BANCA D'ITALIA
EUROSISTEMA

Building a quantum-safe financial system: what role for authorities and for the private sector?

Speech by Luigi Federico Signorini
Senior Deputy Governor of the Bank of Italy

Bank of Italy
Scientific Workshop

24 September 2024

Ladies and Gentlemen,

It is my pleasure to open this seminar on the implications of quantum technology for the financial sector.

Experts agree that we are on the eve of a very significant technological change: one that will redefine our approach to data and to the tools we use to process them, and may well revolutionise important, even critical, aspects of the way financial institutions operate.

Like all significant technological advances, the quantum revolution comes with both promises and threats. Massively enhanced computational power, algorithms that are far more efficient than existing ones, and a much stronger base for artificial intelligence, are expected to offer opportunities for better and cheaper services, but they will also introduce new challenges, not least for financial stability.

Central banks and financial institutions have often been early adopters of technological innovations. To preserve trust, institutions should continue to be bold and imaginative, but at the same time fully aware of the risks. Prudent supervisory guidance is needed to preserve the stability, security and integrity of the financial system. Our seminar will be an opportunity to go beyond generalities and explore the most likely concrete challenges and trade-offs we need to face in the quantum era.

The Bank of Italy has a tradition of actively and rapidly adapting its policies to changes in the data management landscape. Drawing on our experience, we have long contributed to the action of the European System of Central Banks. We continue to work in partnership with academia and in cooperation with national and international institutions.

The most immediate threat most of us currently perceive concerns the protection of the integrity and confidentiality of data. We feel that such a threat calls for a coordinated response, within the G7 and beyond. We shall take the opportunity of this workshop to

share our experiences and ongoing work at the Bank of Italy and to present some real-life examples of useful and feasible cooperation at the national, European and global level. We encourage all participants to do the same.

Since Peter Shor demonstrated, in 1994, that a quantum computer could theoretically solve problems much faster than traditional ones, he has inspired scientists all over the world to imagine the countless possibilities of this technology, and technologists to look for ways to actually build a functioning machine based on it. Thirty years on, while we still lack a fully functional and reliable quantum computer, we seem to be actually getting closer and closer.

As the cybersecurity threat is serious but there are potential ways to fend it off, we cannot afford to wait. Implementing quantum-resistant cryptography tools before quantum computers become practically operational is crucial for data longevity. Sensitive data that are encrypted using today's technology could be stored now by malicious agents and decrypted later, once quantum tools become available; upgrading cryptographic tools as soon as possible is therefore necessary to ensure long-term data security. This is especially relevant for financial institutions. Their core business is ultimately based on the ability to create, manage and use sensitive data, and it is not unlikely that the quantum revolution will hit the financial sector faster and more intensively than other industries.

Awareness of the need to act is growing. In the spring of this year, the European Commission published a 'Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography'. In the US, the National Institute of Standards and Technology (NIST) officially released its first set of finalised post-quantum cryptography (PQC) algorithms last month. This is a major step forward.

In the G7 Finance Track, the Italian presidency identified quantum computing as one of the key strategic cyber issues facing us. It may affect multiple policy areas, including national security, competitiveness, ethics, and skill development.

While solutions to achieve quantum security are starting to become available, there are factors that can make market players reluctant to adopt them quickly. These include uncertainty about the actual urgency of the quantum threat, the fact that a common transition approach has not yet emerged, and the fragmentation of investments, responsibilities and regulatory frameworks across jurisdictions.

The G7 has launched several technical initiatives to foster coordination among the main stakeholders. With today's workshop, we aim to engage key experts in G7 countries, with a view to developing a shared understanding of the most urgent issues, a potential roadmap to address the transition to quantum resilience and, to the extent possible, an agreed policy agenda. We are fortunate today to have speakers and attendants from a wide range of backgrounds: academia, government institutions (including law-enforcement agencies), central banks, international organisations and the finance industry. This promises to be an ideal opportunity to exchange views, in that it brings together a set of distinguished experts with considerably diverse experience. I encourage all participants to be active, ask questions and share their insights.

Ladies and gentlemen, we are also honoured to have Professor Juan Ignacio Cirac Sasturain with us today as a keynote speaker. As many of you will know, our speaker is one of the leading theorists in quantum computation. His contributions range from the physics of quantum computers to quantum algorithms and quantum information theory. Many here will be especially interested in his seminal work on quantum cryptography. Professor Cirac is the Director of the Theory Department at the Max Planck Institute of quantum optics in Garching bei München, Bavaria, and collaborates with many other academic institutions. He has received an impressive number of high-level awards, including the Prince of Asturias Award for Technical and Scientific Research (2006), the BBVA Frontiers of Knowledge Award (2008), the Benjamin Franklin Medal (2010), the Wolf Prize in Physics (2013), the Max Planck Medal (2018), and many others; more are sure to come. The subject of his talk is, very aptly, 'opportunities and challenges of the next generation's computers'. We are certain that his remarks on today's central issue will set the stage for a very productive seminar.

Please join me in welcoming Ignacio Cirac to the stage.

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