



BANCA D'ITALIA
EUROSISTEMA

Does cryptography really matter to central banks?

Giuseppe Zingrillo

Director General for Information Technology of Banca d'Italia

Financial Cryptography in Rome (FCiR26)

Centro C.A. Ciampi

Rome, 6 October 2026

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

It is a privilege to open this conference on cryptography in the financial sector.

I would like to begin with a question. Does cryptography really matter to central banks? I would like to use these opening remarks to explain why my answer is an unequivocal yes.

To explain why, I will start with something that central banks and cryptography have in common: they generate trust.

We seldom pause to consider what gives money its value. Since the end of the Bretton Woods system, our currencies have not been convertible into gold at a fixed rate. People accept public money because they trust the institution that issues it and the framework within which it operates. That trust is earned through a commitment to monetary stability, sound institutions and the ability of money to serve, day after day, as a means of payment and a store of value.

Trust in commercial bank money is closely connected to this public foundation. Consider ten euros held in an account at a bank in Italy and ten euros held at a bank in Bulgaria, Germany or Cyprus. We expect both balances to represent the same ten euros, regardless of where the accounts are held. Central bank money provides the common anchor: commercial bank money can be converted into it at par, while payments between banks ultimately rely on settlement in central bank money. This arrangement is supported by regulation, supervision, deposit protection and the resilience of the payment system. Together, these elements sustain the singleness of our currency, a prerequisite for the orderly functioning of our economies.

What does this have to do with cryptography? A great deal. When we send a confidential instruction, we must be able to trust that it remains confidential. When we receive a payment message, we must know who sent it and whether it has been altered. When a digital asset changes hands, we must establish who is entitled to transfer it and ensure that the same asset cannot be spent twice. Cryptography helps make these assurances possible.

Yet trust does not reside only in algorithms. It depends on which algorithms are selected and how they are implemented; on how keys are generated, stored and renewed; on the design of protocols; and on the processes and relevant controls adopted by the institutions that operate them. A mathematically sound method can still fail if a key is compromised or a system is poorly governed. Trust in cryptographic primitives must therefore be supported by systems whose protections can be examined, tested and maintained.

We can now bring the two ideas together. As money, markets and financial infrastructures become increasingly digital, confidence in the institutions that underpin them depends, in part, on confidence in the cryptographic systems they use.

This is why cryptography matters to central banks, and why the work presented in this conference deserves our attention. It is relevant to the security of payment and settlement systems, to the protection of sensitive information, and to the resilience of the wider financial system. It also raises questions that reach beyond any single institution: which technical properties should we require of cryptographic systems, how can we verify them, and who remains accountable when systems become more and more complex?

The opportunities are substantial. Advanced cryptographic techniques can help us explore new ways to exchange value and information. They can support the tokenisation of assets and enable a wide range of conditional transactions. They can offer ways to protect sensitive information, only revealing what is strictly necessary for a transaction to be validated or for an authority to perform its duties. They can help secure transactions across infrastructures operated by different parties.

At the same time, the technologies on which existing security arrangements rely are being challenged. Advances in quantum computing could eventually undermine some of the cryptographic methods on which today's systems rely. We do not know precisely when a sufficiently powerful quantum computer will be available. But financial infrastructures have long lives, and replacing cryptography across them takes time. Preparing for that transition is therefore a task for the present, even while the threat lies in the future.

Artificial intelligence presents a different challenge. It can help specialists inspect code, identify weaknesses and respond more quickly to threats. It can also help malicious actors search for vulnerabilities in cryptographic systems and operate at greater speed and scale. Perhaps AI does not, by itself, invalidate sound cryptography – although, given the speed of AI-powered advances in mathematics, we cannot rule this out entirely. It does, however, change the environment in which cryptographic systems are designed, deployed and defended. Once again, we need to consider the whole system, including its people and processes.

No institution, however capable, can meet these challenges in isolation. Public authorities can set objectives, assess risks and provide a framework of accountability. Researchers can challenge assumptions, establish what is technically possible and reveal what remains uncertain. Financial institutions and technology providers can turn sound ideas into services that are reliable in daily use. Each contribution strengthens the others.

For central banks, the task is to combine technological curiosity with institutional discipline. We should be ready to understand new technologies and the opportunities they create. We should be equally ready to ask whether they preserve the qualities on which public confidence depends: safety, resilience, accessibility, transparency, and the integrity of money. The answers will require sustained dialogue across the communities represented in this conference.

Today gives us an opportunity to advance that dialogue: to learn from one another, to test ideas and to build relationships. I hope we will leave with a clearer understanding of both the possibilities before us and the work needed to realise them responsibly.

It is in that spirit that I wish you all a fruitful conference. Thank you.