BANCA D'ITALIA
EUROSISTEMA

Journey to the future of the financial system

Speech by Chiara Scotti
Deputy Governor of Banca d'Italia

Speech at the ASSIOM FOREX Annual Congress
Turin, 14-15 February 2025

1. Introduction

Good morning, ladies and gentlemen. First of all, I would like to thank the organizers for inviting me to this session entitled 'Artificial intelligence and the digital transition of the financial system'.

Digitalization – defined in this context as including the development of distributed ledger technologies (DLTs), crypto-assets and artificial intelligence (AI) – is transforming the 'traditional' financial system.[1] New opportunities are emerging in the financial world,[2] from the increase in the efficiency of intermediaries, to the improvement in customer services and the growth in financial inclusion. Yet we cannot ignore the mounting challenges that digitalization brings. Specifically, central banks and supervisory authorities are called upon to identify potential threats to the sound and prudent management of intermediaries, the overall stability of the financial system, the smooth functioning of the payment system, and consumer protection.

In my speech, I will reflect on these changes and how they might evolve. We will journey together in the financial system of the future, through three scenarios that will allow us to identify possible challenges and potentially the most appropriate solutions for balancing financial stability with innovation and efficiency. I will therefore look at how the European Union (EU) is addressing these challenges through the revision of the regulatory framework.

---

1 K. Petralia et al., 'Banking Disrupted? Financial Intermediation in an Era of Transformational Technology', Geneva Reports on the World Economy, 2019; T. Beck et al., 'Will video kill the radio star? Digitalisation and the future of banking (europa.eu)', Reports of the ESRB Advisory Scientific Committee No. 12, January 2022; A. Fuster et al., 'The Role of Technology in Mortgage Lending' Review of Financial Studies, Vol. 32, Issue 5, pp. 1854-1899, May 2019; G. Buchak et al., 'Fintech, Regulatory Arbitrage, and the Rise of Shadow Banks', Journal of Financial Economics, Vol. 130, pp. 453-483, September 2017.

2 S. Cevik, 'Promise (Un)kept? Fintech and Financial Inclusion', IMF Working Paper, June 2024; C. Baba et al., 'Fintech in Europe: Promises and Threats', IMF Working Paper, November 2020.

2. Possible scenarios linked to the digitalization of the financial system

At a time of great political, cultural and technological change, some long-term trends (known as mega-trends) could revolutionize our lives, even more than is already the case, including how we pay, invest and run businesses. I would like to explore three of them in particular: the growing role of Big Techs in financial intermediation, the increased relevance of crypto-assets and digital financial assets, and the great promise arising from the development of artificial intelligence.

These trends do not develop in isolation, but they can reinforce each other. For example, the market power that Big Techs wield over traditional financial intermediaries may be amplified by the economies of scale in digital technologies – think of the computing power needed to run cloud infrastructures and process the enormous volume of data on which artificial intelligence models are based.

These trends are also closely linked to other developments. Quantum computing, for example, promises to speed up the solving of complex problems in fields such as biology, chemistry and finance (e.g. portfolio optimization).[3] In addition, we cannot ignore the effects of the political choices made by some large countries and the resulting international tensions: trade and financial agreements, principles for regulatory cooperation, and public-private or intergovernmental partnerships can suddenly be undermined.

The context in which we – as individuals, private organizations and public institutions – act and make decisions is increasingly marked by the complex interconnections at play, the great uncertainties in forecasting, the doubts about the accuracy of information, and the extreme volatility of the current scenario. Although these issues are not exclusively associated with technological developments, they are exacerbated by them.

Making precise predictions about what will happen in the next few years is impossible. Nobody would have thought in the 1980s that people would need more than 640 KB of memory on their personal computer. Today, my mobile phone has 256 GB of memory and it is almost not enough. If we cannot accurately predict the future and we still have to make decisions, then what strategy should we adopt?

First of all, we need to use a systemic approach. As mentioned above, changes are taking place in many areas, and we need a broad vision that covers economic, political, technological, social and environmental factors. It is equally important to have a medium-term outlook. In a rapidly evolving environment, it is unrealistic – and perhaps even undesirable – to react to every single change; at the same time, we cannot wait for the storm to pass, because it would be too late. We must therefore challenge the logic of making decisions based on the present or on the probable future. The goal should be to develop robust and flexible strategies that are based on a wide range of information and suitable for dealing not only with the most likely scenario, but also with a set of possible

[3] Quantum computing is one of the most promising and revolutionary technologies of recent years. Its computing power could transform many sectors, including the financial one.

alternative scenarios. The ultimate aim is to be able to anticipate the actions needed to manage risks and reduce the impact of adverse events.[4]

To include these considerations in today's discussion, I think it is useful to outline some purely hypothetical future scenarios that can stimulate thoughts on the prospects for the financial system and on the role that regulators and supervisors should play in fostering innovation-related opportunities, while at the same time mitigating financial stability risks.

Together with a number of colleagues from different professional and educational backgrounds,[5] we have therefore tried to consider the prospects offered by digitalization, including DLTs and the transfer of digitally represented values and rights, which I will simply refer to as crypto-assets.[6]

So, let me paint three scenarios for you, three different itineraries for the future of the financial system.[7]

Itinerary A: Modern and digitalized financial intermediaries

In the first scenario, traditional financial intermediaries would develop the technologies they need internally, countering the current outsourcing trend (as in cloud and AI services). They could also capitalize on the potential failure of the business model that has thus far fuelled the development of Big Techs. Traditional intermediaries would acquire the expertise needed to keep pace with technological advancements, driving the adoption of innovation while adapting dynamically to market and consumer needs. Furthermore, they would create technology platforms and solutions capable of competing with those of Big Techs in providing financial services and products, thus limiting outsourcing to specialized players within the financial sector. Customer relations would remain under their control, and operational risks (including IT risks) would be

---

4 The idea takes its cue from 'strategic foresight', a planning technique that broadens the prospects for analysis through the systematic exploration of a number of plausible future scenarios, drawn up with input from various stakeholder categories. Plausible scenarios are those we think could occur based on current knowledge about the world and on certain dynamics, processes, laws of physics or technologies, without thinking about how likely they are. One example of scenario exploration in line with strategic foresight methodology is the analysis in D. Acemoglu, 'The real threat to American prosperity', *Financial Times*, 2025.

5 I would particularly like to thank Andrea Pilati, Francesco Cannata, Luca Serafini, Marcello Bofondi, Giovanni Carletti, Alessio De Vincenzo, Emilia Bonaccorsi Di Patti, Sabina Marchetti, Gabriele Marcelli, Andrea Mele and Anna Maria Viscardi.

6 To round this off, it should be noted that European legislators have recently introduced – with Regulation (EU) 2023/1114 (MiCAR) – a definition of crypto-assets that includes any 'digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology'. It should also be pointed out that the rights and obligations introduced by this Regulation are instead only applicable to crypto-assets that cannot be classified as digital versions of financial products or instruments already regulated by European law, as clarified in the scope of application of the Markets in Crypto-Assets Regulation (MiCAR).

7 These updates and developments are based on the scenarios outlined by the Basel Committee on Banking Supervision, 'Sound Practices: implications of fintech developments for banks and bank supervisors', February 2018.

managed primarily within the financial sector. In summary, financial intermediaries would gain significant, though not necessarily exclusive, control over the technological landscape.[8]

Itinerary B: Banking-as-a-Service

In the second scenario, Big Techs would take the lead in developing and managing technologies, providing advanced solutions and digital channels for distributing financial products. By outsourcing most of the financial services value chain, banks would become increasingly dependent on technology and on crypto-asset service providers, weakening their competitive edge in data access and process control. However, collaboration between banks and Big Techs, e.g. through joint ventures, could foster the development of innovative payment solutions using crypto-assets, increasing the interconnections between digital markets and the traditional financial system.[9, 10]

Itinerary C: A decentralized financial system

In the third scenario, the crypto ecosystem would become mainstream, with decentralized finance (DeFi) serving as the primary method for accessing financial services. Private crypto-assets offered to the public by non-financial entities would take centre stage, enabling value transfers and payments through public/permissionless DLT platforms – bypassing traditional banks altogether.[11] This scenario could unfold in two ways. In the more extreme version, there would be no intermediaries, so financial transactions would take place between end users, via smart contracts that would ensure a direct

---

8 This first scenario would require a level of investment from banks that might be difficult to reconcile with their profitability over the past 30 years, especially compared with Big Techs, which already have a dominant technological advantage. On this topic, see P.O. Klein and L. Weill, 'Bank profitability and economic growth', The Quarterly Review of Economics and Finance, Vol. 84, 2022, pp. 183-199; and L. Di Vito et al. 'Understanding the profitability gap between euro area and US global systemically important banks', ECB Occasional Papers, 327, 2023. However, we cannot rule out an alternative development to what has been observed so far, e.g. the possibility that Big Techs – which have invested heavily in AI – might not achieve significant progress in terms of innovation or productivity growth in the medium term (see also D. Acemoglu, op. cit., 2025).

9 This scenario appears to be the most likely, though its full-scale magnitude remains difficult to quantify. The AI variable introduces additional uncertainty, as its degree of innovation and extent of adoption could lead to further developments that are difficult to predict today. See I. Aldasoro, L. Gambacorta, A. Korinek, V. Shreeti and M. Stein, 'Intelligent financial systems: how AI is transforming finance', BIS Working Papers, 1194, 2024.

10 For example, at the end of 2022, Silvergate Bank suffered from the crisis in these markets triggered by the collapse of the FTX platform in the United States. See Azar et al., 'The Financial Stability Implications of Digital Assets', Federal Reserve Bank of New York, Economic Policy Review, Vol. 30, No. 2, 2024.

11 This scenario may be less likely than the previous ones, partly because it depends on addressing DeFi's security challenges effectively – an area that has proved particularly vulnerable to scams and cyber attacks. Examples of cybersecurity vulnerabilities include the Poly Network hack and the Wormhole attack. These incidents demonstrate how weaknesses in smart contract systems or interoperability mechanisms (such as bridges and oracles) can be exploited to carry out successful cyber attacks. Due to the decentralized nature of these infrastructures, identifying those responsible is often extremely difficult. However, advancements in cryptographic technologies, such as Zero-Knowledge Proof, might not follow a linear trajectory, potentially driving progress at a faster pace than expected.

connection between parties with different needs.[12] In the less radical version, DeFi would remain the primary mode of financial intermediation, but intermediaries could still exist by adapting and by blending decentralized and centralized technologies to ensure security and customized services.

3. How do we identify and address the critical shocks and vulnerabilities in a changing financial system?

I am sure you are all already thinking about further alternative scenarios to those I have described. As I said, these scenarios are not predictive. They are merely narratives that can serve as an exploratory device to anticipate and prepare for future challenges and opportunities.

Central banks must be careful to distinguish between shocks and vulnerabilities in these scenarios. Shocks are sudden events and, by definition, inherently difficult to predict. Vulnerabilities are instead features and components of the financial system and of its operators that might amplify the impact of a shock if it were to materialize. In their supervisory and regulatory capacity, central banks have a role to play in limiting financial sector vulnerabilities[13] that, in the current literature, typically relate to asset valuation pressures, high levels of household and corporate debt, leverage, funding risk for intermediaries, and high levels of interconnectedness within the sector. The range and sources of potential shocks and vulnerabilities could change over time, of course, which is why central banks have teams of cutting-edge researchers, and high-profile inspectors and supervisors studying and identifying new fragilities and developments in the financial system.

Identifying future scenarios helps us understand how potential shocks might impact the financial system and how they might interact with existing or emerging vulnerabilities. This would allow central banks, in their role as regulators and supervisors, to devise forward-looking supervisory measures, and to find strategies that are resilient and adaptable, as well as simple and stable, so as to reconcile financial stability with innovation and efficiency.

What comes out of the three scenarios?

What are the most important elements in the scenarios outlined that might introduce new vulnerabilities into the financial sector or significantly redefine existing ones? Let me focus on just two of them.

---

12 For example, liquidity pools match lenders and borrowers by aligning liquidity, credit risk and risk appetite. The funds are stored in unhosted wallets and everything is managed on blockchains maintained by open-source developers. This scenario is very unlikely at present for a number of reasons, including the constant exposure of users to DeFi scams and hacks. See F. Schar, 'DeFi's Promise and Pitfalls', *IMF Finance and Development Magazine*, September 2022.

13 T. Adrian, D. Covitz and N. Liang, 'Financial stability monitoring', *Annual Review of Financial Economics*, Vol. 7, 2015, pp. 357-395.

The first element is that, as financial markets and banking intermediation evolve, (partly new) vulnerabilities relating to operational and cyber risks,[14] the misuse of information, and decentralized structures of governance could emerge.[15] Non-financial operators with innovative and complex business models, crypto-assets and decentralized technologies do not necessarily comply with principles for information disclosure, consumer protection and market fairness. At the same time, 'traditional' vulnerabilities may also appear in new contexts, such as funding risk or valuation pressures in crypto-assets.

The second element, which is related to the first, is the growing complexity of the traditional financial system and its interconnections with external factors linked to developments in AI, crypto-assets, and decentralized systems. For instance, a sharp drop in the price of Bitcoin could push investors with leveraged positions to sell, amplifying the initial price drop. Similarly, if an intermediary were to suffer crypto-asset losses, its creditors might withdraw their funds on a large scale, thus forcing the intermediary to sell other assets, amplifying the initial price drop and generating a potential spillover to yet more assets.[16]

In a scenario of limited interconnections between digital and traditional markets, crypto-assets would not contribute much to systemic risk. This is the current scenario in which the crypto system is directly providing a modest level of financial services to the real economy. However, as the digitalization process advances, the interconnections between the crypto ecosystem and the traditional financial system are bound to intensify, either in a scenario of Big Tech dominance, through its in-platform tools, or, conversely, in one with fully decentralized financial services. Accordingly, as these interconnections increase, the fragilities of the crypto ecosystem might become destabilizing – especially if those crypto-assets that have no intrinsic

---

14 For instance, quantum computers could threaten the encryption algorithms that currently protect sensitive data. The G7 Cyber Expert Group has recently emphasized the urgency of tackling this challenge, recommending concrete actions to make the financial system quantum-resistant. It is vital that financial institutions, regulators and digital service providers work together to develop and implement post-quantum cybersecurity solutions. Adopting crypto-agile protocols (which enable cryptographic primitives to be modified without having to completely change a system's infrastructure) would be particularly desirable, so that, going forward, post-quantum cryptographic standards can also be adopted (see the standardization project run by NIST, https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization).

15 Decentralized governance models typically apply to permissionless DLTs, where the ledger is ordinarily managed through automated (verification) processes encoded in the consensus protocol. Structural changes to these rules are decided by allocating voting rights in ways that can be open to information asymmetries and opportunistic behaviour. The concentration of voting rights and the difficulty of applying standard regulations in decentralized contexts can undermine market efficiency and investor protection. In addition, the lack of an identifiable central authority makes rule enforcement and conflict management more difficult, leading to greater legal and operational uncertainty. For further discussion, see Gola et al., 'The governance of blockchains and systems based on distributed ledger technology', Banca d'Italia, Questioni di Economia e Finanza (Occasional Papers), 773, 2023 (only in Italian).

16 On the interconnections between the traditional financial system and the crypto ecosystem, see the cases of Signature Bank and Silvergate Bank, detailed in Azar et al., op. cit., 2024.

value (i.e. are not pegged to assets in the real or financial economy)[17] were to gain systemic importance.[18]

How can we deal with these vulnerabilities?

It is clear that the vulnerabilities described call for greater cooperation between the competent authorities in different sectors (not only the financial one) in order to safeguard both the typical aspects of prudential supervision and those equally important for the proper functioning of markets and the respect for individual rights, such as integrity, competition and the protection of privacy and of data security.

Considering the global reach of large technology companies and of decentralized governance models, cooperation and coordination should be at international level, something that could unfortunately be in jeopardy, in light of recent announcements.

In order to tackle emerging risks, a structured and flexible approach might also be preferable, one which takes into account both the activities performed and the characteristics of the entities performing them. In some contexts, an 'activity-based' regulatory approach, which refers to the nature of the activities carried out regardless of those performing them, might be more effective. An 'entity-based' approach could instead safeguard better against risks arising from the combination of different activities and services provided by the same entity (e.g. maturity transformation and the leverage and liquidity risk typical of banks that collect deposits and provide funding).[19]

Nevertheless, including new entities (entity-based approach) or new activities (activity-based approach) in the orbit of the financial supervisor alone is not enough. The latter may not have the appropriate and effective powers, competences and tools to supervise all the risks stemming from innovative business models. It seems neither realistic nor desirable to face the challenges that digitalization poses by just continuously expanding the scope of regulation and by applying the regulatory and supervisory techniques typical of the supervision of financial intermediaries.

This all calls for close cooperation between public and private sectors in order to identify shared standards, promote secure and reliable financial technologies, and foster innovation. This synergy is essential for protecting consumers, ensuring the stability of the financial system and guaranteeing that change happens in a safe, ethical and sustainable way. For Banca d'Italia, one example of this approach is the integrated offer

---

17 This is particularly true in the case of unbacked crypto-assets, such as Bitcoin, which are not designed to maintain a stable value by being pegged to a benchmark asset, or as in the case of algorithmic stablecoins, whose stabilization mechanism is based on an algorithm that conditions their supply and demand on the market, and of meme coins.

18 Azar et al., op. cit., 2024.

19 A. Carstens et al., 'Regulating big techs in finance', BIS Bulletin No. 45, 2 August 2021; C. Borio et al., 'Entity-based vs activity-based regulation: a framework and applications to traditional financial firms and big techs', BIS Occasional Paper No. 19, August 2022.

of innovation facilitators designed to encourage dialogue with the market and support the development of fintech projects (among others, Canale Fintech and Milano Hub).[20]

4. How have the European authorities responded so far?

The European legislators' choice to launch the Digital Finance Strategy in 2020 aims to increase the EU's competitiveness in digital finance, without neglecting consumer protection and financial stability. The lack of coordinated intervention at European level had initially led to fragmented national solutions (with overlaps, inconsistencies and high costs), which were insufficient due to the cross-border nature of the risks, which remained partly undetected or created potential interference between different national authorities.

One key measure of the Digital Finance Strategy is the Digital Operational Resilience Act (DORA),[21] which lays down uniform requirements for the security of the networks and information systems of financial sector operators, as well as for third parties providing them with IT services (including Big Techs). According to DORA, these service providers must increase their resilience against all cyber risks, while financial intermediaries must comply with strict standards to prevent and limit the impact of any incidents. DORA also sets out a specific supervisory framework for providers of cloud computing services to financial intermediaries.

Another equally important step was the approval of the Markets in Crypto-Assets Regulation (MiCAR),[22] which aims to ensure an adequate level of consumer protection,

---

20 Given the complexity of the challenges, Banca d'Italia is also continuing to invest in its role as interlocutor with the market, engaging in dialogue with traditional intermediaries and new entrants on the opportunities and risks arising from innovative activities. It is also showing them what areas need stronger safeguards for mitigating the above-mentioned risks in view of the application of the new regulations. For example, with the entry into force of the Digital Operational Resilience Act (DORA) Regulation in mind, Banca d'Italia has published two Communications for the market, with the aim of: (i) urging intermediaries to carry out a self-assessment of their IT risk management systems, with a particular focus on preventing violations of data confidentiality caused by both malicious attacks and unauthorized access by staff (Communication of 23 December 2024); and (ii) drawing the attention of intermediaries to the main implementation aspects of the Regulation. Specifically, with regard to: the location of the office responsible for controlling cyber risks, in compliance with the principles of proportionality and organizational neutrality; how to report serious ICT-related incidents and significant threats; and conducting advanced cybersecurity tests based on the TIBER-IT methodology, which will become mandatory for some intermediaries and whose results will be incorporated into supervisory processes (Communication of 30 December 2024). Moreover, with reference to MiCAR, Banca d'Italia has intervened several times (see footnote 29 below) to warn supervised intermediaries and those operating in various capacities in decentralized ecosystems, including as users, about the risks connected with using such technologies in finance and especially with crypto-asset activities and services (e.g. custody, exchange and payment services).

21 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience in the financial sector.

22 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on crypto-asset markets. MiCAR regulates three categories of crypto-assets: (i) asset-referenced tokens (ARTs); (ii) e-money tokens (EMTs), both of which count as stablecoins, although they differ in terms of the underlying asset and the rights attributed to the holder; and (iii) crypto-assets other than ARTs and EMTs; the latter are a residual category identified by how they differ from ARTs and EMTs, so as to make the rules 'future proof', i.e. able to apply to possible developments in new crypto-assets as well.

guarantee market integrity and safeguard financial stability. MiCAR thus enables crypto-based initiatives to combine technological innovation, security, efficiency gains and customer benefits.

As regards AI, its use in the financial sector is now partially regulated by guidelines and governance principles.[23] These include the provisions of the AI Act,[24] requiring supervisory authorities to focus on the AI systems used by banks and insurance companies to make decisions that might affect certain customer protection profiles.[25]

The Digital Finance Strategy is a first attempt to adapt the European regulatory and supervisory framework to the new financial ecosystem, in accordance with the principle of technological neutrality and using a risk-based approach. In this perspective, European legislators broadened the scope of financial regulation beyond its traditional boundaries, including entities other than financial intermediaries in the regulatory perimeter (e.g. third-party service providers for DORA, issuers of stablecoins and crypto-asset service providers, or CASPs, for MiCAR).

In doing so, however, they followed different approaches, in line with the above-mentioned need to adapt legal instruments to specific situations: while DORA uses an 'activity-based' approach, focusing on ICT risk management in the European financial sector, MiCAR embraces 'entity-based' principles to extend safeguards to new categories of intermediaries. Both courses of action pay close attention to cross-border operations, introducing forms of enhanced cooperation between supervisors at European level.[26]

In line with this variety of approaches, European regulation considers AI as a tool, rather than a product, and classifies its applications based on risks. For example, systems with full decision-making powers in operations that may undermine fundamental rights are considered 'high-risk'.[27] In other words, the use of AI must follow general guidelines and principles to foster technological development and leverage its versatility, without reducing AI to a rigid and static definition as an end product.

However, some of the challenges posed by digitalization are ongoing and we still have work to do.

---

23 See for example the guidelines of the EBA and EIOPA for the banking and insurance sectors respectively.

24 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on harmonized rules for artificial intelligence.

25 With reference to some emerging risks that might stem from the use of AI, see C. Biancotti, C. Camassa, A. Coletta, O. Judge and A. Glielmo, 'Chat Bankman-Fried? An Exploration of LLM Alignment in Finance', Banca d'Italia, Markets, Infrastructures and Payment Systems series, forthcoming.

26 MiCAR, for example, introduced consultative supervisory colleges for stablecoins (e.g. ARTs and EMTs) that are considered significant based on specific size criteria. These colleges are established and chaired by the EBA, which is in charge of supervising issuers of significant stablecoins. Its members are representatives of the EBA, the ESMA, the national authority in the issuer's home country, the authorities supervising CASPs that provide key services in relation to a specific stablecoin, the ECB or any other central bank where a stablecoin is denominated in non-EU currencies, as well as other supervisory authorities of any third countries.

27 See Article 6(3) of Regulation (EU) 2024/1689.

DORA, for example, gives competent authorities supervisory powers on 'critical' providers alone; in some jurisdictions, medium-sized and small players may therefore remain outside the regulatory scope.[28] In addition, the problem of hyper-concentration of providers (e.g. Big Techs) remains unaddressed.

MiCAR introduced a light-touch regime for crypto-assets other than EMTs and ARTs, which are only subject to notification, fair conduct and transparency requirements vis-à-vis investors. This adds to the problems arising from the impossibility of applying 'entity-based' safeguards to pure DLT models, for which the supervisory authority is unable to identify an obligor.

Finally, the AI Act does not cover financial risks. A high degree of flexibility will therefore be when laying down new regulatory and prudential requirements for the sector, with a view to adapting the existing standards to rapid changes in both AI technology and the AI industry.

Conclusions

Ever-closer interconnections between finance, technology and business digitalization are emerging. These developments must not catch us off guard. In this context, two factors are crucial to managing potential shocks and vulnerabilities: the ability of regulatory and supervisory authorities to anticipate change, including through open dialogue with financial intermediaries and other stakeholders, and to respond promptly to new challenges and opportunities. The actions already taken under the European Digital Finance Strategy and the ongoing efforts are significant steps in this direction. In a rapidly shifting environment, the recent European and national initiatives to identify roles and responsibilities are an important achievement.

However, we must be careful not to create a regulatory framework that is too complex and difficult to interpret. That said, simplification cannot come at the cost of financial stability, smooth market functioning and individual rights. It is essential to protect consumers from fraud and abuse, first and foremost by making them aware that certain services or operations are particularly risky,[29] and to ensure that the financial system remains resilient in an ever-changing environment. This task could prove even more daunting following the new US stance, particularly on crypto-assets, given their global reach.

---

28 As has been the case in recent years, Italy can continue to rely on a regulatory framework that already extends certain powers of the competent authority to smaller providers.

29 For example, with regard to crypto-assets, it should be noted that 'unbacked crypto-assets' have no intrinsic value, are not backed by any redemption rights and, in general, cannot be considered a suitable means of payment due to their high inherent risk. Banca d'Italia has repeatedly warned supervised intermediaries and anyone operating in various capacities in DLT ecosystems, including as users, about the risks associated with the application of this technology in finance and especially with crypto-asset operations and services (e.g. custody, exchange and payment services). See, among others, Bank of Italy Communication on Distributed Ledger Technologies in Finance and Crypto-assets of 15 June 2022 and, more recently, Bank of Italy Communication on Regulation (EU) 2023/1114 on Markets in Crypto-assets (MiCAR) of 22 July 2024 and the subsequent Operational Guidelines of 13 September 2024 (only in Italian).

Setting shared standards, fostering research, developing specialist skills and encouraging close cooperation between public and private sectors are all key to ensuring that new technologies are developed with a view to ensuring sustainability, supporting financially viable projects and business models, and embracing principles of social responsibility.

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