BANCA D'ITALIA
EUROSISTEMA

Communication by Banca d'Italia on Decentralized Technology in Finance and Crypto-assets

Rome, June 2022

Introduction

Like other sectors, today the financial world is exploiting the potential of digitalization more widely and more incisively than ever before.[1] Among the new solutions available, decentralized or distributed ledger technologies (DLT) have gained special prominence. These technologies have potentially very far-reaching applications, including in areas unrelated to finance. This communication focuses on uses related to the holding and transfer of values and rights, which are digitally represented by crypto-assets,[2] even in the absence of a central entity or administrator.

Crypto-assets can pose various risks. A rapid and widespread adoption of these technological solutions could undermine the stability of the financial system owing to the interdependence of participating regulated and non-regulated entities, as well as the lack of controls and tools to limit the effects of adverse events. Indeed, the world of crypto-assets is still largely deregulated. Work is under way at the international and European level to design a new set of rules and controls for these products and their 'ecosystems' (see Section 2 below), but their entry into force will take some time.

Developments in the sector – such as the rapid growth in the number and value of crypto-assets;[3] the extreme volatility of stocks; recurring crises of operators and schemes of this kind, due to fraud, IT incidents or fundamental flaws, which have also recently led to substantial losses for the parties involved; the highly opaque trading and ownership structures of most of these schemes; and in many cases, very volatile prices – all raise concerns about issues falling within the remit of the authorities. Banca d'Italia deals with crypto-assets in the course of exercising its many institutional functions: prudential oversight of supervised intermediaries; oversight of the smooth operation of the payment system; the safeguarding of monetary and financial stability; combating money laundering and terrorist financing; consumer protection.

This communication has two objectives: first, to remind supervised intermediaries, supervised entities and all those who work in various capacities in decentralized ecosystems, including as users, of the opportunities and risks associated with the use of these technologies in finance and with crypto-asset-related activities and services (issuance, custody, trading, loans, payment services, see below); second, to highlight a number of aspects that are important for defining, on the part of the abovementioned entities, safeguards to mitigate the risks associated with the use of decentralized technologies and/or trading in crypto-assets.

---

1 Within the framework of national legislation, pursuant to Article 8-*ter*(1) of Decree Law 135/2018, converted with amendments by Law 12/2019, 'distributed ledger technology' means 'computer technologies and protocols that use a shared, distributed, replicable, simultaneously accessible, architecturally decentralized ledger that is based on cryptography […] allowing the recording, validation, updating and storage of data both in clear text or protected by cryptography but verifiable by each participant, not alterable and not modifiable'.

2 This is a digital representation of a value or rights that can be issued, transferred and stored electronically, using distributed ledger or similar technology.

3 The global aggregate value of crypto-assets relative to that of financial assets is around 1 per cent (Financial Stability Board, *Assessment of Risks to Financial Stability from Crypto-assets*, February 2022), but it should be borne in mind that the scale of the phenomenon does not always reflect potential risks to financial stability. For example, the sub-prime mortgage market prior to the outbreak of the financial crisis in 2007 amounted to around $1.3 trillion, i.e. half of the value of crypto-assets recorded in November 2021.

This document is therefore intended as a reference for users, intermediaries, technology providers, administrators of schemes, digital infrastructures and portfolios operating in crypto-assets, both before the evolving European regulatory framework has been completely defined and afterwards; indeed, this regulatory framework covers neither the entire chain of the entities mentioned above, nor the full complexity of the technological solutions supporting the ecosystems of crypto-assets (see Section 2 below).

Regarding the latter, it is important to note that the use of decentralized models in finance is a quintessentially technological phenomenon, capable of connecting the various systemic stakeholders even in the absence of direct relationships. The technological footprint and the role of the entities that actually contribute to making it – such as the algorithm developers – form an integral part of the schemes and agreements via which, in the context of decentralized solutions, 'transfers of value' are made: the strong links between these phenomena and the need to maintain financial and monetary stability are why central banks observe and monitor the operations of these entities so carefully.

The communication is structured as follows: Section 1 sets out the main features of the application of decentralized technologies to financial services; Section 2 describes the status of international cooperation and the relevant regulatory framework; Section 3 proposes principles and benchmarks for supervised intermediaries and entities falling within the scope of payment system oversight; Section 4 highlights potential risks for users; finally, Section 5 sets out the next steps that Banca d'Italia intends to take to contribute to the orderly and secure development of the new digital solutions discussed here.

1. The main features of the application of decentralized technologies to financial services

The development of decentralized financial services relies on the central role of cryptographic and distributed ledger technologies (DLT/blockchain).[4] The two technological models are highly complementary. The first protects transaction-related data and ensures their non-repudiation; it guarantees the integrity and, where applicable, the confidentiality of the same information and underpins the mechanism for authorizing transactions. The second, (DLT/blockchain), consists of a shared electronic ledger with data protected both by cryptographic techniques and by means of 'redundancy' (copies of the same information can be validated and stored by all active participants).[5]

[4] Blockchain represents a particular type of DLT. Specifically, it is called blockchain because the memorized transactions are grouped in a sequence of 'blocks' linked cryptographically, creating a chronological record that cannot be altered of all transactions made up to that point in time. There are also technological solutions that are decentralized but alternative to DLT/blockchain, such as online peer-to-peer (P2P), or user-matching, allowing two counterparties acting as users (e.g. creditors and debtors) to interact directly without requiring the presence of an intermediary.

[5] The ledger has a dual role. On the one hand, it makes it possible to store data on transactions that cannot be altered in order to prevent their manipulation. On the other hand, it provides a mechanism that enables new information to be added, even in the absence of a central guarantor: the information may not be added to the distributed ledger until agreement is reached among the participants on its validity; this increases the resilience of such ledgers to possible counterfeit attempts. There are many potential use cases of DLT/blockchain, e.g. for public administration services (real estate, voting, digital identities, etc.), health, media, energy and other areas; both financial and non-financial risks are associated with its use.

In principle, DLTs can deliver benefits for users, related to efficiency gains in the provision of financial services, the extension of system operating hours, cost and time savings for cross-border transactions, faster transfer of financial assets and progress on the technological frontier, partly as a result of stronger competition.

For this to happen, DLTs must have the characteristics of more mature technologies, i.e. guarantee business continuity and, in general, resilience to scalable cyber-attacks (i.e. be capable of adapting their capacity to record an increasing number of transactions without any significant deterioration in the speed and quality of services), be economically and environmentally efficient (in particular, by supporting a high volume of operations at low and sustainable costs), and have robust and identifiable governance structures.

DLT solutions create complex ecosystems in which each party – supervised intermediaries, technology providers, other operators (see below) and users – relates to the other in ways that can differ significantly to what happens in the traditional financial system. The role of developers and providers of IT solutions, as well as of entities tasked with developing and managing smart contracts,[6] is key to ensuring the proper functioning of the ecosystem and to guaranteeing financial stability and consumer protection.

This makes it difficult to frame these phenomena within the existing regulations. For example, current regulations envisage an outsourcing mechanism enabling intermediaries to avail of the services of technology providers, but in the case of DLTs, such interaction can arise even in the absence of direct (contractual) links. In this sense, it is the technology that 'links' the objective (instruments, technical and organizational infrastructures) to the subjective (the various operators involved) components of the ecosystems in new products and services, the complete expression of each contribution. The importance of the technological component and of the technology providers themselves leads to a kind of 'algorithmic governance', which bypasses more traditional governance schemes and which therefore must be taken into account.

Speaking of governance, an important distinction ought to be made between permissioned and permissionless DLT. The former requires that users, in order to access and to make changes to the ledger, must first obtain a licence from a central entity or other party, which therefore has *de facto* governance responsibilities. In permissionless DLT, instead, it is difficult or impossible to identify any such responsible entity;[7] transactions can be carried out without the intervention of external entities (e.g. intermediaries) through the use of smart contracts, i.e. as mentioned above, computer programmes that run automatically if specific conditions are met, thereby ensuring methodological

---

6 Smart contracts are referred to in Article 8-*ter*(2) of Decree Law 135/2018, as 'computer programs that operate on distributed registers-based technologies and whose execution automatically binds two or more parties according to the effects predefined by said parties'.

7 Specifically, permissionless networks provide access to any user who chooses to join and participate, by generating new transactions, acting as a miner (validating and finalizing transactions) or simply reading the ledger of stored transactions. By contrast, permissioned networks operate on behalf of a community that shares a common interest, where access to the role of miner is limited to a small number of individuals considered trustworthy (levels of ledger access and of participation in the generation of new transactions may be restricted or not depending on the organization that controls the network).

compliance with the contractual aspects underlying the provision of the service. This feature, which underpins so-called decentralized finance (DeFi),[8] makes it difficult to frame crypto-assets within the existing regulations, and helps to explain the difficulties and delays experienced by the legislator and regulators in this area at the global level.

In this context, the unique role played by smart contracts in decentralized finance technologies has profound implications for the governance of an ecosystem: the rules, rights and obligations are enshrined in protocols and programmes – prepared and made freely available on the infrastructure by its users, including those resident in different jurisdictions – making it difficult to identify a party or central entity to which the governance responsibilities are attributable, and therefore also the competent legal forum and applicable law, especially in the case of permissionless DLTs.

With specific reference to the phenomenon of crypto-assets, it is worth highlighting that the potential applications of new decentralized technologies in the financial sector are not fully covered; moreover, it requires an ability to distinguish between different product categories and uses according to the different levels of risk that characterize them, including on the basis of the existence or otherwise of an intrinsic value.

Notwithstanding what was mentioned earlier as regards permissioned or permissionless DLT, a first distinction concerns the possibility of trading crypto-assets: 1) directly from 'user' to 'user' ('pure DeFi');[9] 2) or through market participants that conduct specific crypto-asset exchange[10] and trading activities (including through recourse to 'off-chain' phases, i.e. outside of DLT, such as, hypothetically, for the settlement of transactions).

Based on another important classification criterion, crypto-assets can be broken down into two categories: 1) unbacked crypto-assets, i.e. assets without any stabilization mechanism anchoring their value to a benchmark activity (i.e. Bitcoin, but also so-called 'algorithmic stablecoins', whose stabilization mechanism is based on an algorithm that conditions demand and supply on the market); 2) asset-linked stablecoins, i.e. crypto-assets backed by underlying assets (e.g. official currencies, credit, commodities, etc.) that aim to maintain a stable value against a fiat currency (e.g. euro or US dollar), a specific good or a pool or basket of assets.

From this last classification stems the possibility of distinguishing more clearly between the different characteristics and functions of a broad variety of digital activities with very different associated risks: some of these can rightly be considered payment instruments, insofar as they are issued by central

---

8 Financial Stability Board, *Decentralised financial technologies: Report on financial stability, regulatory and governance implications*, 2019.

9 In its 'purer' version, DeFi does not envisage intervention by intermediaries and is instead designed to replicate in a fully decentralized form several activities carried out within the traditional financial system through authorized intermediaries.

10 Exchangers provide: 1) services for the exchange of 'crypto' with 'crypto' or of these assets with fiat currencies; 2) other custody-related services for crypto-assets (so-called digital portfolios).

banks;[11] others, consisting of crypto-assets generally defined as 'private tokens', can be more or less stable in value.

The latter include some reserve-backed crypto-assets, which can still be pegged to a single fiat currency and associated with a 'debt' of full repayment borne by an entity (normally the issuer) and used as a means of payment. A trading or store of value function could, to some extent, be associated with crypto-assets (also backed by a reserve) whose value is anchored to low-volatility assets and linked to a lender's right to the market value of the underlying asset. Other crypto-assets, anchored to instruments that are potentially volatile such as financial instruments, though also backed by a redemption right for users, may have an investment function as they are predominantly speculative and therefore characterized by higher risk profiles.

Crypto-assets without any intrinsic value unrelated to any asset in the real or financial economy, without any right of repayment to the owner, cannot, as such, be suited to performing a payment or investment function (these are therefore unbacked crypto-assets, as mentioned earlier): for this reason, and owing to the risks that characterize them, their use should not be in any way be promoted. In this respect, it is important to note that the content of Section 3 must not be interpreted as guidance on how to exclusively and exhaustively counter the risks stemming from these kinds of crypto-asset transactions, whose use, as was said earlier, remains highly risky, with no protections for participants and for this reason is to be strongly discouraged (see below).[12]

° ° °

These aspects can, at least in part, be intercepted and addressed by leveraging on the tasks that fall to Banca d'Italia as regards the supervision of banks and financial intermediaries, consumer protection and oversight of the smooth functioning of the payment system. Complementing this framework, there is also a need to strengthen cooperation with the other supervisory authorities involved in various capacities in this field, in particular Consob, AGCM and IVASS.

It is also important to start developing a system of principles and good practices (see Section 3 below) which, while not binding, mitigate the risks associated with activities in this sector.[13] In particular – especially in the areas furthest from the regulatory perimeter, where the dominance of the technological factor and of those who originate and condition it is more evident – there is scope to work on defining standards to be referred to as 'quality parameters' of the building blocks of

[11] See, for example, the Eurosystem's ongoing work on the digital euro project (https://www.ecb.europa.eu/paym/digital_euro/html/index.it.html#:~:text=L'euro%20digitale%20sarebbe%20come,affiancherebbe%20il%20contante%20senza%20sostituirlo).

[12] In this regard, it is worth noting that Bitcoin reached a low of around $26,350 on 12 May 2022, a marked decline from the all-time high of almost $69,000 reached on 10 November 2021. The value of Ethereum, which was quoted between $ 4,500 and $4,800 from 6 to 13 November 2021, fell below $1,800 on 12 May 2022.

[13] The use of decentralized technologies in finance presents the same types of risk as traditional finance risks (credit, market, operational, cyber, liquidity, etc.), but increases their importance for financial stability, arising, for example, from: i) operational risk within a decentralized ecosystem; (II) risks around elements of vulnerability not yet fully explored in DLT regarding business continuity; (III) cyber security and fraud risks related to the presence of several non-regulated and independent entities; IV) the presence of technological tools and paradigms that are not properly regulated; v) the absence of industry standards for the new systems and vi) the transactional dimension of the phenomenon, which makes it difficult to regulate its influence at the level of individual jurisdictions.

decentralized technologies (such as smart contracts): recourse to forms of public-private partnership can represent, in this respect, a valid option (see Section 3.2).

2. International cooperation and the regulatory environment

Although the use of decentralized technologies in finance is currently not widespread, it nonetheless may pose various risks. A rapid and widespread adoption of these technological solutions could undermine the stability of the financial system owing to the interdependence of participating regulated and non-regulated entities, as well as a lack of controls and tools capable of limiting the effects of adverse events. Indeed, the world of crypto-assets is still largely deregulated. In particular, ever closer interaction between the entities involved complicates the monitoring of risks. This question has been the topic of research and focus of a number of central banks.[14]

Nowadays, crypto-assets are at the centre of attention of a wide range of international authorities, governments, central banks and supervisory authorities interested in understanding whether, and how, to regulate them, taking into account in particular the variety of cases that exist with regard, as highlighted above, to both their possible economic function and different risk profiles. For this reason, a number of international forums (e.g. FSB, BCBS, IOSCO, CPMI)[15] have launched a series of initiatives to integrate these instruments into regulatory frameworks for the supervision of intermediaries, the functioning of financial markets and the oversight of payment systems.[16]

In Europe, two legislative proposals were published in the context of the Commission's September 2020 Digital Finance Strategy: the Markets in Crypto Assets Regulation (MiCAR) and the Digital Operational Resilience Act (DORA). The first introduces a harmonized framework for issuing and offering crypto-assets to the public, as well as for related services (e.g. trading and digital wallet). The second aims to strengthen the digital operational resilience of the financial sector as a whole, including through the introduction of an oversight regime for critical ICT service providers, which may include those providing services for the management of crypto-assets.

In particular, crypto-assets covered by the MiFID definition of financial instruments (tokenized financial instruments) are not included in the scope of application of MiCAR; with regard to tokenized financial instruments, it should be noted that, again within the context of the digital finance strategy, the Regulation on a pilot scheme for market infrastructures based on distributed ledger technology

---

[14] See Federal Reserve: https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf; Bank of England: https://www.bankofengland.co.uk/financial-stability-in-focus/2022/march-2022); Deutsche Bundesbank: https://www.bundesbank.de/resource/blob/707710/3f3bd66e8c8a0fbeb745886b3f072b15/mL/2017-09-distributed-data.pdf.

[15] Financial Stability Board (FSB), Basel Committee on Banking Supervision (BCBS), Committee on Payments and Market Infrastructures (CPMI). This issue is also important for authorities in other sectors, in particular tax authorities: Organisation for Economic Co-operation and Development (OECD).

[16] FSB: https://www.fsb.org/2020/10/regulation-supervision-and-oversight-of-global-stablecoin-arrangements/
BCBS: https://www.bis.org/bcbs/publ/d519.htm
CPMI-IOSCO: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD685.pdf
IOSCO: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf

(DLT pilot regime) was published in the Official Journal of the European Union of 2 June 2022, which, unlike MiCAR, refers to tokenized financial instruments.[17]

In addition to the above, in the context of the anti-money laundering (AML) package, the Commission's proposal to reform the legal and institutional framework for anti-money laundering and counter-terrorist financing (CFT) presented in July 2021 covers all crypto-asset service providers and, in line with the Financial Action Task Force (FATF) standards, extends to transfers in crypto-assets the obligation (already in place for transfers in legal currency) to transmit information on the originator and the beneficiary in order to ensure that they can be traced back and identified in the event of a suspicious transaction.

Banca d'Italia has long been involved in the work on crypto-assets at international and European level and monitors developments in the market. Since 2015, it has published warnings targeted at supervised intermediaries and users, highlighting the risks associated with the purchase and holding of crypto-assets, the complexity of the underlying technologies, the lack of legal and contractual safeguards, and the possibility – ultimately – of losing in full the funds invested (see Section 4 below). Some of these warnings were issued in agreement with CONSOB and the Italian Financial Intelligence Unit (FIU), which operates independently within Banca d'Italia.

While discussions at international level and work to complete the expected regulatory framework in the European Union continue, the links between traditional finance and that using decentralized technologies have increased; new business opportunities are being created, but also greater scope for contagion between the two ecosystems. It is therefore necessary to reconcile the need to avoid excessive risk with the ability of the system to reap the benefits of innovation related to the virtuous development of decentralized technologies applied to the financial sector.

With specific regard to national legislation, it should be stressed that, pending the formulation of MiCAR, there is currently no specific regulatory framework for crypto-assets in Italy.

As for AML/CFT issues, pending the approval of the regulatory proposals in the EU's AML package, the sector is also only partially regulated. Italian anti-money laundering legislation, as laid down in Legislative Decree 231/2007, most recently amended by Legislative Decree 125/2019 implementing AMLD V,[18] incorporates a very broad notion of both virtual currency (which includes crypto-assets for both payment and investment purposes) and virtual asset service provider (VASP), including any natural or legal person offering professional virtual currency-related services.[19] VASPs are required to comply with due diligence, data storage and suspicious transaction reporting requirements.

[17] Regulation (EU) 2022/858 of 30 May 2022 on the DLT pilot regime introduces a pilot regime to allow market infrastructures (which offer securities trading and settlement services) to test the application of DLT to the provision of these services for certain types of financial instruments. The Regulation will apply from 23 March 2023, save for a few exceptions which will come into force earlier than that date.

[18] Directive (EU) 2018/843 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AMLD V).

[19] Specifically, the Italian anti-money laundering decree refers to 'providers of virtual currency usage services' (which include, *inter alia*, virtual currency issuers and providers) and to 'electronic wallet service providers' (collectively referred to as 'VASPs').

Legislative Decree 90/2017 also provided that the Agents and Brokers Organization (OAM) record in a special section (established *ex novo* and active as of 16 May 2022) of the currency exchange register those VASPs that meet certain minimum requirements, in accordance with the procedures laid down by the Decree of the Ministry of Economy and Finance of 13 January 2022. In particular, the decree provides that VASP activity is restricted to persons incorporated in Italy or EU entities with a permanent establishment in Italy, since operations in the form of freedom to provide services are not permitted.

In other respects, such as taxation, it is necessary to establish specific rules and regulations that provide certainty to market operators and investors. Italy does not currently have tax regulations for this sector, whose tax profiles are based on the application, through interpretation, of rules laid down for other types of transactions and activities. Drafting legislation for this area could draw upon the forthcoming regulation at the supranational level, as well as ongoing work at the OECD and the European Commission on the exchange of information between crypto-asset service providers and the tax authorities. [20] Looking ahead, it seems advisable to strike a balance between taking into account the specific features of the sector and the need for consistency between the tax rules on crypto-assets and on other assets, as well as with the legal framework in general, including for reasons of equal treatment.

The approval of MiCAR will help to reduce regulatory uncertainty and facilitate the orderly development of the crypto-asset market. However, although it is a first and important step forward, it does not address all the different components of the crypto-asset ecosystems and their application in decentralized finance. For example, concerning its scope, MiCAR does not cover (at the current stage of negotiations by the EU institutions) unique and non-fungible crypto-assets, i.e. non-fungible tokens or NFTs, such as digital art. As for its intended recipients, the Regulation introduces rules applicable to clearly identifiable entities (i.e. issuers, wallet providers, service providers), which does not exhaust the list of players in decentralized finance systems. Therefore, there will be no rules on smart contract programmers and governance token holders of so-called decentralized autonomous organizations (DAOs); unhosted wallets, i.e. software that allows peer-to-peer transfers between DLT addresses, will also remain outside the scope of application.

In addition, initiatives in this area are already under way – also thanks to agreements between supervised intermediaries and third parties – and others are expected to be launched even before the finalization of the European rules and their full entry into force; this explains the need for the authorities to be proactive in ensuring that market developments are guided from the outset by security considerations.

3. Benchmarks for intermediaries, market participants (scheme operators, wallet providers, payment infrastructure providers) and providers of crypto-asset technology solutions

The use of crypto-assets entails a variety of risks that could undermine the stability of the financial system. Financial risks include liquidity, market, credit and counterparty risks; non-financial risks

[20] See the public consultation on the crypto-asset Reporting Framework and Amendments to the Common Reporting Standard: https://www.oecd.org/tax/exchange-of-tax-information/public-consultation-document-cryptoasset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf

include operational, cyber, legal, reputational, money laundering and terrorist financing, and third-party risks.

In introducing market rules for crypto-assets, which will also make new categories of entities subject to supervision, MiCAR assigns banks and other supervised financial intermediaries an important role. Under the new Regulation they will be able to perform a variety of possible functions within the crypto-asset ecosystems, contributing to their functioning, supporting and facilitating the transfer of tokens, custody, interactions with holders and movements into and out of the ecosystem.

Likewise, crypto-asset activity cannot fail to take into account the objectives underlying the central banks' oversight of the smooth functioning of the payment system, referred to in the draft Regulation as a key factor to be assessed during the authorization phase and during the conduct of the entities' business. In addition to, and even before MiCAR, the new Eurosystem oversight framework (see Section 3.2) is targeted at scheme operators (including when they relate to crypto-assets with a payment function) and the features supporting their supply and use (e.g. digital wallets), as well as at transfer/settlement platforms as part of stablecoin arrangements and technology providers.

In view of the above, the following sub-sections will describe some of the issues requiring the awareness of banks, financial intermediaries and the operators involved in the oversight of payment systems, as well as technology providers. This is without prejudice to the premise, as outlined in Section 1, that there are certain categories of speculative and highly risky crypto-assets whose widespread adoption continues to be strongly discouraged.

3.1 Banks and financial intermediaries[21]

Until the guidance currently being developed at international and European level is completed, regardless of the specific type of crypto-asset activity, the current prudential regimes[22] contain principles to which banks and other supervised intermediaries can immediately refer in assessing and monitoring the risks associated with any start-up in crypto-asset services.

In addition to holdings of crypto-asset exposures, these operations could consist of one or more of the following activities by banks and financial intermediaries:

- issuance and/or redemption of crypto-assets (if applicable);
- custody and management of the reserve in the case of asset-linked stablecoins;
- infrastructure management and transaction validation;[23]

[21] These are the following categories of banking and financial intermediaries in respect of which Banca d'Italia carries out its supervisory tasks: banks and banking groups; securities investment firms (SIMs) and SIM groups; asset management companies (SGRs), open-end investment companies (SICAVs) and closed-end investment companies (SICAFs); electronic money institutions (EMIs); payment institutions (PIs); financial intermediaries in accordance with Article 106 of the TUB.

[22] These include those defined by the Basel Committee and by EU legislation (e.g. CRR/CRD5).

[23] With regard to infrastructure management and transaction validation, see Section 3.2.

- provision of services such as digital wallet, exchange, trading platform, order execution, placement, and receipt and transmission of orders on behalf of third parties, and advisory services.

In relation to these activities – and taking into account the specific characteristics of each of them and the relevant risk types – intermediaries are urged to consider, on the basis of the rules and best practices already applicable, the importance of ensuring:

- the timely involvement of the corporate governance bodies and second and third-level control functions, from the initial phase of study of the initiatives, to assess their compliance with the applicable regulations, consistency with the strategic guidelines, risk governance objectives and policies, and their economic and financial sustainability;

- adequate flows of information to the corporate bodies and internal control functions on the level and trend of their exposure, either directly or indirectly, to all types of risk associated with crypto-asset activities, any deviations from the policies approved by the body responsible for strategic supervision, the type of transactions and services provided and the respective risks; particular attention must be paid to the appropriate monitoring of the risks of money laundering and terrorist financing associated with crypto-asset transactions – including the risk of the avoidance of international sanctions – and reputational and legal risks, also taking into account the changing regulatory framework;

- that the corporate bodies and internal control functions have the appropriate expertise to fully understand the opportunities and risks characterizing crypto-asset activities and the use of decentralized technologies, in relation to the intermediary's competitive environment and business model, its strategy and overall risk profile;

- that the organizational structures are, from time to time, consistent with and suitable for the initiatives undertaken, to ensure effective monitoring of the resulting risks, the protection of customers and the prevention and management of conflicts of interest with other activities carried out. There should be particular emphasis on the adequacy of processes and procedures designed to ensure the identification, assessment and mitigation of risks (reputational or other risks) arising from outsourcing or the use of services provided by third parties, even if they cannot be classified as outsourcing (e.g. operators specializing in the custody of digital assets, digital wallets, trading platforms).

In the case of outsourcing or entrusting to third parties the operational functions related to crypto-asset activities or the use of decentralized technologies, given their innovative nature, the following aspects are of central importance: (i) the assessment of the conditions laid down in the legislation for classification as 'essential' or 'important' functions; (ii) the ability of intermediaries to select and monitor the service provider on an ongoing basis to ensure that the service provider has not only the technical/technological expertise necessary for the proper performance of the service entrusted but also the ability to ensure ongoing compliance with the supervisory rules (in terms of, for example, agreed service levels; adequacy of information flows; security of the data on the intermediary's activities; security of their own systems).

In view of the specific characteristics of crypto-assets, the type of transactions and decentralized technologies, intermediaries also need to ensure:

- the appropriate definition of the customer segments to which it is intended to offer/distribute products or services in crypto-assets, in relation to their complexity and any applicable regulatory provisions, assessing the introduction of qualitative and quantitative operational limits, including in relation to the customer's income and capital situation; this relates, in particular, to wallet services, exchange services, trading platforms, order execution, placing, receiving and transmitting orders on behalf of third parties, advisory services, and indeed to all crypto-asset-related activities;

- fair dealings with customers, with reference in particular to the services and activities mentioned in the previous point, both by means of providing adequate disclosure of the risks and characteristics associated with crypto-asset transactions, including those performed by third parties, and by strengthening the procedures for detecting fraud and handling complaints. Without prejudice to the safeguards put in place by the law, both to protect the integrity of commercial practices undertaken with customers and in the context of other sector rules, and in the absence of specific regulations, care must be taken to protect against legal and reputational risks arising from transactions carried out by those customers through portals or trading platforms to which access is granted or facilitated: specifically, it is strongly recommended that the intermediary does not enable or facilitate such access if there is no way for it to verify that these portals or platforms are able to prevent trading in high-risk crypto-assets (e.g. unbacked crypto-assets);

- the adoption of all the safeguards necessary to limit operational risks – with a particular focus on IT risk – and implementation of cybersecurity measures; in this context, intermediaries need to properly identify and manage the risks associated with the operation of currently unregulated or unmonitored technological infrastructures. Specifically, this type of risk is significant when it comes to services involving the custody of crypto-assets and private keys enabling access to and the exchange of crypto-assets;[24]

- the mitigation of the new dimensions that the financial risks associated with the provision of crypto-asset services or the issuance of crypto-asset services could take on, within the limits of the existing regulatory framework. Financial risks – notably credit, market and liquidity risks – are particularly important where crypto-asset activity is associated with a redemption obligation: (i) funds used by customers (where the redemption is expected to be equal to the nominal value of the crypto-asset); or (ii) the market value of the underlying assets (if redemption is expected to be variable, linked to the value of the assets to which the crypto-asset may relate). In addition, it should be noted that these risks may require that specific emphasis be placed on the management and investment of reserve assets, if any, underlying a crypto-asset;

[24] Such risks may include the loss and theft of cryptographic keys and, consequently, of crypto-assets themselves.

- a thorough assessment of the prudential treatment applicable to potential crypto-asset exposures which, pending the establishment of the relevant legislative framework, must be assessed on a case-by-case basis, in the context of a prior dialogue with the Bank;[25]

- in the asset management sector, the consistency and alignment between the funds' investment strategy, the liquidity profile, the redemption policy and the form thereof, as well as all aspects relating to the protection of investors.

Intermediaries should be aware that crypto-asset transactions must be carefully monitored from the perspective of sound and prudent management. In the absence of full protection against these risks, banks and financial intermediaries need to refrain or withdraw from carrying out these activities. The foregoing should be applied according to the principle of proportionality, in line with the operational complexity, size and organizational complexity of intermediaries and, as outlined above, the actual transactions performed using crypto-assets or decentralized technologies. However, Banca d'Italia reserves the right to carry out further study and analysis at any time, including on a case-by-case basis, with regard to specific initiatives or activities.

3.2 Operators[26] (scheme operators, wallet providers, payment infrastructure providers) and technology providers

For its oversight activities, Banca d'Italia will first draw some insights from the report that the CPMI and IOSCO[27] have addressed to the market and to the competent authorities to analyse how to apply the current international standards to stablecoin arrangements.

The new Eurosystem supervisory framework, known as the PISA framework (Payment Instruments, Schemes and Arrangements), which was published in November 2021 and will come into force in November of this year, is similarly geared to attracting entities operating in crypto ecosystems into the sphere of supervision. With the aim of taking account of the (technical and regulatory) changes in the payments market, the Pisa framework has extended the scope of control to include new payment solutions, such as stablecoins (which are included by virtue of a reference to 'transfer of value' rather than to the traditional concept of 'transfer of funds'). The framework will thus also allow crypto-assets with a payment function and the features supporting their supply and use (e.g. wallets) to be included within the oversight perimeter.

---

[25] The Basel Committee is finalizing a second consultation paper on the prudential treatment of crypto-assets with the aim of publishing the final document by the end of the year. See www.bis.org/press/p220531.htm.

[26] The supervised operators that are financial intermediaries will also refer to the content of Section 3.1.

[27] On 1 December 2021, the public consultation on this report was concluded; see https://www.bis.org/cpmi/publ/d198.pdf. The CPMI and IOSCO – highlighting the prevalent use of these new assets so far, and in particular the 'transfer function' of crypto-assets anchored to a single fiat currency, i.e. the transfer of value between users that is typically associated with the functioning of a payment system – refer to the 'principles for financial market infrastructures' (PFMIs) applicable to payment systems (as well as to other market infrastructures, such as CSDs, which carry out a transfer function) for the infrastructure component of systemic stablecoin projects. This can be seen as a 'strengthening' of the payment features of these assets, also in connection with the impact that they may have on the efficiency and reliability of the payment system as a whole, thus giving a key role to central banks whose tasks include safeguarding these objectives.

Entities providing technology to support banking, financial and payment services[28] are already subject, under certain conditions, to prudential provisions for outsourcing and to oversight controls.[29]

With specific regard to crypto-asset operations and to the use of decentralized technologies in finance, also in relation to systemic risk oversight and the proper functioning of the payment system, operators and technology providers are invited, where applicable, to take into account the following:

- it is essential that technology management is based as much as possible on clear and defined governance as well as on management requirements for different risks (e.g. operational, cyber, and information and data protection) to which reference should be made – in circumstances where this is applicable (particularly in the case of permissioned DLT, in which responsible parties can be identified) – to programme developers that determine the functioning of DLT or to subjects with powers for managing DLT functions (e.g. transaction validation or governance in a broader sense);

- technology service providers, where clearly identifiable, may fall under the supervisory rules as an outsourcee of supervised intermediaries and/or be subject to oversight controls based on the application, under certain conditions, of oversight standards for the payment system. The controls on these entities could extend to the monitoring of peer-to-peer transactions enabled by software ('unhosted wallets'); in this respect, the providers of the technology used and the support functions (e.g. entities that manage DLT by providing the technological support and planning systems) should ensure that adequate reporting information is available,[30] also taking account of the role and constraints of supervised intermediaries and of payment infrastructures under oversight;

- The infrastructures that enable the transfer function of crypto-assets, especially those linked to a single fiat currency and that are a component of the trading platforms on which crypto-assets are traded, should comply with the oversight standards applicable to financial infrastructures, in particular those relating to governance and integrated risk management;

- crypto-assets with a payment function and the features supporting their supply and use (e.g. wallets) should comply with the oversight standards for instruments, schemes, arrangements, especially those concerning legal soundness, governance, and credit and liquidity risk. In particular, to ensure redeemability and to be 'more secure' for users and issuers, the stablecoin

[28] Such as data processing and storage services, the supply of computer and communications networks, and the supply and maintenance of terminals and devices used for payment services.

[29] Specifically, Banca d'Italia oversees, pursuant to its Measure of 9 November 2021, technical infrastructure or service providers that are considered critical for the smooth functioning of the Italian payment system; the services provided by these providers include, but are not limited to, messaging and network services, business applications and/or services that are used for the clearing and/or settlement of payment transactions, and multi-operator interface technology services for third-party access pursuant to Commission Delegated Regulation (EU) 2018/389.

[30] For example, a list of all transactions carried out vis-à-vis unhosted wallets (where this is possible in terms of differences with a list of hosted wallets, such as the list derived from the census of parties carrying out digital portfolio activities held by the OAM), so as to enable specific monitoring activities to be carried out where necessary ('blockchain analysis') and/or for *ex post* reconstruction by the judicial authority ('blockchain forensics').

reserves anchored to assets should reflect as much as possible the composition and value of the basket or individual asset to which they refer.

Notwithstanding the above, if the activity is relevant to the smooth functioning of the payment system or the individual components thereof, also with regard to any 'transfer of value'[31] within complex digital systems, Banca d'Italia also reserves the right to consider using the prerogatives granted to it by Article 146 of the Italian Banking Law (Supervision of the payment system).

Given the difficulty in some cases – for example, in the case of 'pure DeFi' – of identifying specific entities to which to apply certain requirements, the possibility of intervening in the processes of drawing up and developing the technological standards used, with a view to strengthening the necessary risk mitigation safeguards, merits further investigation.

These standards could be 'qualitative' reference points for the development and implementation of smart contracts and other fundamental aspects of decentralized technologies; they should also be defined and managed by a governance model that can exploit the synergies stemming from the public sector's interaction with the private sector, in a co-regulatory way whereby the authorities continuously engage with technological operators to create shared benchmarks, so that technology can evolve in a manner that is consistent and compatible with the rights and safeguards that deserve to be guaranteed.

4. Customer protection – warnings about crypto-asset risks

With specific reference to the protection of customers who intend to buy or trade crypto-assets, Banca d'Italia draws attention again to the content of the warnings it has published since 2015 (also jointly with Consob), and the statements adopted by the European supervisory authorities (EBA, ESMA and EIOPA), in line with the guidelines issued by international bodies (FSB, FATF).[32] Specifically, following similar initiatives undertaken in the past, the abovementioned authorities have recently

[31] From a Eurosystem perspective, in the context of the PISA framework, recent technological developments justify extending the scope of application for the current oversight of payment instruments to all electronic payment instruments that allow 'value transfers' between end-users. The latter consists not only of transfers of funds in euros by electronic means of payment, but also of value statements secured by claims or goods denominated or repayable in euros; or other digital resources accepted according to the rules of a scheme for payment purposes or for fulfilling payment obligations in euros.

[32] Banca d'Italia, in line with the guidance issued by international bodies (FSB, FATF) and the three European supervisoryauthorities (EBA, ESMA, EIOPA, known as the ESAs), has published several warnings on crypto-assets to users and supervised intermediaries since 2015.

Banca d'Italia – Warning on the use of 'virtual currencies' (January 2015) – https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/index.html?dotcache=refresh;

Banca d'Italia – Consumer advice on the risks of virtual currencies on the part of the European Authorities (March 2018) -https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali-2018/index.html?dotcache=refresh;

Consob and Banca d'Italia warn against the risks inherent in crypto-assets (April 2021) – https://www.bancaditalia.it/media/comunicati/documenti/2021-01/CS_Congiunto_BI_CONSOB_cryptoasset.pdf

The ESAs recently published 'EU financial regulators warn consumers on the risks of crypto-assets' (March 2022).

reiterated that crypto-assets are highly risky and speculative instruments and are not suitable for most consumers as an investment or as a means of payment or exchange.

Crypto-assets are currently not subject to the transparency rules for banking products, payment services and investment services and lack any specific protection (i.e. crypto-asset services are not subject to any form of supervision or control by the supervisory authorities, without prejudice to the above).

Customers therefore need to be mindful that they could lose some or even all of the capital invested, of fraud and errors, and of the lack of safeguards available to them. It is particularly important to understand that some crypto-assets are completely lacking in any intrinsic value and not backed by any redemption rights and which, as a general rule, cannot be considered suitable for carrying out a payment or investment function because of their highly risky nature:[33] disclosure to customers should stress that operations involving such crypto-assets are discouraged by Banca d'Italia.

In this context, customers must pay specific attention to the risks of misleading advertising, also via social media and on the part of influencers, and to investment proposals that guarantee high returns.[34]

In any case, Banca d'Italia invites supervised intermediaries and other operators to compile as scrupulously as possible, even in the absence of regulatory requirements, the information to be made available to customers who intend to acquire and hold crypto-assets using channels provided by intermediaries and operators; this is to promote maximum awareness of the significant risks mentioned above, as well as to mitigate the serious legal and reputational risks that such assets may generate.

5. The next steps

Banca d'Italia – in conjunction with the ECB and other national supervisory authorities – will continue to monitor developments in the crypto-asset market and changes in the use of decentralized technologies in finance in order to assess their risks and impacts on financial stability, on banking and financial intermediaries, on the correct functioning of the payment system and on customer protection.

The Bank will continue to cooperate in the various international (FSB, CPMI and BCBS) and European forums to define high-quality standards and strengthen dialogue with market participants with the aim of: i) encouraging the development of sound and sustainable operating models, also with regard to the 'economic impact';[35] (ii) ensuring an adequate level of interoperability (and

[33] For example, care must be taken with asset-linked stablecoins, which are actually pegged to *unbacked crypto-assets* and could therefore, despite appearances, have the same volatility/risk characteristics as crypto-assets, the use of which, as mentioned, should be discouraged.

[34] According to the OAM survey conducted in 2021 in cooperation with the University of Tor Vergata on the attitude of Italians towards crypto-assets, 89 per cent of respondents had only heard about them and 11 per cent knew nothing about the topic; the survey shows that, as the level of knowledge about crypto-assets increases, so does the propensity to invest.

[35] There should be a particular focus on the consensus mechanisms used to validate transactions, which, with specific reference to certain solutions (especially the proof-of-work used by Bitcoin), can have a substantial impact on the

'interoperability standards') between various technological solutions to support decentralized finance and crypto-asset operations; (iii) ensuring compliance with the current legislation, in particular AML legislation; and (iv) fostering a level playing field with other jurisdictions in light of technological development.

Banca d'Italia may also promote and support initiatives aimed at defining standards and good practices that could be a shared point of reference,[36] particularly in areas of activity and development not included in the current and forthcoming rules, thereby increasing the attractiveness of the national financial community.

The Bank is open to dialogue with the various stakeholders, including through the innovation facilitators it manages,[37] in order to promote the definition and development of enabling technological standards to which they may refer if they intend to develop DLT-related services; the goal is to identify and support virtuous and adequately monitored innovation in the financial and payments system, in order to mitigate the risks that it may entail and to maximize the benefits it may provide to the advantage of the economic system and its components: consumers, households, firms and public administration bodies.

As part of the tasks assigned to it, Banca d'Italia, also in close cooperation with the European Central Bank and the other supervisory authorities, will in any case monitor the functioning of the governance and control arrangements and the effectiveness of any internal operational limits and safeguards, including anti-money laundering ones, introduced by intermediaries.

To complete the process of defining the aforementioned European regulatory framework for crypto-assets, the Bank, in agreement with the other competent authorities, may intervene with guidelines also of a pre-emptive nature to help ensure the development of services based on secure, efficient, inclusive and sustainable decentralized technologies.

environment and climate because of energy-intensive consumption. A more recent type of consent mechanism is the proof-of-stake (PoS), which is usually considered to be less energy-intensive. On this topic, see, for example, the FSB, 'Assessment of Risks to Financial Stability from Crypto-assets', February 2022, 9-10.

[36] Such as technological standards linked to the drawing up and implementation of smart contracts and consensus algorithms, or good decentralized governance practices.

[37] This refers to the integrated offering of innovation facilitators managed by Banca d'Italia in order to foster dialogue with the market (Fintech Channel), support the development of FinTech projects (Milano Hub), and allow controlled forms of experimentation (regulatory Sandbox).