BANCA D'ITALIA
EUROSISTEMA

The Financial Cryptography in Rome (FCiR25) conference

Welcome address by Giuseppe Zingrillo
Director General for Information Technology of Banca d'Italia

Centro C.A. Ciampi
Rome, 1st October 2025

Distinguished guests, dear colleagues, ladies and gentlemen, good morning.

1. It is my privilege to open this international conference devoted to a theme that, more than many others, reflects the challenges of our age: cryptography in the financial sector. Your presence here sends a powerful message: the digital transformation we are experiencing is not merely a technological shift, but a structural change in our economy and society.

2. We live in an era where digitalisation is not simply a technical process but a social and economic transformation reshaping the relations between individuals, businesses and institutions. The digital economy is no longer a niche; it has become the backbone of our daily interactions. From e-commerce to online public services, from contactless retail payments to real-time wholesale financial exchanges, digital infrastructures mediate almost every action. This transformation offers us opportunities of efficiency and inclusion that were unthinkable a generation ago, but it also exposes us to new vulnerabilities that we must learn to master.

3. In this environment, security is not an add-on: it is the indispensable condition for trust. And trust, in the financial world, is the very foundation upon which everything else rests. In the digital realm, trust is not guaranteed by default. It must be built and safeguarded through instruments capable of resisting increasingly sophisticated threats. Cryptography, in this respect, emerges not as a marginal technical matter, but as the universal language of security.

4. In recent years, financial institutions have increasingly experimented with distributed ledger technologies – from the settlement of tokenized securities to near real-time collateral management and programmable cash flows that promise automated reconciliation and reduced operational risk. Cryptography does not merely protect; it helps defining the very perimeter of what is possible in a digital environment.

5. For central banks, this is not a theoretical question; it is an essential discipline of infrastructure policy. Money is the ultimate public good, and its credibility rests on stability and security. Today, reflecting on money inevitably means reflecting on

its digital form: guaranteeing payment finality means guaranteeing mathematical properties of protocols and their translation into legal requirements; ensuring interoperability is not just a technical choice: it is a policy decision to contrast market fragmentation, enabling the portability of public trust across platforms and borders. Central bank digital currencies, whether designed for retail use or wholesale settlements, raise unprecedented challenges. On the one hand, they must provide the same simplicity, accessibility and reliability as cash. On the other, they must ensure the highest standards of protection, integrity and resilience in a technologically complex and constantly evolving environment.

6. Within the Eurosystem, the work on the digital euro embodies this challenge. The project does not aim to replace existing forms of money, but to complement and interoperate with them, with the purpose of preserving European monetary sovereignty and offering citizens and businesses a digital means of payment that is safe, accessible, and aligned with the values of our Union. Cryptography lies at the very heart of this effort, not only as a shield against threats but as the key to balancing objectives that might appear irreconcilable.

7. Data protection is one of the most sensitive and pressing of these objectives. Citizens expect their privacy to be respected, and rightly so. At the same time, public authorities have the responsibility to ensure that payment systems are not misused for money laundering, terrorist financing or other illicit purposes. Fraud must be prevented, disputes must be resolved fairly and transparently, and the integrity of the entire financial system must be preserved. How to reconcile all these goals? Here, again, cryptographic research can provide answers. Techniques such as zero-knowledge proofs, homomorphic encryption, and secure multiparty computation show that we are not condemned to choose between privacy and security; with the right tools and the right vision, we can pursue both.

8. The urgency of this challenge becomes even clearer when we consider what lies ahead. Quantum technologies represent a potential turning point. Quantum computers promise substantial speed-ups in solving certain classes of computational problems, with expected benefits ranging from new materials to personalised medicine. But they also pose a threat to the algorithms that currently secure billions of financial transactions every day. Algorithms such as RSA or those based on elliptic curves, the pillars of today's digital infrastructure, could become vulnerable. We cannot afford to wait until this threat materializes: the "harvest now, decrypt later" risk forces us to start working by developing and adopting post-quantum cryptographic solutions. This is no longer a matter for academic research alone: it has become an essential component of global financial resilience.

9. And this is why conferences such as this are so crucial. No institution, however strong, can face these challenges in isolation. Digital security is the product of a collective effort, requiring constant dialogue among the academic community, the private sector, and supervisory and oversight authorities. Each has a vital contribution to make: public institutions provide the framework and strategic direction, researchers develop the knowledge and theoretical foundations, and businesses turn innovation into practical, scalable solutions.

10. The future of cryptography in the financial sector will therefore depend on the ability of these three dimensions to cooperate, to build strong standards and to disseminate best practices. History teaches us that trust can only be built through transparency and cooperation, and this principle holds true – perhaps more than ever – in the digital realm.

11. Looking ahead, we can envisage very different scenarios. The one we look forward to is a global financial system where central bank digital currencies coexist with private solutions, where new cyber threats constantly test our resilience, but where new cryptographic techniques provide us with the means to respond effectively. We can imagine a context in which cryptography is no longer perceived as a narrow field for specialists, but as a common good, an integral part of economic and social stability.

12. With these perspectives in mind, I invite all of us to engage in this conference with openness and collaboration. Over the course of today, we will have the opportunity to exchange ideas, to explore new solutions, to build new valuable relations. The quality of our dialogue will determine our collective capacity to meet the challenges that await us.

13. It is in this spirit that I wish you all a fruitful and inspiring conference.

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