires a different approach than classical programming. Although specific knowledge is required to exploit concepts such as superposition, entanglement and quantum measurement, we are witnessing the development of increasingly accessible and simplified software frameworks.

3.3.1 Programming approach

The steps for creating programs for use in quantum computers can be summarized as follows:

- problem definition;
- choice of the most convenient algorithm for its solution;
- choice of programming type (cf. 3.3.2);
- code writing;
- code execution in simulators or quantum hardware;
- interpretation of the result.

The traditional approach to programming a quantum computer involves the presence of a classical computer that not only drives a quantum processor, but also processes its solutions to allow the iteration of sub-problems in successive steps.

The architecture is similar to that used in supercomputing centers:

- tasks that are to be executed (jobs) are prepared in a classic computer, in batch mode (scheduled mode);
- jobs are sent to the computer (quantum computer) typically via a service provider (Quantum Cloud Provider);
- results are interpreted on a classical computer (example of Figure 4).

[29] https://qt.eu/media/pdf/Strategic-Reseach-and-Industry-Agenda-2030.pdf

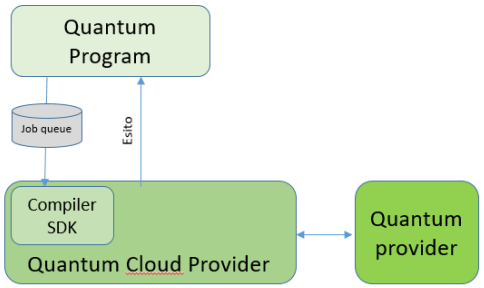


Figure 4 - Approach to programming a quantum computer[30]

Since access to the actual hardware, typically via the cloud, is shared by thousands of users every day, each technology provider normally sets a maximum limit of daily or monthly executions for each user.

For this reason too, the use of a quantum hardware simulator on classical computers is preferable for prototyping or software engineering, since it allows the expected results to be estimated from a real device and the execution to be optimized without having to "consume" access to the quantum hardware. The use of the latter is thus typically relegated to the final stages in which the operation of the application is to be verified.

The use of NISQs, the devices available today with reduced qubits and subject to noise and errors, is based on the repeated execution of the algorithm, which allows the result to be averaged to increase its accuracy.

3.3.2 Quantum programming languages

3.3.2.1 Programming via quantum circuits

Programming based on the construction of "quantum circuits" involves the introduction of a sequence of operations called quantum gates, which in practice can be traced back to mathematical operations. These operations, applied to the individual qubits, change the quantum states of the qubits and their relationships, enabling certain problems to be solved through their manipulation.

In quantum computer programming, measurements are generally performed at the end of the quantum circuit, after all desired gates have been applied. During the execution of quantum operations, the qubit may be in a superposition state, but the final measurement determines the final result in terms of classical bits (0 or 1).

As a result, the development cycle of a quantum computer program follows the classic Build-Compile-Run-Analyze process, but with the peculiarities of quantum computing highlighted so far.

[30] Freely taken from "Quantum Computing Toolkit From Nuts and Bolts to Sack of Tools" - Himanshu Sahu, Hari Prabhat Gupta https://arxiv.org/pdf/2302.08884.pdf

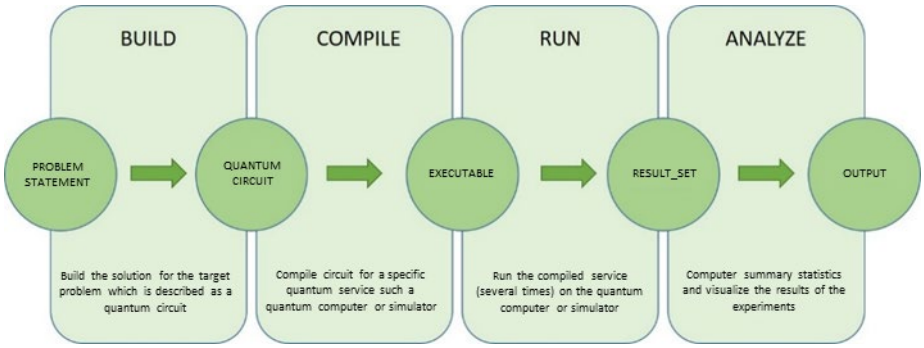


Figure 5 - The quantum development life cycle[31]

Advantages:

- clear "geometric" interpretation of how qubits evolve during the execution of an algorithm;
- control over each applied quantum operation: specific circuits can be designed to meet the requirements of different algorithms;
- gradual construction of the circuit (quantum gates are added one at a time, and the state evolution can be analyzed at each step);
- optimization of specific algorithm performance through increased flexibility.

Disadvantages:

- need a good knowledge of quantum theory and familiarity with linear algebra for understanding interactions.

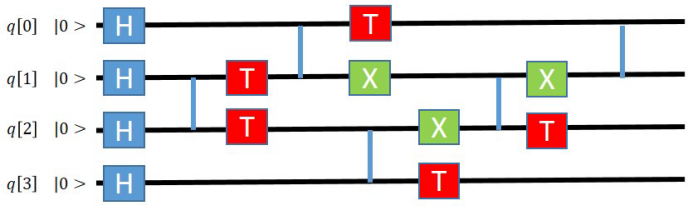


Figure 6 - Example of how a quantum circuit appears graphically: at first, the four qubits are initialized in the |0> state, then various gates are applied (e.g. gate X is the quantum equivalent of the classical NOT operator and transforms the qubit's state from |0> to |1> and vice versa).[32]

3.3.2.2 Programming via high-level languages or Software Development Kit (SDK)

To simplify the programming of quantum computers, libraries have been introduced in recent years to provide a good level of abstraction.

Quantum computing frameworks typically address three areas:

- interface with quantum hardware, provided by the framework manufacturer or others[33];
- simulate executables on classic hardware;
- simplify the development of optimized procedures for quantum computing.

[31] Taken from https://arxiv.org/pdf/2302.08884.pdf

[32] Taken from https://www.redhotcyber.com/post/i-circuiti-quantistici-terza-lezione/

[33] Normally the same SDK is able to interface with different hardware (cf. 4.5.3).

Python is one of the most widely used programming languages, being popular and versatile, easy to learn and equipped with a wide range of libraries and tools available for quantum programming.

Advantages:

- high degree of abstraction that allows programming by non-experts in quantum physics;
- possibility of reusing generic quantum functions in different contexts;
- possibility of integrating classical functionality, allowing for greater interaction.

Disadvantages:

- lack of detailed control over the quantum circuit and its flexibility;
- less efficient implementation than manually optimized circuits by experts.

SDKs can be offered under proprietary or open source licences, and will be briefly described in this report (cf. 4.5.3) only the latter, as they are more widely used and supported by larger communities that evolve them over time.

3.4 Quantum cryptography

3.4.1 Threats to traditional cryptography

Cryptographic mechanisms commonly used to guarantee the confidentiality and integrity of communications involve the combined use of two types of cryptography: asymmetric or “public key” and symmetric or “private key”. In particular, asymmetric cryptography is generally used for the initial exchange of keys that are then used to encrypt data using symmetric cryptography.

The interest in finding further strategies for cryptography, different from those in use, arose with the discovery in 1994, by the US computer scientist Peter Shor, of an algorithm capable of solving the integer factorisation problem whose complexity is at the basis of today's asymmetric key cryptography mechanisms.

Regarding symmetric cryptography, existing algorithms, and in particular the one proposed by Lov Grover in 1966, do not pose a particular risk for its violation: the advantage resulting from quantum computation could easily be curbed by using a longer key[34].

It follows that threats from the availability of quantum computing are directed at the robustness of the asymmetric component of public key cryptography used for key exchange. IT infrastructures and applications rely on solutions (such as RSA - Rivest, Shamir, Adleman or ECC - Elliptic Curve Cryptography) based on this cryptography to guarantee the confidentiality and integrity of data, whether it is transiting between counterparts or stored within data centers.

Cryptographic algorithm	Purpose	Impact availability of QC

[34] Grover's algorithm allows a record in an unordered database to be found in $\sqrt{n}$ steps (the best classical algorithm requires $n/2$). Such an algorithm would reduce the security of symmetric key cryptography by a root factor and would not pose a serious threat to symmetric cryptography at present.

AES-256	Symmetric encryption	Secure
SHA-256	Hash functions[35]	Secure
RSA	Exchange of keys, signature	Violated
ECC	Exchange of keys, signature	Violated
DSA	Exchange of keys, signature	Violated

Table 1 - Security of the main algorithms used in cryptography (source NIST[36])

There are two areas of investigation into alternative solutions to known encryption mechanisms. The first is "post-quantum" cryptography (PQC), based on the use of complex mathematical problems for which there is no quantum algorithm capable of violating security, which would make it possible to make the cipher scheme based on asymmetric keys quantum safe. The second, Quantum Key Distribution (QKD), on the other hand, solves the key exchange problem affecting asymmetric encryption thanks to the possibility offered by the properties of quantum mechanics to guarantee a secure key exchange between two interlocutors. PQC and QKD represent two complementary approaches with a different level of maturity whose use, even in combination, can be envisaged in different scenarios.

3.4.2 Post-Quantum Cryptography

Post-quantum cryptography is the study of cryptographic systems, based on mathematical problems for which no algorithms are known that would make the solution more efficient, such as decomposition into prime factors. The introduction of these mechanisms can be done on classical computers using the already established scheme of public key cryptography and would continue to guarantee confidentiality even in the presence of an attacker who could use quantum computing.

In 2016, NIST, the US standardization body, launched a competition to identify a number of encryption and digital signature algorithms that could be used as standards and initiate the related process (cf. 4.2.3). After a careful selection, also made more stringent by the attack on one of the finalist digital signature schemes[37], four algorithms were identified in summer 2022, three for digital signatures[38] (CRYSTALS-Dilithium, SPHINCS+ and FALCON) and one for encryption (CRYSTALS-Kyber).

Of course, the ultimate goal of PQC is to replace the algorithms currently in use with those that are considered more secure, trying to make the transition as inexpensive as possible. However, the operation is not so simple due to the heterogeneity of the algorithms proposed so far (e.g. they

[35] A hash function is a non-reversible function that maps a string of arbitrary length to a string of predefined length, generally used to verify the integrity of a message.

[36] Getting Ready for Post-Quantum Cryptography: Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms (nist.gov).

[37] "Breaking Rainbow Takes a Weekend on a Laptop" - https://link.springer.com/chapter/10.1007/978-3-031-15979-4_16

[38] However, NIST has declared its intention to reopen the competition for digital signatures because two of the three algorithms are based on lattice mathematics, which makes their robustness more fragile.

differ in the length of the required key). Moreover, their use entails a higher computational cost that may be too much in certain use cases where the frequency of key exchange is high, or in devices with limited hardware capabilities (IoT).

Several software and technology manufacturers are focusing on including the possibility of exploiting such algorithms in their development plans. It should be noted, however, that there are as yet no accepted guidelines at European level for the possible adoption of these standards, although a recommendation has recently been issued[39] (cf. 4.2.3) for the introduction of a shared roadmap for the transition to Post-Quantum cryptography.

3.4.3 Quantum Key Distribution

It is known from information theory that if sender and receiver have a key consisting of a sequence of genuinely random numbers long enough (ideally as long as the message itself), they are able to exchange a message in an "unconditionally" secure manner[40]. The difficulties of this scheme consist precisely in the construction of a random key and its secure distribution, a possibility currently offered by asymmetric key algorithms through the use of the mathematical functions described above, which are vulnerable to the new calculation paradigm.

Quantum Key Distribution (QKD) techniques allow for the secure distribution of random keys, to be used in symmetric encryption by exploiting both the superposition and/or entanglement properties that characterize microscopic systems and the interference role represented by the operation of measuring these physical states.

The subatomic particles most commonly used in this field are those of which light is composed, i.e. photons. These can be easily emitted and transmitted through the optical fibers on which today's network communications are based and detected by specific devices. Information is encoded in particular physical properties of photons such as polarisation (cf. 3.1).

By means of predefined schemes between two previously authenticated interlocutors Alice and Bob, involving, for example, preparation by the sender and measurement by the receiver of the polarisation states of photons, it is possible to make them share a random bit string to be used as an encryption key.

The details[41] of how this can happen can be explored in detail by various sources[122]: in a nutshell, both use polarisers to respectively encode and decode the signal and obtain a key. The latter is extracted from the results of the photon polarisation measurement when both interlocutors use the same basis for the preparation of the photon state (Alice) and its measurement (Bob). These values are random, coincide and are known only to both.

It is important to note that both the communication of the sequence of bases used, as well as the transmission of the signal itself, can take place in an unencrypted channel: any interception would

[39] https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography.

[40] The mathematical demonstration of inviolability is due to Claude Shannon in his article "Communication Theory of Secrecy Systems" (1949).

[41] BB84 represents the first and most widely used working quantum key distribution algorithm, codified and applied on a small scale by the two physicists C. Bennet and G. Brassard in 1984.

be detected due to the fact that, as already pointed out, any attempt to measure the signal would destroy its properties and would be easily recognisable. In fact, the protocol requires Alice and Bob to publicly declare a statistically relevant part of the results of the measurements made to verify that they coincide and that the signal has not been altered.

In practical realizations, a QKD system therefore includes the following components:

- a genuinely random number generator, which can also be obtained by exploiting the random behaviour of quantum variables (cf. 3.5) to produce a random key;
- devices for the emission and detection of single photons;
- a dedicated fiber link to transmit the key (quantum channel);
- a link[42] for the transmission of the encrypted message (classical channel);
- a protocol for processing the key between the counterparts.

The security of the underlying theory of QKD relies on the inescapably stochastic nature of the measurement process in the microscopic world, but the possibility of exploiting this behaviour in practical realizations is linked to the ability to keep the properties of the particles involved inviolate. Consequently, it is easy to understand that current key exchange systems via a direct fiber-optic channel have a limited range due to signal dispersion.

QKD is also demonstrated in satellite communications to achieve considerably greater distances[43] but this type of transmission requires investment on a national or supranational scale.

3.4.3.1 Quantum Communication

The area of quantum communication aims to find hardware, software and protocol solutions to process and exchange quantum information through the network and, in particular, through the light quanta (photons) that are currently commonly used in optical fibers and that can be transmitted through the atmosphere in satellite communication.

The secure information exchange guaranteed by the QKD infrastructure is feasible for point-to-point transmission over limited distances (around 100 km) using solutions already available on the market with a high level of technological readiness (TRL), but challenges remain with regard to integration and interoperability aspects. The use of the QKD scheme described above becomes more complex when dealing with network topologies more articulated than “point-to-point”. The difficulty lies in the impossibility of using intermediate network devices, such as traditional repeaters, which, in manipulating the signal, would interfere with the superposition of states (as would any interference) making the application of the protocol unusable.

[42] Transmission of the key and message data can take place using the same optical channel, but for reasons of interference, the use of a dedicated channel for key distribution is preferable. Coexistence can take place using frequency multiplexing (WDM), time sharing (TDM) or by isolating dedicated fibers (Space Division Multiplexing). It should also be noted that source and receiver need to be authenticated to guarantee the security of the transmission: it is necessary to use pre-shared keys, supplied by the manufacturer, or to use authentication mechanisms based on post-quantum cryptography.

[43] The loss of photons is much lower in satellite transmission than in fiber since they travel mostly in vacuum and are only affected by atmospheric absorption and scattering that occur in the 10 km of atmosphere closest to the earth.

Various technologies are assumed to be used, with different aspects of reliability, security and cost[44]. It is necessary to introduce completely new network elements compared to the equipment commonly used in traditional networks. Research is focusing on different mechanisms to ensure greater distances: trusted nodes (nodes where information is processed and retransmitted), quantum repeaters (based on a combination of entanglement processes) or the use of satellite networks to cover long distances.

The long-term perspective is to be able to realize a quantum communication infrastructure that enables communication to any interlocutor on the planet by exploiting a heterogeneous combination of signal propagation solutions and a multitude of operators spread across the globe.

3.4.4 Post-Quantum Cryptography vs. Quantum Key Distribution

The approaches described in the previous sections have different characteristics and elements of applicability as summarized in the tables below. Their integration into the current security framework should be assessed in a complementary manner.

Post-Quantum Cryptography (PQC)	Quantum Key Distribution (QKD)
Security related to the complexity of mathematical functions, potentially vulnerable when identifying algorithms to do so.	"Unconditional" security, based on the behaviour of particles at the subatomic level.
Requires application changes to software cryptographic calls.	Requires specialized hardware devices, a dedicated fiber connection and interfaces to encryption devices or software.
Does not depend on the transmission medium.	Can only be used via fiber optics or satellite communications.
Costs for identifying and replacing cryptographic calls dependent on the application pool in use.	High costs for setting up the infrastructure for fiber transmission and currently unsustainable for satellite communication.
Not distance-dependent, fully compatible with conventional repeaters.	Communication distance for fiber-optic transmissions limited to about 100 km, need for quantum repeaters, trusted nodes or satellite links for larger-scale transmissions.
Some algorithms require a longer key length.	Standard key length for the symmetric protocol.
Digital signatures or certificates can be used for authentication.	For the exchange of source and receiver keys to be considered trustworthy, they must be authenticated using asymmetric PQC or pre-shared keys encryption.

Table 2 - PQC vs QKD (characteristics)

Post-Quantum Cryptography (PQC)	Quantum Key Distribution (QKD)
General/purposes solution. Some commercial software already has an adoption roadmap.	Suitable solution for very specific use cases such as the protection of connections between processing centers in metropolitan areas.
Security in the short/medium term.	Long-term security.

[44] For an overview see Quantum Key Distribution: A Networking Perspective by Mehic et al.- https://dl.acm.org/doi/abs/10.1145/3402192

Also suitable for signature and authentication algorithms.	Cannot be used for digital signatures.

Table 3 - PQC vs QKD (use case)

It should be emphasized that there is a debate on whether investment in one or the other scenario is appropriate. The NSA, the US national security agency, does not recommend the use of QKD until certain limitations have been overcome (the need to authenticate nodes and the use of dedicated devices that are not available on an industrial scale and with an unconvincing degree of reliability). Even some European agencies, such as the German federal office for information security[45], prefer to maintain a conservative approach to this technology.

In fact, the US government is pushing (cf. 4.3.1.1), to the widespread use of post-quantum cryptography, considering it more cost-effective. The recommendation for the use of the latter algorithms has only recently been formalised by Europe (cf. 4.3.2.6), while China and Russia seem to be oriented towards identifying alternative algorithms to those proposed by NIST .

3.5 Quantum Random Number Generator

The efficient generation of random numbers is of utmost importance in a variety of scientific fields, for instance in carrying out reliable simulations and statistically robust modelling of physical (or econophysical) systems. Also in computer science, in order to guarantee the security of a cryptographic key, it is necessary to ensure its randomness. So-called Pseudo-Random Number Generators (PRNGs) are widely used for this purpose: the actual success of all existing encryption protocols and the success of stochastic simulations such as Monte Carlo simulations depend on them.

Generation of random numbers

Obtaining sequences of random numbers is linked to the use of sources that are capable of generating sequences of bits with high entropy[46]. This is possible by using as a source of entropy the measurement of physical properties of systems that have a non-deterministic time evolution (Figure 7).

In classical computers, however, this source is not easily accessible and this function is realized through programs for generating sequences of numbers (called, in fact, “pseudo-random”) that process input values in a completely deterministic manner. Although very cheap, by their nature these methods have an intrinsic weakness that makes them unsuitable in many contexts, particularly in the use of cryptographic keys.

[45] https://www.squad-germany.de/en/position-paper-on-quantum-key-distribution/

[46] The entropy of a source is defined in information theory (Shannon) as "the expected value of the self-information, i.e. the average information contained in each emitted message". Treating an entropy source as a closed box that generates values, we can see how the amount of entropy it generates is proportional to the information of the bits it emits. A source that emits bits all of the same value has an entropy of 0.

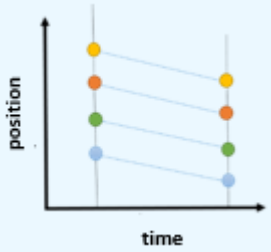


Figure 7 - Deterministic evolution

To improve the quality of random numbers, hardware devices can be used that can convert into a digital signal certain parameters of unpredictable physical phenomena such as those with chaotic evolution (Figure 8) that characterize, for example, turbulent motions in fluid dynamics or meteorological phenomena such that small variations in the initial conditions cause considerable changes in the output.

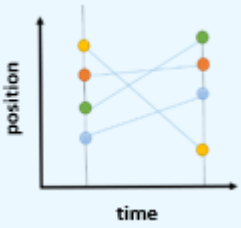


Figure 8 - Chaotic evolution

The output value of such mechanisms cannot be used directly as a random sequence; in fact, techniques are required to remove the bias of the physical source (i.e. the characteristic whereby the probability of observing a given outcome is different from that of another). Moreover, random information sources (entropy sources) of this type, besides not being very efficient, may be subject to attacks that tend to artificially alter their environmental parameters (e.g. temperature) in such a way as to nullify the non-deterministic effects that underlie their operation.

Quantum random number generators (QRNGs), based on the intrinsic indeterminacy of quantum measurements, are the way to obtain that completely unpredictable randomness parameter - the so-called “random seed” - that is needed (Figure 9). They represent a more reliable, faster, and more efficient source of entropy than the available classical generators.

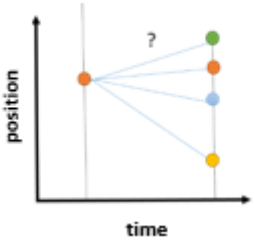


Figure 9 - Random evolution

The earliest QRNGs were based on the process of radioactive decay of certain elements, which unfortunately had the disadvantage of emitting radiation that was harmful to health, limiting its

spread, whereas the most modern devices are based on the use of photons, which are easy and inexpensive to make and can easily be incorporated into practical devices. In particular, unpredictable and equiprobable processes are exploited, for example, the transmission or reflection of photons on a semi-transparent mirror. A photon source (diode or laser) emits photons in superposition of states (each having a 50% probability of being reflected and a 50% probability of being transmitted) towards a semi-transparent surface downstream of which the corresponding value is recorded by two detectors placed in the direction of reflection and transmission.

The sequence of values obtained, suitably translated into binary terms and subjected to techniques to maximize entropy, can be used as the basis for all processes requiring genuinely random numbers.

3.6 Quantum Sensing

The field of quantum sensing cover a range of advanced devices capable of detecting certain values of physical quantities with considerable accuracy by exploiting quantum phenomena. In particular, quantum sensors can be used to measure electromagnetic fields, temperature and pressure with high sensitivity, and their use has already been introduced in different fields of scientific research. In addition to greater accuracy, quantum sensors provide other advantages, such as the possibility of performing non-invasive measurements (especially useful in the field of medical diagnostics) and the speed of measurement (practically real time).

Their basic functioning presents similarities to that exploited in the construction of qubits for quantum processing. For example[47] some of them are based on measuring the properties of atoms or ions confined in a vacuum and cooled to low temperatures, then manipulated by lasers or radiation[48] or on the effects of interaction with single photons.

The main devices on the market are:

- atomic clocks based on the oscillation stability of atoms such as caesium and rubidium;
- magnetometers, gravitometers and thermometers;
- chemical sensors for environmental surveys;
- imaging sensors that use the property of photons and atoms to create high-resolution images of the structure of matter.

Quantum sensors have advantages in many applications such as bio-imaging, spectroscopy, communication, navigation, environmental monitoring, infrastructure monitoring, geographical inspection, and high-energy physics, to name but a few:

[47] https://research.aimultiple.com/quantum-sensors/

[48] For example, when exposed to a magnetic field, isolated atoms and ions within the sensor undergo effects on the distribution of energy levels. These can be detected by laser spectroscopy and allow for the accurate measurement of the magnetic field itself.

- the European Space Agency's Swarm project used[49] quantum magnetometers to create a detailed map of the Earth's gravitational field;
- the US military has planned[50] the use of quantum sensors to improve GPS-based navigation systems;
- researchers at the University of Sussex have developed[51] a quantum sensor capable of intercepting changes in the magnetic properties of tumour cells that could improve diagnostic tools.

Although the maturity level of quantum sensing devices is among the highest in the field of quantum technologies (cf. 4.5.1), no specific applications are known in the banking sector other than the monitoring of environmental parameters, for which there is currently no need for better performance than that provided by classical detectors.

[49] https://earth.esa.int/eogateway/missions/swarm

[50] https://www.iotworldtoday.com/industry/us-air-force-awards-sandboxaq-quantum-navigation-research-contract

[51] https://www.sussex.ac.uk/broadcast/read/55573

4 “Ecosystem” of quantum technologies

4.1 Quantum skills

The nature of the study of quantum technologies is, inevitably, interdisciplinary and requires in-depth knowledge not only in scientific and technical fields (mathematics, physics, computer science and engineering), but, in order to seize opportunities, understand risks, and tackle related projects, these skills must be integrated with economic, social and, at some levels, geopolitical ones. Some analysts[52] estimate that, by 2025, 50% of jobs in the quantum field will remain without candidates due to difficulties in finding people with the necessary skills in the market.

The European Commission promoted the QTEdu[53] project to foster awareness and training in quantum technologies, which, among other things, identifies a competence framework[54] (Figure 10 and Figure 11); such competences are considered strategic for their introduction into the industrial world, also estimating the time needed for their acquisition.

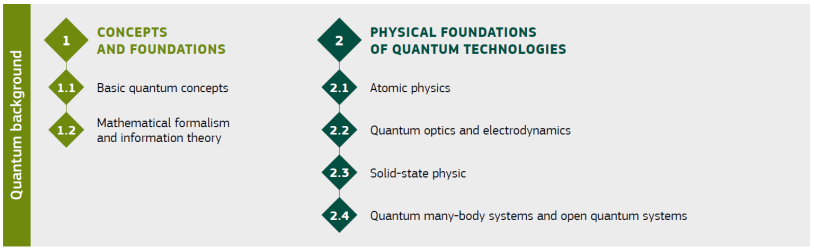


Figure 10 - European Competence Framework for Quantum Technologies - Version 2.0 - Quantum background

[52] https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing

[53] https://qtedu.eu/

[54] Greinert, F., Müller, R. (2024). European Competence Framework for Quantum Technologies 2.5. Zenodo. https://zenodo.org/records/10976836

Figure 11 - European Competence Framework for Quantum Technologies - Version 2.0 - Core device technologies and QT systems and applications.

Major global research centers include the Massachusetts Institute of Technology (MIT)[55], which also offers online courses on the MIT Xpro platform, the Institute for Quantum Computing at the University of Waterloo[56] active since 2002, Harvard University[57] and the Max Planck Society[58]. An overview of the Italian academic offer can be found in section 4.4.3.

Below is a list of events and initiatives that may be useful to broaden one's knowledge of the latest results, learn about the various strategies and create a network of collaboration:

- the QTEdu[53] website where references to resources and initiatives for training at various levels of knowledge and for various stakeholders from primary school onwards are collected;
- different events organized by IEEE[59] (International Conference on Quantum Software and IEEE Quantum Week);
- the annual workshop of CINECA[60] (North East Inter-University Consortium for Automatic Computing) in collaboration with the University of Milan on “High Performance Computing and Quantum Computing”;

55 https://physics.mit.edu/research-areas/quantum-information-science/
56 https://uwaterloo.ca/institute-for-quantum-computing/
57 https://quantum.harvard.edu/
58 https://www.imprs-quantum.mpg.de/
59 https://quantum.ieee.org/
60 https://www.quantumcomputinglab.cineca.it/

- the Observatory of the Politecnico di Milano[61] which includes research activities, opportunities for discussion and in-depth analysis for members and a public conference to present research activities.

Events with greater involvement of industry and commerce:

- events, one of which takes place annually in Europe, of the Inside Quantum Technology[62] company, which provides articles, updates news and produces reports on quantum technologies;
- the Q2B international conference organized by QC-Ware[63] which is a good opportunity to get in touch with both scientific advances and major commercial players.

4.2 Standards

The development of industry standards is of fundamental importance for the spread of technologies and for accelerating the market as they facilitate interoperability between equipment of different vendors by defining interfaces and specifications for the different components. Also for quantum technologies, there are different initiatives to foster standardization at international or local level, with contributions from state or commercial bodies.

Standardization areas are manifold and range from aspects such as enabling technologies to application components.

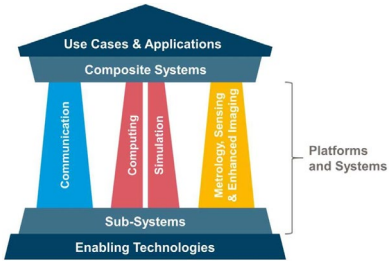


Figure 12 - CEN/CENELEC Standardization Roadmap on QT: 2023-03

The European Union is characterized by the presence of bodies such as ETSI[64] or CEN/CENELEC[65] (a focus group on quantum technologies was established in 2020) that cooperate with other international organizations in the creation of global standards. ISO[66] has a dedicated working group (ISO/IEC JTC 1/WG 14) while IEEE[67] has launched several benchmarking initiatives.

[61] https://www.osservatori.net/it/ricerche/osservatori-attivi/quantum-computing-communication
[62] https://www.insidequantumtechnology.com/
[63] https://www.qcware.com/
[64] https://www.etsi.org/about
[65] https://www.cencenelec.eu/about-cenelec
[66] https://www.iso.org/about-us.html
[67] https://www.ieee.org/about/index.html

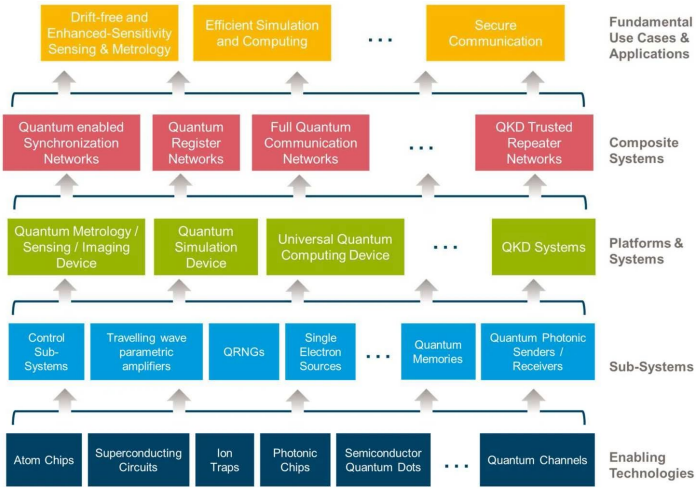


Figure 13: Scope of standard definitions for quantum technologies[68]

4.2.1 Standards for quantum computing

The absence of technology specification standards in this area is a consequence of their low level of maturity and may discourage those considering investing in the adoption of projects involving quantum computing experimentation. In order to reduce the confusion generated by the use of concepts with different meanings and to facilitate communication, a standard (ISO/IEC DIS4879, Information technology - Quantum computing - Terminology and vocabulary) that describes the basic concepts (hardware, software and applications) present in quantum computing is currently being defined.

The following standards are also in the pipeline: ISO/IEC TR 18157 (Information technology - Introduction to quantum computing) which provides an introduction to quantum computing and related technologies, ISO/IEC PWI 18670 (Information technology - Reference framework for quantum computing service platforms), ISO/IEC PWI 18660 (Information technology - Quantum machine learning datasets) which provides a standard benchmark for machine learning algorithms and ISO/IEC PWI 20153 (Quantum Simulation - Taxonomy of quantum simulator architectures and quantum simulation programming).

4.2.2 Standard for QKD

Globally, there is an intense activity aimed at creating standards in the QKD area, despite the fact that this is a relatively new technology. In particular, interest has focused on defining use cases, security specifications and interoperability.

The European Union is present in the standardization work of ISO, IEEE, ETSI and CEN-CENELEC[69]. In particular:

[68] “Towards European Standards for Quantum Technologies” https://arxiv.org/ftp/arxiv/papers/2203/2203.01622.pdf

[69] https://www.iso.org/committee/10138914.html, https://quantum.ieee.org/, https://www.etsi.org/technologies/quantum-safe-cryptography, https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/quantum-technologies/

- ISO/IEC 23837: Security requirements, test and evaluation methods for quantum Key Distribution (2023) - the standards are divided into two main parts. The first part specifies the basic functional requirements and the shared set of tests and evaluation methods for QKD. In particular, the network and quantum optics standard components and the techniques for implementing a QKD protocol are explained. The second part specifies the tests and methods for assessing the security requirements and implementations mentioned above;
- ETSI GS QKD 014: Protocol and data format of REST-based key delivery API - specifications for communication between clients and QKD modules for the use of keys generated via quantum distribution protocol.

4.2.3 Standardization of post-quantum algorithms

In December 2016, NIST initiated a standardization process[70] of cryptographic algorithms capable of withstanding quantum computer-based attacks, launching an international competition open to applicants from companies and research institutions around the world.

NIST Post-Quantum Cryptography Standardization

The deadline for submitting applications, 82 in this first phase (Table 4), was initially set for 30 November 2017. Analyses of the applications were publicly discussed and deepened through the PQC forum, involving 1300 members from all over the world. After only three weeks, the community compromised 12 schemes while a thirteenth was discarded due to shortcomings in the admission requirements. In December 2017, the remaining 69 candidates were officially admitted to the competition.

NIST Post-Quantum Cryptography Standardization

Call for Proposal - First Round

- 82 total submissions received
  - 23 signature schemes
  - 59 Encryption/KEM schemes

	Signatures	KEM/Encryption	Overall
Lattice-based	4	24	28
Code-based	5	19	24
Multi-variate	7	6	13
Hash-based	4		4
Other	3	10	13
Total	23	59	82

Table 4 - Proposals received by NIST classified by type

From 11 to 13 April 2018, the first “NIST Workshop on PQC Standardization” was held in Fort Lauderdale, where the 69 candidates were presented and publicly discussed. The candidates admitted to the competition involved 263 researchers from 24 different countries, including Italy. The evaluation of all candidates began immediately after the announcement of their admission and lasted for over a year. It was conducted by NIST, but with the fundamental contribution of the international community, which independently analyzed all the candidates and shared the results of the analyses via a public mailing list made available by NIST.

[70] https://csrc.nist.gov/News/2016/Public-Key-Post-Quantum-Cryptographic-Algorithms

More than a year later, on 30 January 2019, NIST announced 26 candidates admitted to the second round of the competition. Among them, eight see the involvement of Italian researchers, namely: BIKE, Classic McEliece, CRYSTALS-KYBER, HQC, LEDAcrypt, NewHope and SIKE for encryption and key exchange, as well as Picnic for digital signature. LEDAcrypt is the only one entirely developed by Italian researchers.

In August 2019, a second workshop was held where the remaining candidates were resubmitted and reanalyzed. With the start of the second evaluation round, NIST once again asked the international community to focus on this small group of 26 proposals, which were subjected to further analysis for about a year in order to further verify their security and, at the same time, study their performance on real systems.

The second round ended in July 2020. The algorithms chosen as finalists for the third round were Classic McEliece, CRYSTALS-KYBER, NTRU and SABER for encryption and CRYSTALS-DILITHIUM, FALCON and Rainbow for digital signature. In addition, eight alternative candidate algorithms also entered the third round: BIKE, FrodoKEM, HQC, NTRU Prime, SIKE, GeMSS, Picnic and SPHINCS+.

The third and final round closed in July 2022. The selection process identified the official algorithms for standardization (CRYSTALS-Kyber for encryption and CRYSTALS-DILITHIUM, FALCON and SPHINCS+ for digital signature), as well as a set of alternative algorithms that will continue to be evaluated in a fourth round.

In addition, four of the candidate alternative key-creation algorithms have passed to a fourth evaluation phase: BIKE, Classic McEliece, HQC and SIKE. These algorithms are still being evaluated for future standardization, although some - such as SIKE - have already been deemed insecure.

Many of these post-quantum cryptographic algorithms require larger key sizes than commonly used classical algorithms and also require consideration of computational efficiency, signature size and other parameters[71].

The algorithms being standardized are CRYSTALS-KYBER for encryption and CRYSTALS-Dilithium, FALCON and SPHINCS+ for digital signature. Of the latter, NIST recommends the use of CRYSTALS-Dilithium as the main algorithm and FALCON for applications requiring smaller signatures. SPHINCS+ is less efficient than the other two but was included because it is based on different mathematical problems from the other three.

In the future, NIST will publish a new call for proposals for public key digital signature algorithms to increase and diversify its signature portfolio.

[71] The cryptographic systems proposed for selection by NIST are based on lattices, error-corrected codes, multivariate polynomials, hash functions and isogenies with advantages and disadvantages. For instance, code-based cryptographic algorithm families have a long history of “public” verification, whereas lattice-based cryptography offers extremely fast algorithms but the larger data size involved could prove problematic. NIST, therefore, has moved towards standardizing different algorithms to make their use flexible depending on the context.

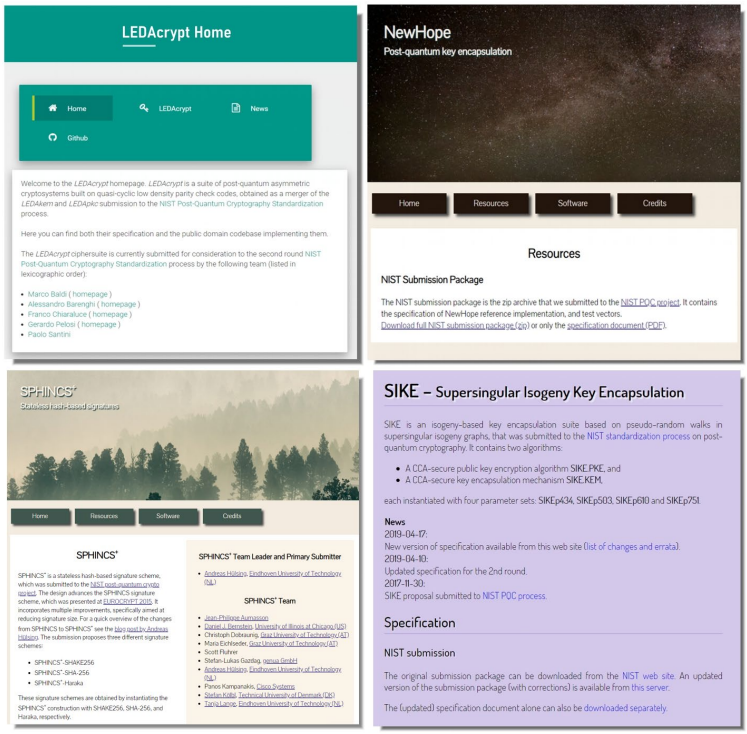


Figure 14: Homepages of some of the still competing encryption schemes

4.3 Institutions

4.3.1 The international context

Much of the global investment in quantum technology research and deployment is made by the public sector and is steadily increasing: more than 30 nations are actively involved in quantum technologies and two-thirds of these nations have formulated an official quantum policy. The public sector's interest is due to an awareness of the need to secure critical national infrastructures from possible cyber attacks, which are increasingly based on innovative technologies.

According to estimates by QURECA[72] also reported by the World Economic Forum[73], the publicly financed investment in quantum technology research and development amounts to a total of EUR 40 billion spread over different time horizons.

[72] https://www.qureca.com/quantum-initiatives-worldwide-2024/

[73] https://www3.weforum.org/docs/WEF_Quantum_Economy_Blueprint_2024.pdf

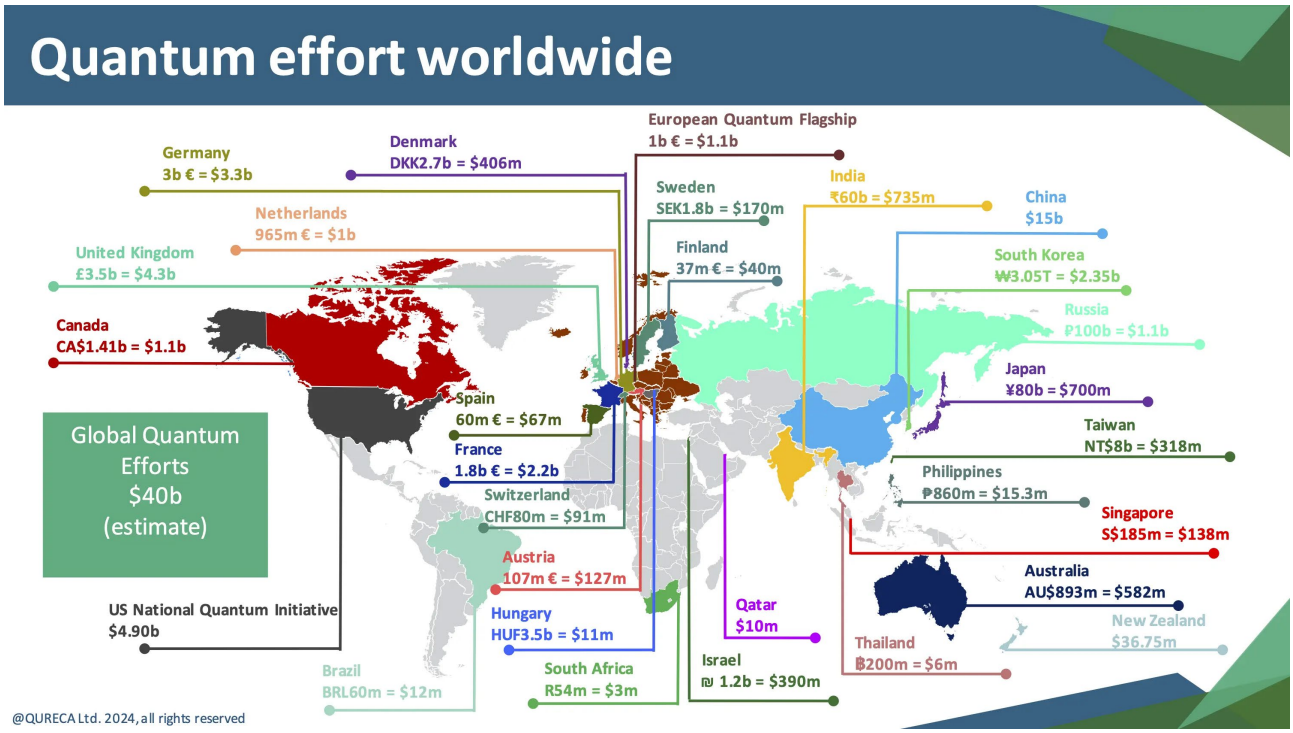


Figure 15: public investment in quantum technologies[74]

Several countries have defined a national strategy for quantum technologies, allocating specific funds. A brief summary of some of them can be found in section 8.1.

What all these initiatives have in common is the funding of research and development activities, collaboration with industry, technology and infrastructure providers, international collaboration through the establishment of bilateral or multilateral partnerships, and academic training to nurture human resources prepared in the coming decades to face the challenges of the quantum world.

4.3.1.1 The US strategy

Among the most noteworthy initiatives is the Biden administration's call to prepare for the adoption of the PQC algorithms announced by NIST in July 2022. In December 2022, the US president signed the “Quantum Computing Security Preparations Act”, which sets out a series of obligations for federal agencies to prepare their transition to post-quantum cryptography with a stringent roadmap[75].

US National Quantum Initiative
America launched its quantum technology strategy in 2018 with the National Quantum Initiative Act - NQIA, which provided for an appropriation of more than $1.2 billion for an initial five-year period, to which were added the allocations established by the various investment plans defined in the other spending initiatives. Subsequently, the NQIA was supplemented or amended by other pieces of legislation in view of the implications of quantum technologies in the commercial and defence fields. The goal of the National

[74] "Overview of Quantum Initiatives Worldwide 2024", QURECA 1 April 2024, https://www.qureca.com/quantum-initiatives-worldwide-2024/

[75] Memo-on-Migrating-to-Post-Quantum-Cryptography, Executive Office of the President, november 2022

Quantum Initiative is to accelerate research and development in quantum technologies for the economic and national security of the United States, also involving the civil, defence and intelligence sectors.

As also reiterated in Executive Order 14073 signed by president Biden in May 2022, the initiative overall involves all federal governments and provides a framework for strengthening and coordinating these activities among US Departments and agencies, private industry, and the academic community.

Research activities are carried out by the agencies mentioned in the aforementioned legislative acts, such as, for example, the National Institute of Standards and Technology (NIST), the National Science Foundation (NSF), the Department of Energy (DOE), the National Aeronautics and Space Administration (NASA), and the Department of Defence (DOD).

In addition to the Executive Order already mentioned, in May 2022, president Biden also signed a National Security Memorandum describing the actions to be taken by the federal government to adopt PQC cyber security to defend against quantum cryptography threats, in line with the four standards approved by NIST in July 2022. In this context, NIST was also tasked with implementing a PQC migration project for the federal government and industry.

In the context of US directives, it is also necessary to mention the Executive Order of 2023 by which the Biden administration banned US investments in sensitive Chinese sectors, including quantum technologies.

4.3.2 The European context

In Europe, the Netherlands, Germany, France, Denmark and Ireland have defined a national strategy, Spain and Sweden are launching theirs, while other countries have investment programmes dedicated to quantum technologies (e.g. Austria). According to the latest McKinsey report[76] on public investment in quantum technologies, Germany has allocated the most funds in 2022, followed by France, the EU and the Netherlands.

The European Commission[77] has promoted investments to launch several long-lasting initiatives (among the main “Quantum Flagships”[78], EuroHPC, EuroQCI) and a specific competence center (ECCC) to coordinate the different initiatives between research institutes, industry and public bodies.

In February 2023, a strategy document[79] related to the development of quantum technologies in Europe was published with the aim of harmonizing roadmaps and goals for science and industry. The document envisages some medium and long-term goals to ensure reliable and available solutions for the entire system.

4.3.2.1 Quantum Flagship

European Quantum Flagship is a European Union initiative to promote research and development in the field of quantum technologies. Launched in October 2018, it aims to consolidate and

[76] https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20technology%20sees%20record%20investments%20progress%20on%20talent%20gap/quantum-technology-monitor-april-2023.pdf

[77] https://digital-strategy.ec.europa.eu/en/policies/quantum

[78] https://qt.eu/about-quantum-flagship/

[79] https://qt.eu/media/pdf/Strategic-Reseach-and-Industry-Agenda-2030.pdf?m=1707900786&

coordinate research efforts across Europe to accelerate progress in quantum technologies and foster European leadership in this emerging and strategic field.

With a budget of EUR 1 billion and a time horizon of 10 years, research is being funded on various aspects of the quantum field: sensing, communications, computing and simulation. Through the introduction of work programmes, collaboration between research organizations, universities, companies and government institutions from various European countries is planned, in order to make the most of the expertise and resources available in Europe and to promote innovation in quantum technologies.

4.3.2.2 ECCC

The European Cybersecurity Competence Centre (ECCC) aims to increase Europe's cyber security capabilities and competitiveness by working with a network of National Coordination Centres (NCCs) to build a strong cyber security community. Headquartered in Bucharest, it will develop and implement, together with Member States, industry and the cyber security technology community, a common agenda for the development of the technology and its wide deployment in areas of public interest and in businesses, especially SMEs.

The ECCC will also have the task of directing strategic investments by making EU resources, and indirectly industry resources, available to Member States to enhance and strengthen cyber security capabilities. The Centre will play a key role in the realization of the cyber security objectives of the Digital Europe Programme[80] and the Horizon Europe programme[81].

4.3.2.3 EuroQCI

The European Commission is working with the 27 EU Member States and the European Space Agency (ESA) to design, develop and deploy a secure and efficient quantum communication infrastructure throughout the Union, the European Quantum Communication Infrastructure (EuroQCI). The aim is to protect sensitive data and critical infrastructure by integrating quantum systems into existing communication infrastructures and provide an additional layer of security based on quantum physics.

The EuroQCI will consist of a terrestrial segment, based on fiber-optic communication networks, connecting strategic sites at national and cross-border level, and a space segment based on satellites. It will be an integral part of IRIS2, the EU's new secure space communication system.

The project started in 2019 and is financed with EUR 1 billion over a 10-year time horizon.

4.3.2.4 EuroHPC

The EuroHPC (European High Performance Computing) project is the cornerstone of the European Union's industrial strategy in the field of supercomputing and data processing. EuroHPC provides funding for innovative projects with the dual aim of developing a pan-European supercomputing infrastructure and supporting cooperation in advanced scientific research in order to increase industrial competitiveness and ensure Europe's technological and digital autonomy.

[80] https://digital-strategy.ec.europa.eu/en/activities/digital-programme

[81] https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

The quantum component of the project will be financed with EUR 1.5 billion until 2027, out of a total of EUR 5 billion.

In October 2022, six European sites (including CINECA, Italy) were identified that will host quantum computers built with different technologies. This represents the first step towards the construction of a European quantum computing infrastructure that is intended to be accessible to academia and industry for the collective growth of the union.

4.3.2.5 OpenQKD

OpenQKD (Open Quantum Key Distribution) is a European initiative that aims to develop and implement quantum key distribution (QKD) technologies in an open and interoperable way. The team is multidisciplinary and includes leading European telecommunications equipment manufacturers, end users, critical infrastructure providers, network operators, QKD equipment suppliers, digital security professionals and scientists from 13 EU countries.

4.3.2.6 Post quantum cryptography in Europe

The European Commission has only very recently commented[82] on the use of post-quantum algorithms. In particular, through a specific recommendation:

- invites Member States to migrate their current digital infrastructures and services for public administrations, as well as other critical infrastructures, to post-quantum cryptography as soon as possible;
- encourages Member States to develop a comprehensive strategy for the adoption of post-quantum cryptography in order to ensure a coordinated and synchronized transition between different Member States and their public sectors;
- indicates the need to follow a roadmap containing a list of actions to be undertaken by Member States with a clear timetable for the different stages and targets to be reached;
- encourages Member States to work closely at EU level with the Union's cyber security experts, the NIS Cooperation Group and the European Union Agency for Cyber Security (ENISA) on the evaluation and selection of suitable post-quantum encryption algorithms and their adoption as EU standards for harmonized implementation throughout the Union;
- immediately after the publication of this recommendation, Member States are invited to set up a sub-group on post-quantum cryptography in accordance with Commission implementing decision (EU) 2017/179 and to appoint expert representatives who should work in close cooperation with the Commission and be in charge of defining and elaborating the roadmap for the coordinated implementation of post-quantum cryptography with a time limit of two years from the publication of the recommendation.

Among the countries of the old continent, there are no public initiatives of note, other European institutions had published specific recommendations such as the German Federal Office for

[82] https://digital-strategy.ec.europa.eu/en/news/commission-publishes-recommendation-post-quantum-cryptography

Information Security, which in 2021 issued a document of recommendations[83] addressed to public and private companies, referenced by the European Commission itself[84].

4.4 The national context

Italy boasts several research centers active in the field of quantum technologies. Universities and research institutes follow advanced research fields in both quantum computing and security. Of particular note are La Sapienza in Rome (photonic qubits), the University of Padua (trapped ions), the Federico II University (superconducting qubits), CINECA (experimentation of the Pasqal processor and hybrid solutions to exploit quantum computation as an accelerator of classical computation) and INRIM (creation of a national quantum network).

The report of the Politecnico di Milano Observatory on 2023[85] shows that the funds allocated in our country by the public sector (EUR 140 million for the three-year period 2023-2025) appear to be largely insufficient not only in comparison to the allocations of North American countries and China, but also in comparison to those of other European countries (billions in ten-year time horizons, cf. Figure 15).

In Italy, moreover, according to the Observatory's estimates, there is a limitation of investment (around EUR 6 million) in the private sector where one is confronted, with greater prominence in the last year, with the allocation of limited human resources and budgets without a medium-to-long-term strategy.

4.4.1 Public sector initiatives

The National Recovery and Resilience Plan (PNRR) is divided into seven missions[86]. Under the “From research to business” component of mission 4 “Education and Research”, the PNRR allocates EUR 1.6 billion to establish national research centers on topics of strategic importance, including simulations, high-performance computing and data analysis, agritech, gene therapy and drug development with RNA technology, sustainable mobility and biodiversity[87]. The national centers are aggregations of universities, research bodies and companies, organized in a “hub and spoke” structure, with the hub being responsible for management and coordination activities and the spokes for research.

[83] https://www.bsi.bund.de/EN/Topics/Crypto/Cryptography/PostQuantumCryptography/post_quantum_cryptography_node.html

[84] ENISA, Post Quantum Cryptography Study, october 2022

[85] The “Quantum Computing & Communication” Observatory of the Politecnico di Milano qualifies as “a pre-competitive reference point on the subject at the Italian level, involving a community of interested companies, the demand and supply side of technology, and experts at the Italian and international level”.

[86] “Digitalization, Innovation, Competitiveness, Culture”, “Green Revolution and Ecological Transition”, “Infrastructure for Sustainable Mobility”, “Education and Research”, “Inclusion and Cohesion”, “Health”, “RePowerEU”.

[87] “PNRR and quantum computing: EUR 320 million for the national center on supercomputing” (osservatori.net)

Name National Centre	Proponent	Hub Headquarters	Number of Total Participants	Number Universities-public research bodies-research organizations	Number of Companies	Financing granted (in euro)
National Centre for HPC, Big Data and Quantum Computing	National Institute of Nuclear Physics (INFN)	Casalecchio di Reno (BO)	49	34	15	319.938.979,26
National Research Centre for Agricultural Technologies (Agritech)	University of Naples Federico II	Naples	46	32	14	320.070.095,50
Sustainable Mobility Center (National Center for Sustainable Mobility - CNMS)	Politecnico di Milano	Milan	49	25	24	319.922.088,03
National Biodiversity Future Center - NBFC	National Research Council (CNR)	Palermo	48	41	7	320.026.665,79
National Center for Gene Therapy and Drugs based on RNA Technology	University of Padua	Padua	49	32	17	320.036.606,03

Figure 16: taken from the MUR statement[88]

In particular, the PNRR envisages an investment of EUR 320 million over three years for the creation of a National Center for HPC, Big Data and Quantum Computing; 34 universities and public research bodies and 15 companies are involved in the project. Spoke 10[89], dedicated to quantum computing, envisages an investment of EUR 30 million.

Below are some initiatives worthy of interest.

The National Quantum Science and Technology Institute[90] (NQSTI) is a consortium consisting of 20 Italian research centers, universities and high-tech industries that fosters collaboration between entities conducting research in the field of quantum science and technology in Italy. The NQSTI coordinates funds amounting to EUR 116 million from one of the investments of mission 4 “Education and Research” - Component 2 “From research to enterprise” dedicated to “Partnerships extended to universities, research centers, enterprises and financing” in the field of quantum science and technology.

CINECA's Quantum Computing Lab is an initiative to develop quantum computing tools for information processing and calculation[91]. Currently, CINECA does not have a quantum computer, but has decided to supplement its high-performance computing offer with quantum computing

[88] https://www.mur.gov.it/it/news/mercoledi-15062022/pnrr-nascono-i-5-centri-nazionali-la-ricerca
[89] https://www.supercomputing-icsc.it/spoke-10-quantum-computing/
[90] https://nqsti.it/
[91] https://www.quantumcomputinglab.cineca.it/

resources, either through hours of computing on quantum machines in the cloud or through classical HPC resources that can emulate quantum computing.

The QUID (Quantum Italy Deployment) project is the Italian implementation of the European Quantum Communication Infrastructure (EuroQCI), promoted by the European Commission with the aim of creating a European infrastructure for quantum communication. The project aims to develop nodes in metropolitan quantum communication networks (QMAN), interconnected through the Italian Quantum Backbone, an infrastructure that covers the Italian territory and distributes standard time and frequency signals using commercial optical fibers[92].

4.4.2 Private sector initiatives

In Italy, the field of quantum technologies is still limited to a few realities, despite the fact that some of them have received international recognition, some examples of which are given below:

- Telsy is the cybersecurity and encryption competence center of TIM Enterprise which, together with its subsidiary QTI Quantum Telecommunications Italy, provides end-to-end encryption systems compatible with today's telecommunications infrastructures for private, government and military applications;
- LevelQuantum is a start-up that exploits quantum technology in the field of cyber security. The start-up was recently selected by NATO in its DIANA (Defence Innovation Accelerator for the North Atlantic) acceleration programme, which aims to promote various innovative technologies;
- QBrain is a start-up that develops and provides quantum software solutions for companies, making use of an artificial intelligence engine designed to optimize both quantum algorithms and hardware;
- G2Q Computing is a start-up specialized in scientific computing, developing advanced hybrid (quantum/classical) applications to solve complex problems and improve performance.

To be highlighted in this context are all the public and private funding initiatives made accessible by innovation incubators, such as the Politecnico di Torino's I3P, the Politecnico di Milano's PoliHub and the Italian network of Business Incubation Centers of the European Space Agency. Incubators provide strategic consulting, coaching, mentoring and fundraising support.

4.4.3 The academic offer

Several Italian universities have set up masters or PhD courses in quantum technologies, also in collaboration with research organizations and foundations. In particular:

- the Federico II University of Naples has activated the master's degree course in Quantum Science and Engineering (duration two years) with the aim of training experts in quantum technologies with multidisciplinary skills (from physics to computer science, from electronic engineering to information and communications engineering). Studies can then continue with the three-year PhD Quantum Technologies, activated at the University in consortium with the CNR in Florence and the University of Camerino;

[92] https://www.quantumlab.it/avvio-progetto-quid-quantum-italy-deployment/

- the Politecnico di Torino offers a master's degree course in Quantum Engineering with the aim of providing a multidisciplinary preparation, with particular reference to three application areas: computation, communication and quantum sensing. The Politecnico has also launched a Master's degree of level II in Quantum Communication and Computing in 2022 in collaboration with the National Institute of Metrological Research and the LINKS Foundation[93];
- the Politecnico di Milano launched in the autumn of 2022 a two-year master's degree course in High Performance Computing Engineering, with the aim of providing a solid background in the main computer technologies and architectures for supercomputing, quantum computing and mathematical-statistical modelling of complex problems;
- the Master of Optics and Quantum Information, now in its eighth edition, the first in Italy and one of the first in Europe, is active at La Sapienza University in Rome. At the university there is the Quantum Computing Lab dedicated to the study and experimental realization of computation protocols with photonic systems. The university also leads EPIQUE, a research project funded with 10 million euros by the European Commission and carried out by 18 partners from 12 countries (including the National Research Council and the University of Florence), which aims to study in depth the potential offered by the development of photonic quantum computing platforms and to realize a European photon-based quantum computer;
- Ca' Foscari University of Venice offers a master's degree course in Engineering Physics with a focus on Quantum Science and Technology and has activated a first-level master's degree course in Quantum Machine Learning with the aim of delving into quantum computing topics, with a multidisciplinary approach involving expertise in quantum computing, machine learning, statistical mathematics, physics, computer science, economics and finance;
- the University of Trieste in cooperation with the International Center for Theoretical Physics (ICTP) has launched the two-year master's degree course in Scientific and Data-Intensive Computing with a focus on high performance computing, scientific computing and quantum computing;
- the University of Trento within the Q@TN consortium has launched a three-year PhD in Quantum Science and Technologies with strong interdisciplinary aspects (physics, mathematics, computer science, engineering). The University of Trento, the Bruno Kessler Foundation, the National Institute of Nuclear Physics and the CNR participate in the Q@TN consortium;
- the University of Pavia has activated a study address in the Physics of Quantum Technologies as part of the master's degree course in Physical Sciences, characterized by a high level of interdisciplinarity (mathematics, information science, bioinformatics, chemistry, electronic and communications engineering), combining the more experimental and technological

[93] LINKS is a Foundation established through an agreement between Compagnia di San Paolo and Politecnico di Torino that has been working for more than 20 years at national and international level in the field of digital transformation with applied research, innovation and technology transfer activities. https://linksfoundation.com/

aspects with the more theoretical ones. Two profiles are defined in the address, one more fundamental/theoretical and one closer to applications.

4.5 The market and technology offer

4.5.1 Diffusion, maturity and prospects of quantum technologies

The maturity of quantum technologies is a topic that deserves a dedicated in-depth study in order to provide concrete elements in a scenario that is often confused by different news and statements (cf. Figure 17).

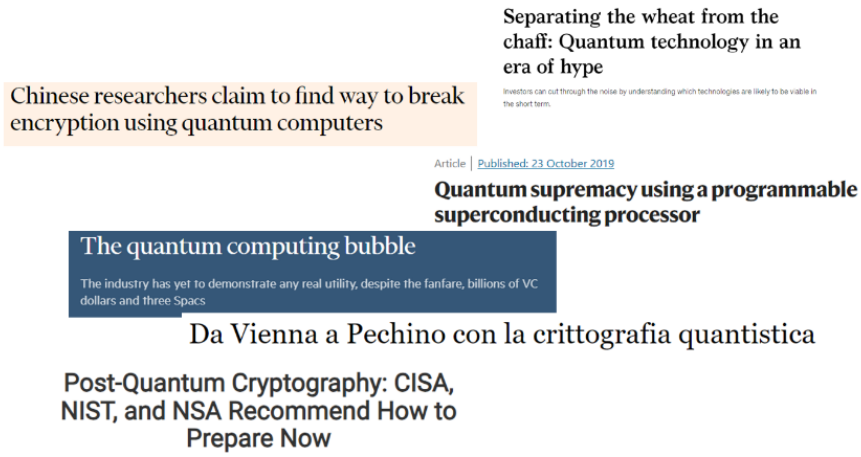


Figure 17 - Collage of some headlines from popular online newspapers

Analysis over time of the number of scientific publications, patents, private investments and start-ups shows an exponential trend over the last decade and suggests opportunities for investment in this area.

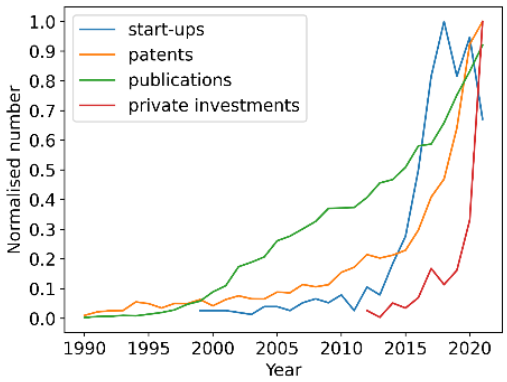


Figure 18 - Trend of different “quantum readiness” indicators[94]

Major elements in favour of the emergence of these technologies in the near future can be summarized as follows:

[94] Building a quantum-ready ecosystem, Abhishek Purohit, Maninder Kaur, https://arxiv.org/abs/2304.06843

- analysts' forecasts, which, albeit with large deviations on some estimates, indicate a gradual increase in investments in these sectors; some[76] estimate overall market growth to reach $106 billion by 2040, a third of which will come from public investment;
- the attention of institutions in the international context with substantial allocations of funds, projects and publications of national strategies;
- the numerous research and experimentation initiatives in all the areas described;
- the issuing of standards;
- the dissemination of business models for the sale of devices and products.

To assess technological maturity, reference is commonly made to the TRL (Technology Readiness Level) scale, known from the world of aeronautics, and uniformly used[95].

Some authors[94], using data from industry conferences, assessments and roadmaps have produced a graph (Figure 19) of the status of the various technologies and the time horizon required to reach level 9.

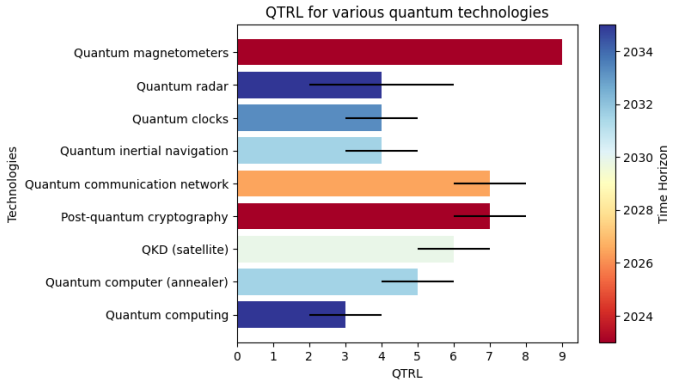


Figure 19 - Quantum TRL and time expectations for different quantum technologies

Although there are subjective aspects to these evaluations, one general finding is that there is an uneven offering where some components (particularly in sensing and communication) represent a higher level of maturity than others. For quantum computing, as repeatedly described, considerable efforts are still needed to overcome the challenges posed by reliability, error correction capability and scalability. For the components of quantum key distribution, quantum random number generators and quantum sensing, on the other hand, there are various apparatuses on the market capable of responding to different needs, thanks also to the role of system integrator offered by many players, especially in the telecommunications sector.

[95] A. Olechowski, S. Eppinger, N. Joglekar, and K. Tomaschek, "Technology readiness levels: Shortcomings and improvement opportunities" Systems Engineering, vol. 23, 03 2020. The first four levels of this scale (ranging from 1 to 9) refer to research phases and laboratory experiments, 5 and 6 to the presence of prototypes, and 7 to 9 to market introduction phases with testing and certification at various levels.

4.5.2 Quantum Computing

The currently available devices are realized through a limited number of qubits, with few interconnections and without an efficient error-correction mechanism, and can therefore perform a limited number of operations.

In the following figures, many of the vendors and research labs that fall under this umbrella are represented, broken down by different technologies.

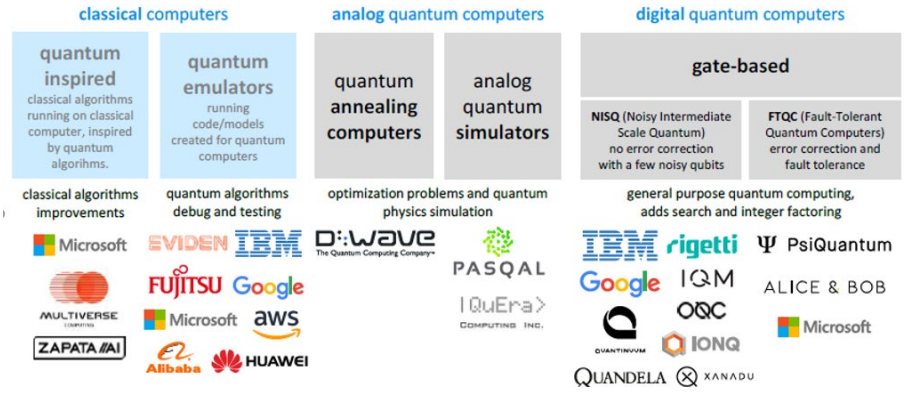


Figure 20 - Different players by technology offering[96]

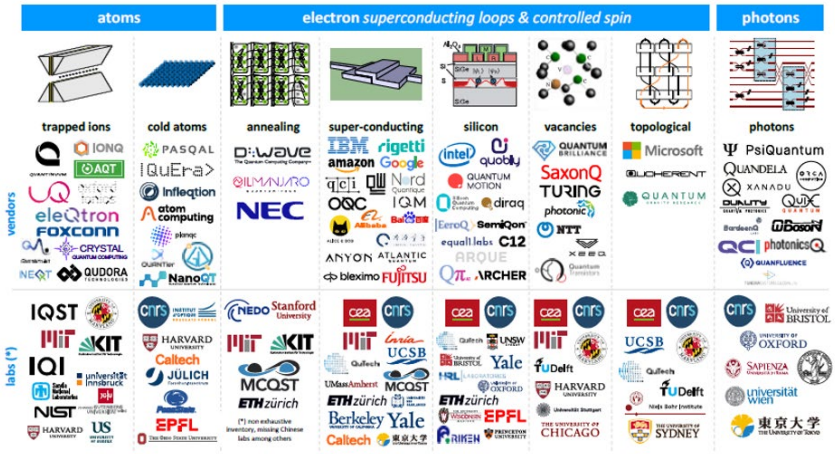


Figure 21 - Map of research laboratories and commercial vendors by qubit technology used[97]

In general, the number of qubits is used as a unit of measurement to represent the state of progress of the various solutions, but the comparison is made difficult by the presence of other variables (frequency of errors, mode of communication between qubits, etc.).

Quantum computing is, mainly, made available in the cloud by the manufacturers themselves such as IBM or D-Wave or offered by service providers such as Amazon or Google.

Below are, by way of example, some of the offers available at the time of writing:

[96] Taken from Olivier Ezratty “Understanding quantum Technologies – 2023” cc

[97] Taken from Olivier Ezratty “Understanding Quantum Technologies” (in turn updated by Gabriel Popkin in Science Mag, Dec. 2016)

TECHNOLOGY QUBIT	PROD	WEB AVAILABILITY	SDK	NOTES
Superconductors	IBM	https://docs.quantum.ibm.com/start/setup-channel#ibm-quantum-platform	QisKit	Processor availability 16 qubit free / 100 qubit paid
Superconductors	Google	https://quantumai.google/cirq/	Cirq	Simulator and interface to various hardware
Ion trap	Alpine QT	https://www.aqt.eu/qc-systems/	AQT API	Free simulator, paid hardware
Annealer	D-Wave	https://cloud.dwavesys.com/leap/signup/	Ocean	Cloud service for D-Wave
Different technologies	Azure	https://azure.microsoft.com/it-it/products/quantum	Q#	Interface to different hardware manufacturers
Different technologies	Amazon	https://aws.amazon.com/it/braket/	Amazon braket Python SDK	Interface to different hardware manufacturers - simulators available free of charge

4.5.3 Quantum Programming

The most important frameworks for quantum programming are briefly described below.

Qiskit [98]

One of the most popular frameworks, developed by IBM in Python. To date, the community supporting Qiskit is estimated to be the largest of all quantum programming frameworks.

It offers the possibility of:

- build circuits also by exploiting an extensive library of quantum algorithms for solving a variety of problems, including optimization, machine learning and cryptography;
- simulate quantum circuits on classical computers to test their circuits before running them on real quantum hardware;
- access to quantum hardware via IBM's quantum computers located in various data centers, as well as hardware from many other suppliers;
- use error mitigation mechanisms through a variety of tools.

Q# [99]

SDK initially introduced for the Azure Quantum service, it has since become hardware agnostic and open source. Q# is an autonomous language that offers a higher level of abstraction than the other frameworks considered. It is possible to write a program with a level of abstraction that does not

[98] https://qiskit.org/

[99] https://learn.microsoft.com/it-it/azure/quantum/overview-what-is-qsharp-and-qdk

consider circuits and qubits but only operations and expressions as in a classical programming language; however, the possibility of writing low-level programs is left.

The following diagram shows the stages through which a quantum program goes from idea to full implementation on Azure Quantum, and the tools offered by the QDK for each stage.

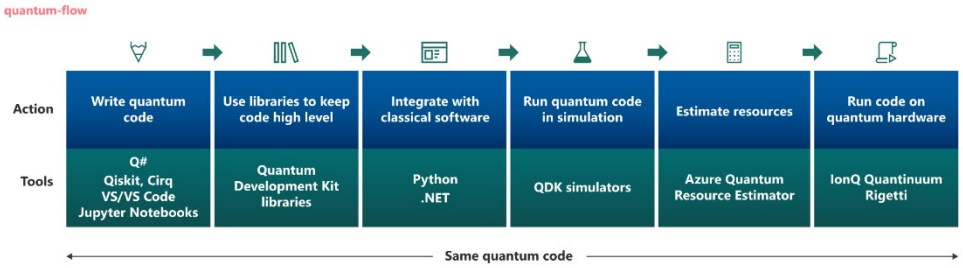


Figure 22 - Deployment diagram on Azure Quantum[99]

In addition to standard libraries, the QDK also includes a quantum machine learning library that provides an implementation of sequential classifiers that exploit quantum computing to perform quantum/classical hybrid ML experiments.
Once an Azure Quantum workspace has been created, it is possible to send Q# programs (also known as jobs) to the Azure Quantum cloud service directly via the development environment; the diagram below shows the program release process, similar to what was done with Qiskit.

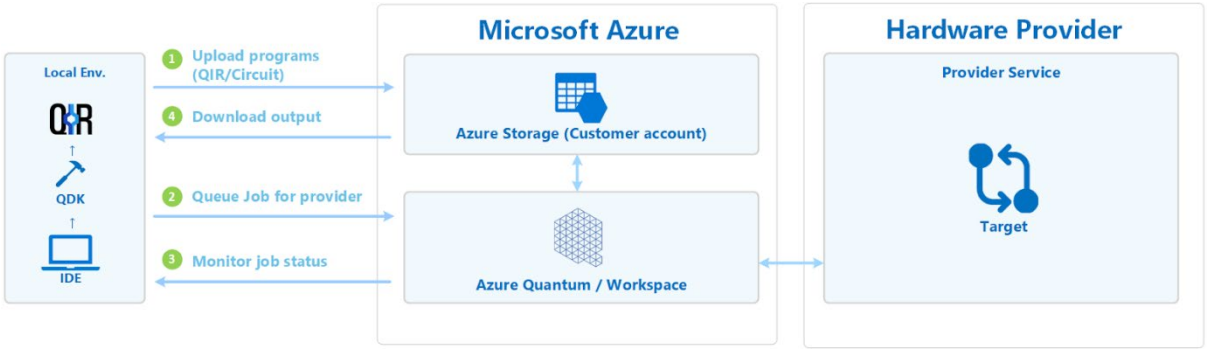


Figure 23 - Program development cycle in the Q# framework[99]

Cirq [100]

Developed by Google AI Quantum is defined as a Python library for writing, manipulating and optimizing quantum circuits and running them on quantum computers and simulators. In the description is already made explicit the approach, which can be described as low-level abstraction (low-level control), of describing circuits and gates similar to Qiskit. Cirq includes, like the other frameworks analyzed, a simulation environment, but with certain special features, such as the possibility of working in a noisy or non-noisy environment, in order to conduct realistic simulations on quantum hardware, or idealised simulations in order to concentrate on writing the Python programs.

[100] https://quantumai.google/cirq

The development cycle is similar to that seen for the other SDKs and involves the use of simulators and batch mode to queue jobs on the Cloud where the Quantum Hardware is located.

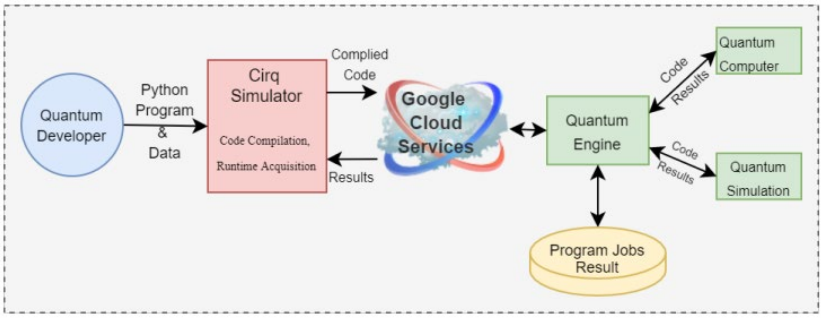


Figure 24 - Program development cycle in the Cirq framework - Source https://arxiv.org/pdf/2302.08884.pdf

The community supporting Cirq is smaller than the others analyzed, but a phenomenon that is becoming increasingly widespread is the collaboration between the various development teams to achieve cross compatibility (interoperability between frameworks).

4.5.4 QKD

Quantum key distribution devices, in general, are based on the emission and detection of photons. From an operational point of view, they integrate into the existing technological infrastructure in the same way as traditional encryption devices, which must be prepared to make use of keys generated in this way.

Several market players offer mature technological solutions for key exchange via QKD: these are dedicated devices, with apparatuses for emitting and receiving photons whose characteristics are used to encode the information intended to constitute the key. The market offer for these devices is now wide and varied, and allows transmission with a key rate of up to hundreds of Mbps for a range of up to 120 km. However, the introduction of these devices entails considerable costs and an appropriate design of use cases to guarantee performance and reliability.

There are various players in this market, from hardware manufacturers to service providers, but given the extreme novelty of the topic and the difficulty of finding expertise in this area, even companies focused on hardware production offer consulting services, accompanied by Proof of Concept.

The use of dedicated optical fiber is recommended for the use of these devices, but some of them also work (with different performance) by sharing the same fiber as the encrypted traffic. In addition, some devices include the possibility of using a QRNG component for generating genuinely stochastic keys.

The market is very diverse: from large market players (Toshiba) or solid companies with this core business (IDQuantique, Quintessence Lab) to start-ups (MagiQ, QTI) to spin-offs from research centers (Max Planck institute, KETS quantum security - University of Bristol, Ki3 Photonics - Montreal National research center, NuQuantum - Cambridge University). There are also companies focused on offering satellite services (LevelQuantum).

The interface towards these devices to guarantee access to symmetric keys by encrypting devices, according to the ETSI GS QKD 014 standard (Protocol and data format of REST-based key delivery API) is provided by the main manufacturers (e.g. Cisco, Ciena, etc.).

4.5.5 QRNG

The production of tools for generating random numbers from physical sources that exploit the principles of quantum physics has seen an increase during the last fifteen years.

Again, one can identify several companies that have developed or are developing expertise in the development of random number generation tools over the years. These include Id Quantique, Quantum Dice, QuintessenceLabs Pty Ltd, Qrypt, Quside, Crypta Labs.

Tools that support the access of multiple applications simultaneously are also proposed, and are particularly suitable for security applications or gaming solutions, from data centers to cloud-based systems[101].

4.5.6 Consultancy services

The complexity of the approach to quantum technologies can be managed by making use of the numerous consultancy firms on the market; in fact, a number of consultancy services have recently sprung up with the aim of assisting companies in facing the challenges and capitalizing on the opportunities arising from quantum technologies. The market is currently very lively and, in addition to the large traditional players, smaller companies, including numerous start-ups, are also offering services of various kinds.

The most common consulting services offered by most specialized companies are as follows:

- support in quantum risk analysis: assessment of impact on business activities, identification of areas of greatest vulnerability and appropriate mitigation actions consistent with corporate strategy;
- support in the introduction of mitigation measures: development and introduction of strategies to protect sensitive data, implementation of a crypto inventory, support in the adoption of post-quantum cryptography algorithms, integration of quantum-resistant security solutions into existing infrastructures;
- evaluation of business opportunities: support for the identification of business opportunities arising from quantum technologies, development of applications and services based on quantum algorithms, optimization of business processes using quantum algorithms or exploration of new business models enabled by quantum computing;
- training and awareness-raising: offering training and awareness-raising programmes to educate company personnel;
- strategic collaborations: interactions with companies, research institutes and quantum technology providers for access to specialized resources.

[101] There are services that provide API access to lab-made strings of random numbers (e.g. https://quantumnumbers.anu.edu.au/).

5 Quantum Safety

The need to quickly identify a strategy for a quantum-safe transition is expressed very intuitively (cf. Figure 25) by what in the literature is mentioned as “Mosca's theorem” (by its author Michele Mosca, professor at the University of Waterloo in Canada).

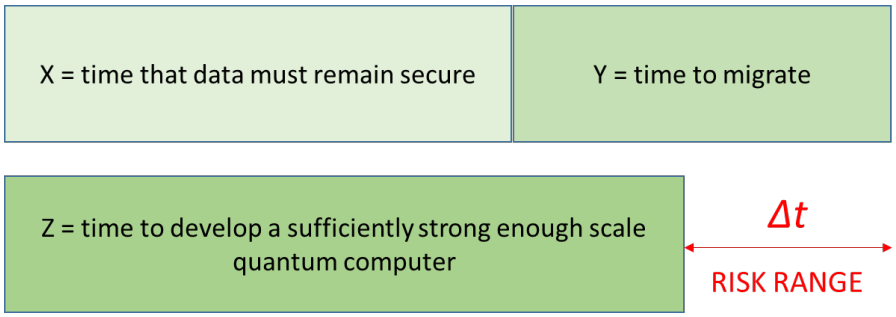


Figure 25 - Representative timeline of a risk exposure impairment for a time Δt if X+Y>Z

If the sum of the time for which data must be kept secure (X) and the time required to migrate infrastructures and applications to quantum safe solutions (Y) is longer than the time (Z) in which the availability of a quantum computer capable of breaching modern encryption systems is estimated, then, for a certain Δ*t*, there would be a serious risk of compromise.

The variables depend strongly on the different realities. There are contexts where, for legal or business reasons, data must remain confidential for decades (X). The variable Y is more difficult to estimate, as it is linked to the complexity of the underlying ICT infrastructure.

With regard to Z variable, i.e. the time needed to develop the technology to pose a risk to the validity of RSA-2048, the estimates of experts, analysts and manufacturers' roadmaps converge, despite a non-negligible margin of uncertainty, towards a time horizon of 20-30 years[102].

The threat also concerns confidential information that is currently encrypted in the classical way. A hacker could breach storage systems and store the stolen datasets, to decrypt them when the technology is mature to do so. This type of attack, known as “harvest now, decrypt later”, is of particular impact for all those sectors where classified information (strategic plans, industrial secrets or military orders) is handled on a daily basis and historicised. As regards the financial world specifically, the use of cryptography is pervasive (Figure 26).

[102] https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/

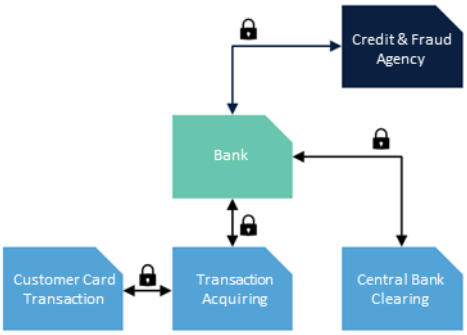


Figure 26 - Use of cryptography in typical banking and finance use cases[103]

In the absence of adequate countermeasures, an attacker equipped with a sufficiently powerful quantum computer could compromise the security of personal and transactional data, authentication systems (including those based on certificates issued by accredited Certification Authorities) of users and applications at interfaces, systems based on Distributed Ledger Technology (DLT), software integrity, digital signatures, and more. In particular, for a banking institution even the compromise of a digital signature is a significant risk, as it would alter the validity of contracts and/or transactions.

The purpose of defining a Quantum Threat Model is precisely to identify the risks associated with vulnerabilities of current encryption algorithms in relation to the advent of a quantum computer. A Threat Model allow to identify priorities in time and economic terms even in relation to events whose occurrence date is not well defined. Below is an example of a Quantum Threat Model presented by Santander during the PKI Consortium in December 2023[104]:

Dimension	Use case	Time validity	External availability	Sensibility	Risk
Confidentiality	Public websites encryption with TLS	1	5	5	25
	Internal access to servers using SSH	2	1	3	6
	Teleworking using VPNs	3	3	5	45
	Site to site VPNs using IPSEC	5	3	5	75
	Encryption of data at rest on premises (disks, backups, etc.)	5	2	3	30
	Encryption of data at rest in the cloud	5	3	5	75
Authentication	Public digital certificates	2	5	5	50
	Internal digital certificates	2	1	4	8
Legal History	Digital signatures in contracts	5	4	5	100

5.1 The migration process to post quantum algorithms

A transition to “post-quantum” cryptographic systems requires a path that goes through a few fundamental steps:

- identification of all use cases of public key algorithms in hardware, network infrastructure, operating systems, application programs, communication protocols, PKIs and access control mechanisms;

[103] UK Finance https://www.ukfinance.org.uk/system/files/2023-11/Minimising%20the%20risks%20-%20quantum%20technology%20and%20financial%20services.pdf (page 20)

[104] https://www.youtube.com/watch?v=RbwwxZSBjyo

- identification of priorities to be assigned to migration components, using a risk management method.

Ideas can be drawn from various documents available online, among them NIST document 1800-38A “Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography”. For a more methodological approach, the publications of various international bodies can be used as inspiration: European Telecommunications Standards Institute (ETSI), World Economic Forum (WEF), Cloud Security Alliance (CSA) or Financial Services Information Sharing and Analysis Center (FS-ISAC).

The following figure shows a comparison of the different methodologies, with a colour mapping identifying similar phases (source: Santander - PKI Consortium - December 2023[104]).

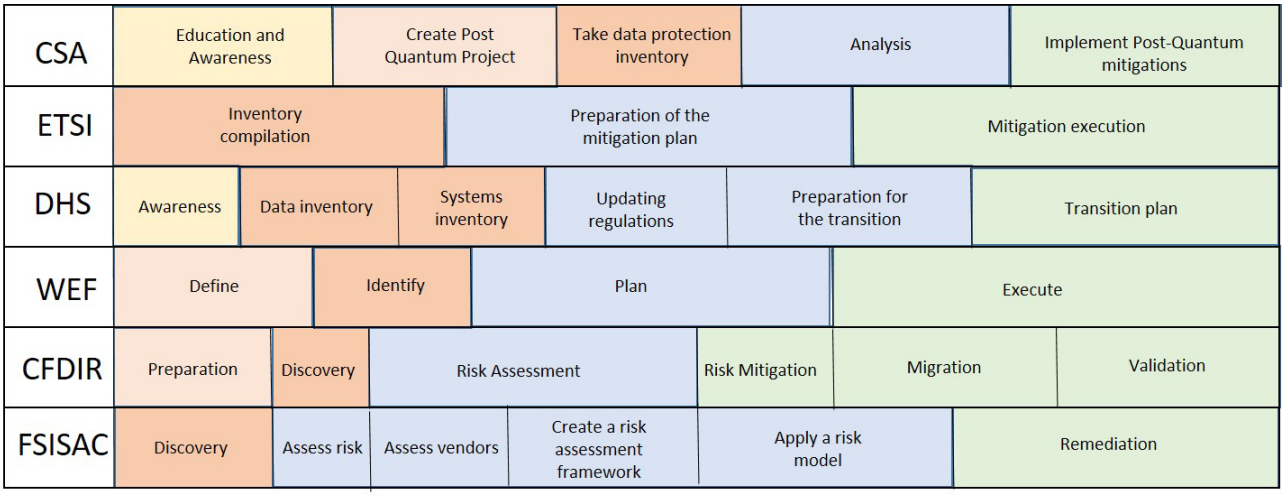


Figure 27 - Comparison of different methodologies for the quantum safe transaction

The number of overall steps and the sequence to be followed may vary depending on the size of the organization, previous activities or the methodology referred to.

Referring to the one described by the World Economic Forum[105], and adding an initial awareness phase, it is suggested to identify five macro-phases of a hypothetical migration plan:

- awareness (or education): involving management in the awareness of the risks associated with delayed management of the issue;
- define (or preparation): definition of objectives, strategy, construction of a roadmap, estimation of the necessary budget, creation of the working group as well as identification of short, medium and long term expectations;
- identify (or discovery): identification of areas where encryption algorithms are used (applications, hardware and services) both internally within the company and by third parties. The primary aim is to build a searchable and up-to-date crypto inventory that makes it possible to identify where to intervene and with what impact, if a used encryption methodology needs to be replaced;

[105] https://www.weforum.org/publications/quantum-economy-blueprint/

- plan (or analysis/risk assessment): action planning in line with a Quantum Threat Model aimed at prioritizing actions. It is essential to consider the life time of the data (e.g. it may not be necessary to protect a contract with an annual validity compared to one with a ten-year validity);
- execute (or mitigate/remediate) tasks: from the use of hybrid logics (PKIs with certificates containing both a traditional algorithm, such as RSA, and a quantum-resistant algorithm such as Dilithium) to the use of fully post-quantum logics.

A more detailed description of these actions is given in chapter 8.2.

Below is another example of a migration plan, with a different approach but still including time references, taken from the 2021 "Canadian National Quantum – Readiness" document[106]. Two macro-phases are envisaged (cf. Figure 28):

1. planning / scope: includes preparation, discovery and risk assessment / analysis

   starting from a Business Impact Analysis it could be possible prioritize core / systemic processes, managing the others in successive waves.

2. implementation: includes risk mitigation, migration to quantum safe systems and validation of what has been implemented.

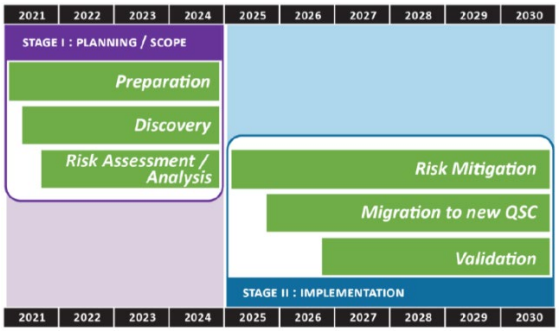


Figure 28 - Example of macro-phase planning[106]

The ultimate goal of a migration to quantum safe encryption is to achieve an agile implementation (crypto agility) that makes it possible to adapt to the evolution of an IT environment, which is by nature highly dynamic and barely predictable, allowing to easily adjust its IT solutions to further updates (such as new encryption standards).

5.2 Crypto Agility

The selection process initiated by NIST has resulted, among other things, in an intense competition between crypto analysts around the world who focused their efforts on identifying vulnerabilities in the various algorithms that are candidates to replace those on which are based the widely used public key cryptographic protocols. Further tests are underway to assess the actual cryptographic security of each of these algorithms against possible attacks, measure their performance and develop secure implementation techniques. It is reasonable to expect that this work will continue

[106] https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/CFDIR-Prati-Tech-Quant-EN.pdf/$file/CFDIR-Prati-Tech-Quant-EN.pdf

in the coming years, also in view of the fact that new computational techniques and approaches may show as vulnerable cryptographic algorithms that seem secure today. With this in mind, algorithms such as Crystals-Kyber, Falcon, SPHINCS+ should not be understood as the final substitutes of RSA or ECC (Elliptic Curve Cryptography), but as the first quantum-resistant solutions currently available, which may in turn be abandoned in favour of more performing or more robust algorithms.

Therefore, it is necessary not to bind to a specific algorithm, but rather to set up their own systems in such a way that they are independent of the component used. Many of the IT systems in use are not designed to facilitate rapid adaptation of new cryptographic primitives and algorithms without making significant changes to the entire system infrastructure. Experience of removing currently deprecated hashing functions, such as MD5 or SHA-1, has shown how cryptographic migration can be difficult and resource-intensive. The NSA itself has stated how migration to new cryptographic logics could take the US national security system up to 20 years[107].

Crypto agility is defined as the ability to react quickly to cryptographic threats, replacing cryptographic algorithms that have become vulnerable so that the impact on the infrastructures involved and business continuity is as low as possible.

The implementation of crypto agility requires a decoupling between encryption and code development logics, so that management is external to the application itself.

The following are some of the benefits that crypto agility can bring:

- alternately use different encryption algorithms without changing the application code or infrastructure;
- enable a rapid transition from one encryption algorithm to another (in case new vulnerabilities on existing algorithms need to be mitigated);
- allow a hybrid implementation where classical and post-quantum algorithms can coexist;
- allow the decision on the type of encryption to be used by security experts according todata classification or internal policies;
- abstracting the API, i.e. hiding the complexity of encryption from application developers;
- support as many platforms as possible (meaning different programming languages and/or different technologies, such as containers);
- easily interoperate with systems using different cryptographic implementations;
- adapt to new regulatory standards, without substantial impacts and minimizing the work required.

Some vendors, many of them members of the cooperative quantum consortium headed by NIST[108], have already entered the market with solutions that allow the implementation of a crypto agility framework. Other vendors, on the other hand, propose crypto agility natively embedded in their

[107] https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF

[108] https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

products/services, thus facilitating upgrades to new standards/protocols/algorithms (e.g. Crypto4A, CryptoNext, DigiCert, Thales).

It is also possible to implement crypto agility through specific features offered by certain programming languages, without necessarily having to resort to third-party tools. For example, the Cryptography API Next Generation (CNG) - replacing CryptoAPI - are provided with cryptographic metadata that allow the immediate identification of the cryptographic technique used and the replacement of cryptographic functions by reconfiguration or patching. Features already present in .NET, Java Cryptography Architecture (JCA), Node.js, Ruby or Go and Python enable natively crypto-agile software.

The focal point where to implement the necessary controls to avoid non-crypto-agile implementations is the DevOps chain. By integrating with existing chains, in a CI/CD logic (continuous integration/continuous delivery), developers can gain access to policy-compliant guidelines. It is good practice to include the implementation of security protocol substitution methods within the reference test book, in order to verify that they are adequate with respect to the confidentiality, integrity and availability requirements adopted.

Lastly, in the IoT world, the approach to crypto agility may prove to be more complex. One of the implementation scenarios for minimising upgrades is the use of tools that can receive keys, new encryption algorithms and security policies to be implemented locally. A firmware-based implementation has as a downside the necessary reboot of the device with a possible impact in terms of disservice if the device becomes, for some reason, unreachable. Being able to dynamically update an encryption algorithm would significantly reduce this risk.

5.3 Adoption of QKD scenarios

Some limitations must be considered, in the adoption of this technology, which many actors, including institutional ones, have already highlighted (with debate[109]) and which can be summarized as follows:

- costs associated with the equipment required for the generation and distribution of quantum keys;
- limited distance of the point-to-point connection due to the dispersion to which the physical means of communication is subject (e.g. optical fiber) in the absence of established widespread technologies for intermediate transmission nodes;
- need to rely on classical mechanisms (pre-shared keys or post-quantum cryptography) for initial authentication;
- increased risk of DoS (Denial of Service) attacks due to high sensitivity to protocol interference.

Furthermore, it must be considered that although QKD devices have been available on the market for some time and with a high degree of maturity, the standards for their operation, the evaluation

[109] "The debate over QKD: A rebuttal to the NSA's objections" - Renato Renner, Ramona Wolf - https://arxiv.org/pdf/2307.15116

of their performance, as well as the degree of interoperability with other devices are still elements of analysis in the introduction of these scenarios.

6 Quantum technologies and the banking and financial sector

6.1 Exploiting the opportunities of quantum computing in financial applications

The financial services[110] is estimated to be the first industrial sector that will benefit from quantum computing in the medium to long term. The list of useful use cases is long, but many of them often refer to the same fundamental algorithms that are reused in multiple contexts. (Figure 29).

Author(s)	Year	Title	Use Case	Methodology	Quantum algorithm	Hardware
Rebentrost and Lloyd	2018	Quantum computational finance: quantum algorithm for portfolio optimization	Determine the optimal portfolio more quickly/accurately.	Optimisation	Solving linear equation systems (HHL)	Gate-based quantum computer
Venturelli and Kondratyev	2019	Reverse Quantum Annealing Approach to Portfolio Optimization Problems	Determine the optimal portfolio more quickly/accurately.	Optimisation	Approximate optimization (QUBO)	Quantum annealer
Braine *et al.*	2021	Quantum algorithms for mixed binary optimization applied to transaction settlement	Settle as many transactions as possible and/or maximise the total value of the settled transactions.	Optimisation	Approximate optimization (VQE and QAOA)	Gate-based quantum computer
Phillipson and Bhatia	2020	Portfolio Optimisation Using the D-Wave Quantum Annealer	Determine the optimal portfolio more quickly/accurately.	Optimisation	Approximate optimization (QUBO)	Quantum annealer
Y. Ding *et al.*	2019	Towards Prediction of Financial Crashes with a D-Wave Quantum Computer	Prediction of financial crashes in a complex financial network.	Optimisation	Approximate optimization (QUBO adapted)	Quantum annealer
Hodson *et al.*	2019	Portfolio Rebalancing Experiments using the Quantum Alternating Operator Ansatz	More quickly/accurately discrete portfolio optimisation under constraints.	Optimisation	Approximate optimization (QAOA)	Gate-based quantum computer
Kerenidis *et al.*	2019	Quantum Algorithms for Portfolio Optimization	More quickly/accurately portfolio optimisation under constraints.	Optimisation	Optimization (QIPM for SOCPs)	Gate-based quantum computer
Orús *et al.*	2019	Forecasting financial crashes with quantum computing	Forecasting financial crashes with quantum computing.	Optimisation	Approximate optimization (QUBO)	Quantum annealer
Rebentrost *et al.*	2018	Quantum Computational Finance: Monte Carlo Pricing of Financial Derivatives	Price derivatives more quickly/accurately	Monte Carlo	Searching and counting (QAE)	Gate-based quantum computer
Martin *et al.*	2021	Toward pricing financial derivatives with an ibm quantum computer	Pricing interest-rate financial derivatives with the Heath-Jarrow-Morton model more quickly	Monte Carlo	Optimization (qPCA)	Gate-based quantum computer
Egger *et al.*	2019	Credit Risk Analysis using Quantum Computers	Estimate credit risk more efficiently.	Monte Carlo	Searching and counting (QAE)	Gate-based quantum computer
Woerner and Egger	2019	Quantum Risk Analysis	Evaluate risk measures such as Value at Risk and Conditional Value at Risk more quickly/accurately	Monte Carlo	Searching and counting (QAE)	Gate-based quantum computer
Stamatopoulos *et al.*	2020	Option Pricing using Quantum Computers	Price options such as vanilla options, multi-asset options, barrier options and path-dependent options more quickly/accurately	Monte Carlo	Searching and counting (QAE)	Gate-based quantum computer

Figure 29 - Overview of proposed use cases in financial literature[111]

[110] McKinsey's Quantum Technology Monitor 2023 estimates that the four sectors (automotive, chemicals, financial services and life sciences) that will see the first benefits from the use of quantum computing could potentially earn up to $1.3 billion by 2035. Of this, half could come from the financial sector.

[111] A Structured Survey of Quantum Computing for the Financial Industry- Albareti et *al*. - 2022 - https://arxiv.org/pdf/2204.10026

The possible applications of quantum computing in finance can be three macro-groups[112]:

- optimization problems: portfolio optimization, credit scoring;
- simulation problems or stochastic modelling: simulation of financial asset trends, stress test scenarios, financial crisis forecasts;
- machine learning: fraud detection algorithms, customization of the offer to the end customer.

A brief mention of these applications is given below, with a reference to the extensive literature on the subject[112] for further details.

6.1.1.1 Optimization problems

Optimization is the process of finding solutions that maximize or minimize a given function. This process can be computationally burdensome in the presence of a large number of variables to be considered. This type of problem arises in many areas, such as finance, arbitrage or credit.

Quantum technology offers new possibilities for tackling combinatorial and convex optimization problems, which are among the most complex. There are various approaches based on quantum computing, such as adiabatic, variational or hybrid algorithms, which exploit the properties of quantum systems to explore the space of solutions (see box below for an example).

The QUBO model (Quadratic Unconstrained Binary Optimization)

QUBO is a useful model for solving a class of problems of a combinatorial nature. In this type of problems, usually there is a set of binary variables whose combination may represent, depending on the problem, a loss or a gain. In very simple terms, QUBO is characterized by a quadratic mathematical function to be minimized as a function of a set of variables that also takes constraints into account.

This model is highly appreciated for its flexibility and its ability to synthesize many variables efficiently: it finds application in many scenarios affecting the banking and financial world in particular[112] such as collateral estimation, portfolio optimization, arbitrage management, but also other areas such as maintenance planning[113] or the optimization of mobile network infrastructure[114].

The possibility of exploiting quantum parallelism would make its resolution faster and more precise. The development of a QUBO quantum algorithm consists of formulating the problem according to this model and using libraries to solve it.

Even in common interface SDKs to quantum hardware, resolution solvers for QUBO have been integrated. In particular, quantum annealers are particularly suitable for this purpose.

112 A Survey of Quantum Computing for Finance - Herman *et al.* - https://arxiv.org/pdf/2201.02773

113 https://www.reply.com/data-reply/it/stories/algoritmi-quantistici-per-l-ottimizzazione-dei-lavori-di-manutenzione

114 https://www.gruppotim.it/content/dam/telecomitalia/it/archivio/documenti/Innovazione/MnisitoNotiziario/2020/2020-1/cap02_quantum-ottimizzazione.pdf

6.1.1.2 Simulation and stochastic modelling problems

Simulation is a useful technique for modelling complex phenomena. In the financial domain, this technique can support investment decisions, optimizing the relationship between return and risk, and facilitate the operational management of banks in various sectors, such as credit or derivatives. The modelling of stress test scenarios, liquidity provisions and financial crisis forecasts are also areas where significant benefits could be identified from the application of this technique. Furthermore, simulation can help banks to comply with the regulatory requirements of international agreements, such as the Basel III agreement, which requires the calculation of risk indicators such as Value at Risk (VaR) and Conditional Value at Risk (CVaR).

To model the stochastic processes that determine the evolution of financial phenomena, stochastic differential equations are used, which generally do not have an analytical solution, but require numerical or Monte Carlo-type methods[115]. Quantum computing[112] offers new possibilities to address these problems, with algorithms that exploit quantum properties to solve partial differential equations (QPDEs - Quantum Partial Differential Equations) or perform Monte Carlo integrations (QMCIs - Quantum Monte Carlo Integrations). These quantum variants offer a significant computational advantage[116] over equivalent classical methods.

6.1.1.3 Machine Learning

Machine learning is an analysis and prediction technology that has found many applications in different industrial sectors. Artificial intelligence - both discriminative and generative - is changing the way large amounts of information are processed to facilitate decision-making.

An innovative perspective is offered by quantum machine learning (QML, cf. 3.2.2), which, although still an emerging discipline and in the process of scientific evaluation, may have advantages in certain application scenarios. The most active areas of research that make use of QML are: asset pricing, implied volatility estimation, forecasting of options with discontinuous payoffs, credit scoring and estimation of exchange rate regime changes. In all these areas, the ability to make accurate forecasts, typical of ML algorithms, is of paramount importance.

The main advantages of QML are related to the higher training speed of the algorithms and greater accuracy in probabilistic simulations.

[115] The idea behind the Monte Carlo method, which actually encompasses a broad category of techniques commonly used for price estimation and risk prediction, is to use random numbers to perform statistical simulations of the process one wishes to study. In an extreme simplification, the performance of the particular process is described by a mathematical expression as a function of a dependent variable x (the solution being sought) and different parameters for whose values probability distributions are assumed (e.g. based on historical data). These distributions are then sampled by generating a series of values for each of the parameters and, by iterating the procedure with the various possible combinations, the respective solutions are calculated with the associated probability estimate and defined margins of error. The reliability of the estimate is linked to the number of repetitions of the procedure; consequently, the consumption of resources and the time required to obtain an estimate with the desired degree of precision are high.

[116] There are numerous papers on the subject, for example: “Quantum computational finance: Monte Carlo pricing of financial derivatives”- Rebentrost *et al.* - Physical Review A 30 April 2018 - https://arxiv.org/abs/1805.00109

6.2 Making systems, applications and infrastructure secure

6.2.1 Making systems and applications secure

As widely described in chapter 5, one of the main aspects, involving the early stages of the transition process, is becoming aware of one's own application and infrastructure fleet.

A crucial distinction is to identify applications made in-house and those acquired from external providers, the details of whose development code are usually unknown and security aspects are left to the guarantees offered by the product developers.

6.2.1.1 Applications developed “in-house”

Two aspects are crucial in this scenario: firstly, knowledge of which algorithms are used, and secondly, the provision of an application development framework that allows easy replacement of these variables.

It may also be useful to use already prepared libraries, protocols and applications to evaluate the cost and functionality of such replacements.

In this regard, the open-source project ”Open Quantum Safe”[117] part of the Linux Foundation's Post-Quantum Cryptography Alliance is worth mentioning. The project involves both the development of libraries for post-quantum algorithms (liboqs) and the integration of applications and protocols into prototypes[118].

6.2.1.2 Commercial products

It is worth considering, in the adoption of current and future commercial products, the provision in the vendor's roadmap of crypto agility mechanisms. This becomes particularly important where the use of cryptography is dedicated to the exchange of sensitive information, financial transactions, authentication or even the issuance of digital certificates.

6.2.1.3 The mainframe environment

In the mainframe area, traditionally found in banks' data centers, a new generation of hardware natively prepared for the use of post-quantum protocols is on the way. In particular, a good precursor is the IBM z16, whose firmware is programmable so that it can, through specific updates, provide for the agile replacement of encryption algorithms.

6.2.2 Making infrastructure secure

The possibility offered by QKD to exchange keys securely and guarantee encryption that safeguards data from compromise in the post-quantum era can already be exploited in network communications.

6.2.2.1 Making peer-to-peer communications between data centers secure

The simplest use case, but characterizing many IT data centers, is the connection between two sites that are usually present in redundant environments typical of critical infrastructures and at a

[117] https://openquantumsafe.org/

[118] https://openquantumsafe.org/applications/

relatively short distance (of the order of 50-100 km to allow efficient synchronous replication of data).

Normally, the network infrastructure that connects the two sites consists of fiber optic channels where the data transits encrypted thanks to devices (ciphers) that use symmetric protocols, such as AES, considered quantum safe. However, the key used for this purpose is exchanged, by the ciphers themselves, over the same channel, using an asymmetric protocol.

The vulnerability of the system to attacks by quantum processors can be found precisely in this exchange (cf. Figure 30).

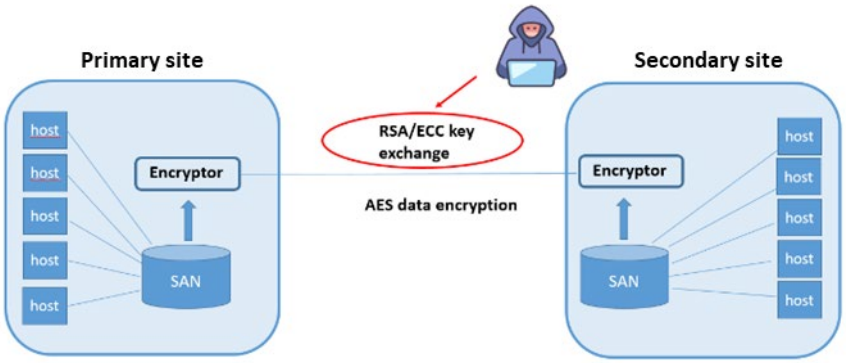


Figure 30 - Vulnerability of intra-data center connections

To make this connection quantum safe, it is necessary to:

- introduce optical devices for key exchange;
- connect them via a dedicated optical fiber[119];
- configure cryptographic devices to use keys generated by optical devices (Figure 31).

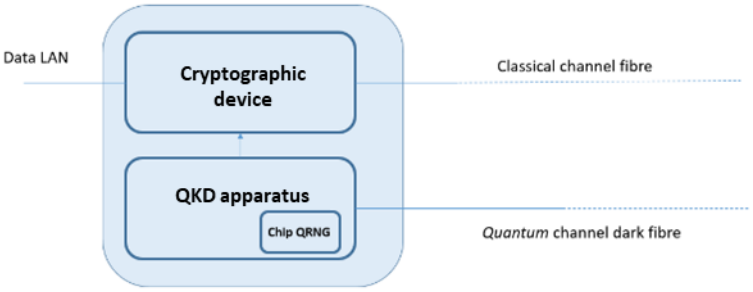


Figure 31 - Logical endpoint diagram for QKD exchange

The diagram of a quantum safe data center connection is depicted in the figure below:

[119] A shared fiber can also be used, using multiplexing techniques, but the interference present may reduce the efficiency of key creation.

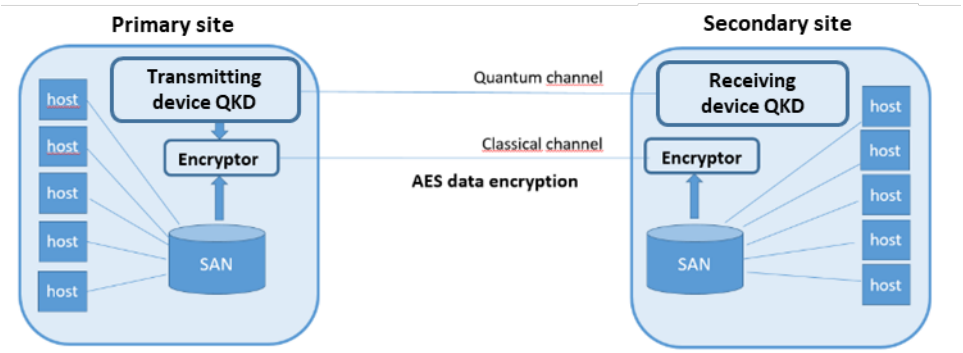


Figure 32 - Quantum safe data center infrastructure

6.2.2.2 Active trust service providers of certified electronic signatures

Even accredited certificate issuing systems for encryption and signatures are, for obvious reasons, exposed to quantum threats. In particular, the qualified electronic signature, on which the trustworthiness of many digitally stored documents is based, requires special attention due to the fact that its validity is demanded over time. Providers of this service in Italy include various banking and financial entities in addition to the Banca d'Italia.

For this reason, manufacturers of technology and solutions for public key infrastructures (PKI) have already included in their roadmap indications for the adoption of post-quantum algorithms and experiments can also be introduced by exploiting open source software[120].

6.2.2.3 Quantum DLT

Distributed ledger technology bases its existence on cryptography and, in particular, on the use of keys for encryption and signature.

Cryptocurrencies are one of the main applications of this technology where public and private key pairs are used to hold addresses and signatures to seal transactions.

Some of the existing blockchain networks have stated[121] that they are currently studying and experimenting to make the infrastructure quantum-resistant.

QKD could, in principle, be used to secure transactions carried out via distributed technologies, but the approaches are, at the moment, rather cumbersome, both because of the difficulty of assuming that all participants in the DLT have a connection (via fiber or satellite) to carry out the exchange of quantum keys, and because the current bit-rate could compromise performance.

Alternatively, a switch to post-quantum (PQC) algorithms is conceivable, although current implementations of digital signature and encryption algorithms (e.g. Crystal Dilithium and Kyber) still appear immature.

[120] https://www.ejbca.org/use-cases/try-quantum-safe-cryptography-pki/

[121] "Future proofing - Quantum resistant" https://ethereum.org/en/roadmap/future-proofing/, "Pioneering falcon post quantum technology on blockchain" (https://www.algorand.foundation/news/pioneering-falcon-post-quantum-technology-on-blockchain)

Several players on the market offer solutions to make DLT-based applications quantum safe: QuantiCor Security and QANPlatform, Sonora Gold and Silver Corp (PQC), Quantum Blockchain or both (QuSecure).

6.3 Experience in the banking and financial sector

The following are some officially disclosed and considered significant experiences from the international banking and financial landscape.

The data that these experiences have in common can be summarized as follows:

- in most projects, collaboration agreements have been introduced with industry represented both by large vendors (which often offer a service including a learning phase, software, hardware availability and development support) and by start-ups offering specific services; the strategy of some banking groups is characterized by direct investment in start-ups considered promising;
- some institutes have identified collaborations with the academic and research world, in particular for the study, application and improvement of existing algorithms; these collaborations result in the joint publication of scientific articles;
- actual experiments are generally preceded by a rather lengthy learning phase and an analysis of use cases of particular interest to the business for which the classical solution is inefficient or limited in its use of parameters such as, for example, optimization of credit risk estimation (credit scoring), fraud detection or portfolio optimization;
- some institutions are setting up dedicated teams, using internal and external training, to follow the evolution of technology and quickly identify migration strategies;
- concerning the quantum network security component, collaboration with research institutions and network infrastructure providers for the realization of connection projects is inevitable;
- albeit with important exceptions, many of the commercial entities that have invested in the topic of quantum technologies have not officially declared major projects for the introduction of quantum-safe countermeasures; instead, institutions such as the Banca d'Italia, several other central banks, ABI and the Bank for International Settlement (BIS) have launched various initiatives internally and to raise awareness among the entire system of the importance of adapting applications and infrastructures in time;
- in general, with regard to the topic of quantum safe transition, individual institutions tend, due to the nature of the topic, to manifest a shared approach in consortia or institutionally promoted initiatives and directions.

6.3.1 Banca d'Italia

The Banca d'Italia has for some time been pursuing an in-depth study of quantum technologies involving the Directorate General for Information Technology and the Directorate General for Economics, Statistics and Research.

A study phase, which saw the publication of specific papers in the Institute's series[122], the participation as speakers at international events and the organization of a dedicated workshop with the participation of the academic world, was followed by experimental phases, which are still ongoing, aimed at increasing knowledge and raising awareness of opportunities and risks in this field.

Figure 33 - Banca d'Italia publications on quantum technology topics

In particular, these experiments were related to:

- reconnaissance of systems and application assets for the use of quantum safe algorithms;
- possibility of exploiting QKD equipment to exchange keys securely between data centers and establish secure international connections;
- Certification Authority (CA) experimentation with the use of software designed to use post quantum algorithms.

With regard to the first aspect, in line with the strategic indications also described in this report, a market analysis of the software offer was preliminarily conducted to identify a suitable solution for identifying and cataloguing the cryptographic algorithms used by the numerous applications developed within the Institute. This information will be integrated into the repository of application assets already in use to build an information base on which to plan priorities and methods of intervention in terms of crypto agility.

With reference to the second aspect, an encrypted data connection between three data centers (with a distance between 10 and 20 Km) was tested using keys generated through optical devices

122 Elena Bucciol and Pietro Tiberi "Quantum safe payment systems" June 2023 - https://www.bancaditalia.it/pubblicazioni/mercati-infrastrutture-e-sistemi-di-pagamento/approfondimenti/2023-035/index.html

Giuseppe Bruno "Quantum computing: a bubble ready to burst or a looming breakthrough?" October 2022 - https://www.bancaditalia.it/pubblicazioni/qef/2022-0716/index.html

Adriano Baldeschi and Giuseppe Bruno "Quantum Computing winks at statistics. Is it a good match?" April 2024 - https://www.bancaditalia.it/pubblicazioni/qef/2024-0843/index.html

for quantum key exchange (QKD). For this purpose, an interface was set up between these and encryption devices from various vendors, enabling the evaluation of efficiency (in terms of key rate), reliability and interoperability requirements. The experience was of great value in assessing the effort and impact required to set up such an infrastructure.

Thanks to the cooperation with the Bank of Canada and the Banque de France, it was possible to establish secure connections using a protocol[123] based on symmetric cryptography for the exchange of encryption keys.

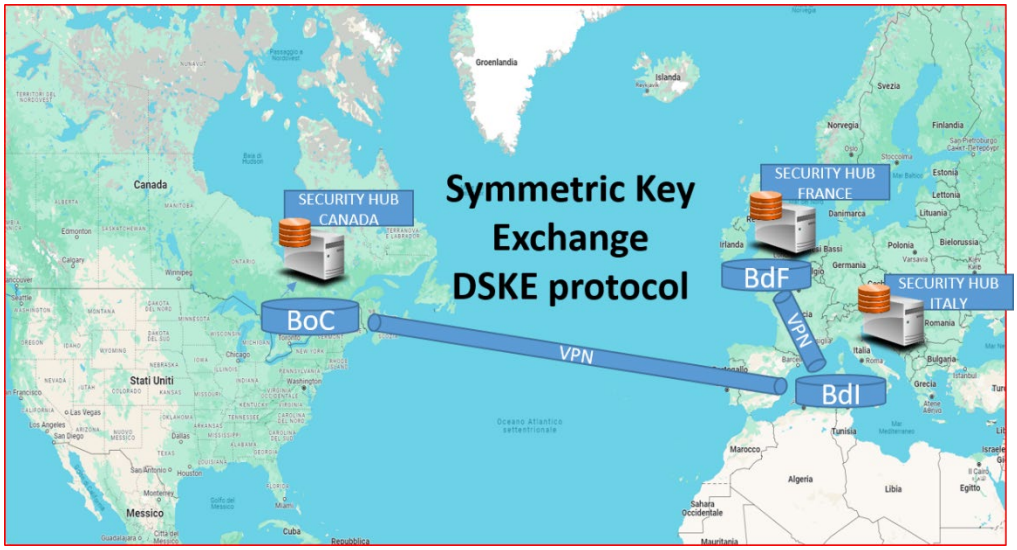


Figure 34 - Intercontinental quantum safe link between three central banks

Within Banca d'Italia, provider of qualified electronic signature services, the issue of quantum safe Certification Authorities was considered of particular importance. To this end, meetings were held with the Agency for Digital Italy and the National Cybersecurity Agency, which participates in the European panels that follow certifications in the cryptographic field. In addition, a Proof of Concept was introduced based on open source software capable of issuing digital certificates based on post quantum algorithms also in hybrid mode (coexistence of both algorithms within the same certificate). This allowed an initial set of functional and non-functional tests to be carried out for the use of such certificates. Further tests are planned based on the release of new software versions and the availability by vendors of hardware cryptographic devices (smart cards, Hardware Security Module - HSM) able to support these algorithms.

As part of the initiatives aimed at fostering the sharing and exchange of information and experiences on these issues, a workshop entitled "Quantum Safe Communications: overview of the state of the art and future prospects in the use of technologies" was held last February, attended by representatives from academia, institutions, companies in the sector, and Banca d'Italia. The

123 " Distributed Symmetric Key Exchange: a scalable, quantum-proof key distribution system"- Hoi-Kwong Lo, Mattia Montagna, Manfred von Willich - https://arxiv.org/abs/2205.00615. This mechanism involves the introduction of security hubs to which clients turn to negotiate a symmetric key to communicate with each other. The method involves an initial phase of exchange (with each security hub present) of a certain amount of random strings (generated via QRNG) pre-shared, delivered physically or distributed via QKD (the authors imagine a network of local distributors facilitating physical transmission or via QKD).

workshop provided an opportunity to discuss the use of quantum technologies such as QKD and PQC in the field of quantum safe communications.

Also the present study, conducted at CIPA, is the result of Banca d'Italia's desire to increase knowledge, raise awareness of the opportunities and risks of quantum technologies among the entire banking and financial system, and act as a reference for a collaborative network.

6.3.2 ABI

The ABI Lab consortium is the Research and Innovation Center for banking promoted by ABI (Italian Banking Association) to facilitate dialogue between banks and ICT companies. It brings together banks, companies and institutions to promote innovation in the Italian financial sector through technical research tables, experimental projects and the organization of events and seminars on the main innovation topics applicable to the banking world.

In particular, it promoted a study day[124] in 2023 with the involvement of key players from research and industry dedicated to exploring emerging scenarios on Quantum Computing, the proceedings of which are available to consortium members.

At European level, it is active on numerous projects funded by the European Commission and working groups where it contributes to the discussion on innovation and cybersecurity. In March 2024, CERTFin - Italian financial CERT, through the Consortium, submitted two funding proposals for as many projects in the quantum field, making itself available to coordinate these initiatives with the aim of fostering positive spin-offs for the entire banking community.

6.3.3 Bank for International Settlements (BIS) Innovation Center

In June 2023, Project Leap was launched by the BIS Innovation Hub Eurosystem Center in cooperation with the Banque de France and the Deutsche Bundesbank to raise awareness and prepare central banks and the entire financial system for the transition to quantum-resistant cryptography.

The first phase of the project[125] aimed to test communication with post-quantum cryptographic protocols between two central banks. A traditional public-key algorithm was implemented together with several quantum-resistant algorithms in a hybrid encryption mode, with the aim of maintaining the confidentiality of messages sent across two distant IT systems. The quantum-resistant communication channel was used to convey payment messages transmitted between the Banque de France and the Deutsche Bundesbank with the aim of testing the performance of existing products and processes using quantum-resistant technology.

[124] Quantum Computing - ABI Lab

[125] https://www.bis.org/publ/othp67.pdf

Figure 35 - Quantum safe VPN realized with “hybrid” quantum encryption

In order to foster a broader understanding of post-quantum cryptography, the first phase of the project explored solutions that incorporate the notion of crypto agility (introducing the possibility of varying the algorithm used for the cipher) and demonstrated that new quantum-resistant schemes can be applied.

In 2024, a second phase of the project began, with the aim of showing how a payment system can be protected from the potential threat of quantum computers, which might be able to break the encryption systems currently used to protect financial transactions in current payment systems. Further use cases of central banks will be explored in this phase with the overall aim of contributing to the quantum-proofing of the financial system. Therefore, more than two central banks will be involved to investigate more complex IT environments in preparation for real-world contexts. A new report will be published that will provide insights into the specificities of central banks' systems in order to facilitate migration plans to quantum-safe environments.

6.3.4 Bank of Canada

The Bank of Canada, in line with national guidance (cf. 8.1), is extremely active in experiments on quantum computing and threat prevention strategies also through numerous partnerships. The strategy is based on four pillars: the resilience objective, the creation of a collaborative ecosystem, the development of human resources and research aimed at identifying applications and use cases.

It recently partnered with evolutionQ, a Canadian company dedicated to customizing solutions using quantum technologies, for security projects specifically related to digital currency. For this project, the developed code will be made available under an open source licence with the aim of providing tools to the development community and accelerating the global post-quantum transition process.

In June 2023, to mention one example, an article[126] was published proposing the use of post-quantum techniques to ensure privacy in payments while protecting users against possible fraud. A practical and interactive credential mechanism is proposed, in which users are issued pseudonymous credentials that can be used to register with financial service providers without revealing personal information. The protocol has proven to be secure and lossless, preserving user privacy regardless of the number of registrations.

[126] https://www.bankofcanada.ca/2023/06/staff-working-paper-2023-33/

6.3.5 Intesa Sanpaolo

Intesa Sanpaolo in 2020 has set up an in-house center of competence on quantum technologies[127] focused on identifying the opportunities offered by quantum computing in the banking and financial sector, dealing with growth and awareness paths, collaborating with the academic world and identifying guidelines for the adoption of these technologies.

Figure 36 - The objectives of Banca Intesa's Quantum Competence Center

Several experimentation initiatives have been undertaken, including the use of quantum computing platforms for testing portfolio optimization algorithms, credit risk analysis and derivative pricing, participation in secure network projects, academic collaborations and investments in start-ups.

In particular Intesa Sanpaolo:

- since 2021 has been running experiments with two different quantum computing platforms (D-Wave - through Data Reply - and IBM), in collaboration with the vendors, to explore their different potentials;
- in 2022 through NEVA (Group Venture Capital) invested in the start-up Classiq, a company specializing in software development with the focus on creating a platform that simplifies the design process of quantum algorithms;
- participated in the PoliQI initiative, one of the first metropolitan quantum networks, set up in collaboration with the Politecnico di Milano, the Lombardy Region and the Italian Army, which ensures quantum-safe communications between the financial, military and institutional districts within the city:

[127] Quantum Computing in Finance: The Intesa Sanpaolo Experience | IEEE Journals & Magazine | IEEE Xplore

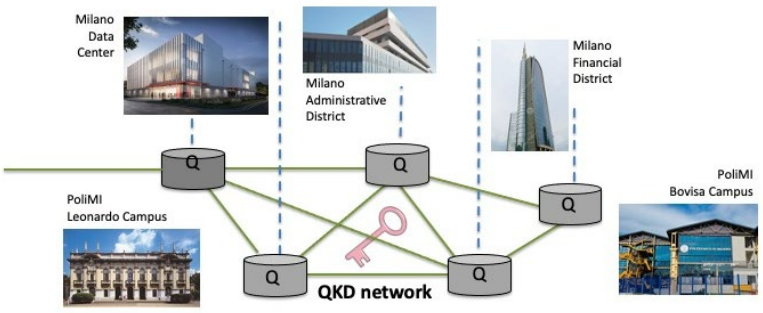


Figure 37 - POLIQI-POLItechnical Quantum Infrastructure diagram[128]

- is a partner of the Politecnico di Milano Observatory in Quantum Computing and Communication (cf. 4.1);
- participates in the national research center in High Performance Computing, Big Data & Quantum Computing financed by the EU Recovery Fund; within this collaboration, two use cases are being investigated: the first one relates to the topic of fraud detection (the recognition of anomalies in order to detect criminal actions perpetrated through the banking system) and the second one relates to credit scoring (i.e. how to ascertain whether an applicant is able to sustain a loan). The classical models for these problems present peculiar difficulties due to the peculiarities of handling the input data and their parameterization;
- supported the creation in 2022 and continues to support editions of the master's degree course in Quantum Computing & Communication promoted by the Politecnico di Torino both through the participation of its own employees and by collaborating on teaching;
- has published several industrial research papers, including a peer-reviewed article in collaboration with IBM and the Politecnico di Torino, in which an improved variant (in the amount of factors introduced into the model and in the flexibility of input data) of quantum algorithms for credit risk assessment is proposed, testing them through both quantum simulators and IBM's actual quantum computer;
- in collaboration with the Politecnico di Torino and the LINKS Foundation, participates in research aimed at identifying which processes can benefit from a quantum approach and develop the relevant Proof of Concept, which has led to the publication of several papers. In particular, the areas identified are: interest and exchange rate risk modelling, default prediction, anomaly detection and, in general, quantum machine learning;
- is working with IBM to identify quantum safe strategies and test the impact of introducing post-quantum algorithms with projects to test various use cases (from simple client/server communications to VPN implementation) using libraries from IBM's Quantum Safe Remediator

[128] Source: Regione Lombardia and PoliMi together for an encrypted communication network and research on 3D printing in the biomedical sector - Industria Italiana

product[129]. It also stated[130] that it intends to exploit the encryption capabilities enabled for the use of such algorithms offered by the z16 mainframe.

Intesa Sanpaolo publicly disseminates its organizational model and its vision on the strategic importance of these issues, also to promote the image of an efficient and innovation-oriented institution, and aims to become a point of reference in the Italian and European banking and financial scene for these issues.

6.3.6 BBVA

Starting in 2019, BBVA has introduced several lines of research to investigate the value of quantum technologies in different use cases. The aim, in general, is to identify and quantify possible benefits, estimate the computational resources required to achieve them and how these scale with respect to the size of the problem.

In particular:

- formed a strategic alliance with the Spanish National Research Council (CSIC) to collaborate on scientific research projects on the design and testing of quantum algorithms that can be used in financial scenarios;
- in collaboration with Fujitsu developed a PoC on Fujitsu's quantum digital annealer (a system that simulates quantum hardware) for the portfolio optimization problem (i.e. the best choice of financial assets that, taking into account various parameters, including the quantification of risk, provides the highest return for the holder). The typical classical solution to this problem involves classifying assets according to their associated risks. The possible combinations, however, increase exponentially with the number of assets and require exorbitant calculation resources to optimize the result;
- conducted various tests with different providers for the dynamic optimization of the portfolio, i.e. the evolution of its performance over time in relation to market trends. For this purpose, various technology platforms were evaluated with the collaboration of Accenture and the Spanish start-up Multiverse. Through a proof of concept, developed together with the latter, the Spanish bank compared different quantum technology platforms to solve a classic problem in finance: the optimization of investment portfolios with real market data. Thanks to this analysis, also published in a scientific article[131], the researchers outlined new formulas that could help speed up this type of calculation, maximizing profitability and minimizing risk[132];
- in cooperation with Accenture and D-Wave assessed margins for the optimization of the credit scoring process by evaluating the expected benefits when introducing additional variables to those normally used in these models;

[129] Intesa Sanpaolo collaborates with IBM in testing post-quantum solutions

[130] Intesa Sanpaolo and IBM: agreement for innovative technology infrastructure

[131] [2007.00017] Dynamic Portfolio Optimization with Real Datasets Using Quantum Processors and Quantum-Inspired Tensor Networks (arxiv.org)

[132] https://www.bbva.com/en/bbva-and-multiverse-showcase-how-quantum-computing-could-help-optimize-investment-portfolio-management/

- introduced, in collaboration with the start-up Zapata Computing, a PoC to evaluate the use of quantum algorithms to optimize procedures for calculating the cost of derivatives, traditionally carried out using Monte Carlo simulations.

In addition to those mentioned, BBVA stated its intention to involve other business units in other topics such as the optimization of Machine Learning processes.

6.3.7 Crédit Agricole

In June 2021, the French bank launched two experimental projects with the aim of assessing the contribution of an algorithmic approach inspired by quantum computing and the potential of quantum computers for finance in two respective fields: the valuation of financial products and the assessment of credit risks[133].

To this end, the bank benefited from a collaboration with the French company Pasqal (one of the European companies designing quantum hardware) and the French start-up Multiverse specializing in quantum algorithms.

The experiments were carried out over a period of more than a year, showing the known limitations of current processors, but pointing out that the 50-qubit processor on which the derivative evaluation tests were carried out showed the same calculation accuracy as traditional systems, making it possible, by means of a projection, to estimate an improvement in the performance of quantum computation over classical computation already with a 300-qubit processor, as already known from the scientific literature on the subject.

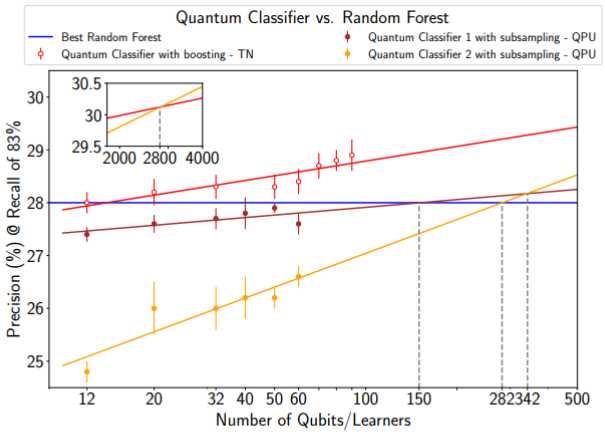


FIG. 8. Scaling of precision P of various proposed quantum classifiers with respect to the number of qubits, keeping $R = 83\%$. The two variations of the subsampling approach (yellow, brown) are implemented on QPU (filled dot) between 12 and 60 qubits. The boosting approach (red) is implemented using the TN optimizer (empty dot) between 12 and 90 qubits. The best performance of the Random Forest classifier acts as threshold (blue). The error bars represent the variability in corresponding performance across 5 iterations/QUBOs. Scaling projections are obtained by linear extrapolation (plain line).

Figure 38 - Comparison projections between a popular classical ML mechanism (Random Forest) and quantum classifiers on neutral atom technology (Pasqal) showing a break event point around 300 qubits[134]

[133] https://pressroom.credit-agricole.com/news/quantum-computing-two-real-world-experiments-conducted-by-credit-agricole-cib-in-partnership-with-pasqal-and-multiverse-computing-produce-conclusive-results-in-finance-cddc-94727.html

[134] 2212.03223.pdf (arxiv.org)

6.3.8 Crédit Mutuel

In December 2023, through a press release on its strategic plan for the three-year period 2024-2027[135], the French group, one of the most active in the country, announced that it had launched applied research programmes in the quantum field, in particular aimed at countering fraud and optimal risk management. The company, which has identified a dedicated team within its Euro-Information technology division, has been collaborating with IBM for several years, which has included an initial phase of learning about how quantum computing works and about the use of IBM's SDK. The most recent objective is to introduce a Quantum Factory, a collaborative structure of technology and industry experts to help spread awareness on quantum issues and prepare the integration process of these technologies.

6.3.9 JP Morgan

JPMorgan's R&D department has been extremely active for years in conducting research on frontier technologies, and the quantum field is not an exception, with two separate threads focused on quantum computing and quantum communication, respectively. The corporate organization has provided for the identification of a team dedicated to these topics.

The use cases covered are numerous and can be viewed directly on the dedicated website[136]; a brief summary is given here.

With regard to the opportunities offered by quantum computing, JP Morgan is currently focusing on a wide range of use cases (portfolio optimization, derivatives estimation, risk analysis, applications in the field of Machine Learning in various scenarios, from fraud detection to Natural Language Processing).

In addition, in cooperation with Toshiba and Ciena, it realized a prototype on secure transmission via QKD in a metropolitan area (specifically, 800 Gbps transmission under standard environmental conditions[137]).

[135] https://investors.bfcm.creditmutuel.fr/static-files/2dea8d23-96b3-4eff-924a-d91a3dafddfe

[136] https://www.jpmorgan.com/technology/applied-research

[137] https://www.jpmorganchase.com/content/dam/jpm/cib/complex/content/technology/publications/qkd-research-prototype-project-5-1.pdf

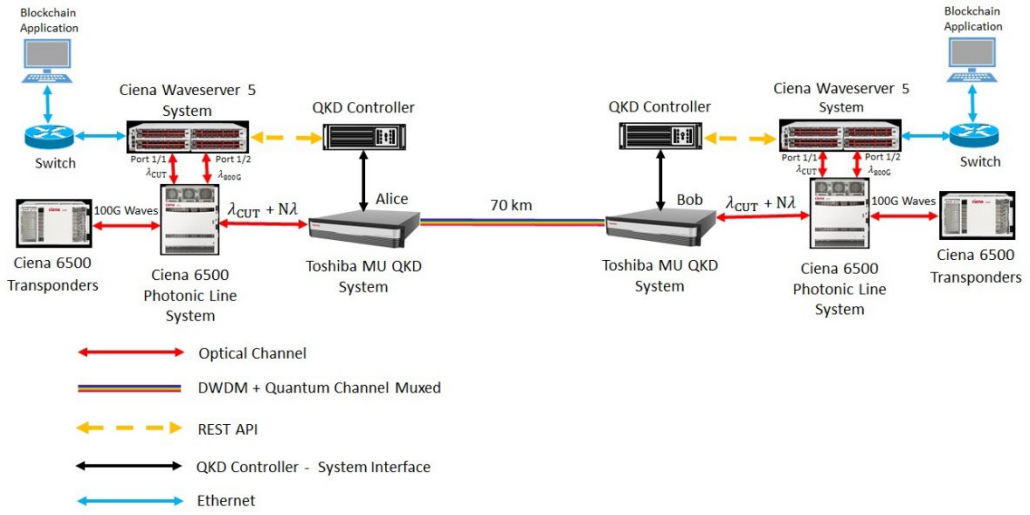


Figure 39 - Setup realized by JPMorgan in cooperation with Toshiba and Ciena for the quantum safe data transmission test of a blockchain application.

JPMorgan, like other financial institutions, has chosen to invest (USD 300 million) in a quantum computing start-up (Quantinuum) with which it has had a partnership since 2020. The new capital is earmarked for the advancement of its quantum computing systems (based on trapped ions) and the expansion of its quantum software capabilities.

6.3.10 HSBC

The institute has created an in-house quantum research team to develop use cases and related patents. The team collaborates with a number of international players such as IBM, Fujitsu and Quantinuum, but also with academia and government institutions[138].

HSBC, with the collaboration of British Telecom, using Toshiba's devices also tested a trading platform by encrypting data via QKD.

6.3.11 Santander Group

The Santander Group introduced a security-focused group (Quantum Threat Group) in 2019, which in 2022 defined the “Quantum Threat Program”, a long-term programme for the transaction to quantum safe cryptography.

In cooperation with Microsoft, it made available on gitlab an open source tool[139] for identifying vulnerabilities and one[140] for interpreting the results.

The group is very active in participating in international committees and disseminating practices related to quantum safety. In particular:

- is an active participant in the consortium, with HSBC and JPMorgan, of the National Cybersecurity US center of excellence on the Post-Quantum Migration project;

[138] https://www.hsbc.com/who-we-are/businesses-and-customers/hsbc-and-quantum
[139] https://codeql.github.com/
[140] https://github.com/Santandersecurityresearch/cryptobom-forge

- is involved in the activities of the World Economic Forum and in the Spanish component of the EuroQCI project (cf. 4.3.2.3);
- is part of the Spanish consortium Caramuel[141] to evaluate quantum satellite communications;
- is part of the steering committee of the Quantum Safe Financial Forum[142], created by the Europol European Cybercrime Center focusing on post-quantum transaction.

The comparison analysis between various quantum safe strategies proposed in chapter 5 of this report is taken from a presentation[143] shown by Santander during the PQC conference held in Amsterdam in 2023.

Santander is also involved in quantum computing, with the publication of several scientific papers.

6.3.12 The data from the survey of the Interbank Convention for Automation (CIPA)

The report "Survey on IT in the Italian banking sector - Economic and organizational profiles"[144], covering the year 2022, contains the results of the analysis dedicated to the topic of quantum technologies in the banking sector carried out by CIPA. The survey addressed both the opportunities and risks of these technologies, taking a snapshot of the situation at 2022 as well as the forecast for the two-year period 2023-2024. The survey, in which 21 banking groups, representing 92.5% of all groups in terms of total assets, and 33 banks took part, showed that seven groups have initiated analysis/study or experimentation activities on quantum and one group plans to do so by 2024, while more than half of the sample has not initiated and does not plan to initiate any initiatives on quantum by 2024.

The most relevant field of study/research is that of quantum algorithms aimed at improving performance (four out of seven responding groups). On the post-quantum cryptography front, two groups are active, a number that is expected to grow by 2024, especially in the activities of analysing their application pool and adopting quantum safe cryptography algorithms on traditional systems.

The survey also shows that expertise in the field of quantum technologies is mainly found through collaborations with the academic and research worlds, complemented by other modalities such as consultancy and specific training.

[141] https://www.hispasat.com/en/press-room/press-releases/archivo-2022/449/un-grupo-de-empresas-espanolas-lideradas-por-hispasat-trabaja-en-la-fase-de-viabilidad-de-caramuel-la-primera-mision-geoestacionaria-de-distribucion-cuantica-de-claves

[142] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/qsff

[143] https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_jaime-gomez_banco-santander_comparing-strategies-for-quantum-safe-cryptography-adoption-in-organizations.pdf

[144] https://www.cipa.it/rilevazioni/economiche/2022/Rilevazione_economica_2022.pdf

7 Conclusions

The working group would like to share, by summarizing them below, the main considerations that emerged in the course of the analysis and research activities on the various topics addressed in the document and in the comparison of the different experiences. It is evident that each recommendation must be assessed within the context of each organization, taking into account its specific characteristics, such as business needs, innovation prospects, investment availability and strategic opportunities.

First of all, a general appreciation emerged for the attention of institutions, such as Banca d'Italia and ABI, in stimulating the in-depth study of this subject. This is particularly noteworthy given the relatively limited national investments and initiatives—both public and private—when compared to the European and international landscape. At this stage of technological maturity, awareness is considered one of the most significant challenges, especially in securing the executive support of top management.

The possibility of comparison between different operators is considered fundamental and should be encouraged at all company levels. At this pre-competitive stage, it is believed that there is no hindering factor in sharing the experiences of individual companies, but that there is an overall benefit in pooling different experiences. This model is publicly pursued successfully by international companies such as JP Morgan, HSBC and Santander.

Participation in national and international events (cf. 4.1) is considered a valuable opportunity to create knowledge network, identify stakeholders and evaluate different use cases. Attention to institutional initiatives, to the state of standards-setting and to updates on advances in academic and industrial research is considered essential to facilitate a fruitful approach to these issues.

It is believed that the main challenge in the business environment is the ability to convey the importance of making dedicated investments right away, which is often limited by the difficulty of perceiving an adequate return on investment (ROI) value in the short to medium term in the face of a market offer that is not always mature and convincing.

Quantum technologies by their very nature are, once mature, expected to be technologies of great impact, but with reduced market availability. The risks of delayed investment could therefore materialize when, as the technology matures, the market does not offer widespread access to these tools, leading to a competitive disadvantage for players who have not invested in time[145].

Moreover, the need to address the risks of compromising the security of data and transactions, associated with the availability of quantum computing, must include the involvement of all actors, especially in the banking and financial context where a vulnerability that emerges and is made public could jeopardize the reliability and reputation of the entire system.

[145] In its paper addressed to the UK financial system (Minimising the risk: quantum technology and financial services - https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/minimising-risks-quantum-technology-and-financial) UK finance identifies as risk areas in relation to the advent of these technologies not only the possibility of traditional cryptography being compromised, but also a possible market instability generated by not investing in these opportunities. This scenario is exacerbated by the shortage of skills and experience in the field and by the technological debt of legacy systems.

It is essential to convey the message that, although there are differences of opinion on the time horizons of availability of quantum computing, the time required for current asymmetric encryption algorithms to become vulnerable may be shorter than envisaged, even just due to advances in classical cryptanalysis. Furthermore, the activities required to adapt IT solutions are costly and require adequate planning. Some of the procedures preparatory to the introduction of such safeguards are profitable independently of the "quantum" risk, as identifying systems and processes that depend on potentially vulnerable cryptography and prioritizing the resources to be protected (personal data, transactions, contracts, etc.) represent traditional continuous improvement processes[146]. In addition, prioritizing crypto agility and identifying flexible solutions, that can be easily updated or modified, can represent an opportunity to modernize the application framework. In some cases, such frameworks may be fragmented and burdened by layers of successive evolutions and maintenance activities.

Although the area of security is a priority for banks, it is equally important to advocate for the development of a strategy to adopt quantum computing in business sectors, particularly for addressing optimization problems and performing stochastic simulations in financial processes[147].

To make this approach as advantageous as possible, it is necessary to start with an inventory of those business applications that could benefit from this new computing paradigm, both in terms of both calculation speed, accuracy of results and, last but not least, the number of computing resources required to guarantee such timeliness and accuracy in the generation of outputs.

Although some scepticism has emerged, justified by the fact that, at least for someone, there are already viable alternatives in the short term with the use of other accelerated computing tools (GPU, TPU[148], etc.), the theoretical superiority of some quantum algorithms in perspective remains a scientifically proven fact. In this regard, the reflection on the environmental impact of the energy-intensive use of classical tools cannot be overlooked in the face of significantly lower consumption for the same computing time, e.g. for the cooling of superconducting quantum computers[149].

With regard to economic aspects, the experience of the group participants indicates that the expense of introducing PoCs to experiment with crypto assessment or the use of post-quantum safe

[146] In this regard, it should be noted that some indications in the recent DORA regulation (Digital Operational Resilience Act, Cpt.1 Art.6 and 7) and in the security standards for electronic payments PCI DSS 4.0 (12.3.3) refer to the implementation of inventory (crypto assets) and processes (crypto agility). These initiatives will therefore be included in the required compliance activities in this area to be implemented by 2025.

[147] . It is reasonable to assume that the near future will see strong developments on these topics, with the realization of industrial applications based on quantum machine learning and other quantum technologies.

[148] Graphical Processing Unit (GPU) and Tensor Processing Unit (TPU) are specialized processors designed to accelerate specific processing functions compared to conventional CPUs.

[149] It should be noted in this regard that other qubit technologies under study do not even require cryogenic technology for their operation.

software as well as access to cloud-based quantum computing resources (or their simulation) to assess the use cases of greatest interest could be low[150].

In this regard, it is also considered useful to suggest the possibility of accessing community resources by participating in projects financed by the European Commission (e.g. paragraph 4.3.2.2).

CERTFin, which in March 2024, through the ABI Lab Consortium, has already submitted two funding proposals for as many projects in the quantum field, is willing to coordinate these initiatives with the aim of fostering positive spin-offs for the entire banking community.

A final aspect of particular importance relates to the skills required in this domain. There was a general difficulty in finding human resources with adequate preparation, given the high specificity of the required skills and their cross-cutting nature in different areas, such as IT, physics and domain knowledge of the specific field of application under investigation. In this context, the proposal to identify partnerships with the academic world and research centers to attract talents and foster their growth is significant. There are many realities in Italy, some of which have also been described in this report.

In light of these considerations, banking and financial institutions are encouraged to reflect on the importance of defining a clear position in the field of quantum technologies. Depending on the context, it may be beneficial to develop a specific strategy or simply to reconsider the risk management process.

In describing the opportunities and dynamics of this complex emerging ecosystem, the working group participants express the hope that a collaborative network between companies, institutions, industries, and research organizations will be established, fostering collective growth.

[150] With regard to the specific technological choices or business partners with whom to start possible collaboration paths, the pros and cons of the two different approaches were analysed: on the one hand, exclusivity in the choice of a single supplier, and on the other, a plurality of agreements with specific vendors. In the first case, in addition to the advantage of managing a single end-to-end technology stack, the offer is often accompanied by comprehensive training and support paths. In the second case, experimenting with different hardware and software solutions, while entailing greater management complexity, reduces the risk of lock-in and makes it easier to change course in case one technological paradigm should prove uncompetitive in the long term. In any case, it seems sensible to start launching roadmaps, PoCs and prototypes, starting with the vendors with which one already has established business relationships. One hypothesis to consider is also that of investing in start-ups engaged in quantum research, contributing to own development and their development at the same time.

8 Insights

8.1 National quantum strategies

Australia has invested since 2015 in quantum technologies under the National Innovation and Science Agenda and then with the Australian Next Generation Technologies Fund and established several quantum centers of excellence, including the Center for Quantum Computation and Communication Technology. In June 2023, it launched the national quantum technology strategy for 2023-2030, based on five main themes: research and development; investment in industry-ready quantum technologies; access to essential quantum infrastructure and materials; skilled workforce; standards and frameworks; building a national quantum ecosystem. In addition to the national plan, Australia has also established partnerships with the US, the University of Singapore (for the creation of quantum telecommunications satellites) and Japan.

Canada defined its national strategy in January 2023, establishing the allocation of funds (CAN $360 million) allocated in April 2021 in research, education and talent development, and marketing. In 2023, the investment plan for the implementation of the quantum technology-based defence strategy, the Quantum 2030 programme, was also established. In addition to the national plan, Canada has also established several partnerships, including in 2022 with the European Union under the EU Quantum Flagship, with three research projects (MIRAQLS for sensing, FoQaCiA for quantum algorithms, HYPERSPACE for communications) and with France under the Canada-France Quantum Alliance.

Germany has been investing in quantum technologies since 2018, and in 2023 announced further investments for the development of a high-dimension quantum computer (between 100 and 500 qubits) by 2026.

France formally launched its strategy for the period 2021-2025 in 2021. In addition to research, infrastructure, training and security projects, part of this strategy is the installation of a hybrid HPC/quantum platform in the Très Grand Centre de Calcul - TGCC managed by the Commissariat à l'énergie atomique et aux énergies alternatives - CEA comprising the Joliot-Curie supercomputer, two 100-qubit Pasqal quantum computers, a photonic quantum computer and a complete quantum emulation environment.

In 2019, the Netherlands published the National Agenda on Quantum Technologies and in 2021 and 2022 allocated funds for the next seven years. Four action lines (research and innovation; ecosystem development, market and infrastructure creation; human capital: education, knowledge and skills; social dialogue on quantum technology) and three development programmes (quantum computing and simulations, national quantum network, quantum sensing applications) are highlighted in the strategy. In 2021 and 2022, funds were earmarked for the National Agenda until 2027. In 2015, funds had already been allocated for a ten-year period for the development of the first quantum computer.

Denmark launched its national strategy for the period 2023-2027 in two parts, in June and September 2023, respectively. The first focuses on international research, innovation, strategic and long-term investment, and improving access to research infrastructure with the aim of converting

research into applicable new technologies. The second part is dedicated to supporting the development, commercialization and application of quantum technologies for the benefit of society, economy, security and international cooperation. Denmark also hosts the NATO Center for quantum technologies, part of the Defence Innovation Accelerator for the North Atlantic - Diana programme, which aims to promote new technologies in Alliance countries and includes a project incubator, test center and laboratory. The initiative is part of the NATO-2030 project, which envisages the establishment of test centers and/or programmes to promote various innovative technologies in NATO nations.

Ireland established a Quantum Center of Excellence in 2020. In November 2023, it launched a national strategy called Quantum 2030 organized around five pillars (research - education - national and international collaboration - innovation, entrepreneurial ability and economic competitiveness - awareness of the benefits of quantum technologies).

Austria defined an investment plan in June 2021 for the period 2022-2026.

The UK defined its plan (National Quantum Technologies Programme - NQTP) in November 2013. In 2019, phase two was launched with investments for the period 2019-2024, while in March 2023 the government announced phase three with new funds for the period 2024-2033. The activities are coordinated by the Engineering and Physical Sciences Research Council. Initially, the funds were mainly allocated to four hubs specialized in computing, security, communications and sensors. These were joined in the second phase by the National Quantum Computing Center - NQCC with the task of developing NISQ and LSQ computers, algorithms, quantum software.

In addition to national plans, there are numerous collaborations between nations, such as the one between France, Germany, and the Netherlands signed in 2022 to increase synergies through the development of shared projects, and bilateral collaborations between the US and several European countries such as France, Finland, Sweden, Denmark, Switzerland and the UK. At the beginning of December 2023, 11 Member States (France, Belgium, Croatia, Greece, Finland, Slovakia, Slovenia, Czech Republic, Malta, Estonia and Spain) endorsed a European declaration on the strategic importance of quantum technologies for the scientific and industrial competitiveness of the European Union, pledging to collaborate on the development of a quantum technology ecosystem.

8.2 Steps for a quantum safe transition

8.2.1 Awareness

In order to raise awareness about the need to plan a migration process towards quantum safe technologies, it is crucial to adopt a strategic and engaging approach. Organizing workshops and informational sessions can effectively highlight the implications of quantum computing for IT security.

At the same time, it is necessary to conduct in-depth analyses of one's own technological infrastructure, assessing the maturity and robustness of existing IT security systems. These assessments should highlight potential vulnerabilities and critical points that could be exposed by the advent of quantum computing.

8.2.2 Define

To describe the phase of the migration process to quantum safe technologies in the banking context, it is crucial to clearly define the strategic objectives of the initiative. Arguably, limiting the perimeter to the security of payment systems alone may not be sufficient.

Strategic objectives should aim to achieve greater maturity of the entire ecosystem and not only of the payment chain, e.g. by ensuring better protection of infrastructures and sensitive data they manage, while guaranteeing business continuity and compliance with security and privacy regulations.

Once the objectives have been established, a detailed strategy must be developed outlining the actions and resources required to achieve them. In this respect, systematic approaches should be taken to migrate from vulnerable algorithms to quantum-resistant algorithms while respecting compatibility with the underlying supporting technology.

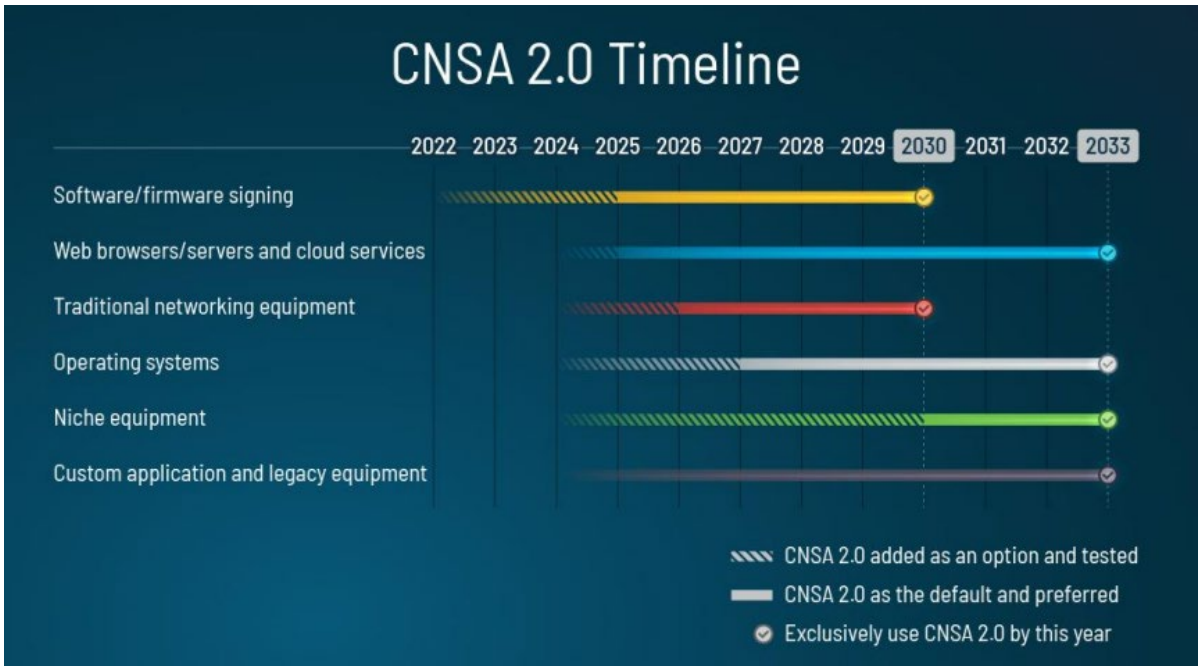
The actions to be taken are:

- draw up an inventory to determine which systems use public key cryptography and how they are used to protect the confidentiality and/or integrity of information used, exchanged or stored;
- support the industry in identifying emerging quantum standards and products, raising awareness of the technical characteristics of solutions that will replace potentially vulnerable components;
- identify technical constraints at an early stage in order to resolve any incompatibilities;
- work with service providers, partners and other stakeholders to better coordinate the adoption of the technical solutions needed to maintain the interoperability and business continuity of cryptographic systems.

The construction of a roadmap is crucial for planning and coordinating migration activities over time. This roadmap should establish a logical sequence of steps, clearly indicating the actors involved, the stages of solution implementation, the expected timeframe for each stage and the dependencies between activities.

Below is a picture with an example of a migration plan defined by the National Security Agency (NSA) relatively to the Commercial National Security Algorithm Suite (CNSA)[151].

[151] https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF



Estimating the necessary budget is another critical component of this phase and of the entire process. It is important to accurately estimate the costs associated with acquiring quantum safe technologies, upgrading existing infrastructure and systems, staff training and change management. This estimate should take into account any risks and contingencies during implementation.

Finally, the creation of a dedicated working group is essential to guide and coordinate the entire migration process. This group should consist of IT security experts and technical specialists from the various business functions involved, but, above all, it should be able to rely on the sponsorship of top management. Collaboration and involvement of different skills and perspectives are crucial for the success of the initiative.

Short-term expectations will necessarily include the completion of the requirements analysis, the selection of quantum safe solutions and the definition of the implementation strategy. In the medium term, it is expected to complete the migration of critical systems and to integrate the new technologies into the operational environment. In the long term, the goal is to ensure durable and resilient protection against emerging threats, while maintaining the efficiency and operational agility of the banking sector.

8.2.3 Identify

In this phase, all areas where encryption algorithms are used (applications, hardware and services) and the type of algorithms must be identified, both internally within the company and by third parties deemed critical. The primary aim is to build a crypto inventory, which can be easily consulted and constantly updated, so that any criticalities can be easily identified and an initial assessment of the impacts of a potential replacement of the encryption methodologies used can be made.

8.2.3.1 Crypto Discovery

In order to populate a crypto inventory, a preparatory step is necessary: using crypto discovery tools. To date, there is no single tool capable of interfacing with all legacy and/or open verticals on

the market (e.g. mainframe, AS400, Oracle DB, MS-SQL, NAS/SAN, etc.) and it is very likely that such a tool will never be available due to the strong heterogeneity of the technologies adopted to implement them.

Cryptographic artefacts can be recovered with network scanners (to intercept protocols such as SSH, TLS, IPSec, etc.), file system scanning to locate certificates, encryption keys, etc., or with other tools capable of analyzing, statically or dynamically, the source code. In general, software that falls into the SAST (Static Application Security Testing) category is potentially able to retrieve cryptographic artefacts directly from the source code. However, only a dynamic scan (run-time tracing) can identify the algorithms actually used and intercept the actual loading of external libraries.

Various open source software exist that can scan SSL/TLS servers in order to retrieve detailed information on the encryption algorithms used, such as, for instance, SSLScan, TLS_prober, TestSSL.sh or NMAP itself. In parallel, there is also proprietary software that can only scan specific technologies (such as mainframes or network equipment).

8.2.3.2 Crypto Inventory

A cryptographic inventory is a useful tool that collects information about the solutions in use, classifies their importance and relationship to business processes, and identifies the cryptographic variables used. Such an inventory is useful regardless of the quantum threat, as it also allows to highlight the possible use of obsolete algorithms (e.g. Data Encryption Standard - DES) that would make applications already exposed to security risks.

As suggested by NIST, an inventory should contain at least the following basic information:

- Encryption algorithms used:
    - Application
    - Type (e.g. AES, RSA, ECC), version and key length (e.g. 256 bit)
    - Operating modes (e.g. AES ECB, CBC, CTR)
    - Purpose of use (integrity, confidentiality, etc.)
- Protocols used:
    - Application
    - Type (e.g. SSH, TLS) and version
- Encryption library used:
    - Application
    - Library Name
    - Vendor
    - Type of licence (proprietary software, open source, ...)
- Digital certificates:
    - Application
    - Location of the certificate

- Type (RSA, ECC) and version
- Creation and expiration dates

Once this information has been recorded, it is also necessary to determine the usage characteristics:

- current key sizes and hardware/software limits on future key and signature sizes;
- latency and throughput thresholds;
- processes and handshake protocols for key creation;
- position of each cryptographic process in the stack;
- how the cryptographic process is invoked (e.g. by calling a cryptographic library, rather than using a process embedded in the operating system, using cryptography as a service, etc.);
- owner/provider of each cryptographic hardware/software/process;
- level of agility in the integration of hardware/software/cryptographic process;
- contractual and legal conditions imposed by and on the supplier;
- support duration and expected end-of-life date of the product, if declared by the supplier.

The crypto inventory should include both on-premises and off-premises environments information such as private/hybrid/public cloud. In addition, once completed, the consistency of the inventory's content with internal security policies should be periodically checked.

Hardware components (HSM, PKI, VPN appliances, firewall, IDS, etc.) also contain cryptographic artefacts and the ability to use specific algorithms. Given the relevance and role they play in corporate security, the inclusion of such equipment in the crypto inventory is essential.

Information from third parties (outsourcing, SaaS applications, etc.) should also be included in the database. However, it should be taken into account that self-declarations by suppliers (or vendors) could lead to the inclusion of partial and/or incorrect information with the risk of generating false positives or false negatives.

Lastly, in order to facilitate the planning of an effective migration, it can be very useful to integrate information on concrete use cases into the inventory. This is helped by the already mentioned document “Canadian National Quantum - Readiness”[152] where, in Annex D, E and F, examples such as Kerberos authentication, PKI/CAs systems and the sFTP protocol are described.

These scenarios are analyzed and inventoried according to this scheme:

- Description of use case
- Corporate value
- Information on volume, validity and purpose of use of data to be protected
- Type of use case (e.g. data in transit, inactive data, data being processed, digital signature)

[152] https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/CFDIR-Prati-Tech-Quant-EN.pdf/$file/CFDIR-Prati-Tech-Quant-EN.pdf

- Threat and technical considerations
- Types of encryption currently in use
- Technical components (e.g. end-point, network, database, file server)
- Locations where cryptographic information exists (e.g. DLL, hardware)
- Technical dependencies (e.g. details of components within this use case that depend on or rely on other systems for their security)
- Ability to support cryptographic algorithms (pre- and post-quantum) simultaneously

Instead, the evaluation of the following aspects can be postponed to a second stage:

- selection of the best algorithm to be used;
- order or sequence of what is to be updated;
- alternative paths to quantum remediation (e.g. full system upgrade, paradigm shift).

It is strongly recommended to create a repository that implements a hierarchical model, that can be interrogated and that keeps track of the relationships/interactions between different systems/objects in a way as to be fully aware of what is impacted by any change of a single item, whether it be an algorithm, a certificate or other.

8.2.4 Plan

To date, there is no firm timetable for the availability of the first quantum computer that could compromise asymmetric encryption. However, there are some indicative estimates[153]:

- 2026: ≈14% chance of violating the RSA-2048 algorithm;
- 2031: ≈50% chance of violating the RSA-2048 algorithm;
- 2035: RSA-2048 no longer secure.

This is sufficient to make some initial broad considerations: for example, if a new automated teller machines (ATMs) supply contract has a ten years life cycle, and the security of firmware is based on classical algorithms, it is clear that signing it up entails a potential risk to be managed. Similarly, it is necessary to plan more carefully the issuance of credit cards in relation to their expected maturity, since these are assets that, on average, remain in the possession of the customer from three to five years.

The first useful action for a proper risk analysis is to make use of what was done in the previous step. By means of the crypto inventory, it is possible to identify hardware, software and services that rely on classic algorithms, which will consequently be assessed at higher risk, especially in relation to their replacement times.

In this sense, one accompanying strategy could be to limit the duration of renewal contracts while accepting a lower discount.

[153] Michele Mosca - University of Waterloo - Canada - https://cryptoexperts.com/awacs2016/slide-awacs2016/awacs-2016.pdf

Generally, having a sufficiently comprehensive crypto inventory at disposal, the analysis can be carried out by following the main steps below:

- identify the presence of potentially vulnerable algorithms;
- understand the data formats used, application interfaces and cryptographic libraries to assess the necessary replacements;
- identify the best hardware implementing the new algorithmic strategies;
- identify all communication devices using vulnerable protocols;
- identify the dependencies of cryptographic protocols from the characteristics of algorithms.

It should be emphasized that the new algorithms may not be completely equivalent to the replaced ones. Indeed, they may not share the same performance or reliability characteristics as the latter due to multiple factors: differences in key size, signature, error handling, number of execution steps required to run the algorithm, complexity of the key creation process, etc.

This determines that, once the replacement algorithms have been selected, the organization will have to develop:

- a risk-based approach that takes into account the impact of substitution on business operations;
- a migration plan, including the timing and resources required;
- tools for validation and verification of implementation;
- extensive updating of processes and procedures used by developers and users;
- a communication plan to be used both internally and with customers and external partners.

The crypto inventory also makes it possible to understand which solution vendors and service providers are of most concern, perhaps because they are PKI or HSM providers. Another useful action is to question one's own third parties in order to investigate their level of quantum awareness, again prioritizing the services/contracts deemed most critical.

At this stage, it would be useful to create a heterogeneous working group within one's own organization that is dedicated to the topic and contributes to a pervasive risk analysis. In addition to the cyber security function, such a group could include, for instance, personnel from the risk department, the procurement department and the compliance department.

A good starting point could be the last Business Impact Analysis carried out, in order to start the analysis from critical functions and systemic processes.

To close the circle, the following questions should be asked:

- which services are you prepared to sacrifice in case you are unable to migrate all applications to post-quantum algorithms in time?
- what recovery plans can be implemented in case a quantum computer becomes available to an attacker and applications/services/hardware are not migrated in time?
- how can the security of data (archives and backups) be guaranteed when protected by classical algorithms that have since become obsolete?

8.2.5 Execute

In this phase, remediation actions are implemented, i.e. the activities defined within the risk treatment plan defined in the previous phase.

Such activities may involve the use of hybrid solutions or, if sufficiently mature, the use of fully post-quantum solutions. One aspect to be prioritized is to orient the infrastructure to have crypto agility features.

9 Bibliography

A few texts are suggested to deepen some of the aspects dealt with briefly in the report.

For an understanding of the fascinating world of quantum mechanics (with chapters on concepts underlying quantum computation and cryptography):

Gian Carlo Ghirardi: "A look at the cards of God" - Il Saggiatore (Milan, 1997)

The "bible" of quantum computing:

Michael A. Nielse, Isaac L. Chuang: "Quantum Computation and Quantum Information" - Cambridge University Press (2010)

For an up-to-date overview of quantum technologies

https://www.oezratty.net/wordpress/2023/understanding-quantum-technologies-2023/ - Sixth edition 2023 - Olivier Ezratty - Le Lab quantique

One of the benchmark reports (*McKinsey&Company*) for analyst assessment, containing several indications:

https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20technology%20sees%20record%20investments%20progress%20on%20talent%20gap/quantum-technology-monitor-april-2023.pdf