Alessandra Perrazzelli: Steering the transition to a quantum-safe world. An internationally coordinated approach

Keynote speech by Ms Alessandra Perrazzelli, Deputy Governor of the Bank of Italy, at the G7 conference on "Building the quantum safe financial system: what role for authorities and for the private sector?", Rome, 24 September 2024.

* * *

Introduction

Good morning and a very warm welcome to this important workshop on how to build a quantum-safe financial system.* I would like to start by thanking Prof. Cirac Sasturain and all the participants in the panel sessions for their insightful and thought-provoking contributions. Let me extend my gratitude to all the speakers, panellists, and attendees who have travelled from near and far to come here in Rome. Your presence and contributions are vital for the success of this workshop. I am confident that through our collective expertise and collaboration in the remainder of the workshop we will succeed in laying out actionable outcomes for steering the financial system's transition towards a quantum-safe world.

Quantum computing, as already noted by many speakers this morning, has the potential to revolutionize the financial system. Thanks to its unparalleled processing power and innovative capabilities, quantum computing can bring about a paradigm shift from the current 'digital economy' to a new era of 'quantum economy'. Such shift encompasses unseen opportunities along with significant challenges for global financial markets, including – in particular – unbalanced access to technology and cybersecurity threats, which we must address with foresight and in a spirit of collaboration.

As central banks and financial supervisors, we recognize the importance of striking a balance between steadfastly embracing technological changes on the one hand, and retaining a more cautious approach on the other, in light of the objective of safeguarding the stability, security, and integrity of our financial systems. It is part of our duty to promote and actively participate in the discussion on how to ensure the financial system's transition to the quantum era in the safest possible way, considering the limitations of current technology.

Quantum computing, while potentially threatening our system for secure communications, will also be instrumental in developing the solutions to restore resiliency in our financial system. In fact, quantum computing is bound to generate an unprecedented combination of opportunities, risks and uncertainties, which must be managed carefully in order to avoid market inertia and fragmentation, and to sustain an orderly and efficient transition to a quantum-safe world.

With today's workshop, we intend to launch a discussion on a possible path for steering the financial system's migration to quantum resilience, within the framework of an internationally coordinated approach involving all the stakeholders: authorities, financial industry, technology providers and academia.

1. The quantum financial system of the future: timeline, opportunities and risks

The quantum revolution is already happening, although the exact timeline for its full deployment can hardly be predicted. Innovation in this field is characterized by pivotal and often unexpected transformative breakthroughs leading to sudden acceleration, and sustained by consistent and sizeable public and private investments. The explosion of artificial intelligence technologies, whose interplay with quantum computing holds the potential for both steering and accelerating the development of far-reaching solutions, is making this path even more unpredictable. Against this backdrop of high uncertainty, we expect that the quantum machine capacity necessary to give rise to a significant cybersecurity threat will be achieved in a foreseeable future.[1]

The financial sector plays a dual role that enables it to look at the quantum phenomenon from two distinct perspectives: firstly, as a user, keen on embracing the capacity of quantum computing for innovation, and secondly, as a highly vulnerable target for quantum-powered cyberattacks.

Although the use of quantum computing in the financial sector is still at an immature stage, experimental results already highlight its ability to improve key financial processes, such as risk and portfolio management, payment services and computationally intensive simulation-based tasks (e.g. analyses related to fraud detection and prevention, and anti-money laundering).

Exploiting the benefits of quantum computing also presents unique challenges for financial institutions. Like other enabling technologies, quantum computing raises issues related to equitable access and market competitiveness; the full integration of this technology into legacy systems poses significant hurdles. Furthermore, the very nature of quantum computing entails a substantial paradigm shift in how financial services operate. Regulators must carefully navigate the new environment to support the smooth adoption and avoid misuse of these technologies from the private and public sectors.

Quantum technologies also bring new risks for the financial sector. In particular, such technologies could be exploited to break the encryption algorithms currently underpinning the security of critical communication systems and digital assets.

Critical financial infrastructures are among the main targets of cyberattacks based on quantum computing. They include the financial infrastructures of the future – which will support, for instance, central bank digital currencies and crypto-assets – as the two techniques of key encapsulation and digital signature currently used are both based on asymmetric encryption, which is vulnerable to the quantum threat. It will be of outmost importance to factor in the risks stemming from quantum computing when designing the central bank digital currencies.

This risk is already on the table with the practice of 'harvest now, decrypt later' used by malicious actors. Information embedded in contracts currently in force needs to be kept secret for years to come. Even just the possibility that some of it will be exposed – as soon as the technology becomes available – is already a potential blow to trust.

2. The state of the art: one problem, many potential technical approaches

As we will see through the lunch session, some solutions to mitigate cyber issues are already available. The heart of cybersecurity lies in cryptography, which – from encrypting data to securing online transactions – is the guardian of our digital world.

As the financial industry and governments prepare to protect against quantum threats, it is necessary that they become 'crypto-agile', adopting a multifaceted security strategy that incorporates a range of easily upgradable quantum-resistant solution. The showcase exercise that will be performed in this session will demonstrate that there are two different but complementary approaches that can be used in order to deal with quantum-safe cryptography.

On the one hand, we can take advantage of quantum properties to establish secure communication channels between parties, where any attempt to eavesdrop or intercept the exchange of encryption keys is detected. On the other hand, considering that the cryptography involves the use of mathematical algorithms to transform readable data into encrypted data and vice versa, it is possible to replace the current algorithms (unbreakable now, but solvable with quantum computing) with others that are more difficult to solve, even for a quantum computer.

Each one of these technologies – or a combination of them – will allow full end-to-end security in our digital communications. At the same time, however, these technologies are all extremely demanding in terms of time and resources. At the current state of the technology, embracing the quantum physics approach is estimated to impose costs of a higher order of magnitude, though it appears to provide a definitive solution to the quantum threat. The showcase exercise will demonstrate how some solutions already available to the market work, leveraging the points I have just mentioned.

Clearly, this is not a technological dilemma that can be solved with a black-or-white answer, and what is optimal now may not be optimal in the medium or long term. Migrating the whole financial system toward a quantum-safe setup is a dynamic process requiring a multifaceted approach. Whatever strategy is chosen, though, we need to have interoperable solutions working at all times for the financial industry within a single jurisdiction and between different jurisdictions.

3. Why authorities should act now

Numerous public and private initiatives have been launched to develop what are known as 'quantum-safe' solutions. However, some key elements of uncertainty are hampering the market's ability to effectively embrace the migration to quantum-resilient solutions.

First, while the implementation timeline for the quantum threat is by no means certain, short-term risk mitigation costs are significant. Second, there is a lack of agreement on a sound migration approach and on suitable interoperable technical standards. Third, the regulatory and capability landscape is fragmented across jurisdictions. These are all obstacles to a timely and orderly transition.

Despite growing awareness of the quantum threat, a comprehensive and widely shared action plan in this area remains elusive. The lack of harmonized regulations and of clear international guidelines and standards concerning the transition to a quantum-safe world may induce protracted inertia in the financial system's migration efforts.

The global nature of the financial system, the interconnectedness of intermediaries within the financial industry, and between them and the technology providers, call for public authorities to take a whole-of-government approach towards addressing the common threat posed by quantum technology. This includes fostering a dialogue between all relevant public and private stakeholders, aimed at establishing priority areas of intervention and ensuring a common path towards a quantum-safe economy through proactive cooperation and international coordination.

A systematic approach involving all international stakeholders is particularly important for financial infrastructures, given their high interconnectedness. We need to protect all links of the chain, especially the weakest.

4. A common path to a quantum-resilient financial system

All these elements make the discussion on the migration strategy something that cannot be put off any longer. The importance of preparing the financial system for the transition to quantum computing is at the heart of this workshop. This is the right time to address the challenges of the transition to quantum computing, to agree on the respective roles of public authorities and of the private sector, and to take concrete action.

To protect the financial system from the threats posed by quantum computing, the Bank of Italy is proposing – in the context of the ongoing work on risks from emerging technologies affecting the financial system that is being carried out in the G7 Finance Track – that G7 member countries jointly develop a 'common roadmap for quantum resilience', providing a unified policy framework for the actions needed to steer the transition to a quantum-safe financial system through an international cooperation approach.

The roadmap should include all initiatives that are essential for a quantum-resilient financial system and could be implemented under the responsibility of different multinational organizations. The monitoring, coordination and governance of the overall roadmap should be undertaken at the highest political level. For example, a shared response at the level of G7 countries would provide a benchmark that could outline the way forward for other jurisdictions so as to cover, eventually, the global financial system.

Whichever migration path we decide to adopt, it has to fulfil certain requirements. First, it needs to build on existing regulation in order to capitalize on best practices and, possibly, avoid over-regulation.

Second, it will entail the standardization of the approaches taken to risk mitigation across jurisdictions, so as to enable synergies and speed up the transition, as the suppliers of technical solutions will work based on shared guidelines.

Third, financial industry players as well as hardware and software providers must participate in the design of the strategy. Their involvement is necessary in order to devise a way forward that hinges on the best and most up-to-date technologies in a field where innovation is characterized by sudden accelerations.

Fourth, preservation of interoperability and quality of services must remain the guiding principle of this transition process together with its gradual and safe implementation and with the principle of proportionality, to strike a balance between short-term fixes and long-term solutions. Continuous monitoring of the progress achieved and of the resources absorbed in this endeavour will be important: on this basis, the roadmap commitments can be reassessed along the way, including with respect to the timeline, by accelerating or delaying some milestones as needed.

Finally, international coordination is a key aspect. The G7 Cyber Expert Group could be the right forum for operatively managing the quantum resilience migration roadmap, as well as for drafting policy guidelines. Other multinational institutions already involved in the adoption of quantum technologies in the financial system, such as the BIS and the standard setting bodies, could contribute proactively in defining guidelines and standards as cornerstones of the migration.

Due to their critical role, financial markets and payment infrastructures, including those that will be supporting the central bank digital currencies, deserve particular attention. The CPMI-IOSCO could be the right organization to lead the work for the quantum resilience of these crucial nodes of the financial system.

* * *

Let me conclude by thanking you all for gathering today to discuss this extremely important topic. Hopefully, the discussion that we initiated today will continue in a fruitful way in the immediate future to deliver as quickly as possible a migration roadmap which can be embraced by all G7 members and possibly also shared with G20 and other countries for wider adoption.

** I would like to thank Silvia Vori, Valerio Paolo Vacca, Giuseppe Bruno, Lorenzo Bencivelli, Mauro De Santis, Cristina Andriani, Sabina Marchetti, Antonio Castellucci and Giovanna Piantanida for their contributions to this speech.*

---

[1] McKinsey & Company, Quantum Technology Monitor, 2023.