BANCA D'ITALIA

EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

The quantum challenge: implications and strategies for a secure financial system

by Cristina Andriani, Lorenzo Bencivelli, Antonio Castellucci, Mauro De Santis, Sabina Marchetti and Giovanna Piantanida

October 2024

Number 877

BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

The quantum challenge: implications and strategies for a secure financial system

by Cristina Andriani, Lorenzo Bencivelli, Antonio Castellucci, Mauro De Santis, Sabina Marchetti and Giovanna Piantanida

Number 877 – October 2024

The series Occasional Papers *presents studies and documents on issues pertaining to the institutional tasks of the Bank of Italy and the Eurosystem. The* Occasional Papers *appear alongside the* Working Papers *series which are specifically aimed at providing original contributions to economic research.*

The Occasional Papers *include studies conducted within the Bank of Italy, sometimes in cooperation with the Eurosystem or other institutions. The views expressed in the studies are those of the authors and do not involve the responsibility of the institutions to which they belong.*

The series is available online at www.bancaditalia.it .

ISSN 1972-6643 (online)

Designed by the Printing and Publishing Division of the Bank of Italy

THE QUANTUM CHALLENGE: IMPLICATIONS AND STRATEGIES FOR A SECURE FINANCIAL SYSTEM

by Cristina Andriani*, Lorenzo Bencivelli†, Antonio Castellucci‡,
Mauro De Santis§, Sabina Marchetti† and Giovanna Piantanida**

Abstract

Quantum computing (QC) is an emerging technology that can potentially solve long-standing computational problems considered intractable with classical computers, including encryption algorithms that protect communication channels and digital assets. While the financial sector is strategically positioned to leverage the benefits of QC, the diffusion of QC may turn into a vulnerability, as encryption protocols underpin the security of communication channels and the integrity of digital assets, including central bank digital currencies (CBDCs). Where there are numerous technological solutions that are not always interoperable or easy to integrate into the existing IT and network infrastructures, the transition to an ecosystem that is robust against QC attacks requires supranational strategies that support the adoption of mutually compatible standards. This paper provides an overview of QC and the possible implications of its diffusion for the security and resilience of the financial sector. It also identifies the most appropriate international cooperation forums for designing and monitoring the implementation of transition plans for the financial sector.

JEL Classification: F42, F50, L63, L86, L96.

Keywords: quantum computing, quantum agility, cryptography, technical standards.

DOI: 10.32057/0.QEF.2024.877

* Bank of Italy, Directorate General for Information Technology.

† Bank of Italy, Directorate General for Economics, Statistics and Research.

‡ Bank of Italy, Directorate General for Financial Supervision and Regulation.

§ Bank of Italy, Directorate General for Markets and Payment Systems.

** Bank of Italy, Directorate General for Planning, Organization and Accounting.

Executive summary[1]

- Quantum computing (QC) **is an emerging technology that can potentially solve long-standing computational problems considered intractable with classical computers**, (e.g. simulation, machine learning and optimisation problems). QC is also **poised to break encryption algorithms** protecting communication channels and digital assets.
- To date, QCs' hardware is still not mature enough for delivering a performing QC to the market. However, **hybrid setups integrating "small" QCs to high performance computers (HPC) and advanced cloud infrastructure are already available**.
- As an established pioneer in adopting emerging technologies, the financial sector is strategically positioned to leverage the benefits of QC. However, this proactive approach introduces a **two-fold challenge**:
    - **as a user**, although advanced digitalization facilitates widespread QC adoption in the financial sector (e.g. for risk management, pricing, capital allocation, and algorithmic trading), it demands consideration of potential unintended consequences (e.g. exploitation of sociological biases and social scoring);
    - **as a target**, advanced digitalization can turn into a vulnerability, with QC threatening security of encryption protocols, underpinning safety of communication channels and integrity of digital assets.
- **As critical financial and payment instruments of the future, including CBDC, crypto assets and other financial digital services, increasingly rely on asymmetric cryptography for storage and communication, they will be a major target for QC-based cyber-attacks (Quantum threat).** Remarkably, risks posed by QC are poised to be also retroactive for many systems as information available on today's cryptographically secure communication networks can be captured and stored, to be deciphered and exploited once technology keeps pace ("*harvest now, decrypt later*").
- Quantum-safe technologies, meant to mitigate the quantum threat, are already available on the market at different maturity state and different implementation costs. However, **the widespread use of QC-vulnerable encryption and the absence of universal agreement on standards and roadmap challenge the design of ad hoc migration plans toward quantum-safe environments, to achieve the so-called quantum resilience.**[2] Moreover, the interconnectedness of the global financial markets requires an enhanced international cooperation between all relevant stakeholders as *quantum safety is only achieved when the weakest link is quantum safe*.

[1] We wish to thank Alessandra Perrazzelli, Silvia Vori, Giuseppe Zingrillo and the other members of the Committee for the Cyber Security of the Financial System at Bank of Italy. We are also thankful to Caterina Beccarini, Giuseppe Bruno and Antonino Fazio for their support throughout the completion of the work. A special mention to Simone Montangero (University of Padua) for thoughtful discussions.

[2] At the international level, discussions to raise awareness and prepare for the security risks of quantum technologies have taken place mainly at the WEF, IMF and BIS. The G7-CEG has established the "Emerging Technology" specific taskforce to support the analysis of the impact of frontier technologies in the financial sector. As part of this mandate, the taskforce has prioritized quantum risks and could issue public communiqués, working papers and eventually policy statements in the course of the year.

- **To protect the financial system from the threats posed by QC, a strategy establishing a "global roadmap for quantum resilience" could be designed to provide a common policy framework for the financial system through an international cooperation approach**.
- **Such a strategy would allow for the monitoring, coordination and governance of initiatives essential for quantum-safe migration within the roadmap**. Individual initiatives could be implemented under the responsibility of different organisations, while it is proposed that the G20/G7 take over the governance of the overall migration roadmap.

Introduction

Quantum technologies have the potential to power next generation computers upscaling the computational capacity by some orders of magnitude without increasing the energy requirements by the same extent[3]. Opportunity will bring along risks, as the increased computing power could be used to solve the mathematical problems at the ground of the current asymmetric cryptography. Although we keep lacking a shared strategy to migrate our systems toward a quantum safe world, several technical solutions are already available.

In this paper we will discuss some key aspects of the migration to a quantum safe world with a specific eye to the financial industry, that is well positioned to pioneer solutions and strategies to exploit opportunities and face the challenges of the quantum revolution.

In the first section we will lay the ground for the discussion, describing the basic concepts and use cases of the quantum technology, the evolution of the market and the geopolitical angle of this nascent (and likely disruptive) industry. In the second section we will discuss concerns related to the implementation of quantum technology in the financial sector, with a focus on the cyber threat possible impacts, listing the available solutions and the possible advantages and drawbacks of each of them.

The final section will discuss a set of challenges and principles to set a regulatory and supervisory framework for the migration toward a quantum secure world. It calls for a globally shared strategy able to avoid the risks of systemic pitfalls while maintaining the market competitive.

1. Quantum Technologies: a revolutionary perspective

To date, Quantum Computing (QC) hardware is still not mature enough for delivering a performing machine to the market. Numerous technical hurdles stand in the way, including operational temperature close to absolute zero. Major companies (IBM, Google, Intel) are committed to large investments in building a practical quantum computer capable to solve problems that are beyond the reach of classical computers by 2030 (so-called *quantum advantage*) [1]. **McKinsey has estimated that 5,000 quantum computers will be operational by 2030 but that the hardware and software necessary for handling the most complex problems won't be available until 2035 or later** [2]. According to a survey of more than 300 firms by Hyperion Research, a prominent US consultancy in HPC and QC, from August through October of 2022, more than 80% of responding companies plan to increase quantum commitments in the following years, and one-third of those companies say they will spend more than $15 million annually on quantum computing efforts [3].

Exploitation of specific quantum mechanics phenomena offers innovative technological solutions to different problems in many sectors (see *Box. What are some potential business use cases for quantum computers?*), bearing the promise of combining increased performances with energy savings. Applications have been now explored for decades, since technology evolution allowed manipulation of materials at quantum level, and can be essentially grouped into three families, with different readiness and implications:

[3]Following several position papers on this topic, a worldwide initiative was launched in 2022, aiming at establishing accurate metrics for quantum technologies energy performances https://quantum-energy-initiative.org/qei2023/

- **quantum computing** refers to accomplishing a computation paradigm no longer based on binary logical elements (i.e. bits), but leveraging on probability density logical elements (quantum bit or qubits – See *Box. What is a Qubit*? in appendix). Despite the limited diffusion of marketable solutions, early quantum hardware products - basically special-purpose quantum computers, also called quantum simulators - are nevertheless already of interest to the industrial world, as they can provide accelerations in specific problems, including for example queue and portfolio optimization [4].
- **quantum communications (QComms)** refers to information transfers, enhanced/secured by quantum mechanisms. It leverages the materials' and light native properties to create networks for transmitting highly sensitive data.
- **quantum sensing (QS)** exploits quantum properties of matter and light to improve sensitivity in measurements (by orders of magnitude). Applications range from atomic clocks to bio-/medical-imaging to defects analysis in materials.

Box. What are some potential business use cases for quantum computers?

Quantum computing could impact 4 areas:

1. *Quantum simulation*. Scientists need to analyze molecules' structure to develop new drugs. Today's computers are not able to deal with accurate simulations, because each atom interacts with other atoms in complex ways. QC could be powerful enough to model even the most complex molecules.
2. *Optimization and search*. Every industry asks to optimize for efficiency and value creation. With classical computing, companies must face with a time-consuming and costly process given the many variables of any situation. Since QC can work with multiple variables simultaneously, they could reduce the complexity and classical computing can then be used to zero in on one precise answer.
3. *Quantum AI.* Mobility Companies would like to use Artificial Intelligence to teach a car to make crucial driving decisions. Quantum computers' ability to perform multiple complex calculations with many variables simultaneously allows for faster training and could speed-up the arrival of self-driving vehicles.
4. *Cybersecurity.* Cryptography is the backbone of cybersecurity systems, as it deals with techniques to store and transmit information in ways that prevent unauthorized access or interference. Modern cryptographic algorithms, when implemented correctly, are highly-resistant to attack – their only weak point is their keys. Breaking through that encryption requires massive computational power, which QC could potentially reach.

Quantum speedup is the ability of a quantum algorithm to solve a specific problem with fewer steps than the most well-known classical algorithm while **q*uantum supremacy*** refers to the point at which a quantum computer can solve ***intractable problems***. When reached, quantum supremacy is a significant achievement that highlights the special powers of quantum computers. Even though this might not have immediate applications in every industry, it might draw funding, encourage creativity, and result in the creation of new quantum technologies and algorithms. Achieving quantum supremacy can position a nation or business as a leader in the field of quantum computing.

[4] https://www.dwavesys.com/learn/customer-success-stories/
https://terraquantum.swiss/?utm_source=Nature&utm_medium=Referral&utm_campaign=April2024&utm_content=MPU

1.1 Quantum technology market and ecosystem: concentration, competition and trends

The development of quantum technologies is highly uncertain. So far numerous unexpected technical hurdles have emerged, raising the question on when will quantum computing be available on the market. Given the amount of investments necessary to develop quantum machines, it is becoming increasingly likely that computers capable of solving major problems will be developed and operated by very few players, leading to an additional layer of technological divide ("quantum divide"). To mitigate such effect, some big tech corporations (IBM, Alibaba Group, Google) are organizing to **provide quantum computing-as-a-service (QCaaS)**[5] together with their own software development kit - often free of charge - in order to create a community of developers and to widen the user base.

Leading technology companies have already developed working prototypes of quantum computers and dozens of known projects, from large companies to start-ups and universities, are underway worldwide to build quantum systems using various basic technologies. Over the past decade **an ecosystem of players along the QT value chains has emerged** attracting increasing amounts of funding and talents. Following Bova et al. [4] "quantum computers may not need to display a quantum advantage to be able to generate a quantum economic advantage for the companies that develop them".

According to McKinsey (2023) [5]**, only in 2022 the quantum industry saw an influx of $2.35 billion**[6] **in investments, primarily into established endeavours, with the financial services presenting the most valuable use cases** (especially in corporate banking, risk management, and cybersecurity scenarios). Despite the record investment and a potentially growing market size (estimated at around $106 billion by 2040 across all quantum technologies), investments in start-ups grew only by a modest 1% in 2022 highlighting the concentration risk in this industry.

A key factor for the industry and the market is the availability of relevant expertise in QT. Between 2021 and 2022, global job openings in the field of quantum technologies went up by 19%, with around a third of those positions remaining unfilled. Thanks to the opening of new advanced programs in quantum technologies by universities, the gap seems to have partially closed in 2023. Upskilling could potentially help narrow the talent gap, given the numbers of graduates with QT-relevant knowledge in adjacent fields [6].[7]

The supply of hybrid solutions, combining quantum computing with traditional technologies to exploit the competitive advantages of each one of the two, is a relevant market development. In principle, hybrid solutions can help in lowering the entry bar and the quantum divide for newcomers, by offering an affordable first batch of quantum accelerated services [7]. On the flipside, combining quantum technologies with cloud computing services and well trained large language models can spur further innovation by leapfrogging costly and demanding simulations to the advantage of BigTech conglomerates with access capacity to the combined set of technologies.

---

[5] https://en.wikipedia.org/wiki/Cloud-based_quantum_computing#Existing_platforms

[6] Being a nascent industry grounded on a technology largely deemed "foundational", public financial commitments often crowd in private investments. Drawing a clear line between these two stream of funding may not be easy. Further considerations on public resources can be found in the next section.

[7] Around 350k graduates of master's level or equivalent in biochemistry, chemistry, electronics and chemical engineering, information and communications technology, mathematics and statistics, and physics.

At the beginning of 2023, the World Economic Forum flagged the issue of a "*quantum divide at country level*": similarly to all enabling technologies, also for quantum the tight concentration of investments [8] raises concerns on inequalities stemming from different access level. Beyond implications on information security, quantum speedup in simulation and optimization problems solving is expected to boost productivity research in many sectors, as finance, climate modeling, biomedicine, thus directly impacting quality of life standards [9, 7].

Prominent public actors in the quantum technology market are distributed across the same three major blocks leading in computing (China, U.S. and European Union). Almost half of the annual global spending of public resources (Qureca estimates approximately $40B [10]) is attributable to China alone; European Union is the second investor (considering both EU programs[8] and investments by single member states[9]), followed by U.S., U.K., Canada, and Japan [8] [5]. Telecommunications, defense, space and microelectronics industries are leading public expenditure on quantum technologies, thereby encouraging new startup, public private partnership and other innovation enhancing endeavors.

Like in other advanced technology sectors, in QC policy makers need to strike a balance between preserving the competitiveness of the market and allowing big corporations to reach the size and the financial strength to invest in extremely costly equipment to be competitive in the global arena.

1.2 Quantum geopolitics: national strategies and governance gaps

Notwithstanding the many expressions of concern on asymmetric access to QC technology, no inclusion policies are currently in place; on the contrary, as the evolution of quantum technology is closely connected to national security risks, many government strategies reflect the criticality of the sector through reinforcing protectionism and hindering exchange of talents and knowledge.

In August 2023, the U.S. has taken a clear position in this direction, by stating in the "**Executive Order on Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern"**[10] (these last being China, Hong Kong and Macao) that: "*Rapid advancement in semiconductors and microelectronics, quantum information technologies, and artificial intelligence capabilities by these countries significantly enhances their ability to conduct activities that threaten the national security of the United States. Advancements in sensitive technologies and products in these sectors will accelerate the development of advanced computational capabilities that will enable new applications that pose significant national security risks, such as the development of more sophisticated weapons systems, breaking of cryptographic codes, and other applications that could provide these countries with military advantages*".

China applies a strict confidentiality to most quantum technology innovation projects, preventing forecasts on the reached computational milestones. However, the country is in full capacity of delivering quantum computers for commercial use, and some teams declared progress in cracking RSA keys [5]. In the field of communications, China has always been at the forefront of Quantum key Distribution (QKD) implementation, both as terrestrial backbone network (the Beijing-Shanghai Backbone Network –more than 2000 km- was put in place already in 2017) and as space-to-ground

[8] For instance: EU Quantum Flagship and European Quantum Communication Infrastructure, also mentioned in Section 2

[9] Quantum public spending exceeds $1B for both Germany and France

[10] https://www.whitehouse.gov/briefing-room/presidential-actions/2023/08/09/executive-order-on-addressing-united-states-investments-in-certain-national-security-technologies-and-products-in-countries-of-concern/

transmission, pioneering satellite link-based quantum network (in 2017, a first intercontinental quantum secure transmission between China and Austria was achieved) [11]; McKinsey reports that, in 2021, China had in place a fully operational QKD network -extended for >4600 kilometers and connecting >150 linked users- combining hundreds of fiber links and two ground-to-satellite links [5]. At the beginning of 2024, the RAND corporation [12] highlighted that, while both the U.S. and China are global leaders in quantum technology, the latter actually leads in quantum communications (and specifically, in QKD), whereas the United States are ahead in quantum computing.

The European Union Commission, in its Digital Europe Programme's priorities, focuses (i) on implementing the European Quantum Communication Infrastructure (EuroQCI), (ii) on promoting Member States own national infrastructures and (iii) establishing a coordination action among all projects. The EuroQCI, in the official claim, *"will reinforce the protection of Europe's governmental institutions, their data centres, hospitals, energy grids, and more, becoming one of the main pillars of the EU's Cybersecurity Strategy for the coming decades"*[11]. Industry projects contributing to the EuroQCI are financed through the EU Quantum technologies flagship[12] whereas satellite-based network is supported by the European Space Agency through the QKD Satellite Partnership Project. Regarding computing, EU industry and research are well positioned- in components development, but quantum computers are still at experimental level.

Extreme protectionism and division across geopolitical blocks could turn out to be a short-sighted approach also to the goal of standardization and (cyber)security. The strong dependency of digital services and infrastructures on transnational supply chains implies that real "quantum safety" is only achieved when the weakest link is "quantum safe" [9]. There is then room for governments' and regulators' action, to be taken before the "winner-take-all" dynamic prevails and backfires.

2. Risks for the financial system

The financial sector has a history as a testing ground for emerging technologies. In line with established patterns characterizing most emerging technologies, this proactive stance enhances the sector's ability to harness the benefits from QC, while it also contributes to widening its risk landscape both as a user and as a target.

By enabling decryption of cryptographic protocols, QC could harm security of communication channels and digital assets, with major consequences. As a user, the advanced degree of digitalization and the technical expertise of its stakeholders could facilitate widespread and rapid adoption of QC. However, QC could also introduce inherent risks from its application. In detail, issues related to QC-powered solutions could undermine service operation in finance and they could pose systemic risks. As a target, the degree of digitalization itself poses vulnerabilities as the protocols underpinning security and functionality of activities in the financial sector could be compromised by advancement in QC.

[11] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci
[12] https://qt.eu/

2.1 Risks from the adoption of QC solutions

The financial services sector is poised to reap significant benefits from quantum-powered solutions. QC could improve efficiency and effectiveness of a number of processes widely used in finance, including **simulation-based methods** (e.g. for risk management or pricing, to explore stress test scenarios) and **optimization processes** (E.g. for portfolio management[13] and algorithmic trading) [13]. To determine the quantum economic advantage, business and technology leaders will have to consider two conditions: (i) whether a quantum computer exists that is sufficiently powerful to solve a particular problem and (ii) how much faster it would be at completing it compared with a comparably priced classical computer [14].

The integration of QC by individual intermediaries must carefully consider any unintended consequences. First, similar to other emerging technologies like AI, the speed of adoption of QC-powered services shall account for process disruptions resulting from overload or multitasking.[14] Second, the migration from established ICT systems to QC-powered solutions necessitates substantial upfront costs. Beyond hardware and software adaptation, a fundamental change in computational logic may be necessary. The introduction of programming complexities may be required to ensure that qubits - which store information - remain coherent in order to reduce errors during calculations. These complexities become more challenging as we scale up the number of qubits to solve more complex problems.

High market concentration of QC might bolster systemic risks referring to services operation and financial inclusion (as anticipated in Section 1.1 Quantum technology market and ecosystem: concentration, competition and trends).[15] Concentration of the industry delivering QC solutions exposes provision to significant disruptions or failures facing potential issues or vulnerabilities. Additionally, since hardware development heavily relies on procurement of critical raw materials to build it [15] (e.g. rare earths for the production of superconductors or helium, to cool down conductivity of electrons in quantum computers), concentration in the upstream processes exposes operation of financial services also to potential disruptions in the supply chains of such materials. Akin other emerging technologies, the lack of a regulation and established technical standards may lead high concentration of the QC market leading to the creation of a ***quantum divide***[16].

2.2 Risks from QC cyber-attacks

Cryptographic algorithms underpin secure operation of the financial system. Particularly, public-key encryption underlies **authentication and authorization processes** for payments, transfers and communications. It also ensures **privacy, confidentiality and integrity of data**, that in the financial

[13] E.g. Citi & Classiq: Quantum Solutions for Portfolio Optimisation | FinTech Magazine

[14] In the context of QC-powered services, overload refers to settings where the process entails too many complex calculations, that increase the interaction with the environment, leading to faster decoherence, i.e. qubits gradually lose their ability to hold quantum information (superposition). Multitasking refers to the simultaneous management and concurrent execution of computational processes; e.g., multiple algorithms, complex calculations, simultaneous handling of different data inputs. Also multitasking can increase decoherence and introduce errors.

[15] Market concentration mainly results from the sizeable costs of hardware technology development, with few tech firms and countries actively investing in hardware technology for QC. Concentration characterizing QC hardware development has been de facto influencing software development as well. See Section 3.

[16] A quantum divide would entail certain actors effectively reaping the benefits of quantum-powered services and others being unable to afford to leverage on quantum technology. This could exacerbate existing disparities in access to financial services, on the demand side.

system may refer to confidential individual or corporate data as well as to digital assets or to bookkeeping of transactions on distributed ledgers.

The relevance of financial networks and their exposure to communication channels (payments and transactions) and digital assets (data security) already make them a major target for eavesdropping and other cyberattacks [16]**.** Against such backdrop, QC could threaten cyber security of the financial system [17], with substantial implications for customer protection, financial stability and privacy [18]. To date, however, most financial operators have been lacking private incentives in internalizing risks stemming from vulnerability of cryptography to QC [17].[17]

QC-powered cyberattacks expose financial services to several risks. Main risks stem from **infrastructural vulnerability** of asymmetric encryption-based communications - QC could tap into public-key encrypted communication channels to authorize transfer of digital assets, to forge transactions and certificates, taking over private networks. Additional risks may arise from potential **brute force cyberattacks** targeting digital assets, cracking cryptographic keys to breach sensitive data as well as distributed ledgers[18]. For many systems, risks are poised to be also retroactive as today's encrypted financial data can be intercepted and hoarded, to be deciphered and exploited once technology keeps pace ("*harvest now, decrypt later*"). Furthermore, advancements in AI technology could boost effectiveness of cyberattacks, providing malicious actors the opportunity to leverage on unforeseeable capabilities of QC to breach security protocols (E.g. generative AI systems could support adaptive hacking of increasingly secure cryptographic keys).[19]

As financial markets increasingly rely on digital payments, their vulnerability to QC-powered cyberattacks exposes systemic operation of financial infrastructures to major risks. This holds significant relevance for traditional payment infrastructures and for blockchain platforms, as central banks are exploring the development of **Central Bank Digital Currencies (CBDC)** and other innovative financial instruments. To protect customers and uphold continuous service operation of payment infrastructures amidst the technological landscape shift brought by advancements in QC, it is key resorting to robust security measures, enhancing operational resilience of authorization protocols and digital signatures underpinning digital payments. The design of the digital euro infrastructure already takes quantum safe native technologies into account[20].

To secure communication channels and safeguard privacy and integrity of digital assets, the financial sector should in principle lay out *ad hoc* migration plans toward quantum-safe environments under the coordination of multilateral regulatory bodies (see Section *2.3 The roadmap to quantum safety: one problem, many possible* approaches). Execution of a migration plan would require burdening inventory compilations, scrutiny of vulnerabilities, as well as preparation of inherently agile migration strategies, to cope with the unsettled nature of quantum technologies.

---

[17] A classical public goods dilemma underlies the lack of private incentives for investment in cybersecurity and operational resilience within systemic financial cyber risk. Individual banks face a situation where network externalities prevent them from fully capturing the benefits of their own cybersecurity investments. This creates an incentive to free-ride on the stronger cybersecurity measures implemented by others, leading to underinvestment in overall cyber defenses. Conversely, strong cybersecurity in a single institution benefits the entire financial system due to the interconnectedness that allows cyberattacks to propagate easily across institutions [40].

[18] Most blockchains rely on public-key RSA, ECC and DH encryption systems to secure transactions.

[19] In turn, QC could boost AI development, yielding increasingly unexplainable systems.

[20] https://www.ibm.com/blogs/digitale-perspektive/2023/08/implementation-of-the-digital-euro/

However, the extensive diffusion of legacy systems and lack of shared quantum-resistant standards may expose any migration plan to prohibitive costs and over-commitment of some actors. Such over-commitment could eventually backfire in case of unanticipated technology developments.[21]

2.3 The roadmap to quantum safety: one problem, many possible approaches

Technical feasibility is just one among the many prerequisites[22] of integration in the network architecture: whatever standalone quantum-safe solution a single organization (or sector) may prefer, **the tight interdependencies between telecommunications/media networks and the carried essential services (including payment and financial systems) call for international coordination and global migration strategies**.

The upcoming challenge for governments and authorities is then the simultaneous optimization of timing, investments, sustainability and permanence of solutions; as network communication capacity is crucial to societies to many extents, some non-negotiable ethical aspects[23] (see Section *3. Response, challenges and role of public* authorities) **could possibly enter the regulation path** [9].

A variety of quantum safe technologies are available, sometimes even commercially. Broadly speaking, standardization processes follow two paths:

i) **Redesigning classically computed protocols so as to make them insensitive to the performances of quantum computing, in the so-called Post Quantum Cryptography (PQC)**: as quantum supremacy does not apply to solution of all mathematical functions, PQC bases public keys on cryptography algorithm of a different kind, but still traditionally computed [19]. Leveraging on state-of-the-art technologies, PQC intended advantage is a reduction of costs and timing of the migration to a quantum safe paradigm. While PQC algorithms already exist, feasibility and non-regression of their implementation is still being explored[24] and their robustness has to be carefully tested. Replacing the prime number factorization with a problem currently untreatable may simply last until the problem becomes treatable; in this respect, hybrid devices combining AI and QC may accelerate considerably the process of breaking PQC algorithms [20].

---

[21] Over-commitment by both public and private financial institutions reflects additional challenges stemming from the digital divide at the firm-level. Bridging the quantum gap toward a coordinated migration of financial sectors toward quantum-resilient standards could reduce exposure of financial networks to local disruptions. Risks associated with a quantum divide would also materialize at the country level, affecting resilience of geopolitical actors (e.g. via asymmetries in warfare [16]) with major economic and societal implications.

[22] In particular, quality of service, interoperability and applicability of a control layer. In fact, quantum safety solutions do not address replacement of the cryptography infrastructure as a whole, but are almost exclusively concerned with asymmetric cryptography (currently used in key agreement, key transport, and digital signatures). Protocols for symmetric cryptography are not seen as endangered by advances in quantum computing performances, even in the long-term perspective.

[23] While ethical aspects have to be recalled in the phasing in of each emerging technology, in this specific case they refer primarily to the necessity for all actors in the financial system to access quantum safe technologies in presence of high entry costs.

[24] The U.S. National Institute of Standards and Technology (NIST) launched a competition for quantum-resistant algorithms, already in 2016: four PQC algorithms have hitherto been selected and standardization rounds are ongoing (finalization within 2024 is expected for at least three of the selected protocols. The Internet Engineering Task Force (IETF) has established a Working Group on Post-quantum use in protocols, and some work in progress on operationalization of the NIST-selected protocols is already available, see, for instance. https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers/ and https://datatracker.ietf.org/doc/draft-ietf-pquip-pqt-hybrid-terminology/01/

ii) **Turning the network infrastructure into a purely quantum-based one, by combining Quantum Key Distribution (QKD) and Quantum Random Number Generators (QRNG)**. Quantum phenomena can provide both true randomness in number generation (QRNG) and an information transport safe from eavesdropping (QKD)**.** QKD/QRNG technologies are already commercially available, they are targeted in the investment strategies of all countries/blocks (See Section *1.2 Quantum geopolitics: national strategies and governance gaps*) and standardization is at a far advanced stage[25]. Drawbacks related to quality of service and transmission performances still exist and limit applications in the short term. Finally, migration would require massive changes in the authentication infrastructure and a global agreement should be reached, in order to achieve interoperability [9, 20, 21]

In conclusion, although **the ideal network infrastructure will exchange quantum safe keys in quantum safe transmissions** and many relevant fora (e.g. Institute of Electrical and Electronics Engineers, Centre for European Policy Studies) recognize **the combination QRNG/QKD as the long term target** [9, 20]**,** real transition can only happen through many intermediate "hybrid" steps and implies co-existence and interoperability with currently operating devices and networks. **This is why PQC is pursued as the immediately applicable, less invasive alternative**, provided that operationalization is reached in the very short term.

As recently recalled in the EU Commission "Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography"[26], migration roadmaps need to be transnational, as would impact value chains in many sectors. High-level proposals and guidelines attempts from authorities and other stakeholders, as already available [22], [23], should then land into common roadmap and standardization candidates. (see also in Section 3. Response, challenges and role of public authorities).

In both cases, preconditions of quantum risks global awareness and promotion of crypto-agile design are indispensable to build the transition. Specifically in relation to payment/financial systems, Banca d'Italia recently illustrated lines of intervention based on QRNG/QKD and proposed a methodological contribution to agile design of cryptographic application [21].

3. Response, challenges and role of public authorities

Quantum technologies are set to disrupt financial organisations, **transforming their "digital economy" business models into new "quantum economy" ones**. Authorities need to act in order to manage the multiple implications of this transformation, which is characterised by an **unprecedented combination of opportunities, risks and uncertainties**.

[25] International Telecommunication Union – Telecommunication standard sector (ITU-T) already delivered several recommendations (Y.3800 series) on network architecture aspects of QKD networks and further others (y.1702 and Y.1710 series) on security aspects of QKD networks https://www.itu.int/en/ITU-T/publications/Pages/default.aspx. The European Telecommunication Standard Institute (ETSI) has an established Industry Specification Group on QKD (ETSI ISG QKD)

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

3.1 Why authorities should act now

As we have already seen, elusiveness of migration plans and lack of clear guidance from authorities across jurisdiction **are hampering industry's effectiveness in quantum-safe migration efforts** [24, 25, 26].[27] In addition, the global nature of the financial system, the interconnectedness of the industry and the common threat posed by quantum technology require public authorities to take a whole-of-government approach. This would include fostering dialogue with all relevant public and private stakeholders, prioritizing areas of intervention and **ensuring a harmonized roadmap towards a quantum-secure economy through proactive cooperation and international coordination**.

3.2 The challenges facing policymakers, regulators and the industry

The intersection of quantum computing and cybersecurity poses diverse issues, including technological, ethical, market, social, regulatory and governance challenges [9]. These challenges affect both financial authorities and market stakeholders. Furthermore, asymmetries between jurisdictions (regulatory frameworks, state of development, availability of investment and resources) amplify the complexity of pursuing a global and interoperable policy and regulatory approach.

The key challenges that need to be (simultaneously) addressed in order to achieve timely, harmonized, coordinated and efficient quantum security policy and regulation are:

- **Uncertain risk timeline.** The exact timeline for developing quantum or hybrid computers that are able to defeat traditional cryptographic protocols is uncertain. While this is increasingly seen as possible within a decade [27], the "harvest now, decrypt later" scheme poses an urgency now. Moreover, the lead time required for the financial sector to implement quantum-safe mitigations is another element that is difficult to predict.
- **Numerous possible solutions, each one carrying a different risk profile** (see section *2.3 The roadmap to quantum safety: one problem, many possible* approaches). While it is positive that more than one potential solution exists, this poses an immediate challenge to both regulators and industry. Indeed, fragmentation of solutions and standards slows down quantum migration in the short term and impacts market efficiency in the long term[28].
- **Need to balance long term risk vs. huge short term investment**. While the risk timeframe, though uncertain (see *Supra*), is long term one, in the short term huge investments of time, money and resources are required to prepare, plan and execute the quantum safe transition. Moreover, leaders struggle to balance between the increased cyber risk in a complex threat landscape and the long term quantum-security risks that are yet to materialize [26]. Authorities should help financial operators find a viable approach between strategic risk prioritization/mitigation and tactical constraints.

[27] Specifically, the lack of clear regulation affects financial institutions (more inertia in preparing and managing the quantum transition), vendor preparedness and investor confidence, resulting in the market maturing slowly.

[28] Fragmentation would challenge global organizations operating in multiple jurisdictions, adding complexity and compliance burdens. Transnational, harmonized migration roadmaps would be particularly important for the financial system, increasingly based on cross-border supply chains.

- **Complex financial infrastructure to be upgraded**. Financial sector organizations rely largely on legacy IT infrastructure[29]. In addition, the financial system is characterized by dense interconnectedness and branched supply chains. As a result, migrating to quantum-resistant cryptography means upgrading this complex infrastructure, which is a resource-intensive and very lengthy process, that needs to be factored into organizations' strategic plans.
- **Global nature, systemic implications**. The hyper-connected, global, and critical nature of financial market and payment system infrastructures require a systemic perspective to protect the overall business continuity. Quantum security policies need to identify and protect the most vulnerable points, including the emerging markets and the small/medium financial entities.
- **Lack of quantum awareness, knowledge and capabilities.** Quantum awareness, skills and capabilities are generally a gap to be bridged for the transition to a quantum-secure economy. Collaboration between regulators, industry, academia and quantum-focused research institutes is a critical requirement.
- **Understanding and prioritization of regulatory gaps**. To avoid regulatory over-engineering, current policies, regulations and tools should be carefully assessed to understand their ability to capture quantum risks, prioritize identified gaps and consider new regulation (only) where necessary.
- **Fragmented landscape.** Jurisdictions present heterogonous regulatory initiatives with minimal international coordination, varying levels of quantum maturity, and widely varying availability of investment and resources.

Most of the challenges outlined above are shared by policymakers, regulators, central banks and financial entities, providing an opportunity for a close collaborative response.

3.3 Observations on the current regulatory landscape

Although a comprehensive analysis of the quantum-relevant regulatory framework is not the ambition of this document, a few observations on key initiatives are outlined below as the groundwork for the discussion. **Globally, several public and private initiatives are taking place to support quantum regulatory development and standard setting. However, these initiatives still lack of harmonization and coordination**.

The **US government** has published a quantum migration deadline of 2035 [28]. The NIST is leading the international effort to establish standards and guidance on post-quantum cryptography solutions by 2024 [16]. On the other hand, **the EU** has not yet set such milestones. As a result, the migration to quantum-resistant cryptographic algorithms still seems to be rather uncoordinated across Europe with national guidelines often diverging and proposing frameworks that are at times challenging to implement [9]. To address this issue, the European Commission has recently issued a Recommendation[30] encouraging Member States to develop a strategy for the adoption of post-quantum cryptography, to ensure a coordinated and synchronized transition across Member States.

[29] Legacy information systems are characterized by being decades old, monolithic software architecture (e.g. mainframes), proprietary data models, minimal ability to interface with other/open systems, and ultimately very complex and costly to maintain and enhance.

[30] The strategy should define clear goals, milestones, and timelines resulting in the definition of a joint Post-Quantum Cryptography Implementation Roadmap. This should lead to the deployment across the Union of Post-Quantum Cryptography technologies into

A simplified and not exhaustive picture of the main international fora of policy makers, standard-setting bodies and industry groups dealing with cyber risk is shown in Figure 1. Organizations carrying out initiatives deeming relevant the cyber risks associated with quantum technology are highlighted and expanded upon below.

Among political/policy institutions, the World Economic Forum [26] and the International Monetary Fund [13] have carried out **mostly awareness initiatives and preparation discussions** on quantum technology security risk.

Among the international standard-setting bodies, **the authors of this paper are not yet aware of any public policy statements by the main authorities**. To this end, the G7-Cyber Expert Group has established a dedicated taskforce to support the analysis of quantum risks in the financial sector, and could issue public communiqués, position papers and eventually policy statements in the course of the year.

Projects and experimentations concerning quantum cybersecurity have been carried out mostly by Think Tanks research institutes so far [9]. It is also worth mentioning the Leap project at the BIS-Innovation Hub [25], a proof of concept to help the financial system move towards a quantum-safe state.

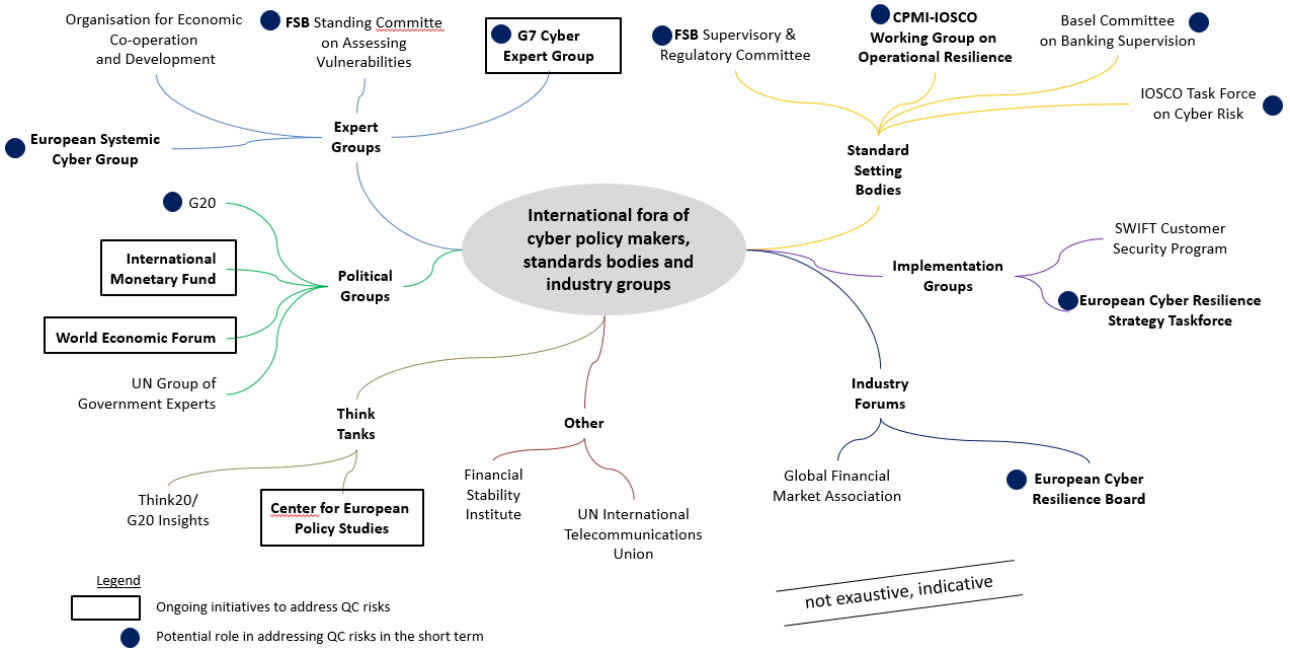

Figure 1 - Landscape of QC risk related international fora – authors' conceptualization

3.4 Initial policy approach and recommendations

Few preliminary steps need to be at the ground of any feasibile regulatory strategy. In particular: (i) promote continuous research to better understand the impacts of quantum on cybersecurity, assess risks and threats; (ii) to do so, there need to be policies to develop quantum skills, specifically in the intersection with cybersecurity; (iii) public policies should also support communication and improve

existing public administration systems and critical infrastructures via hybrid schemes that may combine Post-Quantum Cryptography with existing cryptographic approaches or with Quantum Key Distribution. https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography.

awareness [13, 9, 24, 26, 29]; (iv) finally, policy makers should extensively use regulatory sandboxes to test new regulations.

Building on the results of the initiatives taken so far by public institutions [13, 9, 26], the following recommendations are useful building blocks for defining the approach and directions of quantum cybersecurity policy:

- **Leverage existing regulatory frameworks** and avoid over-regulation to capitalize on existing regulatory assets and industry practices;
- **Standardized approach to risk mitigation** to enable synergies and faster development of a mature response in the presence of cyber threats common across jurisdictions and financial sector organizations;
- **Approach quantum cyber security collectively (public and private sector and across jurisdictions) through harmonized framework** to promote dialogue, collaboration and transparency: most of the challenges in developing a robust response to quantum cyber threats are shared by public authorities and industry organisations;[31]
- **Regulatory harmonization.** Despite their distinct perspectives, many challenges are shared across jurisdictions and have global implications. Harmonisation will be critical to avoid fragmented and conflicting approaches that could hinder the global development and deployment of quantum technologies.
- **Progressive implementation** to keep track of intermediate steps and monitor progresses [13, 30];
- **Balanced regulation.** Balancing the short, medium and long term impacts of quantum computing is key to providing clarity and certainty to the industry without compromising performance through excessive regulation. In addition, the trade-off between long-term risks and short-term investments should be continuously assessed throughout the migration phases.

Several public and private initiatives are underway to support the development of quantum regulations and standards, but there is still a lack of harmonisation and coordination[32].

To protect the financial system from the threats posed by QC, a strategy establishing a "global roadmap for quantum resilience" could be designed to provide a common policy framework for the financial system through an international cooperation approach.

Such a strategy would allow for the monitoring, coordination and governance of initiatives essential for quantum-safe migration within the roadmap.

To achieve this goal, relevant stakeholders – public authorities, standard setters, policy makers and representatives of the financial industry – could engage in initiatives to be included in the roadmap, as well as on its overall coordination and governance. An indicative (and non-exhaustive) list of candidate actions to be suggested under the roadmap could include (i) the development of a G7 CEG fundamental element on quantum cyber resilience; (ii) the extension of the BIS committees' work on cyber risk management frameworks for the digital euro; (iii) the establishment of a

[31] For example, policymakers can help industry by providing clear guidance on the quantum transition, while the market can help regulators identify policy gaps and priorities for intervention.

[32] At the international level, discussions to raise awareness and prepare for the security risks of quantum technologies have taken place mainly at the WEF, IMF and BIS.

quantum resilience task force within the CPMI-IOSCO Operational Resilience Group; (iv) the institution of public-private cooperation fora on vertical issues; etc.

Individual initiatives could be implemented under the responsibility of different organisations, while the G20/G7 could take over the governance of the overall migration roadmap.

Appendix 1 - Why Quantum Computing is powering next generation computers

Quantum computing is a fusion of quantum physics and computer science, incorporating some of the most stunning ideas from twentieth-century physics into an entirely new way of thinking about computation. Quantum physics is the science of describing how tiny particles, on the scale of electrons and photons, behave. Quantum computers use quantum mechanical effects - such as superposition and entanglement (See *Box. What is a Qubit*?) - to take advantage of these powerful concepts in order to achieve quantum advantage or supremacy.

Box. The Quantum Lexicon

The ability of a quantum algorithm to solve a specific problem with fewer steps than the most well-known classical algorithm for that problem is known as ***quantum speedup.*** It is basically the increase in performance that comes from employing a quantum computer for some tasks rather than a classical computer. **The speedup can have a substantial economic impact by expediting the resolution of intricate issues across multiple fields**. This may involve issues with drug development, cryptography, optimization, and other areas.

Instead, the phrase ***quantum advantage*** refers to a broader range of benefits that come from using a quantum computer, including increased performance and capability as well as quicker problem-solving times. Benefits in terms of accuracy, precision, or resolving issues that were thought to be unsolvable for traditional computers can be attributed to this. This broader concept could imply several potential economic benefits: the generic enhancements in precision and effectiveness in diverse computational assignments (machine learning, simulation, and optimization).

From a computational complexity stance, ***intractable problems*** are problems for which there exist no efficient algorithms to solve them. An algorithm is efficient if it's of polynomial time in its worst-case.

Polynomial time: An algorithm is said to be of polynomial time if its running time is upper bounded by a polynomial expression in the size of the input for the algorithm, i.e., $T(n)=O(n^k)$ for some positive constant k.

Exponential time: An algorithm is said to be exponential time, if T(n) is bounded by $2^{poly(n)}$, where $poly(n)$ is some polynomial. More formally, an algorithm is exponential time if T(n) is bounded by (2^{n^k}) for some constant k.

Example: We have 2 algorithms on a computer performing an operation in 10^{-6}sec where $T_1(n)=O_1(n^5)$ e $T_2(n)=O_2(2^n)$.

If we have to perform 30 operations, $T_1(30) = 30^5 * 10^{-6}$ sec $= 24.3$ sec and $T_2(30) = 2^{30} * 10^{-6}$sec $= 17{,}9$min.

If we have to perform 50 operations, $T_1(50) = 50^5 * 10^{-6}$ sec = 5.2 min and $T_2(50) = 2^{50} * 10^{-6}$sec = 35.7 years.

Quantum allows us to perform certain processes in a fundamentally different way . In extreme cases , computing times on conventional computers for exponential problems ,even with the most powerful supercomputers of the moment ,could largely exceed the age of the Universe ,estimated at 13.85 billion years.

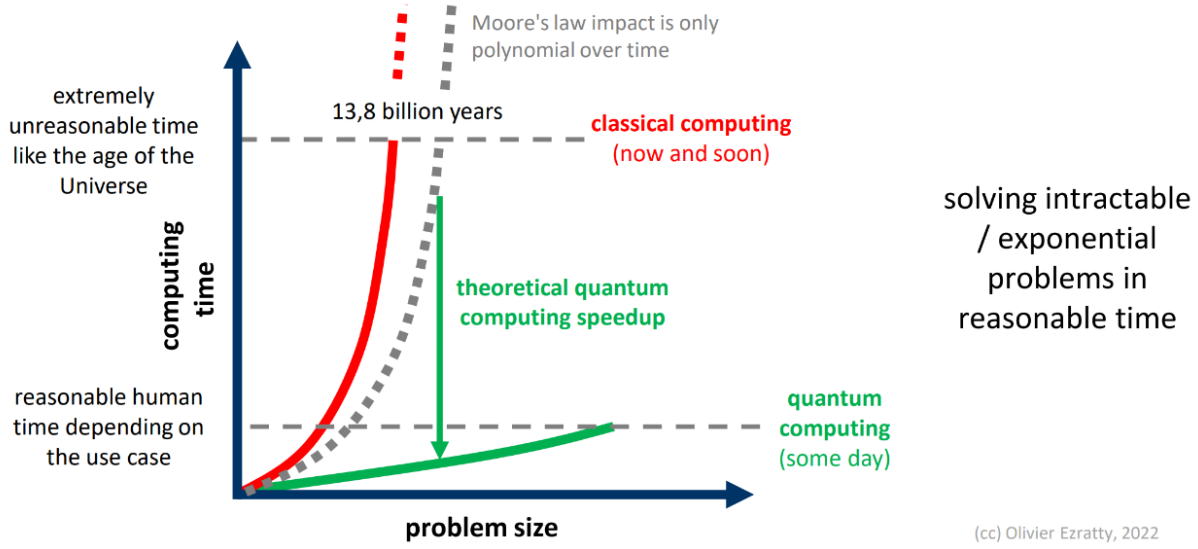

Figure 2 - simplified view of the quantum computing theoretical promise. Before delivering this promise, quantum computers may bring other benefits like producing better and more accurate results and/or doing this with a smaller energy footprint. (cc) Olivier Ez

Box. What is a Qubit?

A **bit** is the basic unit of information in classical computing and can only be in one of two possible states (0 or 1: the standard example is a switch that can be in either the on or off position (on/off).

A **qubit** is the basic unit of information in quantum computing. They can store not only 0 or 1, but also any superposition of them. In quantum computing, **ket notation** $|v\rangle$ is used to denote quantum states and mathematically it denotes a column vector in R^2. A qubit is a two-level quantum system where the two basis qubit states are usually written as $|0\rangle$ and $|1\rangle$ and we can express the state of a qubit, a two-level system, as a linear combination these two basis vectors.

$$\varphi = \alpha|0\rangle + \beta|1\rangle = \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\alpha\\\beta\end{pmatrix}$$

A central feature of quantum mechanics is that, when we perform a measurement to determine whether a state is $|0\rangle$ or $|1\rangle$, we get a random answer, and the probability of measuring a state is given by the squared magnitude of its coefficient: the probability of its being $|0\rangle$ is α^2; the probability of $|1\rangle$ is β^2.

One consequence of this is that, since such a measurement on a qubit state must result in 0 or 1, these squared magnitudes must sum to 1, since they are probabilities.

$$|\alpha|^2 + |\beta|^2 = 1$$

Since a qubit can be any unit ket and there are infinitely many unit kets, there are infinitely many possible values for a qubit. It is important, however, to notice that to get information out of a qubit we have to measure it. When we measure it, we will get either 0 or 1, so the result is a classical bit.

Qubits enable quantum computing because they can exploit two quantum phenomena: **superposition** and **entanglement**. Superposition means that a qubit can be in a combination of 0 and 1 states until it is measured, which collapses it to one definite value. Entanglement means that two or more qubits can share a quantum state and influence each other, even if they are physically separated. These phenomena allow qubits to represent and manipulate more information than bits, and to perform parallel operations on multiple qubits at once.

Quantum computing will quite literally change the world in various sectors, potentially benefitting society in various ways, such as making smarter investment decisions, developing drugs and vaccines faster and improving climate forecasting. However, the most imminent impact of quantum computers on society will be in regard to digital security and privacy, because one disadvantage of quantum computing is that it could break current cryptography [31], [32].

Appendix 2- How will Quantum Computing impact on "traditional" cryptography (Shor algorithm)?

Quantum machines can prove their *advantage* or eventually *supremacy* in solving numeric problems at the ground of modern cryptographic algorithms, such as factoring large numbers and solving discrete logarithms.[33]

Peter Williston Shor [33], an American professor of applied mathematics at MIT, devised a quantum algorithm[34] designed to solve the integer factorization problem, which involves breaking a large composite number into its prime factors. Shor's Algorithm promises to solve this problem in polynomial time, making it much faster and more efficient than any classical algorithm currently available. The worst-case complexity of the Shor's quantum factoring algorithm is $O((\log N)^3)$[35] where N is the integer that we wish to factorize.

A simplified Shor's Algorithm

Factoring large numbers has always been a challenge for mathematicians and computer scientists. Shor's algorithm provides a solution to this problem that grows in polynomial time with the length of the number we have to factorize.

Assume we want to factor *N* into the product of the two primes *p* and *q*. Before moving to the sequence of operations, let us first define two operators:

- *GCD(N,k)* is the Greatest Common Divisor, the largest natural number dividing *N* and *k*. and returning another natural number (e.g. *GCD(18,24) = 6*);
- *N mod k* is the module operator, returning the remainder of the division N/k (e.g. *17 mod 5 = 2*, *5 mod 10 = 5*).

The algorithm:

(1) Choose randomly a number between 1 and *N*, call it *k*.

(2) If *GCD (N, k) = 1* then move to (3).

(3) Find smallest positive integer *r* such that $k^r \bmod N = k \bmod N$. If *r* is odd, go back to (1) and choose a different value of *k.*

(4) Define $p = k^{r/2} \bmod N$. If $p + 1 = N$, then go back to (1) and choose a different *k*.

(5) The factors of *N* are

$f_1 = GCD\ (p+1, N)$

$f_2 = GCD\ (p-1, N)$

Example:

Let's factorize *N = 91*

(1) Pick *k = 3*

(2) *GCD (91,3) = 1*

(3) r = 6

$3^2 \bmod 91 = 9$

$3^3 \bmod 91 = 27$

$3^4 \bmod 91 = 81$

$3^5 \bmod 91 = 61$

$3^6 \bmod 91 = 1$

[33] Much of today's modern cryptography is based on mathematical algorithms able to generate complex cryptographic keys by multiplying large prime numbers. Cracking these keys through the inverse process could take years for a classical computers, even with a brute-force attack. A **brute-force attack** consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an **exhaustive key search**.

[34] Any algorithm that can be executed on a quantum computer is referred to as a "quantum algorithm". However, the term quantum algorithm is applied to algorithms of which at least one of the steps is distinctly 'quantum', using superposition or entanglement.

[35] QUANTUM INFORMATION & COMPUTATION - http://www.qi.damtp.cam.ac.uk/files/QIC-12.pdf

Step 4: $p = 3^{6/2} \bmod 91 = 27$
Step 5: ***91=13x7***
$f_1 = GCD(26, 91) = 13$
$f_2 = GCD(28, 91) = 7$

Once a sufficiently powerful machine can implement Shor's, any schemes relying on the factoring attack being computationally infeasible, like public key encryption schemes used in currently in all secure communication (e.g. RSA), will no longer be secure. These algorithms base their strength on the inaccessibility of large prime factors of a large composite number: while the encrypter takes two (or more) large primes and multiplies them, the decrypter tries to work backwards from the product to the factors. The latest factoring record is RSA-250 in February 2020 [34]. The computation involved tens of thousands of machines worldwide, and was completed in a few months. But a quantum computer of suitable size could factor these large numbers in a much shorter time. For a 1024-bit number, Shor's Algorithm requires on the order of 1024^3, about one billion, operations. I do not have any information on how quickly quantum operations can be executed, but if each one took one second our factorization would last 34 years.

If a quantum computer could run at the speed of today's electronic computers (100 million instructions per second and up) then factorization of the 1024-bit number would be a matter of seconds. From 2001, when IBM computer scientists [35] reported that "15" was factored with 7 qubits using Shor's Algorithm, there have been several successful experimental demonstrations of the factoring algorithm. To date, a factorization method that could break a 2,048-bit RSA key using a quantum system with 20 million of physical qubits takes 8 hours [36].

Notably, while QCs' hardware is still quite far from market penetration, hybrid setups are just reality: even in their current design, quantum computers are not standalone machines, but can be integrated in complex computational architectures: cumulative advantages deriving from combination to high-performance computing (HPC), advanced cloud infrastructure, and Artificial Intelligence/Machine Learning (AI/ML) capabilities can be massive.

Such advantages are reciprocal, and not just in terms of augmented computation potential: some boundaries to HPC and AI/ML full explosion are -in fact- currently settled by physical limits and sustainability constraints to powering capacity.[36]

"Quantum advantage" is then to be regarded at as a relevant, enabling, component of the wider "hightech- advantage": hybrid systems are expected to accelerate solution of simulation and optimization problems and reduce timing of AI/ML training in the near term, well before cryptography violation is achieved [5].

Furthermore, in consideration of the technical limits that prevent a wide market penetration of quantum computers, cloud access could reasonably become the short term preferred way to experiment with quantum computing at a relatively modest entry cost (See Section 3). BigTechs (IBM, Amazon, Xanadu, …) and other advanced QC specialists (like D-Wave) are already leveraging their capabilities and offering the socalled **Quantum computing as a service (QCaaS)**.

[36] Integration with quantum computers for specific processes within resource demanding functions could in principle bring significant efficiency gains in energy consumption.

References

[1] «The Race Toward Quantum Advantage,» 14 9 2023. [Online]. Available: https://semiengineering.com/the-race-toward-quantum-advantage/ .

[2] McKinsey, «What is quantum computing?,» 1 5 2023. [Online]. Available: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing.

[3] B. Sorensen, «QUANTUM COMPUTING EARLY ADOPTERS: STRONG PROSPECTS FOR FUTURE QC USE CASE IMPACT,» 11 2022. [Online]. Available: https://www.dwavesys.com/media/yfohvw1r/hyperion_report_23_final.pdf.

[4] Bova, F., A. Goldfarb and Melko R.G., «Quantum Economic Advantage,» *NBER Working Paper*, n. 29724, 2022.

[5] McKinsey & Company, «Quantum Technology Monitor,» 2023.

[6] Mohr, N., Peltz, K., Zemmel, R. and Zesko, M., «Five lessons from AI on closing quantum's talent gap—before it's too late,» McKinsey Digital, 2022.

[7] Holley, K., «Bridging The Quantum Divide,» *Forbes*, 2023.

[8] Hidary, J and Sarkar, A, «The world is heading for a 'quantum divide': here's why it matters,» in *World Economic Forum Annual Meeting 2023*, Davos, 2023.

[9] Pupillo, L., Ferreira, A., Lipiäinen, V. and Polito, C. , «Quantum Technologies and Cybersecurity: Technology, governance and policy challenges,» Centre for European Policy Studies, Brussels, 2023.

[10] QURECA, «Overview of Quantum Initiatives Worldwide 2023,» QURECA, 19 July 2023. [Online]. Available: https://www.qureca.com/overview-of-quantum-initiatives-worldwide-2023/.

[11] S.-K. L. e. al, «Satellite-Relayed Intercontinental Quantum Network,» *Physical Review Letters*, vol. 120, p. 030501, 18 January 2018.

[12] Harting S., Gonzales D., Mazarr M.J., Schmid J., «Comparative Analysis of U.S. and PRC Efforts to Advance Critical Milittary Technology. Volume 1, analytic Approach for Conducting Comparative Technology Assessment,» RAND Corporation, Santa Monica, Calif., 2024.

[13] Deodoro, J., Gorbanyov, M., Malaika, M., Sedik, T. S., & Peiris, S. J., «Quantum Computing and the Financial System: Spooky Action at a Distance?,» *IMF Working Papers*, n. 071, 2021.

[14] S. Choi, W. S. Moses e N. Thompson, «The Quantum Tortoise and the Classical Hare: A simple framework for understanding which problems quantum computing will accelerate (and which it won't)),» 24 Ottobre 2023. [Online]. Available: https://arxiv.org/abs/2310.15505.

[15] Mans, U.,Rabbie, J. and Hopman, B., «Critical Raw Materials for Quantum Technologies: Towards European technology sovereignty in an emerging industry,» Quantum Delta NL - TNO, 2023.

[16] R. H. R. a. A. T. Jamilov, «The anatomy of cyber risk No.,» *w28906. National Bureau of Economic Research*, 2021.

[17] A. W. A. H. a. Q. A. I. Butler, «Prosperity at Risk: The Quantum Computer Threat to the US Financial System,» Hudson Institute, 2023.

[18] F. J. J. M. L. a. P. W. Herrera Luque, «Cyber risk as a threat to financial stability,» *Revista de Estabilidad Financiera/Banco de España*, vol. 40, pp. 181-205, 2021.

[19] NIST, «NIST,» 24 August 2023. [Online]. Available: https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers.

[20] Xu G., Mao J., Sakk E., and Wang S., «An Overview of Quantum-Safe Approaches: Quantum Key Distribution and Post-Quantum Cryptography,» in *57th Annual Conference on Information Sciences and Systems (CISS)*, 2023.

[21] Bucciol, E. e Tiberi, P. (Banca d'Italia), «Quantum safe payment systems,» *Markets, Infrastructures, Payment Systems*, n. 35, 2023.

[22] CISA, NSA and NIST, «Quantum Readiness: migration to post-quantum cryptography,» 2023.

[23] TNO - Applied Cryptography and Quantum Algorithms and CWI - Cryptology Group and AIVD - Netherlands National Communications Security Agency, «The PQC Migration Handbook: guidelines for migrating to post-quantum cryptography,» Ontwerp, 2023.

[24] Digital Regulation Cooperation Forum (DRCF), «Quantum Technologies Insight Paper,» DRCF, 2023.

[25] Bank for International Settlements - Innovation Hub (BIS-IH). Dupont, A., «Project Leap. Quantum-proofing the financial system,» in *Securing the future monetary system - Cybersecurity for Central Bank Digital Currencies*, Basel, 2023.

[26] World Economic Forum, «Quantum Security for the Financial Sector: Informing Global Regulatory Approaches,» Davos, 2024.

[27] M. P. M. Mosca, «Quantum Threat Timeline Report,» Global Risk Institute, 2022.

[28] A. Pugh, «Tandem, "Financial Institutions & Quantum Computing: A Cybersecurity Compliance Timeline",» 20 10 2023. [Online]. Available: https://tandem.app/blog/financial-institutions-quantum-computing-a-cybersecurity-compliance. [Consultato il giorno 2024].

[29] IBM - Mattei, F., «Quantum Computing and Quantum Safe,» 2023.

[30] ETSI, «TR 103 619 - CYBER; Migration strategies and recommendations to Quantum Safe schemes,» ETSI, Sophia Antipolis Cedex (F), 2020.

[31] FORBES, «15 Significant Ways Quantum Computing Could Soon Impact Society,» 2023.

[32] DIGICERT (Hollebeek, T.), «BLOG > SECURITY 101 > THE IMPACT OF QUANTUM COMPUTING ON SOCIETY,» 2023. [Online]. Available: https://www.digicert.com/blog/the-impact-of-quantum-computing-on-society.

[33] Shor, P.W., «"Algorithms for quantum computation: Discrete logarithms and factoring".,» in *Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press.*, 1994.

[34] F. G. P. G. A. H. N. T. E. Z. P. Boudot, «Comparing the difficulty of factorization and discrete logarithm: A 240-digit experiment,» Agosto 2020. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-56880-1_3.

[35] Vandersypen, L. M. K. ,Steffen, M., Breyta, G., Yannoni, C. S. , Sherwood, M. H. and Chuang, I.L., «Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance,» *Nature*, vol. 414, pp. 883-887, 2001.

[36] C. G. a. M. Ekerå, «How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits,» *Quantum*, vol. 5, p. 433, 2021.

[37] McKay, E., «"Keep the fight unfair": Military rhetoric in quantum technology.,» *arXiv - Quantum Science and Technology*, vol. special issue "Social aspects and impacts of quantum technologies", 2022.

[38] OECD, «A blueprint for building National Compute capacity for Artificial Intelligence,» *OECD DIGITAL ECONOMY PAPERS*, n. 350, 2023.

[39] World Economic Forum, «Quantum Economy Blueprint,» World Economic Forum, 2024.

[40] K. D. C. a. G. P. Anand, «Cybersecurity and financial stability,» *Deutsche Bundesbank,* vol. 08, 2022.