Comitato Digital Finance Assogestioni

ASSOGESTIONI
associazione del risparmio gestito

ITALIAN DIGITAL FUNDS

Guidelines

May 2024

Edited by Roberta D'Apice (Assogestioni),
with the technical and scientific support from PwC Italy and
Osservatorio Fintech & Insurtech of the Politecnico di Milano

www.assogestioni.it

WARNINGS

The Guidelines represent a tool of assistance and support for the establishment and operations of Italian Digital Funds. Therefore, they are neither binding nor exhaustive with respect to the possible choices made by entities operating in the ecosystem of the Italian Digital Funds.

The Guidelines do not alter the meaning of the existing legislation – legislative, regulatory and level 3 – nor can they be interpreted in this sense. The Guidelines do not represent the position of the Supervisory Authorities on the topics discussed, nor do they anticipate or replace the supervisory assessments on the individual initiatives related to the Italian Digital Funds.

All images are from the Getty Images agency.

INDEX

INTRODUCTION

Digital innovation has always developed at a very high speed. Recent times have seen great acceleration. We have witnessed phenomena that were hardly imaginable until some time ago, such as those, for example, related to the development of generative artificial intelligence, but not only. The financial industry is one of the areas of greatest relevance in terms of the potential applications of digitalization. The central role that this industry plays in the correct functioning of economic and social systems is such that it requires, on the one hand, extreme attention, but, at the same time and on the other hand, to understand how to best orient strategies and behaviors to maximize all the potential benefits and mitigate the related risks. In our country, this condition is very important.

Among the most affected sectors of the financial industry, the asset management sector certainly stands out. The asset management industry is central to competitiveness. As well known, indeed, Italy owns the "raw material" of the financial industry, namely savings, in extraordinarily high quantities, and therefore it should promote the development of this industry in order to assist to the increasing growth of the values of efficiency, stability and quality, while preserving the protection of the investor.

The two central assumptions that underpin the Guidelines on Italian Digital Funds (Guidelines), promoted by Assogestioni, in collaboration with the PwC Italy and Osservatorio Fintech & Insurtech of the Politecnico di Milano, are grounded on two observations: on the one hand, digital technological evolution opens new frontiers and generates potentialities, which had never been so broad and pervasive before, and, on the other hand, asset management is one of the foundations of the Italian financial industry, and, by means of the latter, of the entire economic system. The Guidelines are the result of a long journey that began with the exploration of the possible implications of digitization on the asset management industry, and that ultimately led to the identification of two areas of attention. After an initial phase of study and experimentation that, in March 2023, resulted in the publication of the white paper "Beyond Cryptocurrencies – Distributed Ledger Technologies for Asset Management", these areas could be further analyzed with the admission of the project "DLT and Asset Management: opportunities and challenges for the industry" to the Call for Proposals of 2022 by the Milano HUB of the Bank of Italy, whose activities ended at the end of 2023.

The Guidelines have been defined throughout a continuous dialogue and exchange with Milano HUB and represent a valuable support for the development of the digital transformation path of the asset management industry operators in Italy.

The Guidelines are indications to support operators, in a framework that is developing, both at European and national level, to better define the playing field of reference.

The regulations and standards on Crypto–assets (MiCAR), those on digital operational resilience (DORA) or those related to the issuance and circulation of digitized financial instruments (DLT Pilot Regime and, specifically for Italy, the Fintech Decree) as well as the Standards of the Basel Committee on the prudential treatment for banks exposures in Crypto–assets, are just some of the examples that tell us that there are no more "alibis". The "playing field", although not fully defined, is outlined to favor technological development at the service of the financial industry.

The Guidelines are not binding, nor can they be considered exhaustive. However, they aim to provide a benchmark that, the more it is shared, the more it will lead to the establishment of standards at the base of a rapid spread of innovation. At the same time, it is important to underline that such indications do not alter the meaning of the current legislation in this field, nor can they be interpreted in this sense. Therefore, they do not represent the position of the Supervisory Authorities on the issues addressed, nor do they anticipate or replace the supervisory evaluations on the individual initiatives in this area.

The Guidelines intervene to promote an appropriate development of investments in DLT financial instruments and in the Crypto-assets included in the scope of the MiCAR; on the other hand, they aim to orderly accompany the evolution of Italian undertakings of collective investment whose shares or units are issued -and thus are native digital[1] - on a distributed register for digital circulation. On this background of an institutional and regulatory framework that is being shaped - albeit not too far - there is also the trajectory of central bank digital currencies (CBDC) with significant impacts on digitized financial investments. It is better to anticipate it rather than to chase it.

The Guidelines are structured in four parts and are articulated in fourteen points.

The scope of application is delineated in Part I, defined also by sharing the meaning of some recurring terms. Accordingly, the definition of Italian Digital Funds is important, since it summarizes in a single concept the two cases on which the Guidelines insist and that are examined the Parts III and IV: the Italian Funds that invest in Digital Assets (i.e., Italian Crypto Funds) and the Italian Funds whose units/ units are natively issued on a DLT (i.e., Italian DLT Funds). It is left to the Fund Manager to evaluate the establishment of one or the other type of Funds or both.

Part II identifies some safeguards for the operations of Italian Digital Funds (regardless of the specificity of the Fund, i.e., whether Crypto or DLT) which, while being of a general nature, are particularly focused on the topics of governance, control and risk management, supply of information flows, correct definition of organizational structures, in order to preserve an orderly and balanced development of the market. In this context, a specific Guideline was also dedicated to the protection of personal data, with a focus on some (non-exhaustive) elements that are recommended to be considered.

Parts III and IV contain specific indications for the establishment of Italian Crypto Funds and Italian DLT Funds.

With reference to the Italian Crypto Funds, Fund Managers are first and foremost recommended to carefully evaluate the initiatives in this field, taking care to address every relevant aspect, especially regarding the impacts of the initiatives on the stability and integrity of the financial markets. This also considering the need to contrast money laundering and paying attention to the customers to whom the units of the Italian Crypto Funds are offered, to the overall coherence of the initiative with respect to the internal organizational structure and the competencies of its corporate governance bodies and personnel. The Guidelines, based on the current national regulation of undertakings of collective investment, except for any different indication from the legislation or the Authorities,[2] consider the investment in MiCAR Crypto-assets falling within the category of "other assets", referred to in Article 4, paragraph 1, letter f) of the Italian DM n. 30/2015. Accordingly, for these assets it will be necessary to verify at least semi-annually the existence of a market and of a value that can be determined with certainty. Moreover, the Guidelines provide, among other things, some recommendations for the types of Funds that, under the aforementioned Regulation, can invest in such activities (Non-reserved closed-ended AIFs and Reserved AIFs), among which the one to ensure a diversified portfolio composition that allows for investments (and their related risks) fractioning and portfolio optimization.

Particular attention has been paid to identifying the ways in which the role of the Depositary can be carried out in a DLT context. In the absence of specific indications in the UCITSD and AIFMD rules, the Guidelines attempt to find a coordination between the sector regulations and the new developments introduced by the legislation on distributed ledgers (DLT Pilot Regime, MiCAR, Fintech Decree), based on some assumptions: i) the new developments in the regulatory framework have not changed the

1. For information on "native" digital financial instruments, refer to https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm
2. Given the evolution of the regulatory framework and the variety of Crypto-assets, the evaluation could also be carried out on a case-by-case basis.

functions of the Depositary, in terms of ensuring the proper functioning of the Funds and protecting – within the limits of its competences – the interests of the Funds investors, leaving unchanged, among other things, the need to distinguish management functions and custody functions; ii) the needs for certainty and safeguard of the participants require, where possible, that the custody of the assets of each fund or share compartment is entrusted to a single entity, avoiding duplication of roles and limiting the number of entities in the asset management chain; iii) the Depositary is a regulated entity that deeply knows the asset management market; iv) technology affects the operational methods through which the Depositary performs the role assigned to it by the regulations; v) the most recent legislation, both European and national, has contributed to the development of a regulation on the custody of Digital Assets, useful for the purposes of the Guidelines.

The Guidelines also focus on the distribution of Italian Crypto Funds, recommending, among other things, to the Fund Managers and Distributors to be equipped with suitable processes for the selection of the target market of customers to whom offering the Italian Crypto Funds.

In the development of Guidelines on Italian DLT Funds, we started from the relevant provisions contained in the Fintech Decree and in the Consob Delegated Regulation, exclusively regarding the cases of issuance and circulation in digital form of shares and units of undertakings of collective investment not admitted to trading in a trading venue. In this context, the Guidelines are aimed at presenting general rules, such as those contained in the Fintech Decree, considering the specificities of the operational model underlying the issuance and circulation of units or shares of undertakings of collective investment. The Guidelines do not consider, in this first phase, the case of admission to trading on a DLT market infrastructure of the units or shares of undertakings of collective investment falling within the scope of the DLT Pilot Regulation[3].

The Guidelines are followed by technical Annexes that provide indications in terms of implementation and risks. From this perspective, some principles for evaluating Crypto-assets (Annex I) have been identified; the main best practices specified in the security standards have been recalled, such as, for example, those included in the ISO 27001 and the PCI, and more specifically those identified in Cryptocurrency Security Standard (CCSS), ISACA Blockchain Framework and Guidance and OWASP Smart contract Top 10 (Annex II); indications have been given to mitigate the security risks linked to the management of cryptographic assets within the framework of DLT financial instruments, on certain topics such as: i) generation of cryptographic keys; ii) creation of Wallets; iii) storage of keys; iv) use of keys; v) policy in case of key impairment and for allowing and revoking keyholders (Annex 3).

The concept of ecosystem, always invoked in digital transformation processes, finds a fundamental workspace in Annexes 4, 5 and 6. In this perspective, the indications provided in Annex 4 on the functions that each of the entities involved in the operations of the Italian Digital Funds will be able to perform within the DLT and, above all, on the operations that can be encoded on one or more Smart Contracts are of particular importance. Equally important are the considerations made, within the scope of Annexes 5 and 6, on the on-chain settlement methods of the Italian Digital Funds operations, also through the description of the two processes of subscription and redemption of digital units of open-ended Italian Funds differentiated according to the settlement asset used. Annex 7 contains some examples of disclosure to the Investors in Italian Digital Funds.

The Guidelines end with a list of bibliographic indications useful for further analysis of many of the topics covered in them.

3. Namely the units in collective investment undertakings covered by Article 25, paragraph 4, letter a), point iv), of Directive 2014/65/EU, the market value of the assets under management of which is less than EUR 500 million.

The digitalization of the industry, through both investment in Digital Assets and, in particular, native digital issue of undertakings of collective investment shares/units, represents a fundamental step in the search for further efficiency and operational excellence in the industry. Accordingly, this technology can enable a simplification of operational processes in the long term, with a consequent reduction of costs and operational risks. In the specific case of the establishment of Funds that invest in Digital Assets and that, at the same time, issue digital Fund units, the process for calculating the NAV could also be made even more efficient, to the benefit of the final investor.

In conclusion, the real question is what role our asset management industry and, more generally, our Country wants to play in this evolution. Given the nature of these Guidelines, the method with which they were developed, the institutional and professional actors who participated in them, it is possible to argue that, also through their publication, our Country, today more than ever, could play the role of front runner of this transformation, giving Italy the place it deserves even in terms of innovation and value export.

PART I
SCOPE AND DEFINITIONS

Guideline n. 1. Scope

1. These Guidelines provide recommendations for the establishment and operation of Italian Digital Funds to Fund Managers, Depositaries and Distributors of Italian Digital Funds as well as Other Operators in the ecosystem of Italian Digital Funds.

Guideline n. 2. Definitions, regulatory references and Supervisory Communication

Guideline 2.1 – Definitions

1. For the purposes of these Guidelines, the following terms are defined as:

Italian Digital Funds: the Italian Crypto Funds and the Italian DLT Funds.

Italian Crypto Funds: the Italian funds that invest in digital assets.

Italian DLT Funds: the Italian funds whose shares or units are issued on a distributed ledger for digital circulation.

OICR: the undertakings for collective investment referred to in article 1, paragraph 1, letter k), of TUF.

Digital Assets: the DLT Financial Instruments and MiCAR Crypto-assets.

DLT Financial Instruments: the financial instruments issued on a distributed ledger for digital circulation, including the digital financial instruments referred to in article 1, paragraph 1, letter c) of the Fintech Decree.

MiCAR Crypto-assets or "Crypto-assets": the Crypto-assets, other than DLT financial instruments, falling within the scope of MiCAR.

MiCAR defines Crypto assets as "any digital representation of a value or of a right that can be transferred and stored electronically, using distributed ledger technology or similar technology". MiCAR Crypto-assets are divided into three categories, each subject to distinct requirements based on the associated risks: (i) Asset-referenced tokens (ARTs)[4]; (ii) Electronic-money tokens (E-money tokens or EMTs)[5]; and (iii) crypto-assets that are not considered ARTs or EMTs. This third category includes Utility tokens[6].

Distributed ledger technology or "DLT": the technology referred to in Article 2, point 1), of the DLT Pilot Regulation and, namely, the technology that enables the operation and use of distributed ledgers. DLTs are usually classified based on reading and writing aspects. Based on the reading aspects, and therefore on the possibility of accessing them to consult the information contained in the ledger, DLTs are classified into public and private (in the latter case, only some authorized nodes can access the information contained in the ledger). Based on the writing aspects, on the other hand, DLTs are commonly distinguished between permissionless and permissioned according to the modality of participation in the consensus mechanism (in the permissioned ones, only some of the nodes are authorized to participate in the consensus mechanism that allows for the updating of the ledger status). DLTs can also be hybrid, and thus combine permissionless and permissioned operations.

4. A type of Crypto-asset that is not an electronic money token and that purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies [art. 3, paragraph 1 (7)].
5. A type of Crypto-asset that purports to maintain a stable value by referencing the value of one official currency [art. 3, paragraph 1 (6)].
6. A type of Crypto-asset that is only intended to provide access to a good or a service supplied by its issuer [art. 3, paragraph 1 (9)].

Blockchains are a subcategory of DLTs, which are characterized by two properties: (a) their register is structured in the form of blocks of transactions (which are the elementary units for updating the state of the register) and; (b) the blocks are linked together through the use of specific cryptographic functions, making it possible to update the register only by adding data at the end, without being able to modify the previous blocks.

Consensus mechanism: the rules and procedures by which an agreement is reached, among DLT network nodes, on the validation of a transaction.

DLT Network Node: a device or an informatic application that is part of a network and holds a complete or partial copy of records of all the transactions made through the distributed ledger.

Distributed ledger for digital circulation or "Register": a register used for the issuance and circulation of DLT Financial Instruments or MiCAR Crypto assets.

Intermediaries: the Fund Managers, the Depositaries, the Distributors.

Fund Manager(s): the entities referred to in article 1, paragraph 1, letter q-bis) of the TUF.

Depositaries: the entities referred to in article 1, paragraph 1, letter q-ter) of the TUF.

Distributors: the entities authorized to offer and sell funds shares or units.

Other Operators: the technological solutions and/or infrastructures providers, Digital Assets service providers, ICT third-party service providers.

Solution and/or technological infrastructure providers: entities that provide technology to support banking, financial and payment services, including tokenization providers.

Digital activity service providers: in compliance with current regulations, service providers for DLT Financial Instruments and MiCAR Crypto-asset, including key custody providers (i.e., custodians of private cryptographic keys).

ICT third-party service providers: the ICT third-party service providers as defined by the DORA Regulation.

Responsible for the Register for Digital Circulation (Responsible for the Register): the Fund Manager or the third party identified by the Fund Manager as responsible for the register, registered on the list referred to in Article 19, paragraph 1 of the Fintech Decree.

Delivery versus payment or "DVP": the delivery versus payment as defined in Article 2, paragraph 1, point 27, of Regulation (EU) no. 909/2014.

Smart Contract: the smart contract as defined by Article 8-ter of the Simplification Decree, that is a program for elaborator that operates on technologies based on distributed ledgers and whose execution automatically binds two or more parties on the basis of effects predefined by them.

Wallet: the pair of cryptographic keys (public key and private key) that identify each user in the distributed register and allow interaction inside of it to arrange the transfer of the pertaining instruments. Wallets typically differ on the basis of how private keys are managed: if they are kept by the provider, the Wallets are defined as "custodial", while, if the keys are managed by the user, they are defined as "non-custodial".

Gas Fee: the commissions requested for blockchain transactions to cover the costs of creating a new block.

Guideline 2.2 - Regulatory references and Supervisory Communications

1. For the purposes of these Guidelines, the following is intended as:

Communication by the Bank of Italy: the Communication by Bank of Italy on Decentralized Technology in Finance and Crypto-assets, June 2022.

Anti-Money Laundering Regulation: the anti-money laundering regulation provided by the Italian Legislative Decree of November 21, 2007, n. 231 (Anti-Money Laundering Decree) and the related implementing measures.

DM n. 30/2015: the decree of the Ministry of Economy and Finance of March 5, 2015, n. 30, which provides the regulation implementing article 39 of the legislative decree February 24, 1998, n. 58 (TUF) concerning the determination of the general criteria to which Italian undertakings for collective investment must comply.

Fintech Decree: the decree-Law (Decreto Legge) of March 17, 2023, n. 25, on "Urgent provisions on issuing and circulating certain financial instruments in digital form and on simplifying the Fintech experiment" converted, with amendments, by Law n.52 of May 10, 2023.

Simplification Decree: the decree-Law (Decreto Legge) of December 14, 2018, n. 135 on "Urgent provisions concerning support and simplification for companies and public administration", converted with modifications by law n. 12 of February 11, 2019.

Consob Regulation: the Consob regulation on issuing and circulating financial instruments in digital form adopted by Consob with Resolution n. 22923 of December 6, 2023.

DLT Pilot Regulation: the regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU.

DORA Regulation: the regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

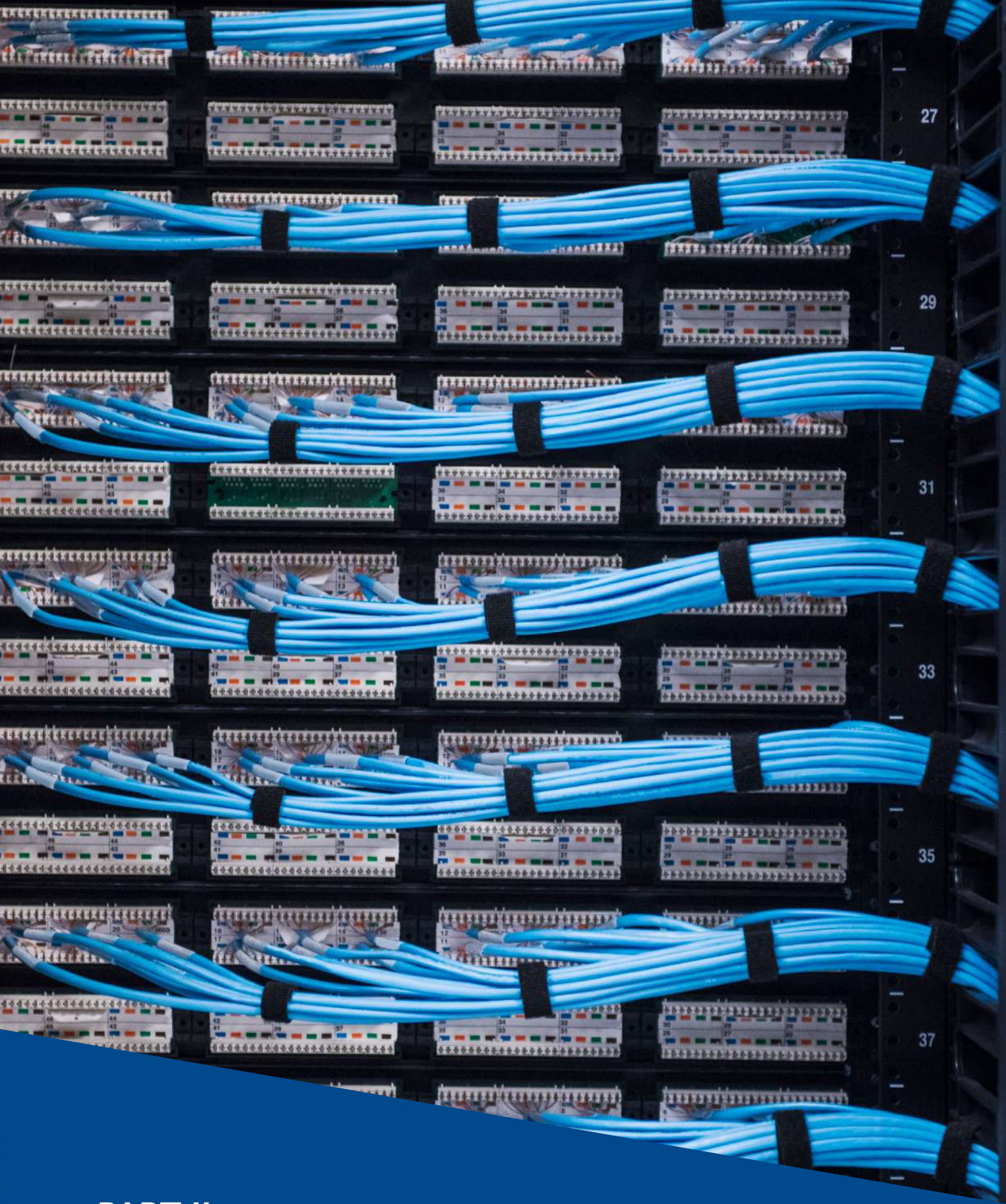
MiCA Regulation (MiCAR): the regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto assets, amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

Regulation on Collective Asset Management: the regulation issued by the Bank of Italy with order of 19 January 2015 as subsequently supplemented and amended.

UCITSD: the directive 2009/65/EC on the on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS).

AIFMD: the directive 2011/61/EU on Alternative Investment Fund Managers.

TUF: the Consolidated Law on Finance pursuant to Legislative Decree of 24 February 1998 n. 58.



PART II
GENERAL SAFEGUARDS FOR THE OPERATION OF ITALIAN DIGITAL FUNDS

Guideline No. 3 - General principles for Intermediaries (Fund Managers, Depositaries, Distributors)

1. Intermediaries shall ensure compliance with the legislation, including sector-specific rules, in force from time to time, the guidelines and measures of the Supervisory Authorities, including the principles contained in the Communication by the Bank of Italy or in others, subsequent, adopted by the Supervisory Authorities. In particular, the Intermediaries shall:

i. ensure the timely involvement of corporate governance bodies and second and third level control functions, from the initial study phase of the initiatives relating to Italian Digital Funds, to assess their compliance with the applicable regulations, consistency with strategic guidelines, risk governance objectives and policies, as well as their economic and financial sustainability;

ii. ensure 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;

iii. ensure 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 the operation of Italian Digital Funds, to any deviations from the policies approved by the body responsible for strategic supervision, to the type of transactions and services provided and their respective risks;

iv. ensure the complete mapping of the risks associated with the initiatives and their mitigation, paying particular attention to the new dimensions that financial risks could assume when connected to the operation of Italian Digital Funds. In particular, Intermediaries shall ensure that risk mapping takes into account the individual type of Italian Digital Fund considered, namely: a) Italian DLT Funds investing in traditional activities; b) Italian DLT Funds investing in DLT Financial Instruments; c) Italian DLT Funds investing in MiCAR Crypto-assets; d) Italian DLT Funds investing in DLT Financial Instruments and in MiCAR Crypto-assets. In defining the risk management system, Intermediaries should not rely exclusively or mechanically on third parties, but should ensure that adequate and independent internal analysis is always performed;

v. pay particular attention to the appropriate monitoring of the risks of money laundering and terrorist financing – including the risk of circumvention of international sanctions – as well as reputational and legal risks, also taking into account the evolving regulatory framework;

vi. ensure the adoption of all necessary safeguards for the containment of operational risks – with particular attention to IT risk – and the protection of cybersecurity; in this context, intermediaries shall identify and appropriately manage risks related to the operation of technological infrastructures. For this purpose, intermediaries are recommended to verify the adequacy of their informatic infrastructures (especially in terms of mitigation of risks related to the use of technology), as well as of their 1st, 2nd and 3rd level controls;

vii. pay particular attention to 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 specialized in the custody of digital assets, Wallets, trading platforms);

viii. ensure the existence of safeguards for the identification of potential investors, through a review of investigations aimed at profiling customers, in order to evaluate their effectiveness in light of the specificities of the Italian Digital Funds considered;

ix. ensure adequate information to investors about the risks and characteristics associated with operations in Italian Digital Funds, also with reference to activities carried out by third parties, and proceed, if necessary, to strengthen procedures for fraud detection and complaints management.

The above-mentioned recommendations must be declined according to the principle of proportionality, in relation to the operational, dimensional and organizational complexity of the Intermediaries as well as, as previously outlined, to the actual operations carried out in Crypto-assets or through the use of decentralized technologies.

Guideline n. 4 – Safeguards in case of outsourcing

1. When Intermediaries intend to entrust to third parties the provision of services or the performance of operational functions, they should carefully evaluate the costs and benefits of such choice, especially compared to the in-house performance of the service or function, carrying out market analysis, evaluating – also prospectively – the impact of technology on their own business and on their own organizational structure, performing in-depth due diligence on providers in light of the criteria identified by the applicable regulations and the additional elements identified in the following paragraphs. When they decide to entrust third parties with the provision of the service or operational function, Intermediaries shall also ensure that the company's bodies, the internal functions concerned and the internal control functions are adequately informed and that their contributions to the decision-making process are formalized.

2. In case of outsourcing or use of services provided by third parties, even if not classifiable as outsourcing of essential functions, Intermediaries set the criteria for selecting providers and technology providers, taking into account various aspects, including: (i) the policies and procedures implemented by the provider to ensure the availability, confidentiality, integrity and non-disputability of data; (ii) the adoption of robust approaches to plan the entire life cycle of the technologies used and to choose the technological standards to adopt; (iii) the procedures used to identify and address situations of malfunctioning and operational and cyber security incidents, as well as to respond to such events; (iv) adequate plans aimed at recovery from emergency situations and for disaster management, with regular periodic checks; (v) the integrity of the governance of the provider, the organizational structures established to identify and manage risks, as well as the pertaining responsibility guidelines; (vi) the ability of the entity to whom the service is entrusted to continuously ensure compliance with regulations and supervisory regulation.

3. In case of outsourcing of operational functions, the Intermediaries shall ensure: (a) the assessment of the conditions laid down in the legislation for the classification as "essential" or "important" functions, taking care to evaluate also prospectively the impact of technology on its internal organization and business; (b) 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 supervisory rules (in terms of, for example, agreed service level; adequacy of information flows; security of to the data on the Fund Manager's activity; security of their systems); (c) the ability of the subject to whom the function is outsourced to ensure ongoing compliance with legislation and supervisory regulation.

Guideline n. 5 - Criteria for the choice of the "Other Operators"

1. The Fund Managers shall carry out a careful evaluation when choosing Other Operators necessary for the operations of the Italian Digital Funds, considering at least if these entities are able to ensure compliance with the principles contained in the Communication by the Bank of Italy or in others, subsequent, measures adopted by the Supervisory Authorities. Fund Managers shall, in particular, ensure:

i. that technology management is based as much as possible on a clear and defined governance as well as on management requirements for different risks (for example operational, cyber, AML, information and data protection);

ii. the availability of adequate reporting information on the activity carried out, also taking account of the role and constraints of supervised intermediaries and of payment infrastructures under oversight;

iii. the adoption of appropriate standards in terms of information security;

iv. the experience achieved in the field of distributed ledger technologies.

Guideline n. 6 – Operability on-chain and off-chain of the Italian Digital Funds

1. The Fund Managers shall identify the functions that each of the entities involved in the operation of the Italian Digital Funds can perform within the DLT and, above all, establish the operations that can be coded on Smart Contracts, taking into account the provisions of Annex 4.

2. In the definition of the Smart Contracts, it is recommended to ensure consistency with the current regulatory system and to keep adequate documentation.

3. The Fund Managers shall promote the settlement of payments through central bank money, including in tokenized form, whenever practical and available or, when it is not practical and available, through commercial bank money, including in tokenized form, or through Electronic money tokens or other assets under the MiCA Regulation, if suitable for payment purposes. In this regard, it is recommended to consider the provisions of Annexes 5 and 6.

4. The Fund Managers shall ensure to use resilient and sustainable operational models and to guarantee, where possible, an adequate level of interoperability (and "conversation standards") between different technological solutions.

Guideline n. 7 – Protection of Personal Data

1. The Fund Managers shall ensure compliance with the principles established by legislation in force on the protection of personal data, paying particular attention, among other things, to:

i. respect the principle of minimization, avoiding as much as possible to insert personal data on-chain and, where necessary, using anonymization/pseudonymization techniques;

ii. comply with the provisions of the legislation in force concerning processing of personal data both on-chain and off-chain (legal basis, disclosure, records of processing activities);

iii. identify the so-called privacy roles in the value chain of the funds (controller, processor, joint controller), especially evaluating, in cases of outsourcing, the privacy role assumed by the outsourcers (delegation of functions and, in any case, involvement of third parties);

iv. identify the methods through which to allow the exercise of rights by the data entities, compatibly with the characteristics of the identified DLT;

v. implement, in accordance with the characteristics of the DLT, technical and organizational measures that guarantee a level of security adequate to the risk, carrying out the necessary assessments (e.g., data protection impact assessment, DPIA).

PART III
SPECIFIC SAFEGUARDS FOR THE OPERATION OF ITALIAN CRYPTO FUNDS

Guideline n. 8 – Investment Activity of the Italian Crypto Funds

1. The Fund Managers shall carefully evaluate the initiatives on Italian Crypto Funds, taking care to address every relevant aspect, especially with regard to the impacts of the initiatives on the stability and integrity of the financial markets, also considering the need to fight money laundering, on the client to whom the units or shares of the Italian Crypto Funds are offered, on the overall consistency of the initiative with respect to the internal organizational structure and the skills of its corporate governance bodies and staff.

2. The Fund Managers who intend to start initiatives on the Italian Crypto Funds, when investing in DLT Financial Instruments, shall ensure compliance with the limits and criteria established for investment in financial instruments of the Bank of Italy pursuant to Article 6, paragraph 1, letter c), of the TUF, as well as compliance with all the sector rules provided for by European and National legislation on investment in financial instruments and those specifically introduced on DLT Financial Instruments by the Fintech Decree.

Notwithstanding the above, Fund Managers intending to establish Italian Crypto Funds, when investing in Crypto-assets shall:

i. unless otherwise specified by regulations or Authorities, invest in Crypto-assets that can be attributed to the category of "other assets" referred to in article 4, paragraph 1, letter f), DM no. 30/2015, for which therefore a market exists and which have a value that can be determined with certainty with at least a semi-annual frequency;

ii. invest in Crypto-assets which, in addition to being attributable to the category of "other assets" (unless otherwise assessed by the regulations or the Authorities), do not have a high degree of price volatility and whose evaluations are reliable and the related risks are manageable. In particular, it is appropriate that the OICR do not invest in Crypto-assets without intrinsic value, not referred to any activity of the real or financial economy and that are not suitable for investment functions (for example, in algorithmic stablecoins, in unbacked Crypto-assets, other Crypto-assets anchored to assets with high volatility and/or Crypto-assets that do not allow an adequate risk control by the Fund Manager);

iii. adopt the categories of non-reserved closed-ended AIFs and reserved AIFs, ensuring compliance with the relevant provisions of the Bank of Italy on the investment activities of the OICR, as well as taking care to monitor and constantly align to the legislative and regulatory evolution or any recommendation – individual or systemic – from the Supervisory Authorities. For the case of non-reserved closed-ended AIFs, and consequently accessible by retail investors, Fund Managers are recommended to pay particular attention to the compatibility of the investment object with the profile of the retail investors to whom the Fund is addressed.

In the case of indirect exposures, through corporate vehicles or other types of schemes, it is always appropriate for Fund Managers to verify that the investment in instruments issued by such vehicles or schemes does not in fact result in investment in crypto-assets not regulated under MiCAR or, more generally, in investments in non-recommended crypto-assets. In a more general perspective, the greatest attention should be paid to the legal and economic effects related to the investment in financial instruments or other securities issued by vehicles or schemes that invest in, are connected to or backed by Crypto-assets.

3. In defining the initiatives related to Italian Crypto Funds that invest in Crypto-assets, Fund Managers shall:

i. ascertain the existence of a market for the Crypto-assets object of investment and that their value can be determined with certainty and on, at least, a semi-annual frequency;

ii. ensure a diversified composition of the portfolio in order to ensure investments diversification and portfolio optimization;

iii. evaluate, depending on the type of Crypto-assets they invest in, how the rules on risk mitigation and diversification should be applied, adopting a prudential approach;

iv. define the methodology for determining the price of Crypto-assets and adopt internal procedures suitable for carrying out the Crypto-assets evaluation. For this purpose, Fund Managers take into account the criteria specified in Annex 1;

v. when they establish, within the limits of what is allowed by the regulation, reserved open-ended OICR, adopt specific policies concerning redemption of shares or units and establish an investment strategy of the Fund consistent with such redemption policies;

vi. perform adequate stress tests on the investment in Crypto-assets. The stress tests must be extreme but possible and must reflect the volatility of the prices of the Crypto-assets, including the potential total loss of the investment value.

4. Fund Managers of Italian Crypto Funds shall ensure to:

i. include in the risk management policy the methods to manage the risks associated with direct or indirect investment in Crypto-assets. For this purpose, Fund Managers shall take into account at least the risk factors indicated in best practices of the sector, such as the ISACA – Blockchain Framework and Guidance, and reported by way of example and not exhaustively in Annex 2;

ii. ensure the consistency and alignment between the Fund's investment strategy, its liquidity profile, redemption policy and form, as well as all the aspects related to underwriters protection;

iii. verify the adequacy of the safeguards for identification of potential investors in order to evaluate their effectiveness in the light of the specificities of the Italian Crypto Funds established, especially in the case of closed-ended retail Funds;

iv. indicate in the Fund's offering documents clear information on the nature of the proposed investment in Crypto-assets and the risks associated with such investment.

Guideline n. 9 – Custody of the Digital Assets of the Italian Crypto Funds

1. In order to identify the tasks and responsibilities of the Depositaries of the Funds that invest in DLT Financial Instruments and in Crypto-assets, the Fund Managers and the Depositaries shall take into account the following recommendations based on the assumptions below: i) the innovations introduced in the regulatory framework have not changed the functions of the Depositary, in terms of ensuring the correct functioning of the Funds and the protection – within the limits of their competences – of the interests of the Fund investors, among other things remaining unchanged the need to distinguish the management functions from those of custody; ii) the needs of certainty and investors' protection, require, where possible, that the custody of the assets of each Fund or compartment is entrusted to a single entity, avoiding duplication of roles and reducing the number

of entities in the asset management chain; iii) the Depositary is a regulated entity that deeply knows the asset management market; iv) technology impacts on the operational methods used by the Depositary to perform the role assigned to him by the legislation; v) the most recent interventions of the European (DLT Pilot Regulation and MiCA Regulation) and national legislator (Fintech Decree) contribute to the development of a legal framework on the custody of digital assets that, despite the complexity of the regulatory interconnections with the "traditional" framework, cannot be ignored for the purposes hereof.

2. Fund Managers perform a careful evaluation in the selection of the Depositary of DLT Financial Instruments and Crypto-assets, considering at least: (i) the structure and mechanisms used for the custody of Digital Assets. For this purpose, the Fund Managers can take into account the adoption by the Depositary of the measures specified in Annex 3; (ii) the experience gained by the Depositary in the custody of Digital Assets.

3. In the case of Crypto-Asset custody, Fund Managers are recommended to select the Depositary also considering the existence of the requirements envisaged for the custody activity by Article 60, paragraph 7 of the MiCA Regulation.

4. Considering the provisions of Article 17 of the Fintech Decree and Article 75 of the MiCA Regulation, Depositaries are recommended to consider the performance of the custody of Digital Assets through the control of the means of access to such Digital Assets, where applicable in the form of private cryptographic keys and of dual-signature protocols, without prejudice to the Fund's ownership of the assets; the Fund Manager and the Depositary define in the agreement the aspects concerning their internal relations as to the control of the means of access to Digital Assets and the respective tasks.

5. In performing the tasks of custody of Digital Assets, Depositaries may use Other Operators specialized in the custody of Digital Assets. In such case, the safeguards of Title VIII, Chap. III, Sec. V of the Regulation on Asset Management remain applicable.

6. Depositaries are recommended, where applicable, to: (i) ensure that the means of access to the Funds' Crypto-assets are clearly identified as such, ensuring that such means of access are kept separately from the means of access to the Digital Assets of the Depositary or from the means of access to the Digital Assets of its clients; (ii) keep a register of positions, opened in the name of each Fund, corresponding to each Fund's rights over the Digital Assets, inserting into such register as soon as possible any movement carried out following the instructions of the Fund Manager. In this case, the Depositary's internal procedures ensure that any movement that impacts the recording of the Digital Assets is enhanced by an operation regularly recorded in the register of positions of the Fund; (iii) establish internal rules and procedures to minimize the risk of loss of the means of access to the Fund's Digital Assets and of the rights connected to such Digital Assets due to fraud, cyber threats or negligence.

7. In the event of loss of the means of access to the DLT Financial Instruments held in custody under Article 17 of the Fintech Decree, the Depositary, unless it can prove that the non-compliance was due to force majeure or fortuitous event, is obliged to return without undue delay DLT Financial Instruments of an identical type or the corresponding value, in addition to liability for any other possible loss suffered by the Fund or investors as a result of intentional or negligent breach of their obligations.

In case of loss of the means of access to Crypto-assets held in custody in compliance with art. 75 of the MiCA Regulation, the Depositary is liable towards the Fund for the loss of the Crypto-assets and of the means of access to the Crypto-assets limitedly to the market value of the lost Crypto-asset at the time of its loss, unless it is an incident not attributable to the Depositary as provided by the same article 75, par. 8, of the MiCA Regulation.

8. The Depositary shall establish internal rules and procedures and shall identifies the mechanisms and devices to be adopted in order to ensure compliance with the other obligations provided by Article 48 of the TUF and any other function performed, in any capacity, in favor of Italian Crypto Funds.

Guideline n. 10 – Distribution of Italian Crypto Funds

1. In the distribution activity of Italian Crypto Funds – while maintaining the safeguards provided by the relevant discipline, and paying attention to monitor and constantly comply with legislative and regulatory developments or any individual or systemic recommendation of the Supervisory Authorities – it is recommended to value the peculiarities that characterize such Funds and, in particular, to:

i. ensure the adequate definition of the target market to which the Italian Crypto Funds are offered, taking into account their complexity and risks;

ii. to care as scrupulously as possible for the disclosure to be provided to customers who intend to purchase Italian Crypto Funds, in order to facilitate the maximum awareness of the relevant risks identified, also using the information contained in Annex 7;

iii. provide the services through qualified personnel, specifically trained on the characteristics of the Italian Crypto Funds offered.

PARTE IV
SPECIFIC SAFEGUARDS FOR THE OPERATION OF ITALIAN DLT FUNDS

The purpose of this Part is to present some of the main general rules contained in the Fintech Decree, taking into account the specificities of the operational model underlying the issuance and circulation of units or shares of OICR. In particular, Guideline No. 11 generally concerns the issuing of units of Italian DLT Funds; Guideline no. 12 explores the case where the Fund Manager does not perform the role of Responsible for the Register; Guideline no. 13 offers an overview of the tasks of the Responsible for the Register, whether it is the Fund Manager or another entity provided for by the Fintech Decree; finally, Guideline no. 14 highlights the importance of correct information during the distribution phase of Italian DLT Funds units.

However, there is still the obligation to comply with all the provisions of the Fintech Decree.

Guideline n. 11 – Issuing of units of Italian DLT Funds

1. Fund Managers that intend to issue, on a DLT, units of Funds not admitted to negotiation on a trading venue, shall ensure compliance with the relevant provisions of the Fintech Decree.

2. The Fund Manager shall evaluate whether: 1) to issue units of Italian DLT Funds on a Register kept by a specialized entity, registered in section 4 of the List kept by Consob, or by a subject registered in section 1 of the List kept by Consob; 2) to carry out the activity of Responsible for the Register with reference to the units of its own Italian DLT Funds (after subscription in section 2 of the List kept by Consob), using, where appropriate, Other Operators for the provision of services/activities.

3. Each issuance of units of Italian Digital Funds is registered on a single Register and each Register is associated with a unique Fund Manager.

4. Registers for digital circulation shall:

a. ensure the integrity, authenticity, non-reputability, non-duplicability and validity of the entries attesting ownership and transfer of the units of the Italian DLT Fund and the related liens;

b. allow, directly or indirectly, to identify at any time the parties in whose favor the entries are made, the kind and number of units of the Italian DLT Fund held by each, and also make the circulation thereof possible;

c. allow the party in whose favor entries are made to access the entries in the register relating to their own units of the Italian DLT Fund at any time and to extract a copy in electronic form for all purposes envisaged by law;

c. bis – prevent the loss or unauthorized alteration of data and entries relating to the Italian DLT Fund units for the entire duration of the entry;

d. allow liens of any kind to be entered on the units of the Italian DLT Fund, as provided for by Article 9 of the Fintech Decree;

e. ensure accessibility by the National Commission for Companies and the Stock Exchange (Consob) and the Bank of Italy in order to exercise their respective functions;

f. allow the identification for the purposes of Article 9 of the Fintech Decree of:

   1. the date the lien was established;

   2. the units of the Italian DLT Fund;

   3. the nature of the lien and any additional information;

4. the reason for the lien and the date of the transaction being entered;

5. the quantity of units of the Italian DLT Fund;

6. the holder of the units of the Italian DLT Fund;

7. the beneficiary of the lien and, where disclosed, the existence of an agreement between the parties for the exercise of rights;

8. the date of expiry of the lien.

5. For the purpose of issuing digital units of Italian DLT Funds, the following information shall appear as univocally linked to each digital units and shall be made available in an accessible and consultable electronic form at all times, possibly also through the Register itself:

a. the name and place of business of the Fund Manager;

b. the name and type of the Fund;

c. the date of constitution of the Fund and its duration;

d. the type of units, whether registered or bearer, as well as the class and the compartment it belongs to, if any;

e. the nominal value of the units, if any;

f. the Depositary;

g. the terms and conditions of the issuance;

The Fund Manager shall evaluate whether to make electronically available also additional information, such as, for example, the currency in which the Fund units are denominated and the income regime.

6. The Fund Manager shall evaluate the adoption of the following models for managing subscriptions and redemptions of the Italian DLT Funds units requested by Investors;

a. Entries on the Register are carried out in favor of the Investor of the units of the Italian DLT Fund; the Investor is the holder of the Wallet and controls directly the means of access to digital units, also in the form of private cryptographic keys (so-called direct or disintermediated model);

b. Entries on the Register are carried out in favor of the Investor of the units of the Italian DLT Fund; the Investor is the holder of the Wallet, but the means of access to digital units, also in the form of private cryptographic keys, are entrusted by the Investor to the Distributor who operates on behalf of the Investor (so-called partially intermediated model);

c. Entries on the Register are made in favor of the bank or investment firm that operates in its own name and on behalf of the Investor of the units of the Italian DLT Fund; the latter (bank or investment firm) is the holder of the Wallet on behalf of the Investor and controls the means of access to digital units, also in the form of private cryptographic keys. In this case, the full and exclusive legitimation to the exercise of rights follows the registration on the account opened by the Investor at the bank or the investment firm, as provided for by article 11 of the Fintech Decree (so-called fully intermediated model).

Please refer to Annex 6 to find an example of the subscription and redemption process of units of Italian DLT Funds using the model sub b).

Guideline n. 12 – Italian DLT Fund Manager

1. The Fund Manager, if not acting as the Responsible for the Register with respect to the units of the Italian DLT Funds of its own institution, shall ensure compliance, in addition to the obligations established in the applicable sector-specific regulation, also with those provided in the Fintech Decree and the implementing secondary regulations. In particular, the Fund Manager shall:

i. rely on a Responsible for the Register registered in section 1 or 4 of the List kept by Consob;

ii. notify to the Consob the characteristics of the issuance of units of the Italian DLT Fund and the corresponding Responsible for the Register, as well as the additional information identified in the Consob Regulation;

iii. make available to subscribers the information referred to in Article 23, paragraph 3 of the Fintech Decree;

iv. ensure to provide the Responsible for the Register with the information referred to in Art. 12, paragraph 6, letter b) of the Fintech Decree;

v. verify, based on the entries of the Register, the entitlement to exercise the rights associated with the units of the Italian DLT Fund;

vi. update the corporate books provided for by DM no. 30/2015 based on the entries in the Register, even if the shareholders book is kept through the Register;

vii. carry out the necessary operations for the change of the financial instruments form and circulation regime in the cases and according to the methods indicated in art. 14, paragraph 2 of the Fintech Decree.

Guideline n. 13 – Responsible for the Register of the Italian DLT Funds

1. The Responsible for the Register, whether it is the Fund Manager or one of the entities listed in section 1 or 4 of the List held by Consob, is required to fulfill the obligations indicated in the Fintech Decree and in the secondary implementing regulations. In particular, the Responsible for the Register shall:

i. ensure that the Register complies with the characteristics envisaged in the Fintech Decree and its implementing provisions;

ii. guarantee the correctness, completeness and continuous updating of the facts relating to issuance information;

iii. ensure the integrity and security of the system, taking into account anti-money laundering needs, by virtue of the issuance and transfer of digital units on the basis of a suitable legal document;

iv. ensure operational continuity and the business recovery, through appropriate mechanisms and devices that include external information security. Operational continuity must also be guaranteed, among other things, in the event of replacement of some actors in the chain, including moments of "shared" management of specific roles on the platform (e.g., in the event of replacement of the Fund Manager or Depositary and the pertaining transitional phase of "handover");

v. prevent the use of digital units by entities other than those entitled;

vi. ensure that the total number of digital units constituting a single issuance cannot be changed;

vii. adopt a transition strategy in accordance with Article 14, paragraph 1 of the Fintech Decree, evaluate its effectiveness at least semi-annually and for this purpose adopt the necessary and appropriate measures and procedures;

viii. make available to the public, in an electronic form accessible and consultable at all times, a document containing information on the operational modalities of the register for digital circulation and of the devices to protect its operation, including the transition strategy;

ix. ensure compliance with the anti-money laundering provisions contained in the legislative decree of November 21, 2007, no. 231.

2. The Responsible for the Register is responsible for damages deriving from register keeping towards the Fund Manager, if it is a different entity from the Responsible for the Register, and towards the entity in favor of whom the entries have been recorded or should have been recorded, unless he proves to have taken all the appropriate measures to avoid damage. The Responsible for the Register is responsible for damages caused to the subject in favor of whom the entry has been recorded or to the investor, if he is a subject different from the former, whether they result from false information or from information that can mislead, or from the omission of due information, unless it proves to have used the necessary diligence to ensure the correctness and completeness of the information according to Article 23, paragraph 3 of the Fintech Decree.

Guideline n. 14 - Distribution of Italian DLT Funds

1. In the distribution activity of Italian DLT Funds – without prejudice to the safeguards provided by the relevant regulation and taking care to monitor and constantly comply with the legislative and regulatory evolution or any recommendations, individual or systemic, of the Supervisory Authorities – it is recommended to value the peculiarities that characterize these Funds and, in particular, to carefully manage the disclosure to be provided to customers who intend to purchase Italian DLT Funds, in order to illustrate the peculiarities of the subscription and redemption process of these Funds and the related risks, also using the information contained in Annex 7.

2. The obligations of the entities subject to anti-money laundering regulations remain unchanged.

ANNEX 1
PRINCIPLES FOR CRYPTO-ASSETS EVALUATION

For the purpose of evaluating the Crypto-assets held by the Fund, the Fund Managers apply, where compatible, what is provided by Title V, Chapter IV, Section II of the Regulation on Asset Management.

Crypto-assets are evaluated on the basis of the most recent price detected on the relevant market, possibly also adjusted on the basis of other available objective elements of assessment, including their eventual appraisal by independent experts. For the correct evaluation of Crypto-assets, it is recommended to:

i. evaluate the Crypto-assets at the price observed on at least three authorized trading platforms or venues;

ii. analyze any interruption in the activity on the trading platform or venue that may affect the evaluation;

iii. adopt specific criteria for price estimation in terms of recognized sources, trading models superior than the average, volume and applied decimal precision;

iv. in the event that the value of Crypto-assets is related to a basket of assets, carry out a due diligence also on the underlying assets and, when possible, evaluate the latter according to the criteria provided by the regulations for the specific type of asset.

With specific regards to the pricing of DLT financial instruments, the Fund Manager also considers the impact that adverse events on distributed ledgers or on DLT market infrastructures (e.g., DLT inefficiencies, changes in the regulatory framework, technological evolution and subsequent obsolescence of previously used technology) can have on the tradability or, more generally, on the value of DLT financial instruments.

ANNEX 2
EVALUATION PROCESS AND RISK MANAGEMENT RELATED TO THE DLT USE

DLT presents possible security and privacy issues, detectable at the level of network, node, Smart Contract, and user. Such risks, accompanied by relevant mitigation technique examples, are described in the "Blockchain Framework and Guidance" published by ISACA, to which reference is made. Please find below an indicative and non-exhaustive list of risks.

A) Risks at infrastructure/network level

1. 51% Attack: The 51% attack is an attack that allows the attacker to take control of the network and potentially carry out malicious operations (e.g., double spending, which is spending the same unit of cryptocurrency twice, or inserting invalid transactions).

Mitigation Techniques:

- Monitor and ensure that network validators are as decentralized and geographically distributed as possible, so that no single entity can take control of at least 51% of the network hash rate.
- Carefully evaluate the consensus algorithms used (some algorithms, like proof of stake, might mitigate this risk by adopting solutions like slashing, which are penalties for malicious actors).
- Require a certain number of confirmations before the final acceptance of the transaction.

2. Eclipse Attack: an Eclipse attack attempts to isolate the victim node by blocking its access to nodes nearby, then tricking the victim node with false transaction information.

Mitigation Techniques:

- Increase the number of connected peers and randomize the selection of nodes.
- Provide a whitelisting of trusted nodes.
- Favor peers with a longer history of successful connections compared to newly discovered nodes.
- Use some of the less recent peers as anchors when restarting the node.

3. Denial of Service (DoS) Attack: this type of attack affects the ability of the blockchain to process blocks, execute Smart Contracts, or enable users to interact with the blockchain. There are several types of DoS attacks, such as, for example, flooding the network with phantom transactions.

Mitigation Techniques:

- Use a preemptive filtering system that prevents suspicious transactions from reaching the block creation phase.
- Use a large pool of block creators.
- Use a dynamic fee system, making it increasingly expensive to carry out the attack as network congestion increases.

4. Sybil Attack: this attack aims to corrupt a peer-to-peer network by creating multiple false identities.

Mitigation Techniques:

- Require attackers to block or spend a significant number of resources to make the attack expensive to carry out (e.g., computational power in the case of PoW or stake in the case of PoS).
- Introduce digital identity or reputation systems.

5. BGP Hijacking or Routing Attack: the attacker advertises short routes between two network segments containing nodes, allowing traffic between these nodes to flow through the attacker and enabling the latter to isolate the two parts of the network and delay transaction processing.

Mitigation Tecniques:

- Use multihomed nodes (nodes with Internet connections to two different segments).
- Use known and reliable paths to communicate with nodes from other segments.
- Use encrypted and authenticated communications.

B) Risks at Smart contract level

In general, a best practice often used in the blockchain and DLT field is to have an external company audit the Smart Contracts used for each new smart contract or for its updates. This activity has almost become a de facto standard for the main applications in the blockchain field, and significantly mitigates many of the risks associated with Smart Contracts.

The main ones are therefore reported below:

1. Access control: if access to the administrative functions of the smart contract is not properly managed, the attacker can access it, potentially causing damage to the organization.

Mitigation techniques:

- Ensure that a Smart Contract is correctly initialized to maintain contract ownership.
- Verify that the function caller is the owner of the contract before executing functions intended for the contract owner.
- Use a multi-signature Wallet to ensure greater protection to the contract owner in case of key theft.

2. Default Visibility: Attackers exploit poorly defined public function calls intended for internal calls to manipulate such functions.

Mitigation Techniques:

- Explicitly indicate the visibility identifier for the function.
- Monitor function calls using applicable blockchain explorers.
- Make the visibility as limited and consistent as possible with the intended use of the invoked functions.

3.Reentrancy: an attack of this type occurs when a contract makes an external call to another Smart Contract before completing its own state updates; the called contract in turn calls back the calling contract (reentrancy) with the possibility of manipulating its state in unforeseen ways.

Mitigation Techniques:

- Observe the Smart Contract design rule of checks-effects-interactions: for a higher level of security, it is necessary to first carry out conditional checks, then apply the effects on the state, and finally perform interactions with external contracts.
- Limit the amount allocated for external calls.
- Use a re-entrancy Guard (e.g., the one offered by the OpenZeppelin library) or a modifier which ensures that a function is not called recursively.

4. Whole number Overflow/Underflow: a condition of overflow or underflow occurs when an operation that requires a fixed-size variable to store a number that is outside its range is performed. Attackers rely on overflow and underflow manipulations to bypass conditional checks and alter mathematical calculations, such as payments, to their advantage.

Mitigation Techniques:
- Use a secure math implementation or reliable math libraries.
- Perform input validation to ensure that user inputs have the correct data type and fall within appropriate lower and upper limit values.

5. Timestamp manipulation: attackers can manipulate the timestamp of a block when this parameter is used in the code of a smart contract.

Mitigation Techniques:
- Avoid assigning a timestamp block to a variable of a Smart Contract.
- Ensure that nodes are required to synchronize date and time with a provider of universal time, and to ensure that the extracted block meets the required threshold.

6. Bad Randomness: any mechanism that generates pseudo-random numbers on the blockchain must be thoroughly examined to identify any faulty implementations.

Mitigation Techniques:
- Use the best random generators derived from oracles or external random services.

7. Front-running: in a front-running attack, the aggressor duplicates the unmined transaction contained in the mempool and pays higher gas fees to preempt the original transaction.

Mitigation Techniques:
- Where possible, use a commit-reveal approach, thus reducing an observer's ability to front-run the transaction.

8. Denial of Service (DoS): in a DoS attack, the aggressor manipulates one or more conditions (block of variable functions), disabling the Smart Contract.

Mitigation Techniques:
- Use expert code review and user testing on a test network with performance assessment or gas fee optimization.

9. Missing Input Validation: when input validation is not performed, values exceed the expected range and can cause problems in the Smart Contract.

Mitigation Techniques:
- Ensure that data types are expected before incorporating their use in Smart Contract functions.

10. Read after write / Bad handling of asynchronous operation: a Smart Contract function can perform a write function to update a state variable but read the updated value without having achieved an asynchronous update.

Mitigation Techniques:
- Ensure that global state variables are updated before use.

C) Risks at user level

1. Fake cryptocurrency exchange, Wallets, airdrops and hard forks scams: these scams entice victims through social engineering techniques to make fraudulent websites appear reliable.

Mitigation Techniques:

- Research thoroughly for all downloads, airdrops and hard forks.
- Carefully check the item before approving a signature within the Wallet and always verify the addresses of the contracts to interact with and the type of actions to undertake.

2.Wallet Exploits: The Wallet can be vulnerable due to design flaws, incorrect configuration by the user, or key storage files that have been left locally after software removal.

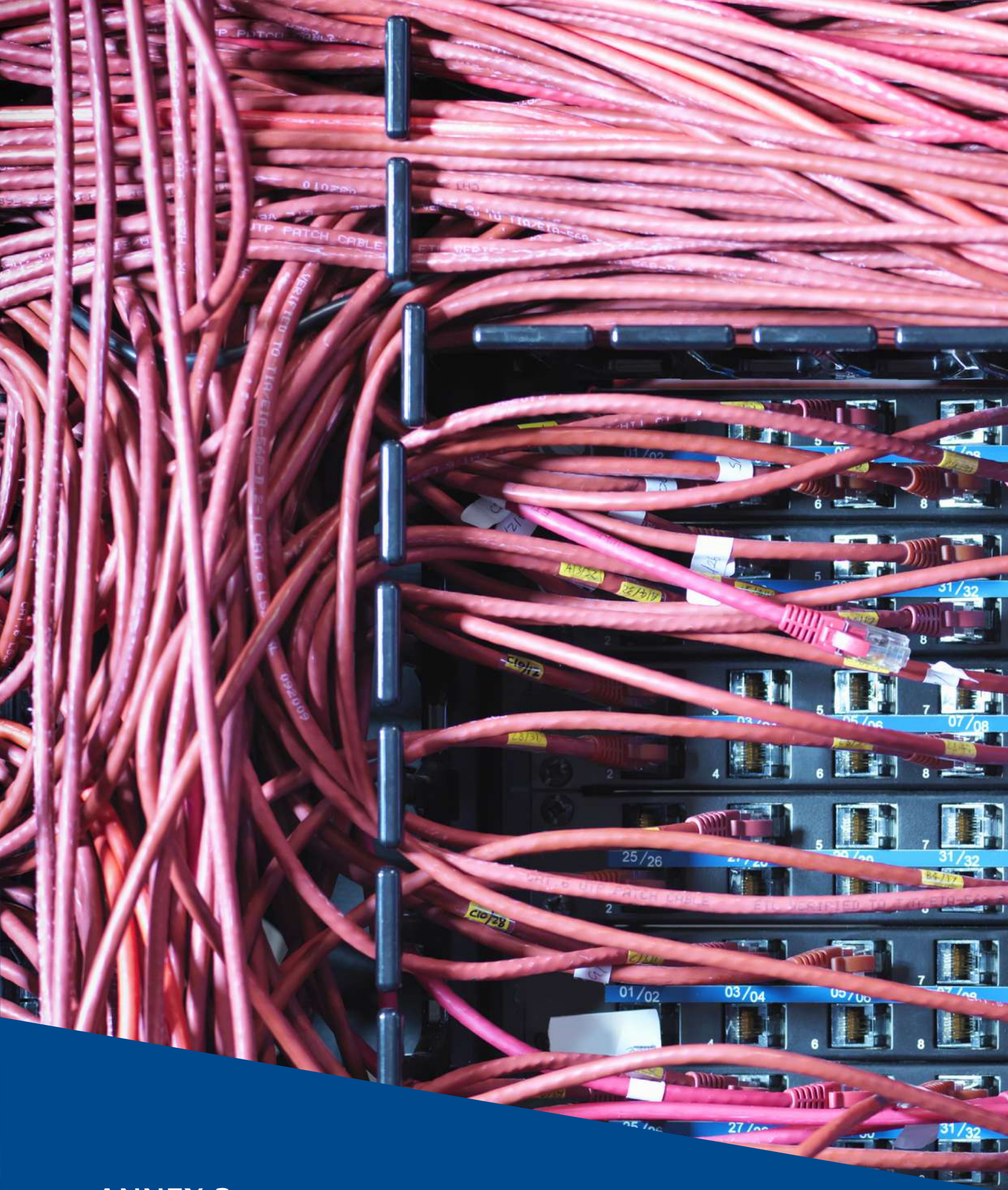
Mitigation Techniques:

- Look for authority sources to ensure that the installed Wallet version does not have known vulnerabilities.
- Enable local memory encryption as soon as the Wallet is installed.
- Do not save the seed phrase in unencrypted local files.

3. SIM Swapping: through SIM swapping, attackers try to gain access to mobile phones, from which users perform multifactor authentication for the login to web wallets.

Mitigation Techniques:

- Request additional levels of verification.
- Do not use the cell phone number for SMS as an authentication tool.



ANNEX 3
SECURITY SAFEGUARDS IN THE MANAGEMENT OF CRYPTOGRAPHIC ASSETS

This Annex intends to provide guidance on the key aspects that are recommended to be considered to mitigate the security risks related to the management of cryptographic assets for access to DLT Financial Instruments. For this purpose, it is recommended to define internal policies and procedures on the management of cryptographic assets, graduating them according to their role and the significance of the assets handled.

By cryptographic assets are meant the "keys" available to the Responsible for the Register to manage the Smart Contracts in support of the Funds operations, the Wallets of the investors and the ones which hold the ownership of the Crypto-assets subject to investment.

The following is taken from the CryptoCurrency Security Standard (CCSS), a standard that focuses on the good practices to manage security of cryptographic assets at enterprise level. The aspects addressed below complement (but do not replace) the best practices indicated in the reference standards in the area of information security (such as ISO 27001) or in the field of payment system security (such as the PCI). For a more detailed list of the measures associated with the aspects reported below, please refer to the CCSS standard.

A. Cryptographic assets management

- **Generation of cryptographic keys and seeds to be used within a DLT:** The secure creation of cryptographic keys and seeds requires, to be secure, confidentiality and the adoption of unpredictable numbers. Confidentiality is necessary to ensure that the newly created keys or seeds are not read/copied by unauthorized subjects. Non-deterministic and unpredictable numbers are necessary to ensure that the newly created key cannot be guessed or determined by an unauthorized party.
- **Creation of Wallets:** Wallets are created using digital signature methodologies that may require the signature of a single key, the signature of multiple keys or a minimum number of signatures from multiple keys. Additionally, Wallets can be created individually (commonly referred to as JBOK Wallets, or "Just a Bunch of Keys") or deterministically, by creating a set of addresses / key pairs from a single master seed. Security in Wallet creation is determined by the integrity of the Wallet against various risks such as loss, theft or key compromise, and the confidentiality of the Wallet which would make it difficult to associate a Wallet with a particular actor.
- **Key storage:** by allocating the Wallet keys in multiple geographical locations, risks associated with local business interruptions (for example, fires, floods, earthquakes, break-ins) do not affect the organization's ability to use the keys.
- **Use of keys:** the adoption of security measures in the use of cryptographic keys and/or seeds aims to safeguard the confidentiality of private keys against a range of risks, including malware and malicious insiders who use their authorized access to send unauthorized transactions. Such risks must be considered even if they stem from the use of key backups, which are only used in case the primary key is lost/damaged/inaccessible.
- **Policy in case of key compromise (KCP – key compromise policy):** the existence and adoption of a protocol that dictates the actions that must be taken in the event that a cryptographic key/seed or its operator/holder are believed to have been compromised. Organizations must be prepared to face a situation where a private key has become determinable or destroyed, even potentially. Examples of when the KCP would be invoked include, for instance, the identification of the tampering of a tamper-evident seal placed on cryptographic material, the apparent disappearance of an operator whose closest friends and family cannot identify where they are,

the performance of unusual operations or the receipt of communications that credibly indicate that an operator or a key is likely at risk of being compromised. The execution of KCP protocols must use approved communication channels to ensure that KCP messages are sent/received only by authenticated actors.

- **Policy and procedures for allowing and revoking keyholders:** namely access to the organization's or end-user's cryptographic keys or seeds by privileged users (superusers of computer systems). Improper management of staff hiring or resignations introduces the risk that access to privileged accounts persists despite resignations or role changes, as well as the possibility that the ability to sign certain transactions with unrevoked keys may remain.

B. Operations

- **Security Test/Audit:** including independent audits of security systems, technical controls, and policies that protect the information system from all forms of risk, as well as the vulnerability and penetration tests designed to identify the vulnerabilities of existing controls.
- **Data sanitization policy:** namely the removal of cryptographic keys from digital supports in the event of voluntary disposal of the supports. Due to the way file systems allocate data on digital supports, digital forensic techniques can be used to read old data that have been previously deleted. Proper sanitization of digital supports ensures the correct removal of all keys, eliminating the risk of information loss from abandoned devices such as servers, hard disk drives, and removable archives.
- **Audit log:** Audit logs are a fundamental tool in the field of computer security, as they provide the sequential list of activities carried out on a specific system. In the event of unexpected behavior or security incidents, audit logs can help investigators understand the causes of incidents and how to resolve inconsistencies to restore the information system to a coherent state.

ANNEX 4
GUIDELINES ON THE ON-CHAIN OPERATIONS OF THE ITALIAN DIGITAL FUNDS

This Annex is a tool to support technology operators in identifying the functions that each of the entities involved in the operation of the Italian Digital Funds can perform within the DLT, and especially to determine the operations that can be coded on one or more Smart Contracts.

In this regard, it is appropriate to note that the existing standards on Smart Contracts (ERC in the case of Ethereum) define guidelines to create specific Smart Contracts. However, each standard is not necessarily tied to a single Smart Contract. In fact, a standard can emerge from a set of interconnected Smart Contracts that work in synergy to achieve complex functionality. The implementation of standards such as ERC-20 ensures that tokens are easily negotiable and can interact without inconsistencies with any application that respects the same standard, providing a set of uniform rules, functions, and properties. These functions, such as total Supply, which provides the total amount of tokens, or transfer (address to, uint256), intended for token transfer, represent the cardinal operations that the token can perform. In addition, there are properties like name, symbol, and decimals that provide basic information about the token, such as its name, symbol, and the number of decimals it supports. In addition to the functions, events play a crucial role, operating as signalers or "notifications" issued by the Smart Contract in response to certain actions, such as the Transfer event, which occurs with the transfer of tokens between addresses. ERC-20, while being the prevalent standard for utility tokens, has some limitations in addressing the specific needs of security tokens and the resulting regulatory compliance. New standards have been introduced in the Ethereum community to address these issues, such as ERC-1400, ERC-1404, and ERC-3643, to name a few. These tokens, in addition to the basic functions of the ERC-20, include additional features such as transfer restrictions, the ability to load associated documentation, and more selective identity management with a system of whitelisting.

In the context of a Fund with units issued in digital form, the fungible token issued must possess the following minimum properties to be correctly identified and to comply with the operating modes of the Funds:

- Name: a descriptive feature to identify the token that represents the Fund units;
- Token Decimals: to the extent of three, to allow for the token thousandth fractionation;
- Chain ID: identifier of the network on which the token is traded;
- Address: address of the Smart Contract managing the token;
- ISIN CODE: international code that uniquely identifies financial instruments;
- Transferability among indicated and enabled subjects: to allow circulation only among known and profiled investors;
- Identification of an owner and possible additional roles: in order to have a greater control over the application and ensure its security, it is appropriate to define an owner. The owner of the Smart Contract is the only one authorized to access its critical functions. The owner can, for instance, be the only one able to issue new tokens or revoke tokens already issued, blacklist users, etc. This concept provides essential access control, preventing unauthorized calls to crucial functions and allowing future updates. This role can overlap with the Responsible for the Register or instead be covered by the Fund Manager or the Depositary. As an alternative, different or joint roles (even performed by multiple actors) can be considered. Each solution must, however, be carefully evaluated within each project according to its characteristics;

7. In this context, Ethereum blockchain is mentioned because most of the market use cases and users currently operate on EVM-compatible blockchains. However, there are other types of blockchains that use different programming languages and standards. Nonetheless, the use of bridges remains a possibility to enable interoperability between different blockchains and tokenized assets.

- Possibility for the owner to force operations: to apply some constraints on-chain. Critical functions should be exercisable only by the owner.

In addition to these basic properties, it is also necessary to determine the functions to be coded within one or more Smart Contracts that will define the standard.

In this perspective, a table of three columns is illustrated below:

i. the first column indicates the "traditional" tasks, actions and responsibilities of the subjects involved in the value chain of an open-ended Fund;

ii. the second column describes the role of technology for each of these tasks, actions and responsibilities. In particular, the following categories were used:

   - "By design" when the task/action/responsibility is somehow directly guaranteed by the technological nature of the register;
   - "Codable in the Smart Contract" when it is possible to automate or facilitate the task/action through Smart Contract;
   - "Partial" in case it is not possible to carry out everything on-chain, but also off-chain steps/checks are required;
   - "No" when technology is not involved in that part of the process;
   - "Incompatible with the nature of digital circulation", such as the issuance of the unit in paper form;

iii. instead, the third column reports some indications on the use of technology.

The indications represent the main activities related to Italian Digital Funds or, depending on the case, to Italian Crypto Funds or Italian DLT Funds, and are to be considered referred to the current state of technology and regulatory framework. In case of developments, it is possible that some tasks, today to be performed necessarily in part or in total off-chain, will become possible also on-chain. On the basis of the specific case, it could be possible to develop other evaluations on further and different activities or operations on units.

Fund Manager's Traditional Tasks and Responsibilities	On-Chain Execution	Notes
Fund administration (tasks and functions of the Fund Manager):		
Calculation of the unit value	No	Off-chain calculation, as such calculation is made on market values that do not always transit on-chain
Unit value registration	Codable in the Smart Contract	Unit registration in the value chain
Matching, settlement and order book management (which would occur with the technical "equivalent" of the DLT)	Codable in the Smart Contract	Order book + related operations managed by a Smart Contract
Maintenance of the journal, management report, semi-annual report	No	Off-chain maintenance of the journal, management report, semi-annual report
Processing, recording and communicating of other information (% daily securities exempted for succession, semi-annual whitelist securities percentage, counterparty ratings, etc.)	No	Off-chain
Assistance to auditors / circular letters	Partial	Off-chain Auditors can verify the shareholders register directly by looking at the history on the DLT
Documentation Keeping	Partial	Off-chain in case of outsourcing On-chain via hash notarization of the documents
Management of flows and data warehouse	No	Off-chain

Line Controls (interaction with other applications):

AML Compliance	Partial	Off-chain identification and KYC/AML controls, preliminary to the user obtaining tokens; possibility of exploiting on-chain data to facilitate subsequent monitoring, noting changes as to the obligations incumbent on the subjects of the anti-money laundering discipline

Information flows (interaction with other applications):

Supervisory reports	No/Partial	Off-chain, supervisory reports must be carried out in a traditional manner The extraction of transactional data from the DLT could be helpful for the creation of reports The use of public platforms with a transparent transaction registry could also facilitate control over the operations carried out
Maintenance of the Single Archive and SARA Notifications and 1st level reports that could lead to the sending of an SOS (i.e. unexpected)	No	Off-chain, the reporting flows are managed in a traditional way There might be the possibility to include in the blacklisting any reported addresses Moreover, the extraction of transactional data from the DLT could assist in the creation of reports

Exchange of information, including documents, with the Depositary, Distributor, customers, and any other subject in the value chain	Partial	Off-chain, it is possible to notarize the hash of particularly important documents on-chain to guarantee their integrity

Interventions on Fund unit circulation (tasks and functions; external events to the DLT; data processing):

Suspension of the subscriptions or redemptions of the units	Codable in the Smart Contract	Flag on the contract settable by the owner that pauses these functions
Application of other liquidity management tools	Codable in the Smart Contract	Even the most recent LMTs provided in the regulatory evolution (UCITSD/ AIFMD review) could be inserted within the Smart Contract (for example, by inserting functions for the "management" of subscriptions/redemptions)
Liquidation in case of absence of the prerequisites and conditions of the subscription, even in case of circulation subsequent to the first issue	Codable in the Smart Contract	Token revocabili da owner / burn o forceback
Imposition of constraints	Codable in the Smart Contract	To be defined during the issuance phase

Interaction with other DLTs	Codable in the Smart Contract	Conferral of assets, which could include DLT Financial Instruments for subscription to the Crypto Fund units

Extraordinary operations between OICR, both in the case of Digital Italian OICR and when only one or some of the Funds involved are Digital Italian Funds (events external to the DLT):

Merging/splitting of Funds, allowing the Fund Manager to set the date from which the operation is effective (also on the platform)	Codable in the Smart Contract	Minting of new redeemable Fund units upon burning of previous tokens
Conversion of the unit into units of other OICR of the same Fund Manager	Codable in the Smart Contract	Can be offered on-chain in the conditions of minting and burning of units
Control of the legitimacy of operations by the Fund Depositary	Partial	Operations can be consulted in the DLT history

Changes to the Fund regulation/ statute (events external to the DLT; data processing):

The Fund Manager must be able to apply the rules provided by the Regulation on Collective Asset Management (in particular, individual communications, suspension, right of redemption without applying redemption fees)	No	Off-chain
Tax obligations (see below) (tasks and functions of the Fund Manager)	No	Off-chain

Personal data protection	Partial	Off-chain identification of personal data with notarization and insertion of hash of documents linked to these (on the blockchain there is not the investor's identity but only the address linked to his Wallet) The blockchain layer is just one of the components of the system; distributed databases are also used. Most of the confidential information is kept in the database and through microservices, some based on Zero Knowledge Proof they are connected to the blockchain layer

Other obligations of competence/implementation under the responsibility of the Fund Manager (tasks and functions of the Fund Manager; events external to DLT):

Contract settlement, including the sending of certificates	No	Off-chain
Custody and administration of Fund units	By design	Possible to offer a Digital Asset custody service on behalf of customers (also with third-party support - e.g. Key custody provider)
Following the relevant amendment of the fund regulation, replacement of the Fund Manager with transfer to the new one of all its functions without any interruption	No	

Fund	On-Chain Implementation	Notes
Application of restriction criteria on participants	Partial	Off-chain evaluation (KYC/ KYB) and white-listing of the addresses enabled on-chain

Duties and responsibilities of the Depositary	On-Chain Execution	Notes
Management of liquid assets and distribution of proceeds:		
The Depositary holds the Fund liquid assets	By design/Codable in the Smart Contract	The tokens deposited in the Fund are sent to the Depositary
It handles the distribution of proceeds in proportion to the number of units held by each participant (the method of payment to be defined)	Codable in the Smart Contract	
In the event that the Fund liquidity is not entrusted directly to the Depositary, it ensures adequate monitoring of cash flows	Partial	Cash flows are publicly available in the DLT history
Issuance and Management of Certificates:		
If the subscriber has requested the issuance of the participation certificate, the Depositary checks the coupons and, in the case of registered certificates, verifies the integrity of the entire certificate and related coupons	Incompatible with the nature of digital circulation	There will be no “physical” certificates, the token represents the unit itself
Starting from the first business day following the settlement day of the subscriptions, it makes the certificates available to the participants in the places provided for by the identifying card	Incompatible with the nature of digital circulation	There will be no “physical” certificates, the token is representative of the unit itself
Information flows:		
The Depositary exchanges information, both documentary and non-documentary, with various stakeholders, including the Fund Manager, Distributor and customers	Partial	Some information related to tokens and their movements can be viewed directly on the on-chain registrer

Operations and Controls:

It is responsible for safeguarding the financial instruments entrusted to it, verifying ownership and maintaining the records of other assets	By design	The Depositary safeguards the financial instruments entrusted to it within its own Wallet
The Depositary verifies the legitimacy of operations such as sale, issuance, repurchase, redemption, cancellation of the Fund units, as well as the destination of the Fund income	Codable in the Smart Contract	Moreover, this information can be retrieved by consulting the history of the DLT
Ensures the correctness of the calculation of the Fund parts value; ensures that in operations related to the Fund, the consideration is remitted within the terms of use	Codable in the Smart Contract	
Carries out the instructions given by the Fund Manager that are not contrary to the law, to the Fund regulation or to the provisions, guidelines or measures issued by the Supervisory Authorities	Codable in the Smart Contract	

Legal Obligations and Liquidation:

It ensures that all payments made by investors during the subscription of units are received and recorded correctly	By design	Guaranteed by transactions saved in the DLT history
In the event of liquidation, collaborates with the Fund Manager to redeem the units to the participants, withdraw and cancel the issued certificates, and inform the participants about the details related to the liquidation	Codable in the Smart Contract	
The sums not collected within three months from the starting date of the payment are deposited in a special account registered to the Fund Manager	Codable in the Smart Contract	

It is responsible towards Fund Managers and participants for any damage resulting from non-compliance. In case of loss of the held financial instruments, the Depositary is required to return the instruments or the corresponding value thereof	No	
Management of access means in case of replacement of a Depositary who had control of the keys	Codable in the Smart Contract	The owner of the Smart Contract can update the address of the Depositary as needed

Tasks and responsibilities of the Responsible for the Register	On-Chain Execution	Notes
Compliance of the Register with the characteristics prescribed in the Fintech Decree and its implementing provisions:		
The register has the requirements established under Article 4 of the Fintech Decree and assigns to the issuance of units and shares the information referred to in Article 12, paragraph 6, letter b), of the same Decree	By design/Codable in the Smart Contract	The Fintech Decree provides that the information referred to in Art. 12, (6) (b) must be made available in an electronic form accessible and consultable at any time, possibly also through the register itself. Therefore, the information may not be directly guaranteed by the technological nature of the register
It ensures the correctness, completeness and continuous updating of the evidence relating to the issuance information	By design	
It also ensures the integrity and security of the system, taking into account the AML requirements, by virtue of the issuance and transfer of digital units on the basis of a suitable title	By design	

The register is structured in such a way as to always guarantee operational continuity, even in the case of replacement of some actors in the chain, including moments of "shared" management of specific roles on the platform (e.g. in case of replacement of the Fund Manager or the Depositary and related phase of managing the transitional phase of "handing over"): therefore, mechanisms should exist that serve this purpose (e.g. specific Smart Contracts)	Codable in the Smart Contract	The "handovers" are encodable in the Smart Contract

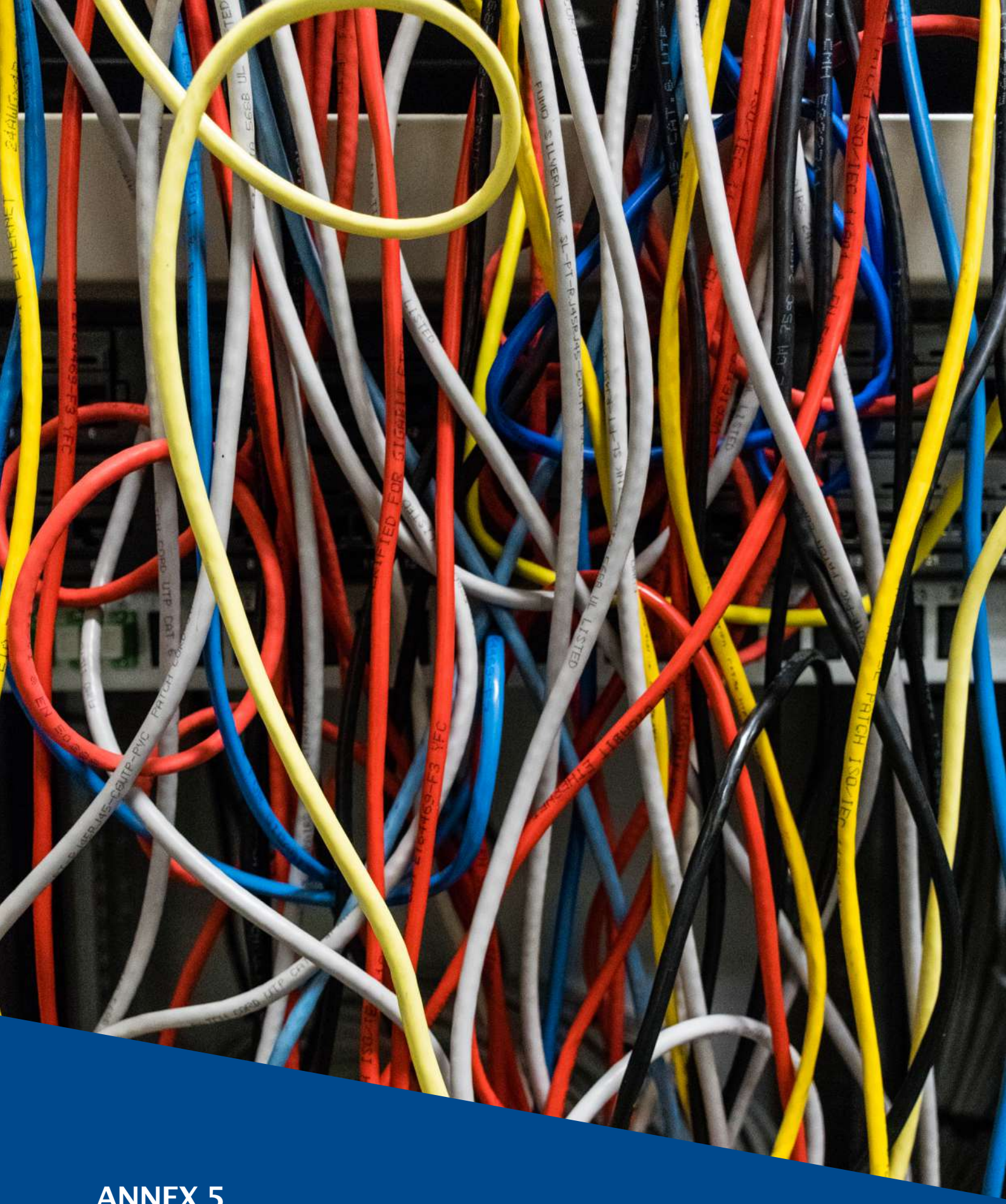
Control Responsibility:

Prevents the use of digital units by parties other than those entitled	Codable in the Smart Contract	Transferability of the token allowed only between identified parties
Ensures operational continuity and restoration of activity, through adequate mechanisms and procedures that also include the external information security	No	
Ensures that the total number of digital units that constitutes a single issuance cannot be modified	Codable in the Smart Contract	The immutability must be guaranteed against external interventions on the DLT and not with respect to variations related to the nature of the Fund
Ensures compliance with anti-money laundering provisions contained in the legislative decree of November 21, 2007, n. 231	Codable in the Smart Contract	The Smart Contract can be of assistance in carrying out anti-money laundering obligations

Information flows:

Requests the subscription/ redemption of the Fund units directly or through a Distributor intermediary acting on behalf of one or more clients	Partial	On-chain notarization hash + off-chain publication of the document

Investor Actions	On-Chain Execution	Notes
Requests the subscription/ redemption of the Fund units directly or through a Distributor intermediary acting on behalf of one or more clients	Codable in the Smart Contract	On-chain delegation provided within the Smart Contracts
Requires the prospectus	No	Off-chain
Requires reinvestment of proceeds	Codable in the Smart Contract	Within the Smart Contract, functionalities could be included that provide the possibility for the investor's administrative rights to be exercised through decentralized governance processes. It would indeed be possible to open votes on decisions to be made, in which investors could express their opinion through a verification of token possession representing the units



ANNEX 5
DLT SETTLEMENT METHODS OF ITALIAN DIGITAL FUNDS

The digital issuance of financial instruments together with on-chain settlements, could enable greater transparency, security, and speed in transaction settlement.

The introduction of settlement on a DLT requires the use of tokens representative of the currency or solutions that are integrated with traditional payment systems.

Settlement assets are fundamental for the functioning of market infrastructures as they are used to fulfill payment obligations among participants.

In general, central bank money represents the safest option for the settlement of financial transactions. However, if the adoption of payment solutions through central bank money, even in a tokenized form, is not practical or possible, the choice to use commercial bank money, also in a tokenized form, or electronic money tokens or other assets provided for by the MiCA Regulation for payment purposes must nonetheless take into account the need to minimize and carefully control the credit and liquidity risk associated with the use of other assets different from central bank money. International standards (CPMI-IOSCO Principles[8] for financial market infrastructures (PFMI) and CPMI-IOSCO Guidance on the Application of the PFMI to stable coin arrangements) establish the criteria to be considered to determine when, in the event that the settlement assets are issued by a private entity, the associated credit and liquidity risk can be considered minimized and carefully controlled and consequently the settlement asset in question can constitute an acceptable alternative to central bank money.

1. Central Bank Money

The Eurosystem has recently started an exploratory work on the use of new technologies for the settlement of wholesale financial transactions in central bank money. In particular, on December 13, 2023, the ECB launched a "Call for Expression of Interest", in which it invited stakeholders to participate in Trials and Experiments, that are experiments of settlement (real or fictitious) of financial transactions, using, inter alia, DVP settlement solutions in central bank money of digital assets represented on DLT infrastructure. In particular, participants can choose between three different solutions based on the interoperability between market DLT platforms and new central bank infrastructures, developed by three central banks, namely: the TIPS Hash-Link solution, provided by the Bank of Italy, the Trigger Solution, proposed by the Deutsche Bundesbank, and the Full-DLT interoperability solution, from the Banque de France.

The basic elements of the experiment and the related conditions are available at the link: https://www.bancaditalia.it/media/notizia/call-for-expression-of-interest-bce-su-sperimentazione-utilizzo-di-nuove-tecnologie-per-il-regolamento-delle-transazioni-finanziarie.

8. Liquidity risk is the risk that a counterparty does not have sufficient resources to fulfill its obligations in the expected manner and time, although it may be able to do so in the future. Credit risk, on the other hand, is the risk that a counterparty fails to meet its payment obligations in the expected time or subsequently.

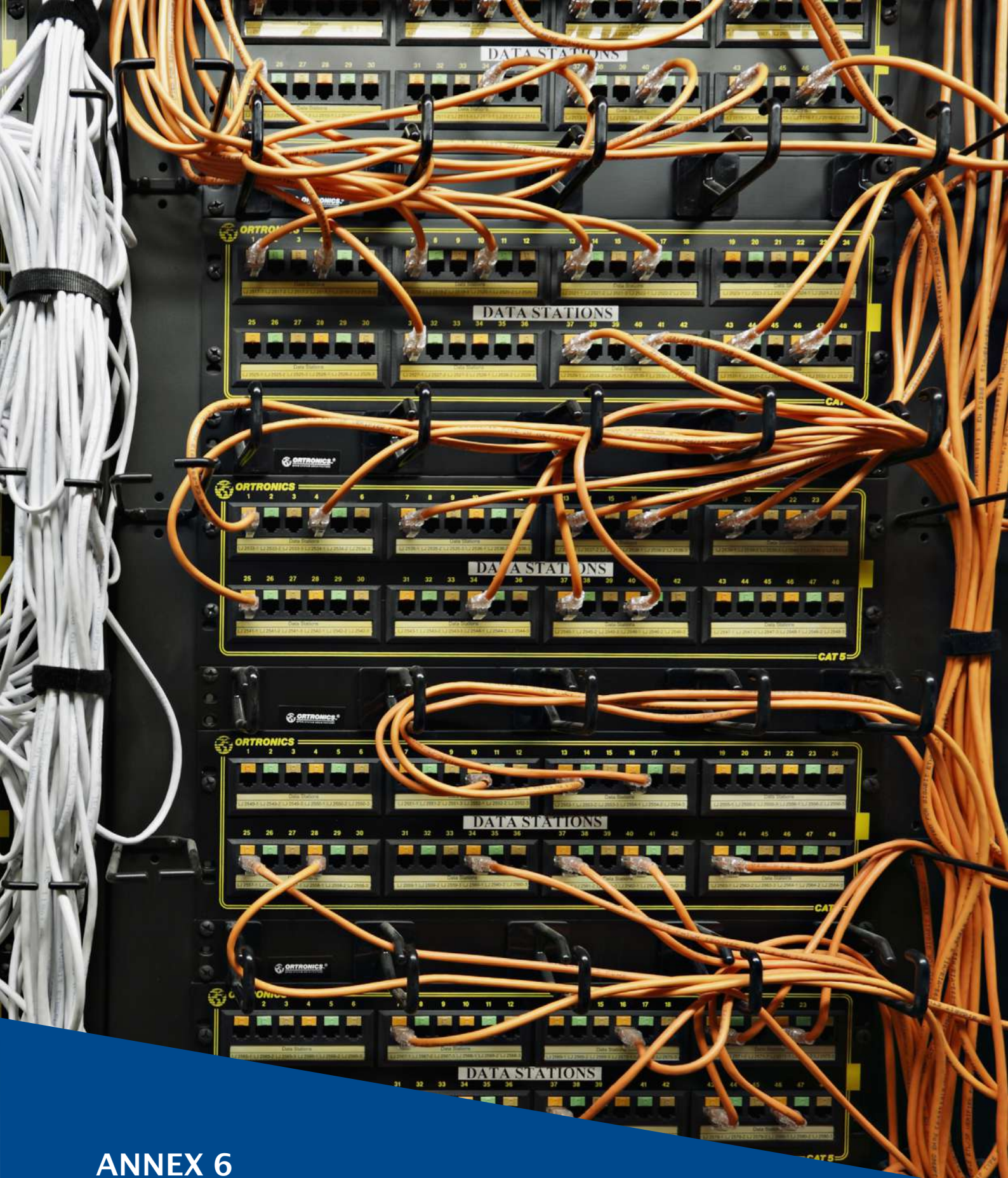
2. E-money tokens and asset-referenced tokens

The MiCA Regulation identifies various types of Crypto-assets that could be used for the settlement of on-chain operations other than central bank money: e-money tokens (EMTs) and asset-referenced tokens (ARTs).

2.1 Electronic money tokens (E-money tokens or EMTs) are a type of Crypto-asset that aim to maintain a stable value by referencing to the value of an official currency. They are considered electronic money (art. 48, par. 2, MiCAR) and are consequently to be considered included in the notion of funds (art. 3, par. 1, n. 14, MiCAR). Their function is "very similar" to electronic money. In fact, like electronic money, e-money tokens are electronic surrogates for coins and banknotes and are "likely" to be used for making payments (recital 18). E-money tokens: (i) are private payment instruments, whose issuance is reserved to authorized private financial institutions (Banks, IMEL); (ii) are issued at par value and on the receipt of funds; (iii) the redemption at par value shall be ensured; (iv) the issuers (and also the Crypto-asset service providers) shall not grant interest or other benefits for the time of holding of such instruments; (v) the issuers are obliged to segregate part of the funds received for the issuance of e-money tokens to grant their refund; (vi) the underlying reference (value represented by the token) is an official currency (legal tender), to whose unit of account the EMTs refer. They have been included in the ECB oversight action (PISA framework).

2.2 Activity-Related Tokens (ARTs) are a type of Crypto-asset that is not an electronic money token and aims to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies. ART issuers can be credit institutions or entities previously authorized by the competent authority of their home Member State. In order to prevent potential negative impacts (monetary substitution effects) linked to the widespread dissemination of ARTs as means of exchange, the MiCA Regulation provides: (i) an ongoing monitoring regime, with quarterly data transmission to the competent authority of transactions associated to the use of Art as a means of exchange (ii) if the average number and the average aggregate value of estimated daily transactions associated with the use of ART as a means of exchange are respectively higher than one million transactions and 200,000,000 euros, a stop to issuances and the submission of a plan to the competent authority to get back "below threshold".

The choice of using electronic money tokens or asset-referenced tokens as a means of exchange for subscription and redemption operations of fund units or units requires careful assessment, also taking into account the following aspects: (i) unlike EMTs, ARTs can only be used as means of payment within certain thresholds and are subject to monitoring by the competent authority (see Art. 22-23 MiCAR); (ii) at the moment, it is not known how the Authorities evaluate the admissibility of the two crypto-assets, EMT and ART, as a settlement cash leg for the subscription of fund units.



ANNEX 6
SAMPLE PROCESS OF DLT SUBSCRIPTION AND REDEMPTION OF ITALIAN DIGITAL FUNDS AND INITIAL ASSESSMENTS[9]

The following processes describe possible ways to subscribe and redeem "on-chain" units of an Italian open-ended DLT fund, in a non-exhaustive and merely indicative way, assuming that (i) subscription and redemption transactions are carried out through the Distributor (so-called partially intermediated model); (ii) the calculation of the fund NAV and the management of subscription and redemption processes are outsourced by the Fund Manager to a third party (Depositary), according to the model that is prevalent in the Italian market today.

The processes are distinguished depending on the settlement method used: settlement in central bank money (wholesale), on one hand, and in e-money tokens/ asset-referenced tokens, on the other.

To enable fund units' subscription and redemption operations, the following preliminary steps are envisaged:

- The Fund Manager decides whether to (i) issue units on a Register held by a specialized entity enrolled in section 4 of the List held by Consob or by an entity registered in section 1 of the List held by Consob, or to (ii) carry out the activity of the Responsible of the Register with reference to the units of its own Italian DLT Funds (after registration in section II of the List held by Consob), possibly using Other Operators for the services/activities provision;
- The Responsible of the Register identifies the technological infrastructure (DLT) and the solutions to issue and manage the digital units of the Fund (so-called Tokenization Platform);
- The Fund Manager identifies the payment methods that can be used for on-chain subscription and redemption operations of the Fund digital units[10];
- The Fund Manager instructs the Key Custody Provider (KCP) to create the Fund Wallet, registered to the Manager himself and to the specific Fund;
- The Fund Manager instructs the Responsible of the Register to create the Fund Smart Contract, taking into account the characteristics of the specific product and the suggestions in Annex 4;
- The Distributor instructs the Key Custody Provider to create the investor's Wallet (so-called wallet of the position)[11].

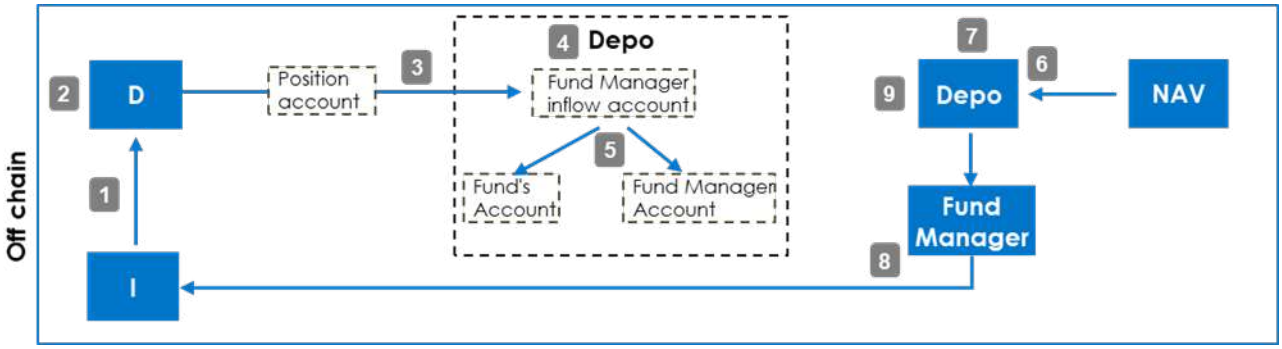
After these preliminary activities, the Distributor and the Fund Manager will have their Wallets on the DLT where the digital units of the Fund will be issued and managed (through Smart Contracts), through which the "ownership" of the Fund units can be managed.

9. The following processes represent a sample model that can be used as a starting point to be modified or updated on the basis of the specific needs of individual operators and of the chosen models, for example with regard to the choices of asset allocation among the different actors in the chain or the adoption of specific technological solutions.
10. For the purpose of identifying the viable payment methods, it should be remembered that for on-chain regulation in central bank currency the relevant entity must be eligible for access to Target services.
11. The sample process presented below considers the segregated solution, where the Distributor manages a wallet for each individual Investor.

1. Sample process of DLT subscription and redemption of Italian Digital Funds

1.1 "As is" subscription and redemption process of Italian Fund units

"As is" subscription process of Italian Fund units[12]



Value date: T+0

1. The Investor sends to the Distributor the order to subscribe to the Fund units.
2. The Distributor, before subscribing the Fund units on behalf of the Investor, carries out the identification process, KYC and AML of the Investor, the executor, and the beneficial owner off-chain. This is done in order to ensure the correct acquisition of the necessary information that will then be recorded on-chain in the Register. The obligations incumbent on the entities impacted by the anti-money laundering discipline do not change.
3. The Distributor transfers the order amount from the position account to the Fund Manager's inflow account (EoD).

Value date: T+1

4. The Depositary[13] carries out Transfer Agency checks (e.g., Minimum purchase lot, subscription days, etc.)
5. The Depositary applies fixed rights to the gross amount. The gross amount, net of fixed rights, is transferred from the Fund Manager's inflow account to the Fund Account (NAV Date). The subscription unit corresponding to fees/fixed rights is credited to the Fund Manager's Account (fees).

Value date: T+2

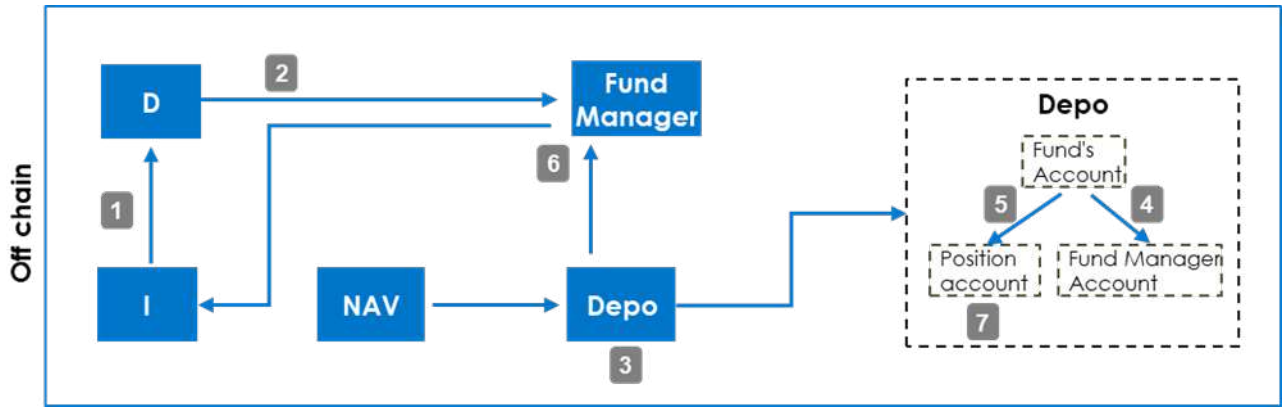
6. The Depositary calculates the value of the fund units based on the Fund NAV.
7. The Depositary validates the issuance of certificates (registered or bearer) or, if the Investor does not request physical delivery, updates the cumulative certificate.

Value date: T+3

8. The Depositary informs the Fund Manager of the execution of the order, who sends the confirmation letter to the investor to confirm the execution of the order.
9. The Depositary carries out ex post checks (e.g., checks on issued units and cash movements).

12. The timing of checks execution can vary based on the specific operations of individual actors. This representation does not consider the specificities of individual operational models.
13. In the represented model, the Depositary also plays the role of TA.

"As is" process of redemption of units of Italian Funds



Value date: T+0

1. The Investor sends to the Distributor the order to redeem a number of Fund' units.

Value date: T+1

2. The Distributor sends on behalf of the Investor the order for redemption (in number of units) to the Fund Manager.

Value date: T+2

3. The Depositary, once the checks have been completed successfully and having calculated the NAV, calculates the units value and the gross redemption value. Subsequently, it calculates the amount of applicable taxes and determines the net redemption value.

Value date: T+3

4. The Depositary applies the amount of taxes to the gross amount. The pro rata share of the redemption amount corresponding to the applicable taxes is credited to the Fund Manager's Account.
5. The Depositary performs the payment in favor of the Investor in accordance with the provisions set by the Fund rules.
6. The Depositary informs the Fund Manager of the successful execution of the order, who then sends a confirmation letter to the investor to confirm the execution of the order.

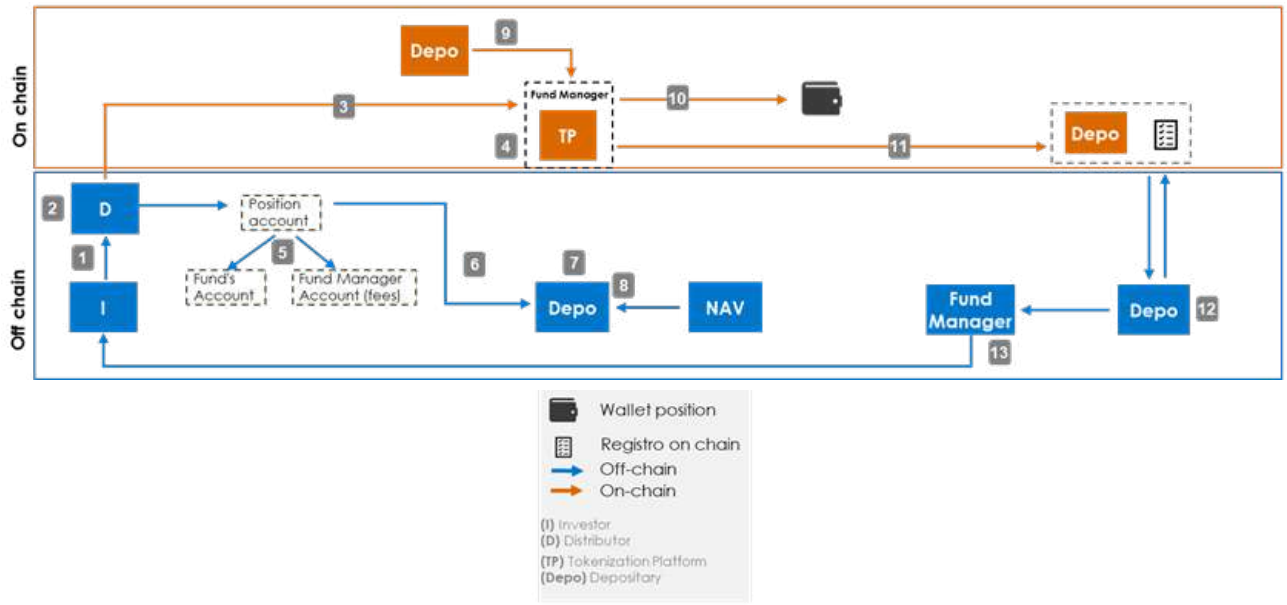
Value date: T+4

7. The net redemption value is made available in the Investor's account.

14. For illustrative simplicity, this process does not illustrate the case in which the investor sends the redemption order directly to the Manager.

1.2 Process of subscription and redemption of Italian DLT Funds units with settlement in central bank money

Process of subscription of Italian DLT Funds units with settlement in central bank money



Value Date: T+0

1. The Investor sends to the Distributor the order to subscribe units of the Italian DLT Fund.
2. Before subscribing the units of the Italian DLT Fund on behalf of the Investor, the Distributor performs off-chain the process of identification and KYC and AML of the Investor, the executor and the beneficial owner, in order to ensure the correct acquisition of the necessary information that will then be recorded on-chain on the Register. The obligations of the entities impacted by the anti-money laundering discipline do not change.
3. The Distributor, on behalf of the Investor, sends the subscription order, through the Tokenization Platform, to the Fund Manager.
4. The checks provided for the validity of the order are carried out through the Tokenization Platform.
5. The Distributor transfers the liquidity from the position account to: a) the Fund account for the net amount of the commissions; b) the Fund Manager's account for commissions.
6. The Distributor informs the Depositary of the cash transfer.
7. The Depositary carries out off-chain checks not performed by the logic embedded in the Smart Contract.

Value Date: T+1

8. Once the off-chain checks have been successfully completed, the Depositary calculates the value of the Fund units based on the NAV.
9. The Depositary authorizes the issuance of units via the Fund Smart Contract.
10. The Fund units are issued and attributed to the Wallet of the position.

11. All transactions are recorded on the blockchain that maintains an unchangeable and traceable registry of the Fund activities, taking into account what is stated in Guideline no. 13.

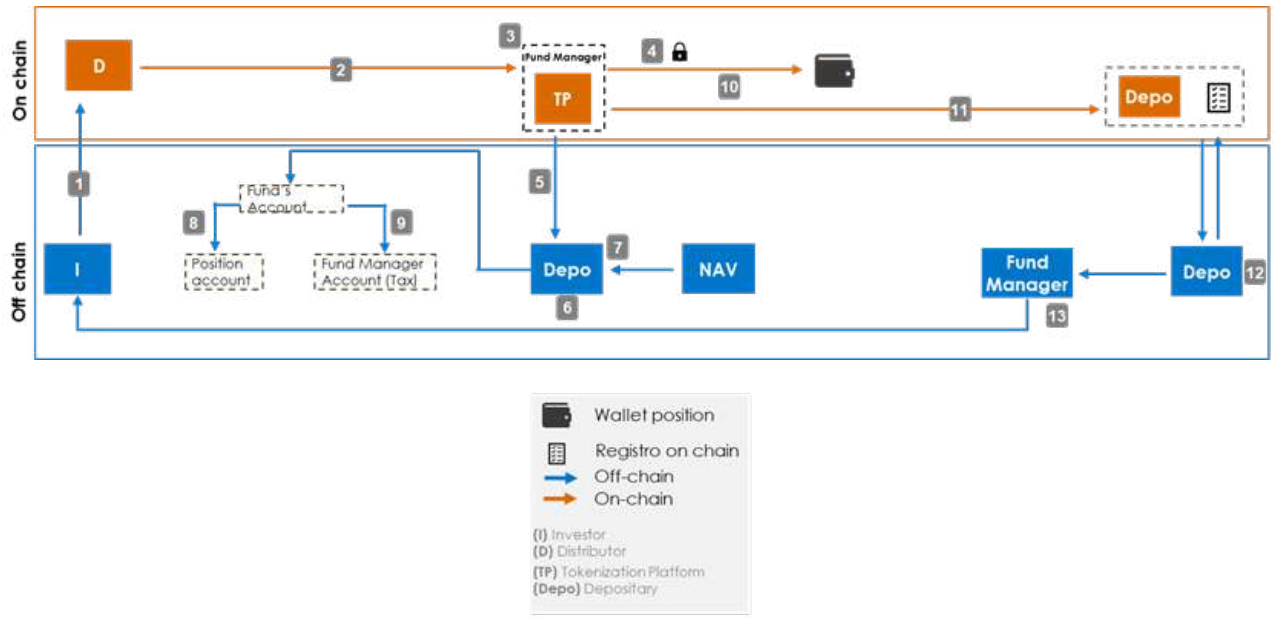
Ex-post

12. The Depositary conducts ex post checks (e.g., checks on digital units).

13. The Depositary informs the Fund Manager of the successful execution of the order, who then sends a confirmation letter to the investor to confirm the execution of the order.

Please note that the indicated timings are subject to change based on the settlement cut offs of central bank money payment operations.

Redemption process of Italian DLT Funds digital units with settlement in central bank money



Value Date T+0

1. The Investor sends the Distributor the order to redeem the number of the Fund's units.

2. The Distributor, on behalf of the Investor, sends the redemption order (in number of units) to the Fund Manager.

3. The Fund's Smart Contract performs the expected checks on the validity of the order. Among these, there may be some checks that concern, for example, the balance capacity, etc.

4. The Fund Manager binds the digital units on the Wallet of the position through the Tokenization Platform, interacting with the specific function of the Smart Contract.

5. The Fund Manager communicates to the Depositary the approval of the redemption order.

6. The Depositary carries out the off-chain checks not performed by the logic embedded in the Smart Contract.

Value Date T+1

7. The Depositary, once the off-chain controls are successfully completed and the NAV is calculated, calculates the value of the Fund units and the gross redemption value. Subsequently, it performs off-chain the calculation of the amount of applicable taxes and determines the net redemption value

Value Date T+1/T+2

8. The Depositary carries out the transfer of cash from the Fund account to the position account, in relation to the part to be reimbursed.

9. The Depositary carries out the transfer of cash from the Fund account to the Fund Manager's account, for the part related to taxes.

10. At the same time, the Fund Manager, having received the input from the Depositary, carries out the burning of the digital units through the Tokenization Platform, interacting with the corresponding function of the Smart Contract.

11. All transactions are recorded on the blockchain which maintains an immutable and traceable register of the activities related to the Fund taking into account what is reported in Guideline no. 13.

Ex-post

12. The Depositary carries out ex post checks (e.g., checks on reimbursed units, liquidity).

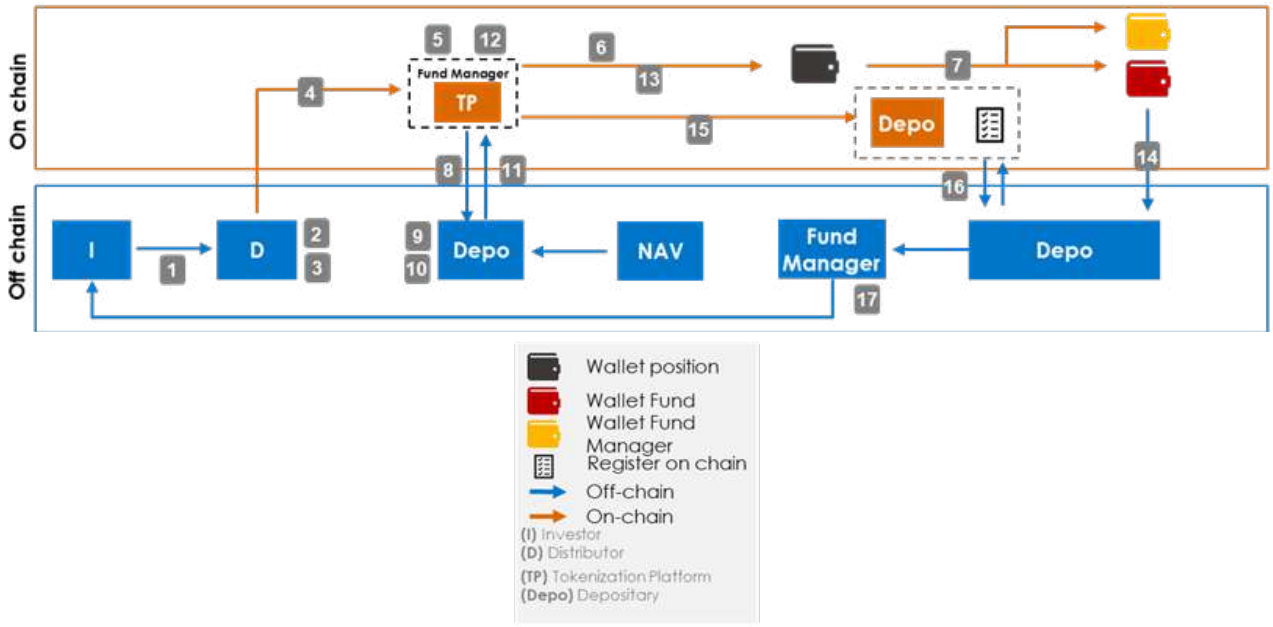
13. The Depositary informs the Fund Manager of the successful execution of the order, who sends the confirmation letter to the investor to confirm the execution of the order.

Please note that:

- the conclusion of the redemption process at T+1 or T+2 is affected by operational constraints related to the need to establish the necessary liquidity in order to process the redemption;
- the indicated timelines are subject to changes based on the settlement cut offs of central bank money payment operations.

1.3 Subscription and redemption process of Italian DLT Fund units with electronic money tokens/ asset-referenced tokens[15]

Subscription process of Italian DLT Fund units with electronic money tokens/ tokens linked to activities



Value Date: T+0

1. The Investor sends to the Distributor the order to subscribe Italian DLT Fund units.
2. Before subscribing the Italian DLT Fund units on behalf of the Investor, the Distributor carries out the off-chain identification process and KYC and AML of the Investor, the executor and the beneficial owner, in order to ensure the correct acquisition of the necessary information that will then be recorded on-chain on the Register. The obligations incumbent on the entities impacted by the anti-money laundering discipline do not change.
3. The Distributor requests the conversion from fiat Euro (from the Investor's current account) to electronic money tokens.
4. The Distributor sends the subscription order on behalf of the Investor to the Fund Manager.
5. The Smart Contract of the Fund carries out the required checks on the validity of the order. Among these, there may be some checks related, for example, to the minimum purchase lot, the subscription days, etc.
6. The Fund Manager authorizes, through the Tokenization Platform, the order and the transfer of the electronic money token from the position Wallet to the Fund Wallet.
7. The electronic money token is transferred from the Position Wallet to: a) Fund Wallet for the net amount of the fees; b) Fund Manager Wallet, for the fees. The electronic money tokens remain bound in such Wallets.
8. The Fund Manager communicates to the Depositary the approval of the subscription order.
9. The Depositary performs the off chain checks not carried out by the logic embedded in the Smart Contract.

15. In the following examples, for brevity, only electronic money tokens are referred to.

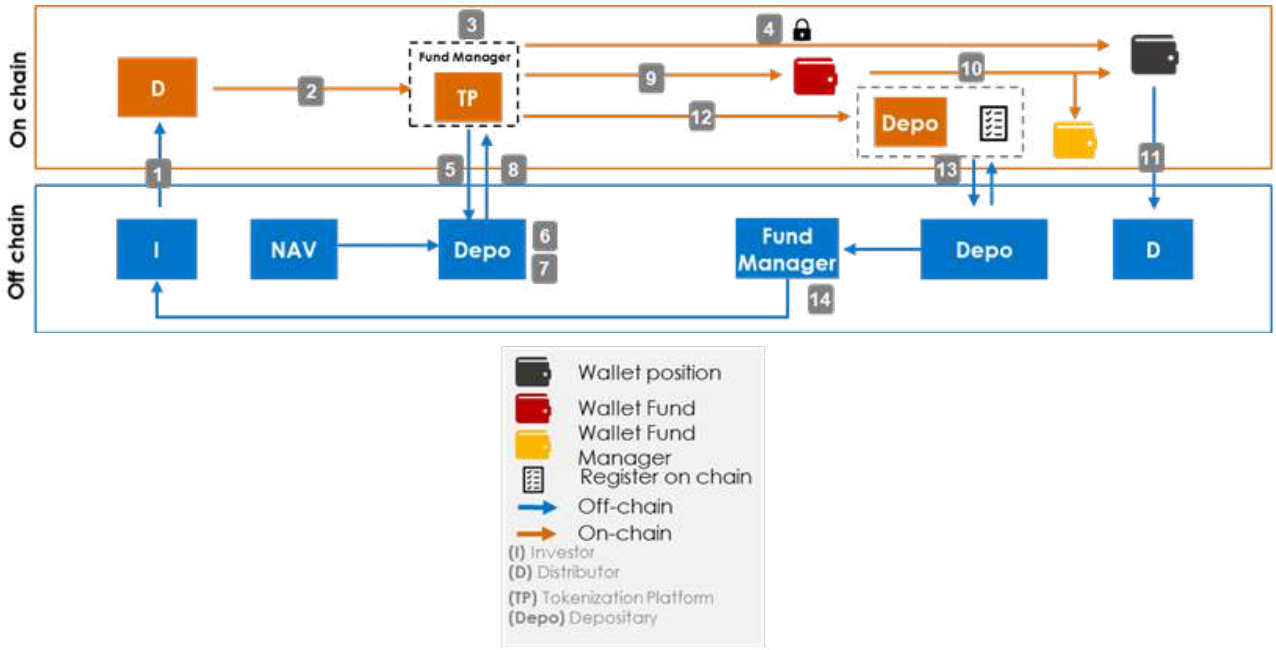
Value Date: T+1

10. The Depositary, once the off-chain checks have been completed with a positive outcome, directly calculates the value of the Fund' units based on the NAV.
11. The Depositary requests the release of the electronic money tokens and the issuance of digital units (indicating the number) to the Fund Manager.
12. The Fund Manager, through the Tokenization Platform, having received the input from the Depositary, unlocks the electronic money tokens and issues the digital units.
13. The issued digital units are credited to the Wallet of the position.
14. The electronic money tokens can be redeemed in fiat Euro by the Tokenization Platform at the request of the issuing entity and credited to the current account of the Fund held by the Depositary.
15. All transactions are recorded on the blockchain that maintains an unchangeable and traceable record of the activities related to the Fund, taking into account what is stated in Guideline No. 13.

Ex-post

16. The Depositary carries out ex-post checks (e.g. checks on issued units, fiat Euro and electronic money tokens).
17. The Depositary informs the Fund Manager of the successful execution of the order, who sends the confirmation letter to the investor to confirm the execution of the order.

Redemption process of digital units of Italian DLT Funds with settlement in electronic money tokens / asset-referenced tokens



Value Date T+0

1. The Investor sends the Distributor the order to redeem the number of Fund units.
2. The Distributor, on behalf of the Investor, sends the redemption order (in number of units) to the Fund Manager through the Tokenization Platform.

3. The Smart Contract of the Fund carries out the expected checks on the validity of the order. Among these, there may be some checks that concern, for example, the balance capacity, etc.
4. The Fund Manager pre-authorizes the order and binds the digital units on the Wallet of the position through the Tokenization Platform, interacting with the specific function of the Smart Contract.
5. The Fund Manager communicates to the Depositary the approval of the redemption order.
6. The Depositary performs the off-chain checks not carried out by the logics inherent in the Smart Contract.

Value Date T+1

7. The Depositary, once the off-chain checks have been completed with a positive outcome and having calculated the NAV, calculates the value of the units and the gross redemption value. Subsequently, it performs off-chain the calculation of the amount of applicable taxes and calculates the net redemption value.

Value Date T+1/T+2

8. The Depositary requests the redemption of the units (indicating their equivalent in electronic money tokens) to the Fund Manager through the Tokenization Platform.
9. The Fund Manager, through the Tokenization Platform, having received the input from the Depositary, interacting with the specific function of the Smart Contract, carries out the burning of the digital units and unlocks the transfer of the electronic money tokens from the Fund's Wallet.
10. Electronic currency tokens are transferred from the Fund's Wallet to: a) the position Wallet, relative to the part to be reimbursed; b) Fund Manager's Wallet for taxation.
11. Euro fiat can be redeemed from the Tokenization Platform, at the request of the issuing entity and credited to the position account held with the Distributor.
12. All transactions are recorded on the blockchain that maintains an unchangeable and traceable record of activities related to the Fund, taking into account what is reported in Guideline no. 13.

Ex-post

13. The Depositary carries out ex post checks (e.g. checks on redeeemed units, Euro fiat and electronic money tokens).
14. The Depositary informs the Fund Manager of the completion of the order, who sends the confirmation letter to the investor to confirm the execution of the order.

Please note that the conclusion of the redemption process at T+1 or at T+2 is affected by operational constraints related to the need to constitute the liquidity necessary for the refund process.

2. Some initial assessments

2.1 General benefits of fund units tokenization

Benefits related to the Subscription process:

- Shortening of the transaction settlement cycle with availability of units to the subscriber in advance compared to the as-is process due to the automatic crediting of digital units in the

position Wallet. Specifically, the Fund Manager through the Tokenization Platform issues the digital units and assigns them to the position Wallet, where the units are immediately available to the Investor as soon as they are evaluated. This represents an advantage over the current model where units are made available the day after their evaluation.

- Credit of cash in the Fund Wallet in T0 with an improvement compared to the as-is process, for orders placed within the cut off. The introduction of Wallets for the management of electronic money tokens allows the immediate transfer from the position Wallet to the Fund Wallet, without the need to carry out the transfer through a transitional account, as in the case of the inflow account of the Fund Manager used in the traditional process.
- Certainty of the unit value (time to market) in advance compared to the as-is process, for orders placed within the cut off time. As described in the previous point, the amount intended for subscription is credited to the Fund Wallet (to be then constrained) in T0, making it possible to take the T0 NAV date as reference.

Benefits related to the Redemption process:

- Enabling of DvP through the burning of units simultaneous to the transfer of electronic money tokens.
- Reduction of the transaction settlement cycle with availability for the investor of cash in advance compared to the as-is process.
- Certainty of the unit value (time to market) concurrent with the sending of the order (for orders placed within the cut off) in advance compared to the as-is process.

Other benefits:

- Execution of on-chain checks: reduction of the perimeter of checks performed off-chain, by moving them on-chain (eg. in case of operation rejection, the immediacy of the return of funds to the investor and possible timely remedial action).

- The Registry of subscribers is on-chain and is updated automatically and contextually with the completion of order execution, potentially reducing the management costs of the Registry of subscribers compared to legacy systems.

2.2 Further considerations

- With reference to closed-ended funds, the initial subscription process could fully benefit from the opportunities of the DvP. In this specific case, indeed, the initial subscription and the confirmation of the number of subscribed units is not subject to issues relating to NAV calculation and unit valuation – which represent an off-chain constraint to the simultaneity of transactions.
- In the case of the establishment of Italian Digital Funds (namely, Funds that invest in Digital assets and at the same time issue digital fund units), a series of potential advantages could be obtained, including:

  a. the process for calculating the NAV could be made more efficient;

  b. the enablement of additional services (e.g. staking) through a modality which reduces price point, fees, and operational complexity;

  c. lower costs on the Fund, as the costs of managing control flows and data processing, delegated to DLT, are reduced.

ANNEX 7
GUIDELINES ON ITALIAN DIGITAL FUNDS DISCLOSURE FOR INVESTORS

In the Disclosure for Investors, it is necessary to include considerations on the technology underlying the Italian Digital Funds, also highlighting the emerging associated risks. Hereafters are some indicative and non-exhaustive guidelines on the information that should be disclosed to the Investor, taking into account the considered investor target.

What is Distributed Ledger Technology?

Distributed Ledger Technology is a technology that allows the recording and storage of data in specific distributed databases, where it is only possible to add information (append-only) according to shared rules. To achieve consensus on a single version of the unalterable ledger, in the absence of trust and of a central entity, cryptography is used and consensus algorithms are employed.

What is a Blockchain?

A Blockchain is a particular type of DLT whose name derives from the structure of the ledger, namely a data structure that contains a sequence of transactions usually grouped in chained blocks. The transactions to be included and their order in the block are established through a consensus mechanism to which anyone can participate (permissionless platforms) or only subjects who have satisfied certain access conditions (permissioned platforms), and which typically relies on economic incentives and disincentives, implemented through assets accounted for in the Blockchain itself.

What are the technological risks of an Italian DLT Fund?

The distributed ledger technology underlying the units of an Italian DLT Fund can involve various risks, including:

Technological risks

i. the possibility of not yet identified technical defects in the DLT, for example in the process through which the transactions are recorded;

ii. the possibility that cryptographic security measures or other security measures that authenticate previous transactions for a DLT may be compromised, or "hacked", which could allow an attacker to alter the DLT and therefore compromise the ability to confirm the recorded transactions;

iii. the possibility that new technologies or services inhibit access to a DLT;

iv. the risk that the nodes participating in the DLT network may be few in number, and this fact may negatively impact the level of decentralization, security and stability of the network itself;

v. the risk of service disruptions, operational anomalies, inefficiencies or vulnerabilities of technologies other than the DLT but instrumental: for the storage of units in DLT and for access to related information or for the exercise of rights attributed by the units (such as, for example, digital access interfaces or communication networks);

vi. risks related to the peculiarities of consensus formation protocols (e.g., proof-of-work or proof-of-stake) that could affect the security, efficiency, and sustainability, including environmental, of the DLT network;

vii. the risk that the technology used to represent units in DLT may change, completely or partially, during the lifecycle of the units, and it may be necessary to transfer them to a new protocol or technology. In particular, the Fund, also due to the maintenance by third parties of the registers in which the DLT units subject to investment are represented, could be exposed to the risk of loss or unavailability of the investment instruments due to cyber-attacks, human errors, failures or other technical disruptions;

viii. the risks related to the fact that DLTs could undergo significant structural and protocol changes over time, with a consequent negative impact on the value of the Fund and the related units;

ix. the risks related to the technical shortcomings or inefficiencies of the DLT used to represent the DLT units can have a negative impact on the value of the Fund units as well as a change in the regulatory framework applicable to DLTs at a national or supranational level;

x. the risks derived from possible sudden changes in the operating rules of blockchain networks, known as "forks" or "splits", which could materially affect services. In particular, in some cases (so-called hard fork), such changes can be so radical as to invalidate previous transactions and blocks, thus posing the risk of losses of the subscriber's units or actions to the subscriber.

What are the risks associated with investing in an Italian Crypto Fund?

The Italian Crypto Fund may invest in DLT Financial Instruments and MiCAR Crypto assets (Digital Assets).

DLT Financial Instruments are financial instruments issued on a distributed ledger for digital circulation, including the digital financial instruments referred to in Article 1, paragraph 1, letter c) of the Fintech Decree.

MiCAR Crypto Assets are crypto-assets, other than DLT Financial Instruments, falling within the scope of the Regulation (EU) 2023/1114 (Markets in Crypto-assets Regulation – MiCAR).

Investing in DLT Financial Instruments and MiCAR Crypto-assets is subject to technological risk arising from the use of distributed ledger technologies (see above). In particular, a Fund that invests in Digital Assets may be exposed to technological concentration risk if most of the Digital Assets in which the fund is invested are based on a specific protocol or technology.

Investment in MiCAR Crypto-assets, although they are regulated assets, presents the following additional risks:

i. extreme price movements: many Crypto-assets are subject to sudden and extreme price movements and are speculative because their price often depends solely on consumer demand (for example, there may be no hedging activities or another tangible value). You could lose a huge amount of or even all the money invested. Extreme price movements also mean that many Crypto-assets are not suitable as a store of value and as a means of exchange or payment.

ii. products complexity: some products that provide exposure to Crypto-assets are very complex, sometimes with features that can increase the magnitude of losses in case of unfavorable price developments. These products, given their complexity, are not suitable for many consumers.

Warning: Several issuers and Crypto-assets service providers, including Crypto-asset exchanges and wallet providers, have suffered cyber-attacks and serious operational issues. Many consumers have lost their Crypto-assets or suffered losses both due to these breaches and disruptions and because they lost the private keys that provide access to their assets.

Bibliography

Alternative Investment Management Association (2022), Digital Asset Custody an AIMA Industry Guide

Association of National Numbering Agencies and DTI Foundation (2023), ISIN-DTI Guide

Association of National Numbering Agencies (2023), Isin Uniform Guidelines Relating To ISO 6166 (8th edition)

Assogestioni (2023), Beyond Cryptocurrencies. Distributed ledger technologies for asset management

Bank of Italy, Università Cattolica del Sacro Cuore, Università Roma Tre (2023), Caratteristiche degli Smart Contract, Consultation Document

Bank of Italy (2023), Audizione sul disegno di legge n. 605 di conversione in legge del decreto-legge 17 marzo 2023, n. 25, recante disposizioni urgenti in materia di emissioni e circolazione di determinati strumenti finanziari in forma digitale e di semplificazione della sperimentazione FinTech Intervento di Piero Cipollone

Bank of Italy (2022), Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e Cripto-attività, Rome

Basel Committee on Banking Supervision (2023) Consultative Document Cryptoasset standard amendments

Basel Committee on Banking Supervision (2023), Consultative Document Disclosure of cryptoasset

exposures

Basel Committee on Banking Supervision (2022), Prudential treatment of cryptoasset exposures

Bassan F. and Rabitti M. (2023), "Recenti evoluzioni dei contratti sulla blockchain. Dagli smart legal contracts ai "contracts on chain", Rivista di Diritto Bancario, 561

BIS, Bank for International Settlements (2023), The crypto ecosystem: key elements and risks Report submitted to the G20 Finance Ministers and Central Bank Governors

BIS-IOSCO (2022), Principles for Financial Market Infrastructures

BIS-IOSCO (2022), Application of the Principles for Financial Market Infrastructures to stablecoin arrangements

BVI (2022), Kryptoleitfaden

Calastone (2023), Whitepaper - Practically Applying Tokenisation in Asset Management

Carriere P., De Luca N., De Mari M., Gasparri G., Poli T.N. (2023), Tokenizzazione di azioni e azioni token, Quaderni Giuridici Consob, n. 25

Central Bank of Ireland (2023), AIFMD Questions and Answers

Ciocca N. (2022), Servizi di custodia, negoziazione e regolamento di cripto-attività, in Oss. dir. civ. comm., 79

Ciraolo F. (2022), La disciplina degli e-money tokens tra proposta di Regolamento MiCA e normativa sui servizi di pagamento. Problematiche regolatorie e possibili soluzioni, in Riv. reg. mer., 239

Commission de Surveillance du Secteur Financier (2022), FAQ Virtual Assets – Undertakings for Collective Investment

Commission de Surveillance du Secteur Financier (2022), FAQ Virtual Assets – Credit Institutions

Commission de Surveillance du Secteur Financier (2022), White Paper "Distributed Ledger Technologies & Blockchain_Technological risks and recommendations for the financial sector"

Commission de Surveillance du Secteur Financier (2022), FAQ – Authorisation and organisation of entities acting as UCI administrator

CONSOB (2023), Audizione presso la 6ª Commissione (Finanze e tesoro) del Senato della Repubblica, del Responsabile dell'Ufficio Post Trading, Dott. Salvatore Giovanni Lo Giudice, nell'ambito dell'esame dell'A.S. n. 605 recante "conversione in legge del decreto-legge 17 marzo 2023, n. 25, recante disposizioni urgenti in materia di emissioni e circolazione di determinati strumenti finanziari in forma digitale e di semplificazione della sperimentazione FinTech"

CryptoCurrency Security Standard (CCSS)- Version 8.1

Deloitte (2018), Impacts of the blockchain in fund distribution.

Deloitte Middle East and the Dubai Financial Services Authority (DFSA) (2020), A Market Overview of Custody for Digital Assets Digital Depositary Whitepaper

EBA, European Banking Authority (2024), Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849- (EBA/GL/2024/0)

EPRS, European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 634.445 – (2019) - Blockchain and the General Data Protection Regulation

ESMA, European Securities and Markets Authority (2024), Consultation paper On the draft Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments – (ESMA75-453128700-52)

ESMA, European Securities and Markets Authority (2023), Question & Answer on application of AIFMD- (ESMA34-32-352)

ESMA, European Securities and Markets Authority (2023), "Decentralised Finance: A categorisation of smart contracts". TRV Risk Analysis

n Securities and Markets Authority (2023), "Decentralised Finance in the EU: Developments and risks". TRV Risk Analysis

ESMA, European Securities and Markets Authority (2022), "Crypto-assets and their risks for financial stability". TRV Risk Analysis

ESMA, European Securities and Markets Authority (2019), Advice. Initial Coin Offerings and Crypto-Assets- (ESMA50-157-1391)

ESRB, European Systemic Risk Board (2023). "Crypto-assets and decentralised finance: Systemic implications and policy options"

European Parliament Research Institute (2019), Blockchain and the General Data Protection Regulation

FSB, Financial Stability Board (2023), High-level Recommendations for the Regulation, Supervision and Oversight of Crypto Assets and Markets Final report

Frank Dornseifer (2022), The Use of DLT in the Asset Management Sector – Assets, Infrastructure and Regulation in Transition

Genovese A. (2023), La circolazione dei valori mobiliari su blockchain, in Riv. dir. comm., 197

Glaser P. (2020), Melon Protocol: Data Analysis of an On-Chain Asset Management Platform

Global Research Institute (2018), What Distributed Ledgers Means For Asset Management

Gola C., Cappa V., Fiorenza P., Granata P., Laurino F., Lesina L., Lorizzo F., Marcelli G. (2023), La governance delle blockchain e dei sistemi basati sulla tecnologia dei registri distribuiti, Occasional Papers, Bank of Italy

Article 29 data protection working party (2014) - Opinion 05/2014 on anonymization techniques

ISACA - Blockchain Framework and Guidance

IOSCO (December 2023), Policy recommendation for decentralized finance (DeFi)

IOSCO (November 2023), Policy recommendation for crypto and digital asset market final report

La Rocca R., Mancini R., Benedetti M., Caruso M., Cossu S., Galano G., Mancini S., Marcelli G., Martella P., Nardelli M. and Olivie C. (2022), Integrazione della DLT con le infrastrutture di mercato: analisi e proof-of-concept per un DvP sicuro tra TIPS e piattaforme DLT Research Papers, Bank of Italy

Lener R. (2023), Criptoattività e cripto valute alla luce degli ultimi orientamenti comunitari, in Giur. Comm, 376

LhoFT, PWC, ALFI (2023), Crypto-Assets Management Survey 2nd Edition

Luxembourg House of Financial Technology (2022), Luxembourg: The Epicenter of the Tokenization Era White Paper

Italian Ministry of Economy and Finance (2022), Libro Verde sulla competitività dei mercati finanziati italiani a supporto della crescita

Monetary Authority of Singapore and BIS (2023), Project Guardian

Mouton J. (2021),Regulating Smart Contracts in the Domain of Financial Trading, California Western Law Review

OCC (2022) Comptroller's Handbook for Custody Services

OECD (2020) The Tokenisation of Assets and Potential Implications for Financial Markets

OWASP Smart Contract Top 10

Paracampo M.T. (2023) I prestatori di servizi su cripto-attività. Tra mifidizzazione della MICA e tokenizzazione della Mifid, Turin

PWC (2023), Asset and wealth management industry continues to embrace digital assets: What asset managers need to know, available at the following link

Sebastiaan Niels Hooghiemstra (2022), DLT versus Tokenized Fund Units/Shares under Luxembourg Law, Luxembourg Fund Law Update

SEC (2024) –Statement on the approval of spot bitcoin exchange-traded products

SEC (2021) - Staff Statement on Funds Registered Under the Investment Company Act Investing in the Bitcoin Futures Market

SEC (2020) - Staff Statement on WY Division of Banking's "NAL on Custody of Digital Assets and Qualified Depositary Status" - Division of Investment Management Staff in Consultation with FinHub Staff

SEC (2018), Staff Letter: Engaging on Fund Innovation and Cryptocurrency-related Holdings

SEC (2018), Statement on Potentially Unlawful Online Platforms for Trading Digital Assets

Suvvaru Surya Prasadarao, Vijaya Kittu Manda, Prasada Rao S.S. (2018), Blockchain Technology for the Mutual Fund Industry

The European Blockchain Observatory and Forum (2023), Trends Report

The European Union Blockchain Observatory and Forum (2018), Blockchain and the GDPR

The IA (2023), UK Fund tokenization: a blueprint for implementation

Zetzsche D. A., Annunziata F. & Sinnig J. (2023) - Digital Assets, MiCA & EU Investment Fund Law

Zetzsche D.A. - Buckley R. Arner D. – Van Ek M. (2023), Remaining Regulatory Challenges in Digital Finance and Crypto-Assets after MiCA, Committee on Economic and Monetary Affairs (ECON), Paper No. 23-27

Todd Gibson and Tyler Kirk (2016), Blockchain 101 for Asset Managers", The Investment Lawyer Covering Legal and Regulatory Issues of Asset Management

Trinkler R. and El Isa M., (2019) Melon Protocol: a Blockchain Protocol for Digital Asset Management Draft

Who is Assogestioni

Assogestioni is the representative association of the Italian investment management industry. It represents most of the Italian and foreign investment management companies operating in Italy, as well as banks and insurance companies involved in investment management, including pension schemes.

The association's main purpose is to foster the investment management industry in Italy through the establishment of a regulatory and market environment in Italy which is conducive to growth. To achieve these goals, Assogestioni offers to its members advice and technical support on legal, fiscal and operational matters. It also encourages its members, financial and public institutions to debate on themes involving savings, investments, sound corporate governance and regulatory and operational improvements.

Acknowledgments

The realization of these Guidelines was possible thanks, first and foremost, to the members of Assogestioni's Digital Finance Committee (ComDigit) and, in particular, to Giovanni Sandri (BlackRock), Chairman of ComDigit, Edoardo Del Bosco (Generali), Vice Chairman of ComDigit, Roberta D'Apice (Assogestioni) Secretary of ComDigit, as well as Maria Canali De Rossi (Assogestioni), Francesca Sesia (Blackrock), Rossella Cobelli (Eurizon Capital SGR), Marco Basurto (Amundi SGR), Betti Francesco (Anima SGR), Ceretti Riccardo (Arcafondi SGR), Riccardo Veglio (Mediolanum SGR), Michele Quinto (Franklin Templeton).

Special thanks are then due to those who made technical and scientific contributions to the drafting of the Guidelines and, in particular, to Mauro Panebianco, Andrea Laurenti, Stefano Rossi, Alessia Maria Selenia Moia, Francesco Losso, Andrea Castellaneta, Luca Fumagalli (PwC Italy) and, for the Osservatorio Fintech & Insurtech of the Politecnico di Milano, to Marco Giorgino, Laura Grassi, Claudio Garitta and Jacopo Fracassi.

Finally, I would like to thank ABI, ABI Lab, Societe Generale Securities Services and Metier Securities Services BNP Paribas SA – Italian subsidiary for their helpful comments.

Fabio Galli, General Manager, Assogestioni

ASSOGESTIONI

associazione del risparmio gestito