



Comitato Digital Finance Assogestioni



ASSOGESTIONI

associazione del risparmio gestito

FONDI ITALIANI DIGITALI

Linee Guida
Maggio 2024

A cura di **Roberta D'Apice (Assogestioni)**,
con il supporto tecnico e scientifico di PwC Italia e
dell'Osservatorio Fintech & Insurtech del Politecnico di Milano

www.assogestioni.it



AVVERTENZE

Le Linee Guida rappresentano uno strumento di ausilio e supporto per l'istituzione e l'operatività di Fondi Italiani Digitali. Esse, pertanto, non sono né vincolanti né esaustive rispetto alle possibili scelte effettuate dai soggetti operanti nell'ecosistema dei Fondi Italiani Digitali.

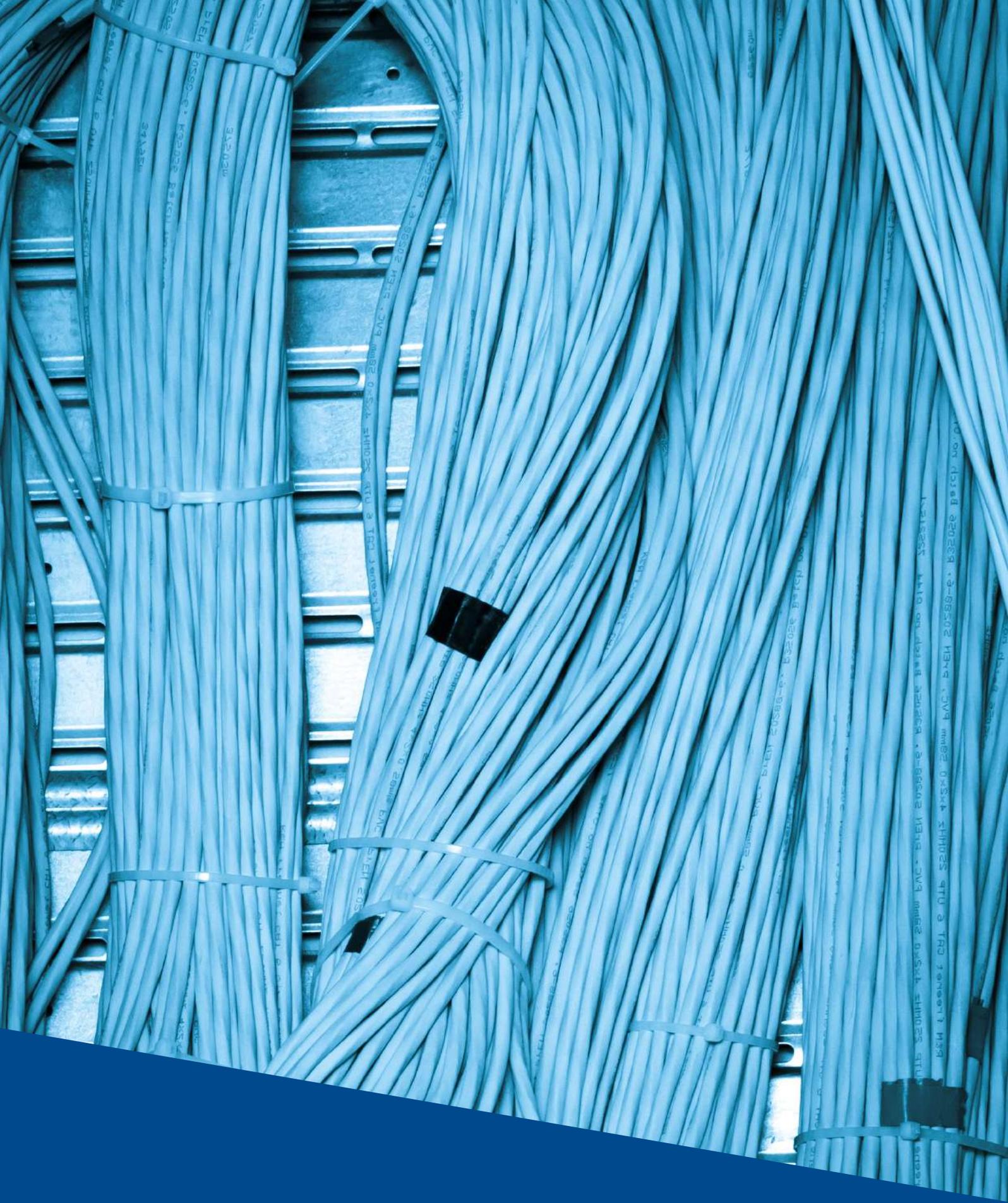
Le Linee Guida non alterano il significato della normativa – legislativa, regolamentare e di livello 3 – vigente in materia, né possono essere interpretate in tal senso. Le Linee Guida non rappresentano la posizione delle Autorità di Vigilanza sulle tematiche trattate, né anticipano o sostituiscono le valutazioni di vigilanza sulle singole iniziative relative ai Fondi Italiani Digitali.

Tutte le immagini sono dell'agenzia Getty Images.

INDICE

INTRODUZIONE	5
Parte I – Ambito di applicazione e Definizioni	10
Linea Guida n. 1 Ambito di applicazione	11
Linea Guida n. 2 Definizioni, riferimenti normativi e orientamenti di vigilanza	11
Linea Guida n. 2.1 Definizioni	11
Linea Guida n. 2.2 Riferimenti normativi e orientamenti di vigilanza	13
Parte II – Presidi generali per l’operatività dei Fondi Italiani Digitali	14
Linea Guida n. 3 Presidi generali per gli Intermediari (Gestori, Depositari, Distributori)	15
Linea Guida n. 4 Presidi in caso di esternalizzazione	16
Linea Guida n. 5 Criteri per la scelta degli “Altri Operatori”	17
Linea Guida n. 6 Operatività on-chain e off-chain dei Fondi Italiani Digitali	17
Linea Guida n. 7 Tutela dei dati personali	18
Parte III – Presidi specifici per l’operatività dei Fondi Italiani Cripto	19
Linea Guida n. 8 Attività d’investimento dei Fondi Italiani Cripto	20
Linea Guida n. 9 Custodia delle Attività digitali del Fondo Italiano Cripto	21
Linea Guida n. 10 Distribuzione di Fondi Italiani Cripto	23
Parte IV – Presidi specifici per l’operatività dei Fondi Italiani DLT	24
Linea Guida n. 11 Emissione di quote di Fondi Italiani DLT	25
Linea Guida n. 12 Gestore di Fondi Italiani DLT	27
Linea Guida n. 13 Responsabile del registro di Fondi Italiani DLT	27
Linea Guida n. 14 Distribuzione di Fondi Italiani DLT	28
Allegato 1 – Principi di valutazione delle Cripto-attività	29
Allegato 2 – Processo di valutazione e gestione dei rischi relativi all’utilizzo della DLT	31
Allegato 3 – Presidi di sicurezza nella gestione degli asset crittografici	36
Allegato 4 – Indicazioni sull’operatività on-chain dei Fondi Italiani Digitali	39

Allegato 5 – Modalità di regolamento on-chain delle operazioni dei Fondi Italiani Digitali	52
1. Moneta di Banca Centrale	53
2. Token di moneta elettronica e token collegati ad attività	54
Allegato 6 – Processo esemplificativo di sottoscrizione e rimborso di quote di Fondi Italiani DLT e prime valutazioni	55
1. Processo esemplificativo di sottoscrizione e rimborso di quote di Fondi Italiani DLT	57
1.1 Processo “as is” di sottoscrizione e rimborso di quote di Fondi Italiani	57
1.2 Processo di sottoscrizione e rimborso di quote di Fondi Italiani DLT con regolamento in moneta di banca centrale	59
1.3 Processo di sottoscrizione e rimborso di quote di Fondi Italiani DLT con token di moneta elettronica/ token collegati ad attività	62
2. Alcune prime valutazioni	64
2.1 Benefici generali della tokenizzazione di quote di fondi	64
2.2 Ulteriori considerazioni	65
Allegato 7 – Indicazioni sull’Informativa per gli Investitori di Fondi Italiani Digitali	66
Bibliografia	69
Chi è Assogestioni	72
Riconoscimenti	73



INTRODUZIONE

La velocità con la quale l'innovazione digitale avanza è sempre molto elevata. I periodi più recenti sono stati peraltro di grande accelerazione. Si è assistito a fenomeni solo difficilmente immaginabili fino qualche tempo fa, come quelli, ad esempio, riferiti allo sviluppo dell'intelligenza artificiale generativa, ma non solo. L'industria finanziaria rappresenta uno degli ambiti di maggiore rilevanza rispetto al potenziale di applicazione della digitalizzazione. Il ruolo centrale che tale industria riveste nel corretto funzionamento dei sistemi economici e sociali è tale da richiedere estrema attenzione, da un lato, ma, al tempo stesso e dall'altro, di comprendere come poter orientare al meglio strategie e comportamenti per valorizzare tutto il beneficio potenziale mitigandone i relativi rischi. Nel nostro paese, questa condizione è molto importante.

Tra i comparti dell'industria finanziaria maggiormente interessati spicca certamente quello del risparmio gestito. L'industria del risparmio gestito è centrale per la competitività. Come ben noto, infatti, l'Italia ha la "materia prima" dell'industria finanziaria, ossia il risparmio, in quantità straordinariamente elevate ed è quindi chiamata a far evolvere tale industria in modo da vedere crescere sempre di più i valori dell'efficienza, della stabilità e della qualità, sempre preservando la tutela del risparmiatore.

Dalla osservazione di come, da un lato, l'evoluzione tecnologica digitale apra nuove frontiere e generi potenzialità mai prima così ampie e pervasive, e di come, dall'altro, il risparmio gestito sia una delle fondamenta dell'industria finanziaria italiana, e attraverso di questa dell'intero sistema economico, emergono due presupposti centrali su cui nascono le Linee Guida sui Fondi Italiani Digitali (Linee Guida), promosse da Assogestioni, in collaborazione con PwC Italia e l'Osservatorio Fintech & Insurtech del Politecnico di Milano. Esse sono il risultato di un lungo percorso partito con l'esplorazione delle possibili implicazioni della digitalizzazione sull'industria del risparmio gestito che ha portato alla identificazione, tra quelli possibili, di due ambiti, in modo particolare, di attenzione. Tali ambiti, dopo una prima fase di studio e sperimentazione che è sfociata a marzo 2023 nella pubblicazione del white paper "Oltre le criptovalute – Tecnologie a registro distribuito a servizio dell'asset management", hanno avuto la possibilità di essere approfonditi con l'ammissione del progetto "DLT e Asset Management: opportunità e sfide per l'industria" alla Call for Proposals 2022 di Milano HUB di Banca d'Italia le cui attività si sono chiuse a fine 2023.

Le Linee Guida sono state definite attraverso un continuo raccordo e confronto con Milano HUB e rappresentano un supporto prezioso per sviluppare la traiettoria di trasformazione digitale degli operatori dell'industria del risparmio gestito in Italia.

Le Linee Guida sono indicazioni a supporto degli operatori, in un quadro che si sta sviluppando, sia a livello europeo sia a livello nazionale, per meglio delineare quale sia il playing field di riferimento. I regolamenti e le normative sui Cripto-attività (MiCAR), quelli sulla resilienza operativa digitale (DORA) o quelli in materia di emissioni e circolazione di strumenti finanziari digitalizzati (DLT Pilot Regime e, specificamente per l'Italia, il Decreto Fintech) nonché gli Standard del Comitato di Basilea sul trattamento prudenziale per le esposizioni delle banche in cripto-attività, sono solo alcuni degli esempi che ci dicono che non ci sono più "alibi". Il "campo di gioco", pur non essendo completamente definito, è delineato per favorire lo sviluppo tecnologico a servizio dell'industria finanziaria.

Le Linee Guida non hanno natura vincolante né possono essere considerate esaustive. Hanno, però, l'obiettivo di fornire un punto di riferimento che quanto più verrà condiviso tanto più porterà all'affermazione di standard alla base di una veloce diffusione dell'innovazione.

È altrettanto importante sottolineare come tali indicazioni non alterino il significato della normativa vigente in materia, né possono essere interpretate in tal senso. Esse, quindi, non rappresentano la posizione delle Autorità di Vigilanza sulle tematiche trattate, né anticipano o sostituiscono le valutazioni di vigilanza sulle singole iniziative in questo ambito.

Le Linee Guida intervengono per favorire un adeguato sviluppo degli investimenti in strumenti finanziari DLT e in Cripto-attività incluse nell'ambito di applicazione della MiCAR; dall'altro, esse hanno l'obiettivo di accompagnare in modo ordinato l'evoluzione degli organismi di investimento collettivo del risparmio italiani le cui quote o azioni sono emesse – e quindi sono native digitali¹ – su un registro distribuito per la circolazione digitale. Su questo sfondo di un quadro istituzionale e regolamentare che si va a comporre – ma neanche tanto lontano – vi è poi la traiettoria delle valute digitali di banca centrale (CBDC) con effetti rilevanti sugli investimenti finanziari digitalizzati. È meglio anticiparla piuttosto che inseguirla.

Le Linee Guida sono strutturate in quattro parti e articolate in quattordici punti.

Nella Parte I viene delimitato l'ambito di applicazione, che viene definito anche attraverso la condivisione del significato di alcuni termini ricorrenti. In tale contesto assume rilevanza la definizione dei Fondi Italiani Digitali, che riassume in una unica fattispecie le due ipotesi sulle quali insistono le Linee Guida e su cui poi vertono le Parti III e IV: i Fondi Italiani che investono in attività digitali (c.d. Fondi Italiani Cripto) e i Fondi Italiani le cui quote sono emesse nativamente su una DLT (c.d. Fondi Italiani DLT). Con ciò viene demandata ai Gestori la valutazione in ordine all'istituzione dell'una o dell'altra tipologia di Fondi o contemporaneamente di entrambe.

La Parte II individua alcuni presidi per l'operatività dei Fondi Italiani Digitali (a prescindere quindi dalla specificità del Fondo e cioè se Cripto o DLT) che, pur essendo di carattere generale, pongono grande attenzione ai temi di governance, di controllo e gestione dei rischi, di alimentazione dei flussi informativi, di corretta definizione degli assetti organizzativi al fine di preservare uno sviluppo ordinato ed equilibrato del mercato. In tale contesto è stata inoltre dedicata una specifica Linea Guida alla tutela dei dati personali, con un focus su alcuni elementi (non esaustivi) che si raccomanda di tenere in considerazione.

Le Parti III e IV contengono indicazioni specifiche per l'ipotesi di istituzione di Fondi Italiani Cripto e Fondi Italiani DLT.

Con riferimento ai Fondi Italiani Cripto si è anzitutto raccomandato ai Gestori di valutare attentamente le iniziative in questo ambito, avendo cura di affrontare ogni profilo rilevante, specie con riguardo agli impatti delle iniziative sulla stabilità e sull'integrità dei mercati finanziari, anche tenendo conto dell'esigenza di contrasto al riciclaggio, sulla clientela alla quale sono offerte le quote dei Fondi Italiani Cripto, sulla coerenza complessiva dell'iniziativa rispetto alla struttura organizzativa interna e alle competenze dei propri organi di governo aziendale e del personale addetto. Le Linee Guida riconducono, ai sensi dell'attuale disciplina nazionale degli OICR, salvo diversa indicazione da parte della normativa o delle Autorità², l'investimento in Cripto-attività MiCAR nella categoria degli "altri beni" di cui all'articolo 4, comma 1, lett. f), DM n. 30/2015, per le quali andrà verificata l'esistenza di un mercato e di un valore determinabile con certezza con una periodicità almeno semestrale fornendo, tra l'altro, alcune raccomandazioni per le tipologie di OICR che, ai sensi della suddetta disciplina, possono investire in tali attività (FIA chiusi non riservati e FIA riservati), tra cui quella di assicurare una composizione diversificata del portafoglio che permetta il frazionamento degli investimenti (e dei relativi rischi) e l'ottimizzazione del portafoglio.

1. Sugli strumenti finanziari digitali "nativi" si rinvia a <https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm>

2. In considerazione dell'evoluzione del quadro normativo e dell'eterogeneità delle Cripto-attività, la valutazione potrebbe essere effettuata anche caso per caso.

Una particolare attenzione è stata poi dedicata alla individuazione delle modalità attraverso le quali svolgere, in un contesto DLT, il ruolo del Depositario. In assenza di indicazioni specifiche nella disciplina UCITS e AIFMD, le Linee Guida si sforzano di individuare un coordinamento tra la normativa di settore e le novità introdotte dalla normativa sui registri distribuiti (DLT Pilot Regime, MiCAR, Decreto Fintech), sulla base di alcuni presupposti: i) le novità introdotte nel quadro normativo non hanno mutato le funzioni del Depositario, in termini di tutela del corretto funzionamento dei Fondi e di protezione – nei limiti delle proprie competenze – degli interessi degli investitori dei Fondi, rimanendo tra le altre cose invariata l'esigenza di distinguere le funzioni gestorie da quelle di custodia; ii) esigenze di certezza e garanzia dei partecipanti richiedono, ove possibile, che la custodia dei beni di ciascun Fondo o comparto sia affidata a un unico soggetto, evitando duplicazioni di ruoli e contenendo il numero di soggetti nella filiera del risparmio gestito; iii) il Depositario è un soggetto regolamentato che conosce in profondità il mercato del risparmio gestito; iv) la tecnologia impatta sulle modalità operative con cui il Depositario svolge il ruolo attribuitogli dalla normativa; v) la più recente normativa, europea e nazionale, ha contribuito all'elaborazione di una disciplina sulla custodia degli asset digitali, utile ai fini che qui interessano.

Le Linee Guida si soffermano anche sull'attività di distribuzione dei Fondi Italiani Cripto, raccomandando, tra l'altro, ai Gestori e ai Distributori di dotarsi di processi adeguati alla selezione del target market di clientela a cui offrire i Fondi Italiani Cripto.

Nella elaborazione delle Linee Guida sui Fondi Italiani DLT si è partiti dalle disposizioni rilevanti contenute nel Decreto Fintech e nel Regolamento Consob di attuazione, limitatamente all'ipotesi di emissione e circolazione in forma digitale di azioni e quote di OICR non ammesse a negoziazione in una sede di negoziazione. In tale contesto, le Linee Guida sono finalizzate a presentare norme di carattere generale, come quelle contenute nel Decreto Fintech, tenendo conto delle specificità del modello operativo sottostante alla emissione e circolazione di quote o azioni di OICR. Le Linee Guida non considerano, in questa prima fase, l'ipotesi di ammissione a negoziazione su una infrastruttura di mercato DLT delle quote o azioni di OICR rientranti nell'ambito di applicazione del Regolamento DLT Pilot³.

Le Linee Guida sono accompagnate da alcuni Allegati tecnici che forniscono indicazioni, sia in termini attuativi sia in termini di fattori di rischio. In questa prospettiva sono stati individuati alcuni principi di valutazione delle Cripto-attività (Allegato 1); sono state richiamate le principali best practices indicate negli standard di sicurezza, come l'ISO 27001 e il PCI, e più specificamente individuati in CryptoCurrency Security Standard (CCSS), ISACA Blockchain Framework and Guidance e OWASP Smart contract Top 10 (Allegato 2); sono state fornite indicazioni per mitigare i rischi di sicurezza legati alla gestione degli asset crittografici nell'ambito degli strumenti finanziari DLT, su temi quali: i) generazione delle chiavi crittografiche; ii) creazione dei wallet; iii) storage delle chiavi; iv) uso delle chiavi; v) policy in caso di compromissione delle chiavi nonché per concessione e revoca dei keyholder (Allegato 3).

Il concetto di ecosistema sempre richiamato nei processi di trasformazione digitale trova negli Allegati 4, 5 e 6 uno spazio di lavoro fondamentale. In questa prospettiva assumono particolare rilievo le indicazioni fornite nell'Allegato 4 sulle funzioni che ciascuna delle entità coinvolte nell'operatività dei Fondi Italiani Digitali potrà svolgere all'interno della DLT e, soprattutto, sulle operazioni che possono essere codificate su uno o più smart contract. Altrettanto rilevanti sono le considerazioni svolte, nell'ambito degli Allegati 5 e 6, sulle modalità di regolamento on-chain

3. E cioè le quote di organismi di investimento collettivo di cui all'articolo 25, paragrafo 4, lettera a), punto iv), della direttiva 2014/65/UE, il cui valore di mercato delle attività gestite è inferiore a 500 milioni di EUR.

delle operazioni dei Fondi Italiani Digitali, anche mediante la descrizione di due processi di sottoscrizione e rimborso di quote digitali di Fondi Italiani aperti, distinti a seconda dell'asset di regolamento utilizzato.

Nell'Allegato 7 sono infine riportate alcune indicazioni esemplificative sull'informativa destinata agli Investitori di Fondi Italiani Digitali.

Le Linee Guida si chiudono con un elenco di indicazioni bibliografiche di supporto per l'approfondimento di molti dei temi in esse trattati.

La digitalizzazione dell'industria attraverso sia l'investimento in attività digitali sia, in particolare, come emissione nativa digitale di quote di OICR rappresenta un passaggio fondamentale per la ricerca di ulteriore efficienza ed eccellenza operativa nell'industria. Tale tecnologia, infatti, può abilitare nel lungo periodo una semplificazione dei processi operativi con conseguente contenimento dei costi e dei rischi operativi. Nel caso specifico di istituzione di Fondi che investono in Attività digitali e che allo stesso tempo emettono quote di fondi digitali, il processo per il calcolo del NAV potrebbe inoltre essere reso ancora più efficiente, a beneficio dell'investitore finale.

In conclusione, la domanda da porsi è dunque quale ruolo vogliono avere la nostra industria del risparmio e, più in generale, il nostro paese in questa evoluzione. Anche attraverso la pubblicazione di queste Linee Guida per la natura che hanno, per il metodo con cui sono state sviluppate, per gli attori istituzionali e professionali che vi hanno partecipato, è possibile argomentare che questo ruolo oggi più che mai può essere di front running di questa trasformazione dando all'Italia il posto che merita anche in termini di esportazione di innovazione e di valore.



PARTE I
AMBITO DI APPLICAZIONE E DEFINIZIONI

Linea Guida n. 1 – Ambito di applicazione

1. Le presenti Linee Guida forniscono raccomandazioni per l’istituzione e l’operatività di Fondi Italiani Digitali ai Gestori, ai Depositari e ai Distributori di Fondi Italiani Digitali nonché agli altri operatori nell’ecosistema dei Fondi Italiani Digitali.

Linea Guida n. 2 – Definizioni, riferimenti normativi e orientamenti di vigilanza

Linea Guida n. 2.1 – Definizioni

1. Ai fini delle presenti Linee Guida si intende per:

Fondi Italiani Digitali: i Fondi Italiani Cripto e i Fondi Italiani DLT.

Fondi Italiani Cripto: gli OICR italiani che investono il loro patrimonio in Attività digitali.

Fondi Italiani DLT: gli OICR italiani le cui quote o azioni sono emesse su un registro distribuito per la circolazione digitale.

OICR: gli organismi di investimento collettivo del risparmio di cui all’articolo 1, comma 1, lettera k), del TUF.

Attività digitali: gli Strumenti finanziari DLT e le Cripto-attività MiCAR.

Strumenti finanziari DLT: gli strumenti finanziari emessi su un registro distribuito per la circolazione digitale, ivi compresi gli strumenti finanziari digitali di cui all’articolo 1, comma 1, lettera c) del Decreto Fintech.

Cripto-attività MiCAR o «Cripto-attività»: le cripto-attività, diverse dagli Strumenti finanziari DLT, rientranti nell’ambito di applicazione del Regolamento MiCAR.

Il Regolamento MiCAR definisce le Cripto-attività come “ogni rappresentazione digitale di un valore o di un diritto che può essere trasferito e memorizzato elettronicamente, utilizzando la tecnologia a registro distribuito o una tecnologia analoga”. La categorizzazione delle cripto-attività ai sensi del Regolamento MiCAR è suddivisa in tre sottocategorie di Cripto-attività, ognuna delle quali è disciplinata da requisiti distinti in base ai rischi associati: (i) Asset-referenced token (ART)⁴; (ii) E-money token (EMT)⁵; e (iii) Cripto-attività che non sono considerati ART o EMT. Questa terza categoria comprende gli Utility token⁶.

Tecnologia a registro distribuito o «DLT»: la tecnologia di cui all’articolo 2, punto 1), del Regolamento DLT Pilot e cioè la tecnologia che consente il funzionamento e l’uso dei registri distribuiti. Le DLT vengono solitamente classificate in base ai profili di lettura e scrittura. In base ai profili di lettura, e quindi alla possibilità di accedervi per consultare le informazioni contenute nel registro, le DLT sono classificate in pubbliche e private (questo secondo caso prevede che solo alcuni nodi autorizzati possano accedere alle informazioni contenute nel registro). In base ai profili di scrittura, invece, le DLT sono comunemente distinte tra permissionless e permissioned in accordo alla modalità di partecipazione al meccanismo di consenso (nelle permissioned, solo alcuni dei nodi sono autorizzati a partecipare al meccanismo di consenso che permette

4. Un tipo di cripto-attività che non è un token di moneta elettronica e che mira a mantenere un valore stabile facendo riferimento a un altro valore o diritto o a una combinazione dei due, comprese una o più valute ufficiali [art. 3, comma 1 (7)].

5. Un tipo di cripto-attività che mira a mantenere un valore stabile facendo riferimento al valore di una valuta ufficiale [art. 3, comma 1 (6)].

6. Un tipo di cripto-attività destinato unicamente a fornire l’accesso a un bene o a un servizio prestato dal suo emittente [art. 3, comma 1 (9)].

l'aggiornamento dello stato del registro). Le DLT possono essere anche ibride, e cioè combinare operatività permissionless e permissioned.

Costituiscono un sottoinsieme delle DLT le blockchain, le quali sono dotate di due proprietà: (a) il loro registro è strutturato sotto forma di blocchi di transazioni (che costituiscono le unità elementari di aggiornamento dello stato del registro) e; (b) i blocchi sono concatenati tra di loro grazie all'utilizzo di particolari funzioni crittografiche, che rendono possibile aggiornare il registro solamente aggiungendo dati alla fine, senza poter modificare blocchi precedenti.

Meccanismo di consenso: le regole e le procedure con cui si raggiunge un accordo, tra i nodi di rete DLT, sulla convalida di un'operazione.

Nodo di rete DLT: un dispositivo o un'applicazione informatica che è parte di una rete e che detiene una copia completa o parziale delle registrazioni di tutte le operazioni eseguite tramite il registro distribuito.

Registro distribuito per la circolazione digitale o «Registro»: un registro utilizzato per l'emissione e la circolazione di Strumenti finanziari DLT o di Cripto-attività.

Intermediari: i Gestori, il Depositario, i Distributori.

Gestori: i soggetti di cui all'articolo 1, comma 1, lettera q-bis) del TUF.

Depositari: i soggetti di cui all'articolo 1, comma 1, lettera q-ter) del TUF.

Distributori: i soggetti abilitati all'offerta e alla vendita di quote o azioni di OICR.

Altri Operatori: i Fornitori di soluzioni e/o infrastrutture tecnologiche, i Fornitori di servizi per le Attività digitali, i Fornitori terzi di servizi ITC.

Fornitori di soluzioni o di infrastrutture tecnologiche: i soggetti che forniscono la tecnologia a supporto dei servizi bancari, finanziari e di pagamento, ivi inclusi i Tokenization Providers.

Fornitori terzi di servizi per le Attività digitali: in linea con la normativa vigente, i fornitori terzi di servizi per gli Strumenti finanziari DLT e le Cripto-attività, ivi inclusi i Key Custody Providers (e cioè i custodi delle chiavi crittografiche private).

Fornitori terzi di servizi ICT: fornitori terzi di servizi ICT come definiti dal Regolamento Dora.

Responsabile del registro: il Gestore o il soggetto terzo individuato come responsabile del registro dal Gestore, iscritto nell'elenco di cui all'articolo 19, comma 1 del Decreto Fintech.

Consegna contro pagamento o “DVP”: la consegna contro il pagamento come definita all'articolo 2, paragrafo 1, punto 27, del regolamento (UE) n. 909/2014.

Smart Contract: lo smart contract come definito dall'articolo 8-ter del Decreto Semplificazioni e cioè un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse.

Wallet: la coppia di chiavi crittografiche (chiave pubblica e chiave privata) che identificano ciascun utente nel registro distribuito e permettono di interagire all'interno dello stesso per disporre il trasferimento degli strumenti di propria pertinenza. I Wallet si differenziano tipicamente per la loro gestione delle chiavi private: se sono conservate dal provider sono definiti “custodial”, se invece sono gestite dallo stesso utente sono definiti “non-custodial”.

Gas Fee: le commissioni richieste per le transazioni blockchain a copertura dei costi per la creazione di un nuovo blocco.

Linea Guida n. 2.2 – Riferimenti normativi e orientamenti di vigilanza

1. Ai fini delle presenti Linee Guida si intende per:

Comunicazione della Banca d'Italia: la comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e Cripto-attività, giugno 2022.

Disciplina Antiriciclaggio: la disciplina antiriciclaggio contenuta nel Decreto legislativo 21 novembre 2007, n. 231 (Decreto Antiriciclaggio) e relativi provvedimenti attuativi.

DM n. 30/2015: il decreto del Ministero dell'Economia e delle Finanze del 5 marzo 2015, n. 30 recante regolamento attuativo dell'articolo 39 del decreto legislativo 24 febbraio 1998, n. 58 (TUF) concernente la determinazione dei criteri generali cui devono uniformarsi gli Organismi di investimento collettivo del risparmio (OICR) italiani.

Decreto Fintech: il 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" convertito, con modificazioni, dalla legge 10 maggio 2023, n. 52.

Decreto Semplificazioni: il decreto-legge 14 dicembre 2018, n. 135 recante "Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione", convertito con modificazioni dalla legge 11 febbraio 2019, n. 12.

Regolamento Consob: il regolamento Consob sull'emissione e circolazione in forma digitale di strumenti finanziari adottato con Delibera Consob n. 22923 del 6 dicembre 2023.

Regolamento DLT Pilot: il regolamento (UE) 2022/858 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito e che modifica i regolamenti (UE) n. 600/2014 e (UE) n. 909/2014 e la direttiva 2014/65/UE.

Regolamento DORA: il regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011.

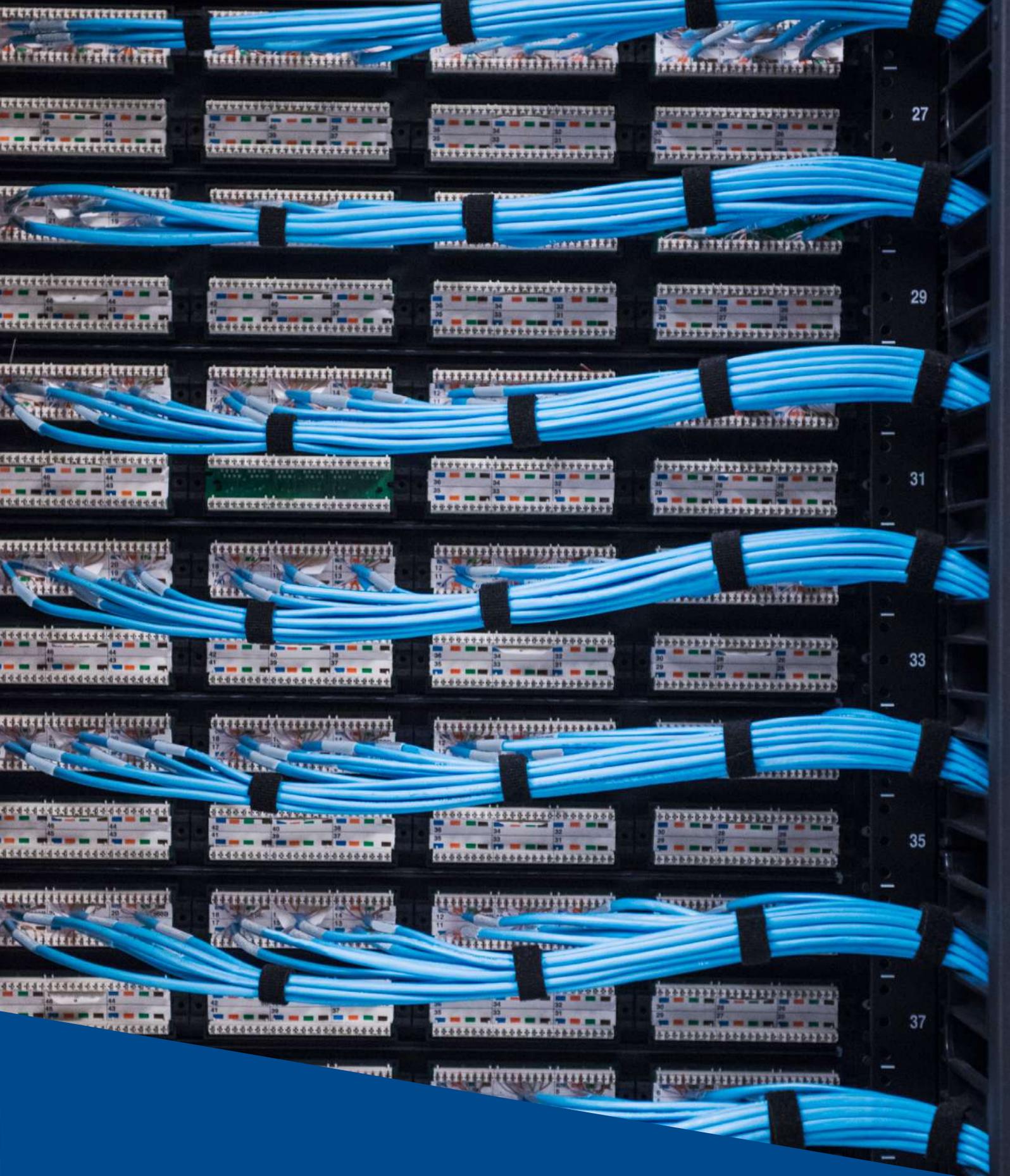
Regolamento MiCAR: il regolamento (UE) 2023/1114 del Parlamento Europeo e del Consiglio del 31 maggio 2023, relativo ai mercati delle Cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937.

Regolamento sulla Gestione Collettiva del Risparmio: il regolamento della Banca d'Italia adottato con provvedimento del 19 gennaio 2015 e s.m.i.

UCITS: la direttiva 2009/65/CE concernente il coordinamento delle disposizioni legislative, regolamentari e amministrative in materia di taluni organismi d'investimento collettivo in valori mobiliari (OICVM).

AIFMD: la direttiva 2011/61/UE sui gestori di fondi di investimento alternativi.

TUF: il testo unico delle disposizioni in materia di intermediazione finanziaria di cui al decreto legislativo 24 febbraio 1998, n. 58.



PARTE II PRESIDI GENERALI PER L'OPERATIVITÀ DEI FONDI ITALIANI DIGITALI

Linea Guida n. 3 – Presidi generali per gli Intermediari (Gestori, Depositari, Distributori)

1. Gli Intermediari assicurano il rispetto della normativa, anche di settore, di volta in volta vigente, degli orientamenti e degli atti delle Autorità di Vigilanza, ivi compresi i principi contenuti nella Comunicazione della Banca d'Italia o in altre, successive, adottate dalle Autorità di Vigilanza. In particolare, gli Intermediari:

- i. assicurano il coinvolgimento tempestivo degli organi di governo aziendale e delle funzioni di controllo di secondo e di terzo livello, sin dalla fase iniziale di studio delle iniziative relative ai Fondi Italiani Digitali, per valutarne la conformità alla regolamentazione vigente, la coerenza con gli indirizzi strategici, gli obiettivi e le politiche di governo dei rischi, nonché la relativa sostenibilità economica e finanziaria;
- ii. assicurano che gli assetti organizzativi siano, tempo per tempo, coerenti ed adeguati alle iniziative intraprese, per assicurare l'efficace presidio dei rischi da essi derivanti, la tutela della clientela, la prevenzione e gestione dei conflitti di interesse rispetto alle altre attività svolte;
- iii. assicurano adeguati flussi informativi verso gli organi aziendali e le funzioni di controllo interno in merito al livello e all'andamento della loro esposizione, diretta o indiretta, a tutte le tipologie di rischio collegate all'operatività dei Fondi Italiani Digitali, agli eventuali scostamenti rispetto alle politiche approvate dall'organo con funzione di supervisione strategica, alla tipologia di operazioni e servizi prestati e ai rispettivi rischi;
- iv. assicurano la mappatura completa dei rischi collegati alle iniziative e la loro mitigazione, prestando particolare attenzione alle nuove dimensioni che i rischi finanziari potrebbero assumere quando collegati all'operatività dei Fondi Italiani Digitali. In particolare, gli Intermediari assicurano che la mappatura dei rischi tenga conto della singola tipologia di Fondo Italiano Digitali considerata cioè: a) Fondi Italiani DLT che investono in attività tradizionali; b) Fondi Italiani DLT che investono in Strumenti finanziari DLT; c) Fondi Italiani DLT che investono in Cripto-attività; d) Fondi Italiani DLT che investono in strumenti finanziari DLT e in Cripto-attività. Nella definizione del sistema di gestione dei rischi gli Intermediari non si affidano esclusivamente o meccanicamente a terze parti, ma assicurano che siano sempre condotte adeguate e autonome analisi interne;
- v. prestano particolare attenzione all'adeguato presidio dei rischi di riciclaggio e finanziamento del terrorismo – incluso il rischio di elusione di sanzioni internazionali – nonché dei rischi reputazionali e legali, tenuto conto anche del quadro normativo in evoluzione;
- vi. assicurano l'adozione di tutti i presidi necessari al contenimento dei rischi operativi – con particolare attenzione al rischio informatico – e alla tutela della cybersecurity; in questo contesto gli intermediari identificano e gestiscono opportunamente i rischi connessi al funzionamento di infrastrutture tecnologiche. A tal fine si raccomanda agli Intermediari di verificare l'adeguatezza delle proprie infrastrutture informatiche (soprattutto a livello di mitigazione dei rischi connessi all'uso della tecnologia), nonché dei controlli di 1°, 2° e 3° livello;
- vii. prestano particolare attenzione all'adeguatezza dei processi e delle procedure volte ad assicurare l'identificazione, valutazione e mitigazione dei rischi (reputazionali o di altro genere) derivanti dall'esternalizzazione o dal ricorso a servizi prestati da terze parti, anche ove non qualificabili come esternalizzazioni (es. operatori specializzati nella custodia di Attività digitali, Wallets, piattaforme di trading);
- viii. assicurano la presenza di presidi per l'identificazione dei potenziali investitori, attraverso una

revisione delle indagini volte alla profilatura della clientela al fine di valutarne l'efficacia alla luce delle specificità dei Fondi Italiani Digitali considerati;

- ix. assicurano un'adeguata informativa agli investitori sui rischi e sulle caratteristiche connessi con l'operatività in Fondi Italiani Digitali, anche con riferimento alle attività svolte da terze parti, e procedono, ove necessario, a un rafforzamento delle procedure per la rilevazione delle frodi e per la gestione dei reclami.

Le raccomandazioni che precedono devono essere declinate secondo il principio di proporzionalità, in relazione alla complessità operativa, dimensionale e organizzativa degli Intermediari nonché, come sopra delineato, alla concreta operatività svolta in cripto-attività o mediante utilizzo di tecnologie decentralizzate.

Linea Guida n. 4 – Presidi in caso di esternalizzazione

1. Quando gli Intermediari intendono affidare a terzi la prestazione di servizi o lo svolgimento di funzioni operative, valutano attentamente i costi e benefici di tale scelta specie in comparazione alla prestazione in house del servizio o della funzione, effettuando analisi di mercato, valutando – anche prospetticamente – l'impatto della tecnologia sul proprio business e sulla propria struttura organizzativa, compiendo approfondite due diligence sui fornitori alla luce dei criteri identificati dalla normativa applicabile e agli ulteriori elementi individuati nei paragrafi che seguono. Quando decidono di affidare a terzi la prestazione del servizio o della funzione operativa, gli Intermediari assicurano inoltre che gli organi aziendali, le funzioni interne interessate e quelle di controllo siano adeguatamente informati e che siano formalizzati i loro contributi nel processo decisionale.

2. In caso di esternalizzazione o di ricorso a servizi prestati da terze parti, anche ove non qualificabili come esternalizzazioni di funzioni essenziali, gli Intermediari fissano i criteri per selezionare gli operatori e fornitori tecnologici, tenendo conto di vari aspetti, tra cui: (i) le politiche e le procedure implementate dal fornitore per garantire la disponibilità, la riservatezza, l'integrità e la non contestazione dei dati; (ii) l'adozione di approcci robusti per pianificare l'intero ciclo di vita delle tecnologie impiegate e per scegliere gli standard tecnologici da adottare; (iii) le procedure utilizzate per identificare e affrontare situazioni di malfunzionamento e incidenti operativi e di sicurezza informatica, nonché per rispondere a tali eventi; (iv) piani adeguati volti al recupero da situazioni di emergenza e per la gestione di situazioni di disastro, con regolare verifica periodica; (v) l'integrità della governance del fornitore, le strutture organizzative istituite per individuare e gestire i rischi, nonché le relative linee guida di responsabilità; (vi) la capacità del soggetto a cui il servizio è affidato di assicurare nel continuo il rispetto della normativa e della regolamentazione di vigilanza.

3. In caso di esternalizzazione di funzioni operative, gli Intermediari assicurano: (a) la valutazione delle condizioni previste dalla normativa per la qualificazione come funzioni "essenziali" o "importanti" delle stesse, avendo cura di valutare anche prospetticamente l'impatto della tecnologia sulla sua organizzazione interna e sul business aziendale; (b) la capacità di selezionare e monitorare nel continuo il fornitore dei servizi, in modo da assicurare che quest'ultimo disponga non solo delle competenze tecniche/tecnologiche idonee al corretto svolgimento del servizio affidato ma anche della capacità di assicurare nel continuo il rispetto delle regole di vigilanza (in termini, ad esempio, di livello di servizio concordato; adeguatezza dei flussi informativi; sicurezza delle informazioni relative all'attività del Gestore; sicurezza dei propri sistemi); (c) la capacità del soggetto a cui è esternalizzata la funzione di assicurare nel continuo il rispetto della normativa e della regolamentazione di vigilanza.

Linea Guida n. 5 – Criteri per la scelta degli “Altri Operatori”

1. I Gestori effettuano un’attenta valutazione nella scelta degli Altri Operatori necessari per l’operatività dei Fondi Italiani Digitali, considerando almeno se questi soggetti assicurano il rispetto dei principi contenuti nella Comunicazione della Banca d’Italia o in altre, successive, adottate dalle Autorità di Vigilanza e, in particolare assicurano:

- i. che la gestione della tecnologia sia basata nella misura più ampia possibile su una governance chiara e definita nonché su presidi volti a mitigare i diversi rischi rilevanti (ad esempio operativi, cyber, AML, riguardanti la protezione delle informazioni e dei dati);
- ii. la disponibilità di adeguata rendicontazione informativa sull’attività svolta, anche considerando il ruolo e i vincoli che fanno capo agli intermediari vigilati e alle infrastrutture di pagamento sottoposte alla sorveglianza;
- iii. l’adozione di standard appropriati in materia di sicurezza delle informazioni;
- iv. l’esperienza maturata nell’ambito delle tecnologie a registro distribuito.

Linea Guida n. 6 – Operatività on-chain e off-chain dei Fondi Italiani Digitali

1. I Gestori individuano le funzioni che ciascuna delle entità coinvolte nell’operatività dei Fondi Italiani Digitali potrà svolgere all’interno della DLT e, soprattutto, stabiliscono le operazioni che possono essere codificate su Smart Contract, tenuto conto di quanto previsto nell’Allegato 4.

2. Nella definizione degli Smart Contract si raccomanda di assicurare la coerenza con il sistema normativo vigente nonché di conservare adeguata documentazione.

3. I Gestori promuovono l’adozione di modalità di pagamento tramite moneta di banca centrale, anche in forma tokenizzata, se pratica o possibile oppure, ove non sia pratica o possibile, tramite moneta di banca commerciale, anche in forma tokenizzata, o tramite token di moneta elettronica o altre attività previste dalla normativa MiCAR, ove utilizzabili a fini di pagamento. A tal riguardo si raccomanda di considerare quanto riportato negli Allegati 5 e 6.

4. I Gestori assicurano di utilizzare modelli operativi solidi e sostenibili nonché di garantire, ove possibile, un adeguato livello di interoperabilità (e “standard di colloquio”) tra diverse soluzioni tecnologiche.

Linea Guida n. 7 – Tutela dei dati personali

1. I Gestori assicurano il rispetto dei principi sanciti dalla normativa vigente in materia di protezione dei dati personali, prestando particolare attenzione, tra le altre cose, a:

- i. rispettare il principio di minimizzazione, evitando per quanto possibile di inserire dati personali on-chain e, ove necessario, ricorrendo a tecniche di anonimizzazione/pseudonimizzazione;
- ii. adempiere alle previsioni della normativa nel trattamento dei dati personali sia on-chain sia off-chain (base giuridica, informativa, registro dei trattamenti);
- iii. individuare i c.d. ruoli privacy nella catena del valore dei fondi (titolari, contitolari, responsabili del trattamento), segnatamente valutando nei casi di esternalizzazioni, il ruolo privacy da questi assunto (deleghe di funzioni e, in ogni caso, di coinvolgimento di soggetti terzi);
- iv. individuare le modalità attraverso le quali consentire l'esercizio dei diritti da parte degli interessati, compatibilmente con le caratteristiche della DLT individuata;
- v. implementare, compatibilmente con le caratteristiche della DLT, misure tecniche ed organizzative che garantiscano un livello di sicurezza adeguato al rischio, effettuando le valutazioni necessarie (es. valutazione d'impatto della protezione dei dati, DPIA).



PARTE III
PRESÌDI SPECIFICI PER L'OPERATIVITÀ
DEI FONDI ITALIANI CRIPTO

Linea Guida n. 8 – Attività d’investimento dei Fondi Italiani Cripto

1. I Gestori valutano attentamente le iniziative sui Fondi Italiani Cripto, avendo cura di affrontare ogni profilo rilevante, specie con riguardo agli impatti delle iniziative sulla stabilità e sull’integrità dei mercati finanziari, anche tenendo conto dell’esigenza di contrasto al riciclaggio di proventi di attività illecite, sulla clientela alla quale sono offerte le quote o azioni dei Fondi Italiani Cripto, sulla coerenza complessiva dell’iniziativa rispetto alla struttura organizzativa interna e alle competenze dei propri organi di governo aziendale e del personale addetto.

2. I Gestori che intendono avviare iniziative su Fondi Italiani Cripto, quando investono in Strumenti finanziari DLT, assicurano il rispetto dei limiti e dei criteri stabiliti per l’investimento in strumenti finanziari dalla Banca d’Italia a norma dell’articolo 6, comma 1, lettera c), del TUF nonché il rispetto di tutte le regole di settore previste dalla normativa europea e nazionale sull’investimento in strumenti finanziari e quelle specifiche introdotte sugli Strumenti finanziari DLT dal Decreto Fintech.

Fermo restando quanto sopra, i Gestori che intendano istituire Fondi Italiani Cripto, quando investono in Cripto-attività:

- i. salvo che non risulti diversamente dalla normativa o dalle Autorità, investono in Cripto-attività che possono essere ricondotte alla categoria degli “altri beni” di cui all’articolo 4, comma 1, lett. f), DM n. 30/2015, per le quali quindi esiste un mercato e che hanno un valore determinabile con certezza con una periodicità almeno semestrale;
- ii. investono in Cripto-attività che, oltre ad essere riconducibili alla categoria degli “altri beni” (salvo diversa valutazione della normativa o delle Autorità), non abbiano un elevato grado di volatilità dei prezzi, le loro valutazioni siano affidabili e i relativi rischi gestibili. È opportuno in particolare che gli OICR non investano in Cripto-attività prive di valore intrinseco, non riferite ad alcuna attività dell’economia reale o finanziaria e che non siano idonee a svolgere funzioni di investimento (ad esempio, in stablecoin algoritmiche, in unbacked Crypto assets, altre Cripto-attività ancorate ad asset con elevata volatilità e/o Cripto-attività che non consentano un adeguato controllo dei rischi da parte del Gestore);
- iii. adottano le tipologie dei FIA chiusi non riservati e dei FIA riservati, assicurando il rispetto delle pertinenti disposizioni della Banca d’Italia sulle attività di investimento degli OICR, nonché avendo cura di monitorare e di allinearsi costantemente all’evoluzione normativa e regolamentare o alle eventuali raccomandazioni – individuali o di sistema – delle Autorità di Vigilanza. Per il caso di FIA chiusi non riservati, quindi accessibili da parte della clientela retail, si raccomanda ai Gestori di prestare particolare attenzione alla compatibilità dell’oggetto d’investimento con il profilo della clientela retail a cui il Fondo è destinato.

Nel caso di esposizioni indirette, attraverso veicoli societari o schemi di altra natura, è sempre opportuno che i Gestori verifichino che l’investimento in strumenti emessi da tali veicoli o schemi non si traduca di fatto nell’investimento in cripto-attività non regolamentate dalla MiCAR o, più in generale, in investimenti in cripto-attività non raccomandate. In ottica più generale è sempre opportuna la massima attenzione sugli effetti – giuridici ed economici – relativi all’investimento in strumenti finanziari o altri titoli emessi da veicoli o schemi che investono, sono collegati o hanno come sottostante Cripto-attività della specie.

3. Nella definizione delle iniziative relative ai Fondi Italiani Cripto che investono in Cripto-attività, i Gestori:

- i. si assicurano dell'esistenza di un mercato delle Cripto-attività oggetto d'investimento e che queste abbiano un valore determinabile con certezza con una periodicità almeno semestrale;
- ii. assicurano una composizione diversificata del portafoglio al fine di garantire il frazionamento degli investimenti e l'ottimizzazione del portafoglio;
- iii. valutano, a seconda della tipologia di Cripto-attività in cui investono, come devono essere applicate le regole in materia di contenimento e di frazionamento del rischio, adottando un approccio orientato alla prudenza;
- iv. definiscono la metodologia per determinare il prezzo delle Cripto-attività e si dotano di procedure interne idonee a effettuare la valutazione delle Cripto-attività. A tal fine i Gestori tengono conto dei criteri indicati nell'Allegato 1;
- v. quando istituiscono, nei limiti di quanto ciò sia ammesso dalla normativa, OICR aperti riservati, si dotano di specifiche politiche sui rimborsi delle quote o azioni di tali OICR e stabiliscono una strategia di investimento del Fondo coerente con tali politiche di rimborso;
- vi. effettuano prove di stress adeguate sull'investimento in Cripto-attività. Le prove di stress devono essere estreme ma plausibili e riflettere la volatilità dei prezzi delle Cripto-attività, compresa la potenziale perdita totale di valore dell'investimento.

4. I Gestori di Fondi Italiani Cripto assicurano di:

- i. indicare nella politica di gestione dei rischi le modalità di gestione dei rischi connessi all'investimento diretto o indiretto in Cripto-attività. A tal fine i Gestori tengono conto almeno dei fattori di rischio indicati nelle best practice di settore, quali ad esempio l'ISACA – Blockchain Framework and Guidance, e riportati a titolo esemplificativo e non esaustivo nell'Allegato 2;
- ii. verificare la coerenza e l'allineamento tra la strategia di investimento del Fondo, il relativo profilo di liquidità, la politica di rimborso e la forma degli stessi, nonché tutti i profili attinenti alla tutela dei sottoscrittori;
- iii. verificare l'adeguatezza dei presidi per l'identificazione dei potenziali investitori al fine di valutarne l'efficacia alla luce delle specificità del Fondo Italiano Cripto istituito, specie nel caso di Fondi chiusi retail;
- iv. indicare nella documentazione d'offerta del Fondo informazioni chiare sulla natura dell'investimento proposto in Cripto-attività e sui rischi associati a tale investimento.

Linea Guida n. 9 – Custodia delle Attività digitali del Fondo Italiano Cripto

1. Al fine di individuare i compiti e le responsabilità dei Depositari dei Fondi che investono in Strumenti Finanziari DLT e in Cripto-attività, i Gestori e i Depositari tengono conto delle raccomandazioni che seguono elaborate sulla base dei seguenti assunti: i) le novità introdotte nel quadro normativo non hanno mutato le funzioni del Depositario, in termini di tutela del corretto funzionamento dei Fondi e di protezione – nei limiti delle proprie competenze – degli interessi degli investitori dei Fondi, rimanendo tra le altre cose invariata l'esigenza di distinguere le funzioni gestorie da quelle di custodia; ii) esigenze di certezza e garanzia dei partecipanti richiedono, ove possibile, che la custodia dei beni di ciascun Fondo o comparto sia affidata a un unico soggetto,

evitando duplicazioni di ruoli e contenendo il numero di soggetti nella filiera del risparmio gestito; iii) il Depositario è un soggetto regolamentato che conosce in profondità il mercato del risparmio gestito; iv) la tecnologia impatta sulle modalità operative con cui il Depositario svolge il ruolo attribuitogli dalla normativa; v) i più recenti interventi del legislatore europeo (Regolamento DLT Pilot e Regolamento MiCAR) e nazionale (Decreto Fintech) contribuiscono alla elaborazione di una disciplina sulla custodia delle Attività digitali che, pur nella complessità delle interconnessioni normative con la disciplina “tradizionale”, non può essere ignorata ai fini che qui interessano.

2. I Gestori effettuano un’attenta valutazione nella scelta del Depositario di Strumenti finanziari DLT e di Cripto-attività, considerando almeno: (i) la struttura e i meccanismi utilizzati per la custodia delle Attività digitali. A tal fine i Gestori possono tener conto dell’adozione da parte del Depositario dei presidi indicati nell’Allegato 3; (ii) l’esperienza maturata dal Depositario nella custodia di Attività digitali.

3. Nel caso di custodia di Cripto-attività, si raccomanda ai Gestori di effettuare la scelta del Depositario anche tenendo conto della presenza dei requisiti previsti per l’attività di custodia dall’articolo 60, paragrafo 7 del Regolamento MiCAR.

4. Tenuto conto di quanto previsto dall’articolo 17 del Decreto Fintech e dall’articolo 75 del Regolamento MiCAR, si raccomanda ai Depositari di valutare di svolgere la custodia delle Attività digitali attraverso il controllo dei mezzi di accesso alle Attività digitali anche sotto forma di chiavi crittografiche private e protocolli a doppia firma, ferma restando la proprietà dei beni da parte del Fondo; il Gestore e il Depositario definiscono nella convenzione gli aspetti relativi ai rapporti interni con riguardo al controllo dei mezzi di accesso alle Attività digitali e i rispettivi compiti.

5. Nello svolgimento dei compiti di custodia delle Attività digitali, i Depositari possono avvalersi di Altri Operatori specializzati nella custodia di Attività digitali. In tal caso restano fermi i presidi di cui al Titolo VIII, Cap. III, Sez. V del Regolamento sulla Gestione Collettiva del Risparmio.

6. Si raccomanda ai Depositari, ove applicabile, di: (i) garantire che i mezzi di accesso alle Cripto-attività dei Fondi siano chiaramente identificati come tali, assicurando che tali mezzi di accesso siano tenuti in modo distinto rispetto ai mezzi di accesso alle Attività digitali del Depositario o ai mezzi di accesso alle Attività digitali dei suoi clienti; (ii) tenere un registro delle posizioni, aperte a nome di ciascun Fondo, corrispondenti ai diritti di ciascun Fondo sulle Attività digitali, inserendo quanto prima in tale registro qualsiasi movimento effettuato seguendo le istruzioni del Gestore. In tal caso, le procedure interne del Depositario garantiscono che qualsiasi movimento che incida sulla registrazione delle Attività digitali sia corroborato da un’operazione regolarmente registrata nel registro delle posizioni del Fondo; (iii) stabilire norme e procedure interne per minimizzare il rischio di perdita dei mezzi di accesso alle Attività digitali del Fondo e dei diritti connessi a tali Attività digitali a causa di frodi, minacce informatiche o negligenza.

7. In caso di perdita dei mezzi di accesso agli Strumenti finanziari DLT detenuti in custodia ai sensi dell’articolo 17 del Decreto Fintech, il Depositario, se non prova che l’inadempimento è stato determinato da caso fortuito o forza maggiore, è tenuto a restituire senza indebito ritardo strumenti finanziari DLT della stessa specie o una somma di importo corrispondente, salva la responsabilità per ogni altra perdita subita dal Fondo o dagli investitori in conseguenza del mancato rispetto, intenzionale o dovuto a negligenza, dei propri obblighi.

In caso di perdita dei mezzi di accesso alle Cripto-attività detenute in custodia secondo quanto previsto dall’art. 75 del Regolamento MiCAR, il Depositario è responsabile nei confronti del Fondo della perdita di Cripto-attività o dei mezzi di accesso alle Cripto-attività limitatamente al valore di mercato della Cripto-attività persa al momento della sua perdita, salvo che si tratti di un incidente non attribuibile al Depositario secondo previsto dallo stesso articolo 75, par. 8, MiCAR.

8. Il Depositario stabilisce norme e procedure interne e individua i meccanismi e dispositivi da adottare al fine di assicurare il rispetto degli altri obblighi previsti dall'articolo 48 del TUF e ogni altra funzione svolta, a qualsiasi titolo, per i Fondi Italiani Cripto.

Linea Guida n. 10 – Distribuzione di Fondi Italiani Cripto

1. Nell'attività di distribuzione di Fondi Italiani Cripto – fermi restando i presidi previsti dalla pertinente disciplina e, avendo cura di monitorare e di allinearsi costantemente all'evoluzione normativa e regolamentare o alle eventuali raccomandazioni, individuali o di sistema, delle Autorità di Vigilanza – si raccomanda di valorizzare le peculiarità che caratterizzano tali Fondi e, in particolare di:

- i. assicurare l'adeguata definizione del target market a cui si intende offrire Fondi Italiani Cripto, tenuto conto della complessità e dei rischi degli stessi;
- ii. curare nel modo più scrupoloso possibile l'informativa da rendere alla clientela che intenda acquistare Fondi Italiani Cripto, al fine di facilitare la massima consapevolezza in ordine ai rischi rilevanti individuati, anche utilizzando le informazioni riportate nell'allegato 7;
- iii. prestare i servizi attraverso personale qualificato, specificamente formato sulle caratteristiche dei Fondi Italiani Cripto offerti.



PARTE IV
PRESÌDI SPECIFICI PER L'OPERATIVITÀ
DEI FONDI ITALIANI DLT

Finalità della presente Parte è quella di presentare alcune delle principali norme di carattere generale contenute nel Decreto Fintech, tenendo conto delle specificità del modello operativo sottostante alla emissione e circolazione di quote o azioni di OICR. In particolare, la Linea Guida n. 11 concerne, in via generale, l'operazione di emissione di quote di Fondi Italiani DLT; la Linea Guida n. 12 approfondisce l'ipotesi in cui il Gestore non svolga l'attività di Responsabile del registro; la Linea Guida n. 13 offre una panoramica dei compiti del Responsabile del registro, sia esso Gestore o altro soggetto previsto dal Decreto Fintech; infine, la Linea Guida n. 14 evidenzia l'importanza di una corretta informazione in fase di distribuzione delle quote di Fondi Italiani DLT.

Resta comunque l'obbligo di conformarsi a tutte le disposizioni del Decreto Fintech.

Linea Guida n. 11 – Emissione di quote di Fondi Italiani DLT

1. I Gestori che intendono emettere su una DLT quote di Fondi Italiani non ammessi a negoziazione in una sede di negoziazione assicurano il rispetto delle pertinenti previsioni del Decreto Fintech.

2. Il Gestore valuta se: 1) emettere quote di Fondi Italiani DLT su un Registro tenuto da un soggetto specializzato, iscritto nella sezione 4 dell'Elenco tenuto dalla Consob, ovvero da un soggetto iscritto nella sezione 1 dell'Elenco tenuto dalla Consob; 2) svolgere l'attività di Responsabile del registro con riferimento alle quote dei propri Fondi Italiani DLT (previa iscrizione nella sezione 2 dell'Elenco tenuto dalla Consob), avvalendosi, se del caso, di Altri Operatori per lo svolgimento di servizi/attività.

3. Ogni emissione di quote di Fondi Italiani Digitali è iscritta su un solo Registro e a ciascun Registro è associato un unico Responsabile.

4. I registri per la circolazione digitale:

a. assicurano l'integrità, l'autenticità, la non ripudiabilità, la non duplicabilità e la validità delle scritturazioni attestanti la titolarità e il trasferimento delle quote del Fondo Italiano DLT e i relativi vincoli;

b. consentono, direttamente o indirettamente, di identificare in qualsiasi momento i soggetti in favore dei quali sono effettuate le scritturazioni, la specie e il numero delle quote del Fondo Italiano DLT da ciascuno detenuti, nonché di renderne possibile la circolazione;

c. consentono al soggetto in favore del quale sono effettuate le scritturazioni di accedere in qualsiasi momento alle scritturazioni del Registro relative alle proprie quote del Fondo Italiano DLT ed estrarre copia in formato elettronico per tutti i fini previsti dalla legge;

c. bis prevengono la perdita o la modifica non autorizzata dei dati e delle scritturazioni relative alle quote del Fondo Italiano DLT per l'intera durata della scritturazione;

d. consentono la scritturazione dei vincoli di ogni genere sulle quote del Fondo Italiano DLT, secondo quanto previsto dall'articolo 9 del Decreto Fintech;

e. garantiscono l'accessibilità da parte della Commissione nazionale per le società e la borsa (Consob) e della Banca d'Italia per l'esercizio delle rispettive funzioni;

f. consentono di identificare ai fini dell'articolo 9 del Decreto Fintech:

1. la data di costituzione del vincolo;

2. le quote del Fondo Italiano DLT;

3. la natura del vincolo ed eventuali altre indicazioni supplementari;

4. la causale del vincolo e la data dell'operazione oggetto di scritturazione;
5. la quantità delle quote del Fondo Italiano DLT;
6. il titolare delle quote del Fondo Italiano DLT;
7. il beneficiario del vincolo e, ove comunicata, l'esistenza di una convenzione fra le parti per l'esercizio dei diritti;
8. l'eventuale data di scadenza del vincolo.

5. Ai fini dell'emissione in forma digitale di quote di Fondi Italiani DLT risultano univocamente connesse a ciascuna quota digitale e sono rese disponibili in una forma elettronica accessibile e consultabile in ogni momento, eventualmente anche per il tramite del Registro medesimo, le seguenti informazioni:

- a. la denominazione e la sede del Gestore del Fondo;
- b. la denominazione e la tipologia del Fondo;
- c. la data di istituzione del Fondo e la durata;
- d. la tipologia della quota, se nominativa o al portatore, nonché la classe e il comparto di appartenenza ove presenti;
- e. il valore nominale delle quote, ove presente;
- f. il Depositario;
- g. i termini e le condizioni dell'emissione;

Il Gestore valuta se rendere disponibili in forma elettronica anche ulteriori informazioni come, ad esempio, la valuta di denominazione delle quote del Fondo e il regime dei proventi.

6. Il Gestore valuta l'adozione dei seguenti modelli di gestione delle sottoscrizioni e rimborsi delle quote del Fondo Italiano DLT da parte dell'Investitore:

- a. le scritturazioni sul Registro sono effettuate a favore dell'Investitore delle quote del Fondo Italiano DLT; l'Investitore è intestatario del Wallet e controlla direttamente i mezzi di accesso alle quote digitali, anche in forma di chiavi crittografiche private (modello c.d. diretto o disintermediato);
- b. le scritturazioni sul Registro sono effettuate a favore dell'Investitore delle quote del Fondo Italiano DLT; l'Investitore è intestatario del Wallet, ma i mezzi di accesso alle quote digitali, anche in forma di chiavi crittografiche private, sono affidati dall'Investitore al Distributore che opera per conto dell'Investitore (modello c.d. parzialmente intermediato);
- c. le scritturazioni sul Registro sono effettuate a favore della banca o dell'impresa di investimento che opera in nome proprio e per conto dell'Investitore delle quote del Fondo Italiano DLT; quest'ultima (banca o impresa d'investimento) è intestataria del Wallet per conto dell'Investitore e controlla i mezzi di accesso alle quote digitali, anche in forma di chiavi crittografiche private. In tal caso, la legittimazione piena ed esclusiva dell'esercizio dei diritti consegue alla registrazione sul conto aperto dall'Investitore presso la banca o l'impresa di investimento, secondo quanto previsto dall'articolo 11 del Decreto Fintech (modello c.d. totalmente intermediato).

Per un esempio di processo di sottoscrizione e rimborso di quote di Fondi Italiani DLT mediante l'adozione del modello sub b) si rinvia all'Allegato 6.

Linea Guida n. 12 – Gestore di Fondi Italiani DLT

1. Il Gestore, ove non svolga l'attività di Responsabile del registro con riferimento alle quote di Fondi Italiani DLT di propria istituzione, fermo restando l'adempimento degli obblighi previsti dalla disciplina di settore applicabile, assicura altresì il rispetto degli obblighi previsti dal Decreto Fintech e dalla disciplina secondaria di attuazione. In particolare, il Gestore:

- i. ricorre a un Responsabile del registro iscritto nella sezione 1 o 4 dell'Elenco tenuto dalla Consob;
- ii. notifica alla Consob le caratteristiche dell'emissione di quote del Fondo Italiano DLT e il relativo Responsabile del registro, nonché le ulteriori informazioni individuate nel Regolamento Consob;
- iii. rende disponibili ai sottoscrittori le informazioni di cui all'articolo 23, comma 3 del Decreto Fintech;
- iv. assicura di fornire al Responsabile del registro le informazioni di cui all'art. 12, comma 6, lett. b) del Decreto Fintech;
- v. verifica, sulla base delle scritturazioni del Registro, la legittimazione all'esercizio dei diritti connessi alle quote del Fondo Italiano DLT;
- vi. aggiorna i libri sociali previsti dal DM n. 30/2015 sulla base delle scritturazioni del Registro, anche ove il libro dei soci sia tenuto attraverso il Registro;
- vii. effettua le operazioni necessarie per il mutamento del regime di forma e circolazione degli strumenti finanziari nei casi e secondo le modalità indicate dall'art. 14, comma 2 del Decreto Fintech.

Linea Guida n. 13 – Responsabile del registro di Fondi Italiani DLT

1. Il Responsabile del registro, sia esso il Gestore o uno dei soggetti iscritti nella sezione 1 o 4 dell'Elenco tenuto dalla Consob, è tenuto all'adempimento degli obblighi indicati nel Decreto Fintech e nella disciplina secondaria di attuazione. In particolare, il Responsabile del registro:

- i. assicura la conformità del Registro alle caratteristiche prescritte dal Decreto Fintech e dalle relative disposizioni attuative;
- ii. garantisce la correttezza, la completezza e l'aggiornamento continuo delle evidenze relative alle informazioni sull'emissione;
- iii. garantisce l'integrità e la sicurezza del sistema, tenendo anche conto delle esigenze di antiriciclaggio, in forza dell'emissione e del trasferimento delle quote digitali sulla base di un titolo idoneo;
- iv. assicura la continuità operativa e il ripristino dell'attività, attraverso meccanismi e dispositivi adeguati che comprendono la messa in sicurezza esterna delle informazioni. La continuità operativa deve essere garantita, tra l'altro, anche nel caso di sostituzione di alcuni attori della catena, ivi compresi i momenti di gestione "condivisa" di specifici ruoli nella piattaforma (es. in caso di sostituzione del Gestore o del Depositario e relativa gestione della fase transitoria di "passaggio delle consegne");
- v. impedisce l'uso delle quote digitali da parte di soggetti diversi da quelli legittimati;
- vi. assicura che il numero complessivo di quote digitali che costituisce una singola emissione non sia modificabile;

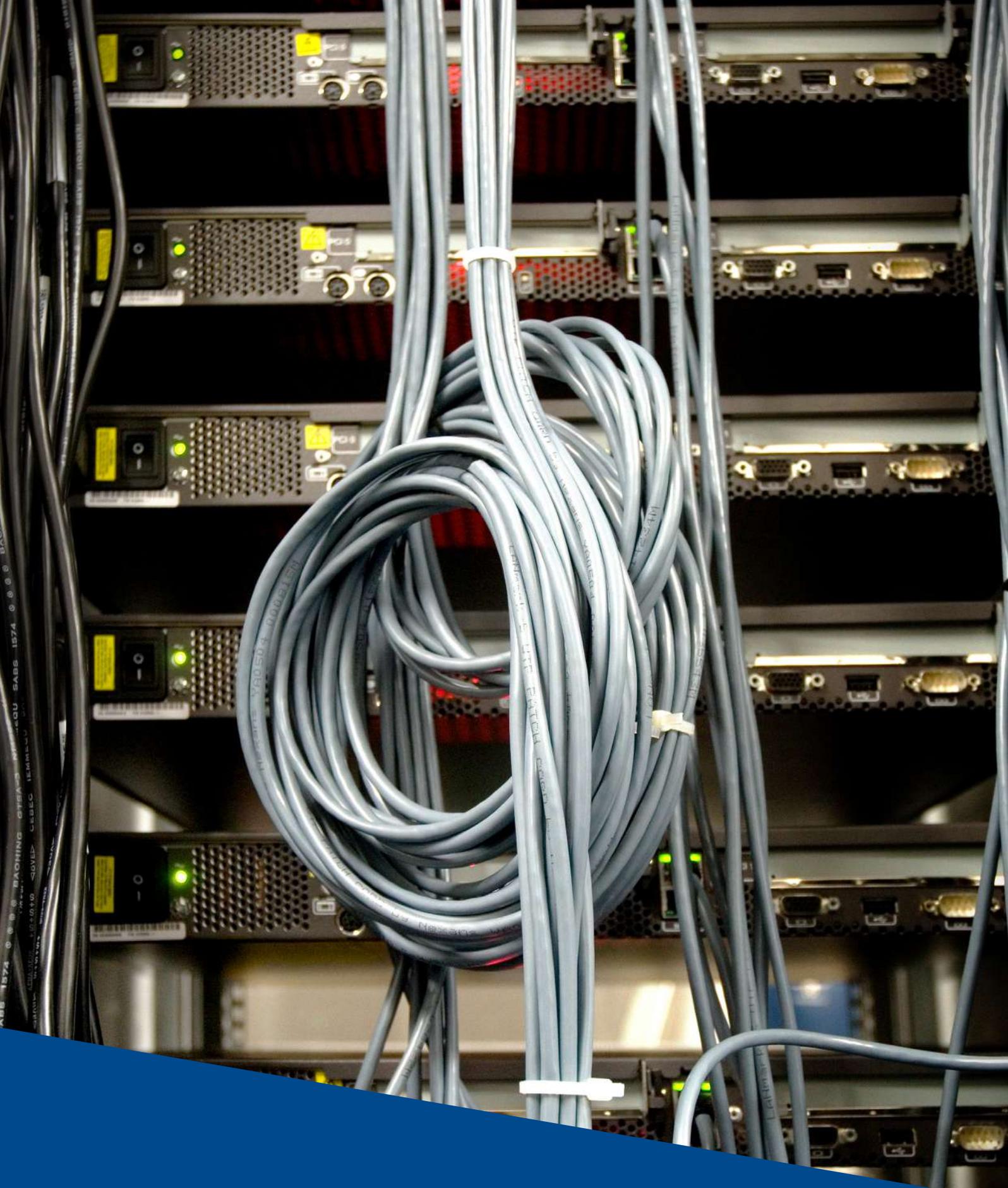
- vii. adotta una strategia di transizione conformemente a quanto previsto dall'articolo 14, comma 1 del Decreto Fintech, ne valuta almeno semestralmente l'efficacia e a tal fine adotta le misure e le procedure necessarie ed appropriate;
- viii. rende disponibile al pubblico, in una forma elettronica accessibile e consultabile in ogni momento, un documento contenente le informazioni relative alle modalità operative del registro per la circolazione digitale e ai dispositivi a tutela della sua operatività, tra cui la strategia di transizione;
- ix. assicura il rispetto delle disposizioni antiriciclaggio contenute del decreto legislativo 21 novembre 2007, n. 231.

2. Il Responsabile del registro risponde dei danni derivanti dalla tenuta del registro verso il Gestore, se soggetto diverso dal Responsabile del registro, e verso il soggetto in favore del quale le scritturazioni sono state effettuate o avrebbero dovuto essere effettuate, salvo che dia prova di avere adottato tutte le misure idonee ad evitare il danno. Il Responsabile del registro risponde dei danni cagionati al soggetto in favore del quale è avvenuta la scritturazione o all'investitore, ove si tratti di soggetto diverso dal primo, sia che discendano da false informazioni o da informazioni comunque suscettibili di indurre in errore, sia che discendano dall'omissione di informazioni dovute, salvo che dia prova di avere adoperato la diligenza necessaria ad assicurare la correttezza e completezza delle informazioni di cui all'articolo 23, comma 3 del Decreto Fintech.

Linea Guida n. 14 – Distribuzione di Fondi Italiani DLT

1. Nell'attività di distribuzione di Fondi Italiani DLT – fermi restando i presìdi previsti dalla pertinente disciplina e avendo cura di monitorare e di allinearsi costantemente all'evoluzione normativa e regolamentare o alle eventuali raccomandazioni, individuali o di sistema, delle Autorità di Vigilanza – si raccomanda di valorizzare le peculiarità che caratterizzano tali Fondi e, in particolare, di curare nel modo più scrupoloso possibile l'informativa da rendere alla clientela che intenda acquistare Fondi Italiani DLT, al fine di illustrare le peculiarità del processo di sottoscrizione e rimborso di tali Fondi e dei relativi rischi, anche utilizzando le informazioni riportate nell'allegato 7.

2. Restano fermi gli obblighi dei soggetti destinatari della disciplina antiriciclaggio.



ALLEGATO 1 PRINCIPI DI VALUTAZIONE DELLE CRIPTO-ATTIVITÀ

Ai fini della valutazione delle Cripto-attività detenute dal Fondo, i Gestori applicano, ove compatibile, quanto previsto dal Titolo V, Capitolo IV, Sezione II del Regolamento sulla Gestione Collettiva del Risparmio.

Le Cripto-attività sono valutate in base al prezzo più recente rilevato sul mercato di riferimento, eventualmente rettificato anche sulla base di altri elementi oggettivi di giudizio disponibili, compresa l'eventuale valutazione degli stessi effettuata da esperti indipendenti. Ai fini della corretta valutazione delle Cripto-attività, si raccomanda di:

- i. effettuare la valutazione delle Cripto-attività al prezzo osservato su almeno tre piattaforme o sedi di negoziazione autorizzate;
- ii. analizzare qualsiasi interruzione dell'attività sulla piattaforma o sulla sede di negoziazione che possano influire sulla valutazione;
- iii. adottare criteri specifici per la valutazione del prezzo in termini di fonti riconosciute, modelli di negoziazione superiori alla media, volume e precisione decimale applicata;
- iv. nel caso in cui il valore delle Cripto-attività sia correlato a un paniere di attività, svolgere una due diligence anche sul sottostante e, quando possibile, effettuarne la relativa valutazione secondo i criteri previsti dalla normativa per la specifica tipologia di asset.

Con specifico riguardo al pricing degli strumenti finanziari DLT, il Gestore considera anche l'impatto che eventi avversi sui registri distribuiti o sulle infrastrutture di mercato DLT (es. inefficienze della DLT, mutamento del quadro normativo, evoluzione della tecnologia e conseguente obsolescenza della tecnologia fino a quel momento utilizzata) possono produrre sulla negoziabilità o più in generale sul valore degli strumenti finanziari DLT.



**ALLEGATO 2
PROCESSO DI VALUTAZIONE E GESTIONE
DEI RISCHI RELATIVI ALL'UTILIZZO DELLA DLT**

La DLT presenta possibili problemi di sicurezza e privacy, riscontrabili a livello di rete, di nodo, di Smart Contract, e di utente. Tali rischi, corredati dai relativi esempi di tecniche di mitigazione, sono descritti nel “Blockchain Framework and Guidance” pubblicato da ISACA, al quale si rinvia. Di seguito si riporta una lista esemplificativa e non esaustiva.

A) Rischi a livello di infrastruttura/rete

1. Attacco 51%: l’attacco 51% è un attacco che consente all’aggressore di prendere il controllo della rete e di poter potenzialmente eseguire operazioni malevoli (es. double spending, cioè la doppia spesa della stessa unità di criptovalute, oppure l’inserimento di transazioni invalide).

Tecniche di mitigazione:

- Monitorare e garantire che i validatori della rete siano il più possibile decentralizzati e distribuiti geograficamente, così che nessuna singola entità possa prendere il controllo di almeno il 51% del tasso di validazione della rete.
- Valutare attentamente gli algoritmi di consenso utilizzati (alcuni algoritmi, come la proof of stake, potrebbero mitigare questo rischio adottando soluzioni come lo slashing, ovvero le penalità per eventuali attori malevoli).
- Richiedere un certo numero di conferme prima dell’accettazione finale della transazione.

2. Attacco Eclipse: un attacco Eclipse cerca di isolare il nodo vittima bloccandone l’accesso ai nodi adiacenti, per poi ingannare il nodo vittima con false informazioni sulle transazioni.

Tecniche di mitigazione:

- Aumentare il numero di peer connessi e la randomizzazione della selezione dei nodi.
- Prevedere un whitelisting di nodi fidati.
- Favorire peer con una storia di connessioni riuscite più lunga rispetto ai nodi scoperti di recente.
- Utilizzare alcuni dei peer meno recenti come ancore al riavvio del nodo.

3. Attacco Denial of Service (DoS): questo tipo di attacco influisce sulla capacità della blockchain di elaborare i blocchi, eseguire gli Smart Contract o abilitare gli utenti ad interagire con la blockchain. Esistono diversi tipi di attacchi DoS, come, ad esempio il flooding della rete con transazioni fantasma.

Tecniche di mitigazione:

- Utilizzare un sistema di filtraggio preventivo che impedisca alle transazioni sospette di raggiungere la fase di creazione del blocco.
- Utilizzare un ampio pool di creatori di blocchi.
- Utilizzare un sistema di commissioni dinamico, che rende sempre più costoso perpetrare l’attacco man mano che aumenta la congestione della rete.

4. Attacco Sybil: tale attacco mira a corrompere una rete peer-to-peer formando diverse identità false.

Tecniche di mitigazione:

- Richiedere agli aggressori di bloccare o spendere una quantità significativa di risorse in modo da rendere costosa la messa in opera dell’attacco (es. potenza computazionale nel caso del PoW o stake nel caso di PoS).
- Introdurre sistemi di identità digitale o di reputazione.

5. BGP Hijacking o attacco di Routing: l'aggressore pubblicizza brevi percorsi tra due segmenti di rete contenenti nodi, consentendo al traffico tra questi nodi di fluire attraverso l'aggressore e abilitano quest'ultimo a isolare le due parti della rete e a ritardare l'elaborazione delle transazioni.

Tecniche di mitigazione:

- Utilizzare nodi multihomed (nodi con connessioni Internet a due segmenti diversi).
- Utilizzare percorsi noti e affidabili per comunicare con i nodi di altri segmenti.
- Utilizzare comunicazioni crittografate e autenticate.

B) Rischi a livello di smart contract

In generale una best practice spesso utilizzata in ambito blockchain e DLT è quello di far svolgere un audit agli smart contract utilizzati da parte di una società esterna per ogni nuovo smart contract o per gli aggiornamenti dello stesso. Questa attività è diventata quasi uno standard de facto per le principali applicazioni in ambito blockchain e permette di mitigare notevolmente molti dei rischi associati agli smart contract.

Di seguito sono quindi riportati i principali:

1. Controllo degli accessi: qualora non venga gestito correttamente l'accesso alle funzioni amministrative dello Smart Contract l'aggressore può accedervi creando potenziali danni per l'organizzazione.

Tecniche di mitigazione:

- Assicurare che uno Smart Contract sia inizializzato correttamente per mantenere la proprietà del contratto.
- Verificare che il chiamante della funzione sia il proprietario del contratto prima di eseguire le funzioni destinate al proprietario del contratto.
- Utilizzare un wallet multifirma come proprietario del contratto in modo da avere maggiori tutele in caso di furto delle chiavi.

2. Default Visibility: Gli aggressori sfruttano chiamate di funzioni pubbliche definite in modo errato e destinate a chiamate interne per manipolare tali funzioni.

Tecniche di mitigazione:

- Indicare esplicitamente l'identificatore di visibilità per la funzione.
- Monitorare le chiamate di funzione utilizzando i blockchain explorers applicabili.
- Rendere la visibilità il più possibile limitata e coerente con l'uso previsto delle funzioni richiamate.

3. Rientranza: un attacco di questo tipo avviene quando un contratto effettua una chiamata esterna ad un altro smart contract prima di aver completato i propri aggiornamenti di stato; il contratto chiamato richiama a sua volta il contratto chiamante (rientranza) con la possibilità di manipolare il suo stato in modi non previsti.

Tecniche di mitigazione:

- Osservare il design pattern degli Smart Contract checks-effects-interactions: per un maggior livello di sicurezza è necessario anzitutto effettuare i controlli sulle condizioni, poi applicare gli effetti sullo stato e infine effettuare le interazioni con i contratti esterni.
- Limitare la quantità di destinata alle chiamate esterne.

- Utilizzare una re-entrancy Guard (es. quella offerta dalla libreria di OpenZeppelin) ovvero un modificatore che assicura che una funzione non venga chiamata ricorsivamente.

4. Overflow/Underflow di numeri interi: una condizione di overflow o underflow si verifica quando viene eseguita un'operazione che richiede a una variabile di dimensioni fisse di memorizzare un numero fuori dal proprio intervallo. Gli aggressori si basano sulle manipolazioni di overflow e underflow per aggirare i controlli condizionali e alterare i calcoli matematici, come i pagamenti, a loro vantaggio.

Tecniche di mitigazione:

- Utilizzare un'implementazione matematica sicura o librerie matematiche affidabili.
- Eseguire la validazione degli input per garantire che gli input dell'utente abbiano il tipo di dati corretto e rientrino nei valori limite inferiori e superiori appropriati.

5. Manipolazione del timestamp: gli aggressori possono manipolare il timestamp di un blocco quando questo parametro viene utilizzato nel codice di uno Smart Contract.

Tecniche di mitigazione:

- Evitare di assegnare un timestamp di blocco a una variabile di uno Smart Contract.
- Verificare che i nodi siano tenuti a sincronizzare data e ora con un provider di tempo universale, e ad assicurarsi che il blocco estratto soddisfi la soglia richiesta.

6. Bad Randomness: qualsiasi meccanismo che generi numeri pseudo-casuali sulla blockchain deve essere esaminato a fondo per individuare eventuali implementazioni errate.

Tecniche di mitigazione:

- Utilizzare i migliori generatori casuali che derivano da oracoli o servizi casuali esterni.

7. Front-running: in un attacco front-running, l'aggressore duplica la transazione pendente contenuta nella mempool e paga gas fee più elevate per annullare la transazione originale.

Tecniche di mitigazione:

- Ove possibile, utilizzare un approccio commit-reveal, riducendo così la capacità di un osservatore di fare front-running rispetto a tale transazione.

8. Denial of Service (DoS): in un attacco DoS, l'aggressore manipola una o più condizioni (blocco di funzioni variabili), disabilitando lo Smart Contract.

Tecniche di mitigazione:

- Utilizzare expert code review e user testing in una rete di prova con valutazione delle prestazioni o ottimizzazione delle gas fee.

9. Mancata validazione dell'input: quando non viene eseguita la validazione dell'input, i valori fuoriescono dall'intervallo previsto e possono causare problemi nello Smart Contract.

Tecniche di mitigazione:

- Assicurare che le tipologie di dati siano previste prima di incorporarne l'uso nelle funzioni dello Smart Contract.

10. Lettura dopo la scrittura/gestione scorretta dell'operazione asincrona: una funzione dello Smart Contract può eseguire un'operazione di scrittura per aggiornare una variabile di stato, ma leggere il valore aggiornato senza aver effettuato un aggiornamento asincrono.

Tecniche di mitigazione:

- Assicurare che le variabili di stato globali siano aggiornate prima dell'uso.

C) Rischi a livello di utente

1. Truffe riguardo falsi scambi di criptovaluta, Wallet, Airdrop e Hard Fork: queste truffe attirano le vittime attraverso tecniche di social engineering per rendere i siti web fraudolenti apparentemente credibili.

Tecniche di mitigazione:

- Effettuare ricerche approfondite su tutti i download, gli airdrop e le hard fork.
- Controllare attentamente l'oggetto prima di approvare una firma all'interno del wallet e verificare sempre gli indirizzi dei contratti con cui si sta interagendo e la tipologia di azione che si sta effettuando

2. Exploits dei Wallet: il Wallet può essere vulnerabile a causa di difetti di progettazione, configurazione errata da parte dell'utente, o file di archiviazione delle chiavi che sono stati lasciati in locale dopo la rimozione del software.

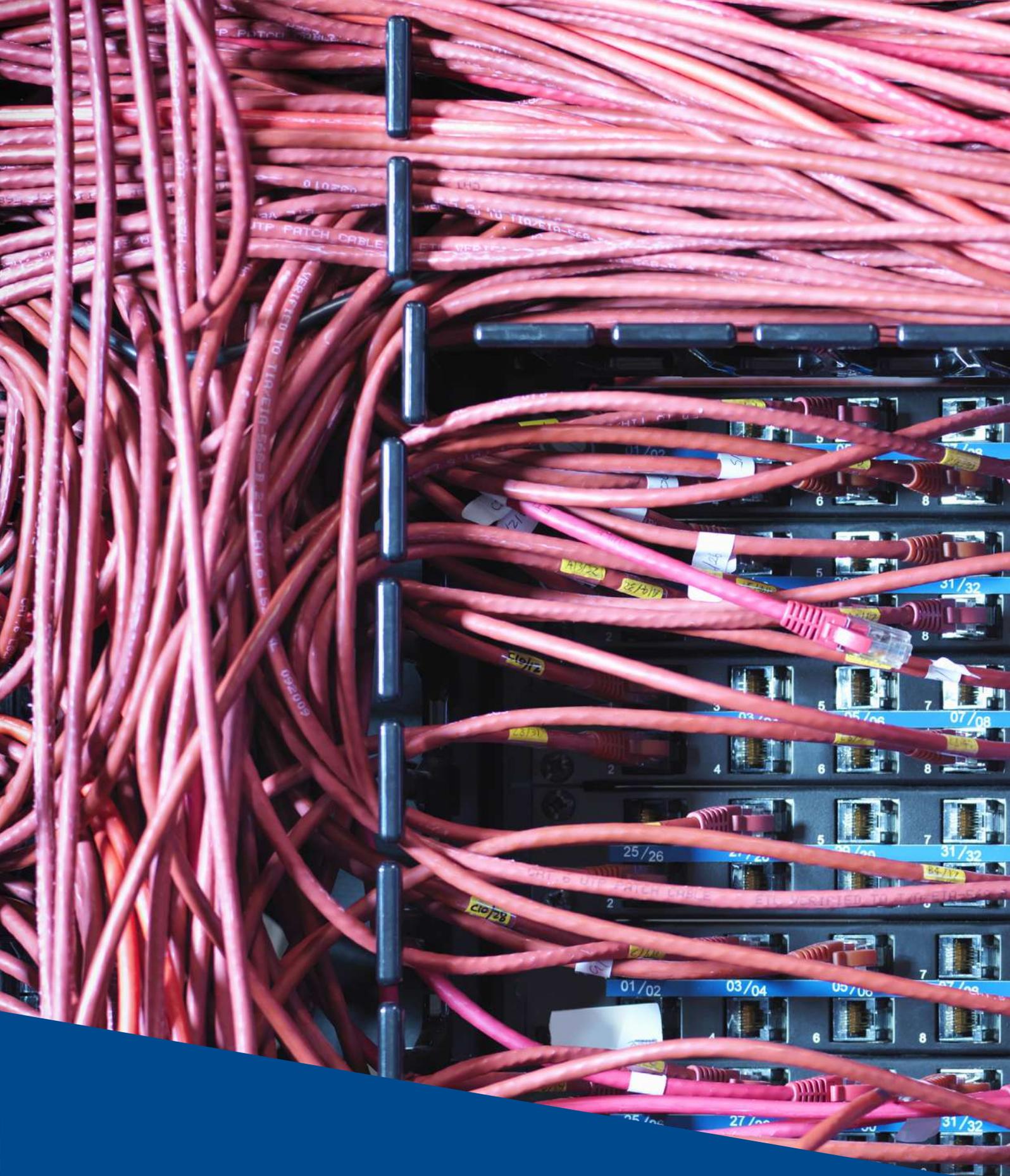
Tecniche di mitigazione:

- Cercare fonti autorevoli per assicurarsi che la versione del Wallet installata non presenti vulnerabilità note.
- Abilitare la crittografia della memoria locale non appena il Wallet viene installato.
- Non salvare la seedphrase in file locali non cifrati.

3. Scambio di SIM: attraverso lo scambio di SIM gli aggressori cercano di ottenere l'accesso ai telefoni cellulari, da cui gli utenti effettuano l'autenticazione multifattoriale per il login ai portafogli web.

Tecniche di mitigazione:

- Richiedere ulteriori livelli di verifica.
- Non utilizzare il numero di cellulare per gli SMS come strumento di autenticazione.



ALLEGATO 3 PRESIDI DI SICUREZZA NELLA GESTIONE DEGLI ASSET CRITTOGRAFICI

Il presente Allegato intende fornire indicazioni sugli aspetti chiave che si raccomanda di tenere in considerazione per mitigare i rischi di sicurezza legati alla gestione degli asset crittografici per l'accesso agli Strumenti finanziari DLT. A tal fine si raccomanda di definire politiche e procedure interne in materia di gestione degli asset crittografici, calibrandole in funzione del proprio ruolo e della significatività degli asset trattati.

Per asset crittografici si intendono sia le “chiavi” a disposizione del Responsabile di registro per gestire gli Smart Contract a supporto dell'operatività dei Fondi, sia i Wallet degli investitori che i Wallet che detengono la proprietà di cripto-attività oggetto di investimento.

Quanto di seguito è tratto dal CryptoCurrency Security Standard (CCSS), uno standard che si focalizza sulle buone pratiche di gestione della sicurezza degli asset crittografici a livello enterprise. Gli aspetti illustrati nel seguito costituiscono un complemento (ma non sostituiscono) le buone prassi indicate negli standard di riferimento in ambito information security (quale ad esempio l'ISO 27001) o in ambito sicurezza dei sistemi di pagamento (quale ad esempio il PCI). Per un elenco di maggior dettaglio dei presidi associati agli aspetti riportati di seguito, si rimanda allo standard CCSS.

A. Gestione degli asset crittografici

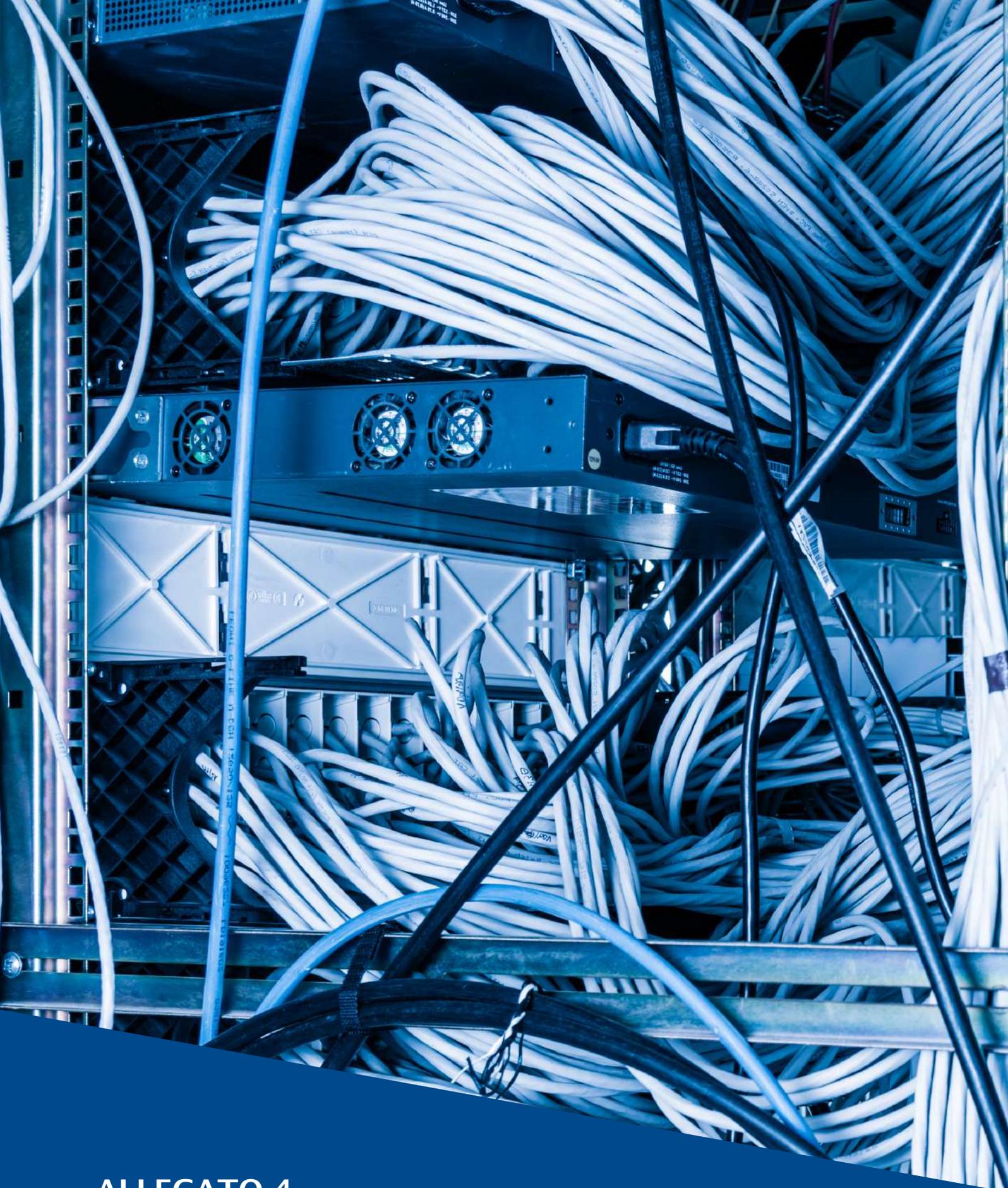
- **Generazione di chiavi crittografiche e semi che verranno utilizzati all'interno di una DLT:** la creazione sicura di chiavi crittografiche/seed richiede per essere sicura, la riservatezza nonché l'adozione di numeri imprevedibili. La riservatezza è necessaria per garantire che le chiavi/seed appena creati non vengano letti/copiati da soggetti non autorizzati. Sono necessari numeri non deterministici e imprevedibili per garantire che la chiave appena creata non possa essere indovinata o determinata da una parte non autorizzata.
- **Creazione dei Wallet:** i Wallet vengono creati utilizzando metodologie di firma digitale che possono richiedere la firma da parte di una singola chiave, la firma da parte di più chiavi o un numero minimo di firme da più chiavi. Inoltre, i Wallet possono essere creati individualmente (comunemente indicati come Wallet JBOK, o “Just a Bunch of Keys”) o in modo deterministico, mediante la creazione di un insieme di indirizzi / coppie di chiavi da un singolo seme master. La sicurezza nella creazione del Wallet è determinata dall'integrità del Wallet rispetto a vari rischi quali la perdita, il furto o la compromissione della chiave e dalla riservatezza del Wallet che renderebbe difficile associare un portafoglio a un particolare attore.
- **Storage delle chiavi:** allocando le chiavi del portafoglio in più posizioni geografiche, i rischi associati a interruzioni locali delle attività (ad esempio, incendi, inondazioni, terremoti, effrazioni) non influiscono sulla capacità dell'organizzazione di usare le chiavi.
- **Uso delle chiavi:** l'adozione di misure di sicurezza nell'uso di chiavi crittografiche e/o di semi mira a salvaguardare la riservatezza delle chiavi private a fronte di una serie di rischi, tra cui malware e insider malintenzionati che utilizzano il loro accesso autorizzato per inviare transazioni non autorizzate. Occorre considerare tali rischi anche se derivanti dall'utilizzo dei backup delle chiavi, che vengono utilizzati solo nel caso in cui la chiave primaria sia persa/danneggiata/inaccessibile.
- **Policy in caso di compromissione delle chiavi (KCP – key compromise policy):** l'esistenza e l'adozione di un protocollo che detta le azioni che devono essere intraprese nel caso in cui si ritenga che una chiave crittografica/seed o il suo operatore/detentore siano stati compromessi. Le organizzazioni devono essere preparate ad affrontare una situazione in cui una chiave privata sia diventata determinabile o distrutta, anche

potenzialmente. Esempi di quando la KCP verrebbe invocata includono ad esempio l'identificazione della manomissione di un sigillo antimanomissione posto sul materiale crittografico, l'apparente scomparsa di un operatore i cui amici e familiari più stretti non possono identificare dove si trovino, l'effettuazione di operazioni non usuali o la ricezione di comunicazioni che indichino in modo credibile che un operatore o una chiave sia probabilmente a rischio di essere compromesso. L'esecuzione dei protocolli KCP deve avvalersi di canali di comunicazione approvati per garantire che i messaggi KCP siano inviati/ricevuti solo da attori autenticati.

- **Policy e procedure di concessione e revoca dei keyholder:** ossia dell'accesso a chiavi crittografiche o seed dell'organizzazione o dell'utente finale da parte di utenti privilegiati (superutenti dei sistemi informatici). La gestione impropria di assunzioni o dimissioni del personale introduce il rischio che l'accesso agli account privilegiati permanga a fronte di dimissioni o cambio ruolo, oltre alla possibilità che permanga la possibilità di firmare certe transazioni con chiavi non revocate.

B. Operations

- **Test/audit di sicurezza:** compresi gli audit indipendenti dei sistemi di sicurezza, dei controlli tecnici e delle policy che proteggono il sistema informativo da tutte le forme di rischio, nonché i vulnerability e penetration test progettati per identificare le vulnerabilità dei controlli in essere.
- **Policy di sanitizzazione dei dati:** ossia la rimozione delle chiavi crittografiche dai supporti digitali in caso di dismissione volontaria del supporto. A causa del modo in cui i file system allocano i dati sui supporti digitali, le tecniche forensi digitali possono essere impiegate per leggere vecchi dati che sono stati precedentemente cancellati. Una corretta sanitizzazione dei supporti digitali garantisce la corretta rimozione di tutte le chiavi, eliminando il rischio di perdita di informazioni da dispositivi dismessi come server, unità disco rigido e archivi rimovibili.
- **Audit log:** gli audit log sono uno strumento fondamentale nell'ambito della sicurezza informatica, in quanto riportano l'elenco sequenziale delle attività svolte su uno specifico sistema. In caso di comportamenti imprevisti o incidenti di sicurezza, gli audit log possono aiutare gli investigatori a capire le cause degli incidenti e come risolvere le incongruenze per riportare il sistema informativo a uno stato coerente.



ALLEGATO 4
INDICAZIONI SULL'OPERATIVITÀ ON-CHAIN
DEI FONDI ITALIANI DIGITALI

Il presente Allegato costituisce uno strumento di ausilio per gli operatori tecnologici al fine di individuare le funzioni che ciascuna delle entità coinvolte nell'operatività dei Fondi Italiani Digitali potrà svolgere all'interno della DLT e, soprattutto, al fine di stabilire le operazioni che possono essere codificate su uno o più Smart Contract.

A tal riguardo giova anzitutto rilevare che gli standard esistenti in tema di Smart Contract (ERC nel caso di Ethereum⁷) definiscono linee guida per creare specifici Smart Contract. Tuttavia, ogni standard non è necessariamente legato ad un singolo Smart Contract. Infatti, uno standard può emergere da un insieme di Smart Contract interconnessi che operano in sinergia per realizzare una funzionalità complessa. L'implementazione di standard come l'ERC-20 assicura che i token siano facilmente negoziabili e possano interagire senza incongruenze con qualsivoglia applicazione che rispetti lo stesso standard, fornendo un insieme di regole, funzioni e proprietà uniformi. Queste funzioni, come ad esempio `totalSupply`, che fornisce l'ammontare totale di token, o `transfer(address to, uint256)`, destinata al trasferimento di token, rappresentano le operazioni cardinali che il token può effettuare. Inoltre, ci sono proprietà come `name`, `symbol` e `decimals` che forniscono informazioni basilari riguardo al token, come il suo nome, simbolo e il numero di decimali che supporta. Parallelamente alle funzioni, gli eventi svolgono un ruolo cruciale, operando come segnalatori o "notifiche" emesse dallo Smart Contract in risposta a determinate azioni, quali l'evento `Transfer`, che si manifesta con il trasferimento di token tra indirizzi. L'ERC-20, pur essendo lo standard prevalente per gli utility token, ha alcune limitazioni nell'affrontare le specifiche esigenze dei security token e della conseguente conformità normativa. Nella comunità Ethereum sono stati introdotti nuovi standard che mirano a risolvere queste problematiche come ad esempio ERC-1400, ERC-1404 e ERC-3643 per menzionarne alcuni. Questi token, oltre alle funzioni base dell'ERC-20, includono funzionalità aggiuntive come restrizioni sul trasferimento, possibilità di caricare della documentazione associata e una gestione più selettiva delle identità con un sistema di whitelisting.

Nel contesto di un Fondo con quote emesse in forma digitale, il token fungibile emesso deve possedere le seguenti proprietà minime per essere identificato correttamente e per rispettare le modalità di funzionamento dei Fondi:

- Nome: caratteristica descrittiva per identificare il token che rappresenta le quote del Fondo;
- Decimali del token: in misura di tre, per permettere il frazionamento millesimale del token;
- Chain ID: identificativo della rete su cui viene scambiato il token;
- Address: indirizzo dello Smart Contract che gestisce il token;
- ISIN CODE: codice internazionale che identifica univocamente gli strumenti finanziari;
- Trasferibilità tra soggetti indicati e abilitati: per permettere la circolazione solo fra investitori conosciuti e profilati;
- Identificazione di un owner e di possibili ruoli aggiuntivi: al fine di avere un maggior presidio sull'applicazione e garantirne la sicurezza, è opportuno definire un owner. L'owner dello smart contract è l'unico autorizzato ad accedere a funzioni critiche dello stesso. L'owner può essere ad esempio l'unico in grado di emettere nuovi token o revocare token già emessi, blacklistare utenti, etc. Questo concetto fornisce un controllo degli accessi essenziale,

7. In questo contesto viene citata la blockchain Ethereum in quanto ad oggi la maggior parte degli use case di mercato e degli utenti operano su blockchain EVM compatibili. Vi sono tuttavia altre tipologie di blockchain che utilizzano diversi linguaggi di programmazione e standard differenti. Rimane comunque ferma la possibilità di utilizzo di bridge per abilitare l'interoperabilità tra diverse blockchain

impedendo chiamate non autorizzate a funzioni cruciali e permettendo futuri aggiornamenti. Questo ruolo può coincidere con il Responsabile del Registro o invece essere ricoperto dal Gestore o dal Depositario, in alternativa possono essere valutati ruoli diversi o condivisi (anche svolti da più attori). Ogni soluzione deve comunque essere valutata attentamente all'interno di ogni progettualità secondo le caratteristiche della stessa;

- Possibilità da parte dell'owner di forzare operazioni: per esercitare on-chain alcuni vincoli. Le funzioni critiche devono essere esercitabili solo dall'owner.

Oltre a queste proprietà di base, è necessario determinare anche le funzioni da codificare all'interno di uno o più Smart Contract che definiranno lo standard.

In questa prospettiva, si riporta qui di seguito una tabella che si compone di tre colonne:

- i. nella prima colonna sono riportati i compiti, le azioni e le responsabilità "tradizionali" dei soggetti coinvolti nella catena del valore di un Fondo aperto;
- ii. nella seconda colonna è riportata, per ognuno di questi compiti, azioni e responsabilità, il ruolo della tecnologia. In particolare, sono state usate le seguenti classificazioni:
 - "Da disegno" quando il compito/azione/responsabilità è in qualche modo garantito direttamente dalla natura tecnologica del registro;
 - "Codificabile nello Smart Contract" quando è possibile automatizzare o facilitare il compito/azione tramite Smart Contract;
 - "Parziale" nel caso in cui non sia possibile svolgere tutto on-chain, ma siano necessari anche dei passaggi/verifiche off-chain;
 - "No" quando la tecnologia non è coinvolta in quella parte del processo;
 - "Incompatibile con la natura della circolazione digitale", come ad esempio l'emissione in forma cartolare della quota;
- iii. nella terza colonna invece sono riportate alcune indicazioni sull'utilizzo della tecnologia.

Le indicazioni rappresentano le principali attività relative Fondi Italiani Digitali ovvero, a seconda dei casi, ai Fondi Italiani Cripto o ai Fondi Italiani DLT, e sono da considerarsi allo stato attuale della tecnologia e del quadro normativo. In caso di evoluzioni, è possibile che alcuni adempimenti necessariamente da svolgere oggi parzialmente o totalmente off-chain siano possibili anche on-chain. Valutazioni su ulteriori e diverse attività od operazioni sulle quote possono essere svolte sulla base del caso specifico.

Compiti e responsabilità (tradizionali) del Gestore	Svolgimento on-chain	Note
---	----------------------	------

**Fund administration
(compiti e funzioni del Gestore):**

Calcolo del valore della quota	No	Calcolo off-chain, essendo tale calcolo effettuato su valori di mercato che non sempre transitano on-chain
Registrazione del valore della quota	Codificabile nello Smart Contract	Registrazione della quota nella catena del valore
Matching, settlement e tenuta registro ordini (che avverrebbe con "l'equivalente" tecnico della DLT)	Codificabile nello Smart Contract	Registro ordini + relative operazioni gestite da uno Smart Contract
Tenuta del libro giornale, relazione di gestione, relazione semestrale	No	Tenuta off-chain del libro giornale, relazione di gestione, relazione semestrale
Elaborazione, registrazione e comunicazione di altre informazioni (% giornalieri titoli esenti per successione, percentuale semestrale titoli white list, rating controparti, ecc.)	No	Off-chain
Assistenza a revisori/lettere di circolarizzazione	Parziale	Off-chain I revisori possono verificare il registro dei partecipanti direttamente guardando lo storico sulla DLT
Conservazione della documentazione	Parziale	Off-chain in caso di esternalizzazione On-chain tramite notarizzazione dell'hash dei documenti
Gestione flussi e datawarehouse	No	Off-chain

**Controlli di linea
(interazione con altri applicativi):**

Adempimenti AML	Parziale	Controlli da svolgere off-chain per identificazione e adeguata verifica propedeutici all'ottenimento dei token da parte dell'utente; possibilità di sfruttare i dati on-chain per agevolare il monitoraggio successivo, fermi restando gli obblighi in capo ai soggetti destinatari della disciplina antiriciclaggio
-----------------	----------	--

**Flussi informativi
(interazione con altri applicativi):**

Segnalazioni di vigilanza	No/Parziale	<p>Off-chain, le segnalazioni di vigilanza devono essere eseguite in maniera tradizionale</p> <p>L'estrazione dei dati transazionali dalla DLT potrebbe essere d'ausilio per la creazione delle segnalazioni</p> <p>L'utilizzo di piattaforme pubbliche con registro delle transazioni trasparente potrebbe inoltre agevolare il controllo sulle operazioni svolte</p>
Tenuta dell'Archivio Unico e Segnalazioni SARA e Segnalazioni 1° livello che potrebbero portare all'invio di una SOS (i.e. inattesi)	No	<p>Off-chain, i flussi segnaletici vengono gestiti in maniera tradizionale</p> <p>Potrebbe esserci la possibilità di inserire in blacklisting eventuali address segnalati</p> <p>Inoltre, l'estrazione dei dati transazionali dalla DLT potrebbe essere d'ausilio per la creazione delle segnalazioni</p>

Scambio delle informazioni, anche documentali, con il Depositario, il Distributore, i clienti e ogni altro soggetto della catena del valore	Parziale	Off-chain, eventualmente può essere notarizzato on-chain l'hash di documenti particolarmente importanti per garantire la loro integrità
---	----------	---

Interventi sulla circolazione delle quote dei fondi (compiti e funzioni; eventi esterni alla DLT; elaborazione dati):

Sospensione delle sottoscrizioni o dei rimborsi delle quote	Codificabile nello Smart Contract	Flag sul contratto settabile dall'owner che mette in pausa queste funzioni
Applicazione di altri strumenti di gestione della liquidità	Codificabile nello Smart Contract	Anche i più recenti LMT previsti nell'evoluzione normativa (UCITSD/AIFMD review) potrebbero essere inseriti all'interno dello Smart Contract (ad esempio tramite l'inserimento di funzioni per la "gestione" delle sottoscrizioni/ rimborsi)
Liquidazione in caso di assenza dei presupposti e delle condizioni della sottoscrizione, anche in caso di circolazione successiva alla prima emissione	Codificabile nello Smart Contract	Token revocabili da owner / burn o forceback
Apposizione di vincoli	Codificabile nello Smart Contract	Da definire in fase di emissione

Interazione con altre DLT	Codificabile nello Smart Contract	Conferimento beni, tra i quali potrebbero rientrare gli strumenti finanziari DLT per la sottoscrizione di quote del Fondo Cripto
---------------------------	-----------------------------------	--

Operazioni straordinarie tra OICR, sia nel caso di OICR Italiani Digitali e sia quando solo uno o alcuni dei fondi considerati sono Fondi Italiani Digitali (eventi esterni alla DLT):

Fusione/scissione dei Fondi, consentendo al Gestore di impostare la data a partire dalla quale l'operazione è efficace (anche sulla piattaforma)	Codificabile nello Smart Contract	Minting quote nuovo Fondo riscattabili previo burn dei token precedenti
Conversione della quota in quote di altri Fondi dello stesso Gestore	Codificabile nello Smart Contract	Può essere offerta on-chain nelle condizioni di minting e burn delle quote
Controllo della legittimità delle operazioni da parte del Depositario del Fondo	Parziale	Operazioni consultabili nello storico della DLT

Modifiche al regolamento/statuto del Fondo (eventi esterni alla DLT; elaborazione dati):

Il Gestore deve essere in grado di applicare le regole previste dal Regolamento sulla gestione collettiva del risparmio (in particolare, comunicazioni individuali, sospensione, diritto di rimborso senza applicare commissioni di rimborso)	No	Off-chain
Adempimenti in materia fiscale (cfr. infra) (compiti e funzioni del Gestore)	No	Off-chain

Protezione dei dati personali	Parziale	<p>Identificazione off-chain dei dati personali con notarizzazione e inserimento hash di documenti legati a questi (sulla blockchain non è presente l'identità dell'investitore ma solo l'address legato al suo Wallet)</p> <p>Il layer blockchain è solo una delle componenti del sistema; si fa uso anche di database distribuiti. La maggior parte delle informazioni riservate sono mantenute nel database e tramite microservizi, alcuni basati su Zero Knowledge Proof, vengono collegate con il layer blockchain</p>
-------------------------------	----------	---

Altri adempimenti di competenza/implementazione a carico del Gestore (compiti e funzioni del Gestore; eventi esterni alla DLT):

Regolamento dei contratti, compreso l'invio di certificati	No	Off-chain
Custodia e amministrazione di azioni o quote di organismi di investimento collettivo	Da disegno	Possibile offrire servizio di custodia degli asset digitali per conto della clientela (anche con supporto di terzi - e.g. Key custody provider)
A seguito della relativa modifica del regolamento, sostituzione della SGR con "passaggio" alla nuova di tutte le prerogative senza alcuna soluzione di continuità	No	
Fondo	Svolgimento on-chain	Note
Apposizione di criteri di restrizione sui partecipanti	Parziale	Valutazione Off-chain (KYC/ KYB) e white-listing degli address abilitati on-chain

Compiti e responsabilità del Depositario	Svolgimento on-chain	Note
--	----------------------	------

Gestione delle disponibilità liquide e distribuzione dei proventi:

Il Depositario detiene le disponibilità liquide del Fondo	Codificabile nello Smart Contract / Da disegno	I token depositati nel Fondo vengono inviati al Depositario
Si occupa della distribuzione dei proventi in proporzione al numero di quote possedute da ogni partecipante (da definire il mezzo di pagamento)	Codificabile nello Smart Contract	
Nel caso in cui la liquidità del Fondo non sia affidata direttamente al Depositario, questi assicura un adeguato monitoraggio dei flussi di cassa	Parziale	I flussi di cassa sono disponibili pubblicamente nello storico della DLT

Emissione e Gestione dei Certificati:

Qualora il sottoscrittore abbia richiesto l'emissione del certificato di partecipazione, il Depositario controlla le cedole e, nel caso di certificati nominativi, verifica l'integrità dell'intero certificato e delle cedole correlate	Incompatibile con la natura della circolazione digitale	Non ci saranno certificati "fisici", il token è rappresentativo della quota stessa
A partire dal primo giorno lavorativo successivo al giorno di regolamento delle sottoscrizioni, mette a disposizione dei partecipanti i certificati nei luoghi previsti dalla scheda identificativa	Incompatibile con la natura della circolazione digitale	Non ci saranno certificati "fisici", il token è rappresentativo della quota stessa

Flussi informativi:

Il Depositario scambia informazioni, sia documentali che non documentali, con vari stakeholder, tra cui il gestore, il distributore e i clienti	Parziale	Alcune informazioni relative ai token e alle loro movimentazioni sono visualizzabili direttamente sul registro on-chain
---	----------	---

Operazioni e Controlli:

Ha la responsabilità di custodire gli strumenti finanziari a esso affidati, verificando la proprietà e mantenendo le registrazioni di altri beni	Da disegno	Il Depositario custodisce gli strumenti finanziari ad esso affidati all'interno del proprio Wallet
Il Depositario verifica la legittimità delle operazioni come la vendita, emissione, riacquisto, rimborso, annullamento delle quote del Fondo, nonché della destinazione dei redditi del Fondo	Codificabile nello Smart Contract	Inoltre, queste informazioni possono essere reperite consultando lo storico della DLT
Accerta la correttezza del calcolo del valore delle parti del Fondo; Accerta che nelle operazioni relative al Fondo la controprestazione sia rimessa nei termini d'uso	Codificabile nello Smart Contract	
Esegue le istruzioni impartite del Gestore che non siano contrarie alla legge, al regolamento del Fondo o alle disposizioni, agli orientamenti o ai provvedimenti emanati dalle Autorità di Vigilanza	Codificabile nello Smart Contract	

Obblighi Legali e Liquidazione:

Assicura che tutti i pagamenti fatti dagli investitori durante la sottoscrizione delle quote o azioni siano ricevuti e registrati correttamente	Da disegno	Garantito dalle transazioni salvate nello storico della DLT
Nel caso di liquidazione, collabora con il Gestore per rimborsare le quote ai partecipanti, ritirare e annullare i certificati emessi, e informare i partecipanti sui dettagli relativi alla liquidazione	Codificabile nello Smart Contract	
Le somme non riscosse entro tre mesi dalla data di inizio del pagamento sono depositate in un conto speciale intestato al Gestore	Codificabile nello Smart Contract	

È responsabile nei confronti dei Gestori e dei partecipanti per qualsiasi danno derivante da inadempimenti. In caso di perdita degli strumenti finanziari detenuti, il Depositario è tenuto a restituire gli strumenti o un importo equivalente	No	
Gestione dei mezzi di accesso in caso di sostituzione di un Depositario che aveva il controllo delle chiavi	Codificabile nello Smart Contract	L'owner dello Smart Contract può aggiornare l'indirizzo del Depositario secondo necessità
Compiti e responsabilità del Responsabile del Registro	Svolgimento on-chain	Note

Conformità del registro alle caratteristiche prescritte dal Decreto Fintech e dalle relative disposizioni attuative:

Il registro dispone dei requisiti stabiliti ai sensi dell'articolo 4 del Decreto Fintech e attribuisce alle emissioni di quote e azioni le informazioni di cui all'articolo 12, comma 6, lett. b), del medesimo Decreto	Da disegno/ Codificabile nello smart contract	Il Decreto fintech prevede che le informazioni di cui all'art. 12, (6) (b) debbano essere "rese disponibili in forma elettronica accessibile e consultabile in ogni momento, eventualmente anche per il tramite del registro medesimo". Pertanto, le informazioni potrebbero non essere direttamente garantite dalla natura tecnologica del registro
Garantisce la correttezza, la completezza e l'aggiornamento continuo delle evidenze relative alle informazioni sull'emissione	Da disegno	
Garantisce inoltre l'integrità e la sicurezza del sistema, tenendo anche conto delle esigenze di AML, in forza dell'emissione e del trasferimento delle quote digitali sulla base di titolo idoneo	Da disegno	

Il registro è strutturato in modo tale da garantire sempre continuità operativa, anche nel caso di sostituzione di alcuni attori della catena, ivi compresi momenti di gestione “condivisa” di specifici ruoli nella piattaforma (es. in caso di sostituzione del Gestore o del Depositario e relativa fase di gestione della fase transitoria di “passaggio delle consegne”): dovrebbero quindi esistere meccanismi che servano allo scopo (es. specifici smart contract)	Codificabile nello Smart Contract	I “passaggi delle consegne” sono codificabili nello Smart Contract
--	-----------------------------------	--

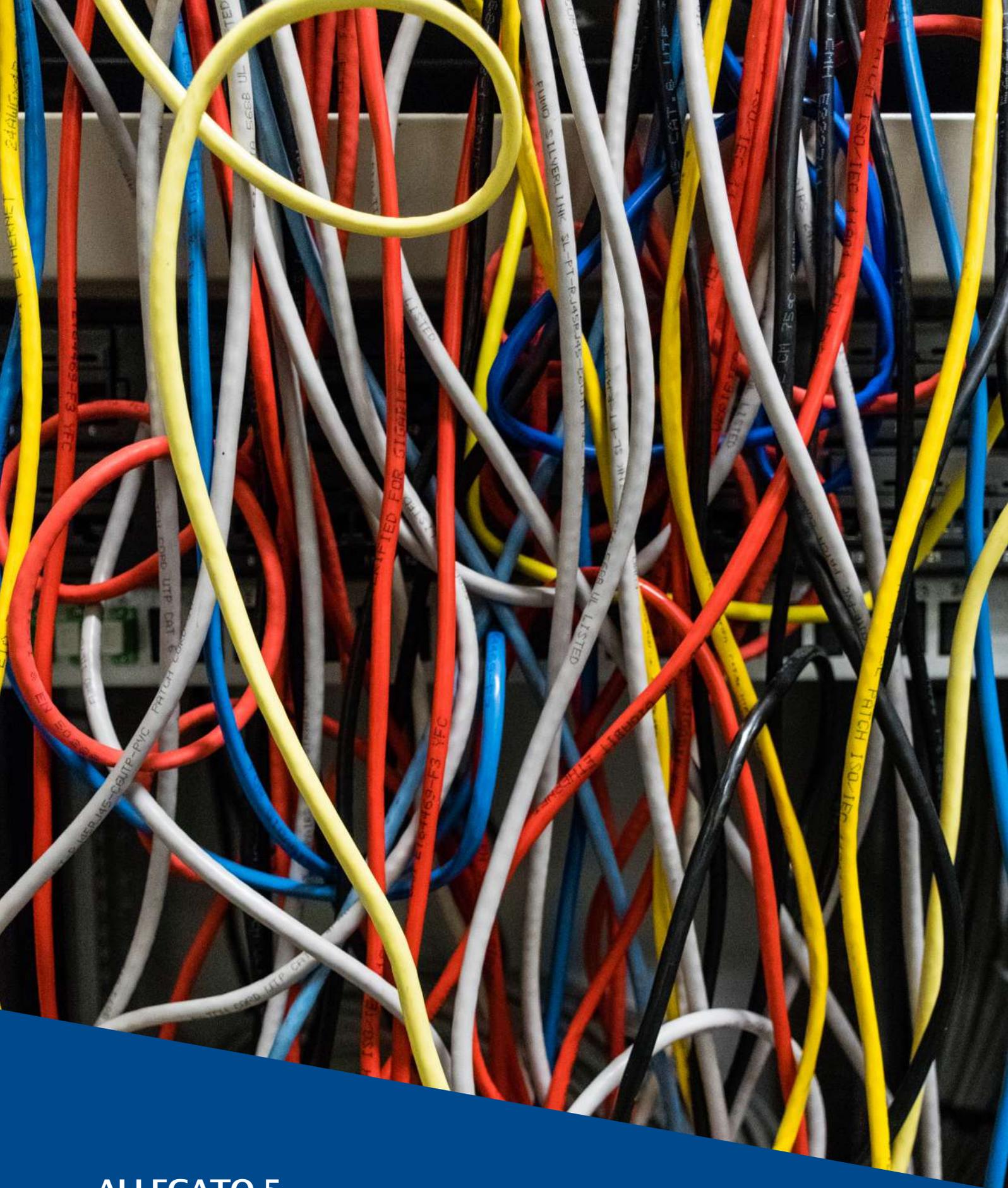
Responsabilità di controllo:

Impedisce l’uso delle quote digitali da parte di soggetti diversi da quelli legittimati	Codificabile nello Smart Contract	Trasferibilità del token ammessa solo tra soggetti identificati
Assicura la continuità operativa e il ripristino dell’attività, attraverso meccanismi e procedure adeguati che comprendano anche la messa in sicurezza esterna delle informazioni	No	
Assicura che il numero complessivo di quote digitali che costituisce una singola emissione non sia modificabile	Codificabile nello Smart Contract	La non modificabilità deve essere garantita rispetto ad interventi esterni sulla DLT e non rispetto a variazioni legate alla natura del Fondo
Assicura il rispetto delle disposizioni antiriciclaggio contenute del decreto legislativo 21 novembre 2007, n. 231	Codificabile nello Smart Contract	Lo Smart Contract può essere di ausilio nello svolgimento degli obblighi antiriciclaggio

Flussi informativi:

Rende disponibile al pubblico, in una forma elettronica accessibile e consultabile in ogni momento, un documento contenente le informazioni relative alle modalità operative del registro per la circolazione digitale e ai dispositivi a tutela della sua operatività, tra cui la strategia di transizione	Parziale	Notarizzazione on-chain hash + pubblicazione off-chain del documento
---	----------	--

Azioni dell'Investitore	Svolgimento on-chain	Note
Richiede la sottoscrizione/ rimborso delle quote del Fondo direttamente o per il tramite di un intermediario distributore che agisce in nome proprio e per conto di uno o più clienti	Codificabile nello Smart Contract	Delega on-chain prevista all'interno degli Smart Contract
Richiede il prospetto informativo	No	Off-chain
Richiede il reinvestimento dei proventi	Codificabile nello Smart Contract	All'interno dello Smart Contract potrebbero essere inserite delle funzionalità che prevedono la possibilità che i diritti amministrativi dell'investitore possano essere esercitati tramite processi di governance decentralizzata. Sarebbe infatti possibile aprire delle votazioni sulle decisioni da prendere, su cui gli investitori potrebbero esprimere la propria opinione tramite una verifica del possesso dei token che rappresentano le quote



**ALLEGATO 5
MODALITÀ DI REGOLAMENTO ON-CHAIN
DELLE OPERAZIONI DEI FONDI ITALIANI DIGITALI**

L'emissione in forma digitale di strumenti finanziari ove accompagnata dal regolamento on-chain potrebbe garantire una maggiore trasparenza, sicurezza e velocità nel regolamento delle operazioni.

L'introduzione di modalità di regolamento su una DLT richiede l'utilizzo di token rappresentativi della moneta o di soluzioni che si integrano con sistemi di pagamento tradizionali.

Gli asset di regolamento sono fondamentali per il funzionamento delle infrastrutture di mercato poiché vengono utilizzati per adempiere agli obblighi di pagamento tra i partecipanti.

In generale, la moneta di banca centrale rappresenta l'opzione più sicura per il regolamento delle operazioni finanziarie. Tuttavia, se l'adozione di modalità di pagamento tramite moneta di banca centrale, anche in forma tokenizzata, non è pratica o possibile, la scelta di utilizzare moneta di banca commerciale, anche in forma tokenizzata, o token di moneta elettronica o altre attività previste dalla normativa MiCAR utilizzabili a fini di pagamento deve comunque tener conto dell'esigenza di minimizzare e controllare attentamente il rischio di credito e di liquidità associato all'utilizzo di altre attività diverse dalla moneta di banca centrale. Gli standard internazionali (CPMI-IOSCO Principles for financial market infrastructures (PFMI) e CPMI-IOSCO Guidance on the Application of the PFMI to stablecoin arrangements) stabiliscono i criteri da considerare per determinare quando, nel caso in cui gli asset di regolamento siano emessi da un ente privato, il rischio di credito e liquidità associato possa ritenersi minimizzato e attentamente controllato e conseguentemente l'asset di regolamento in questione possa costituire un'alternativa accettabile alla moneta di banca centrale.

1. Moneta di Banca Centrale

L'Eurosistema ha recentemente avviato una sperimentazione sull'utilizzo delle nuove tecnologie per il regolamento di transazioni finanziarie wholesale tramite moneta di banca centrale. In particolare, il 13 dicembre 2023, la BCE ha lanciato una "Call for Expression of Interest", nella quale ha invitato gli stakeholders a prendere parte a Trials and Experiments, cioè a sperimentazioni di regolamento (reale o fittizio) di transazioni finanziarie, utilizzando, inter alia, modalità di regolamento DVP in moneta di banca centrale di asset digitali rappresentati su infrastruttura DLT. In particolare, i partecipanti potranno scegliere tra tre diverse soluzioni basate sull'interoperabilità tra piattaforme di mercato DLT e nuove infrastrutture di banca centrale⁸, sviluppate da tre banche centrali, e segnatamente: la TIPS Hash-Link solution, fornita dalla Banca d'Italia, la Trigger Solution, proposta dalla Deutsche Bundesbank, e la Full-DLT interoperability solution, della Banque de France.

Gli elementi di base della sperimentazione e le relative condizioni sono disponibili al 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. Il rischio di liquidità è il rischio che una controparte non abbia le risorse sufficienti per adempiere alle sue obbligazioni nei modi e tempi previsti, sebbene potrebbe essere in grado di adempiere in tali termini nel futuro. Il rischio di credito, invece, è il rischio che una controparte non riesca a soddisfare i propri obblighi di pagamento nei tempi previsti né successivamente.

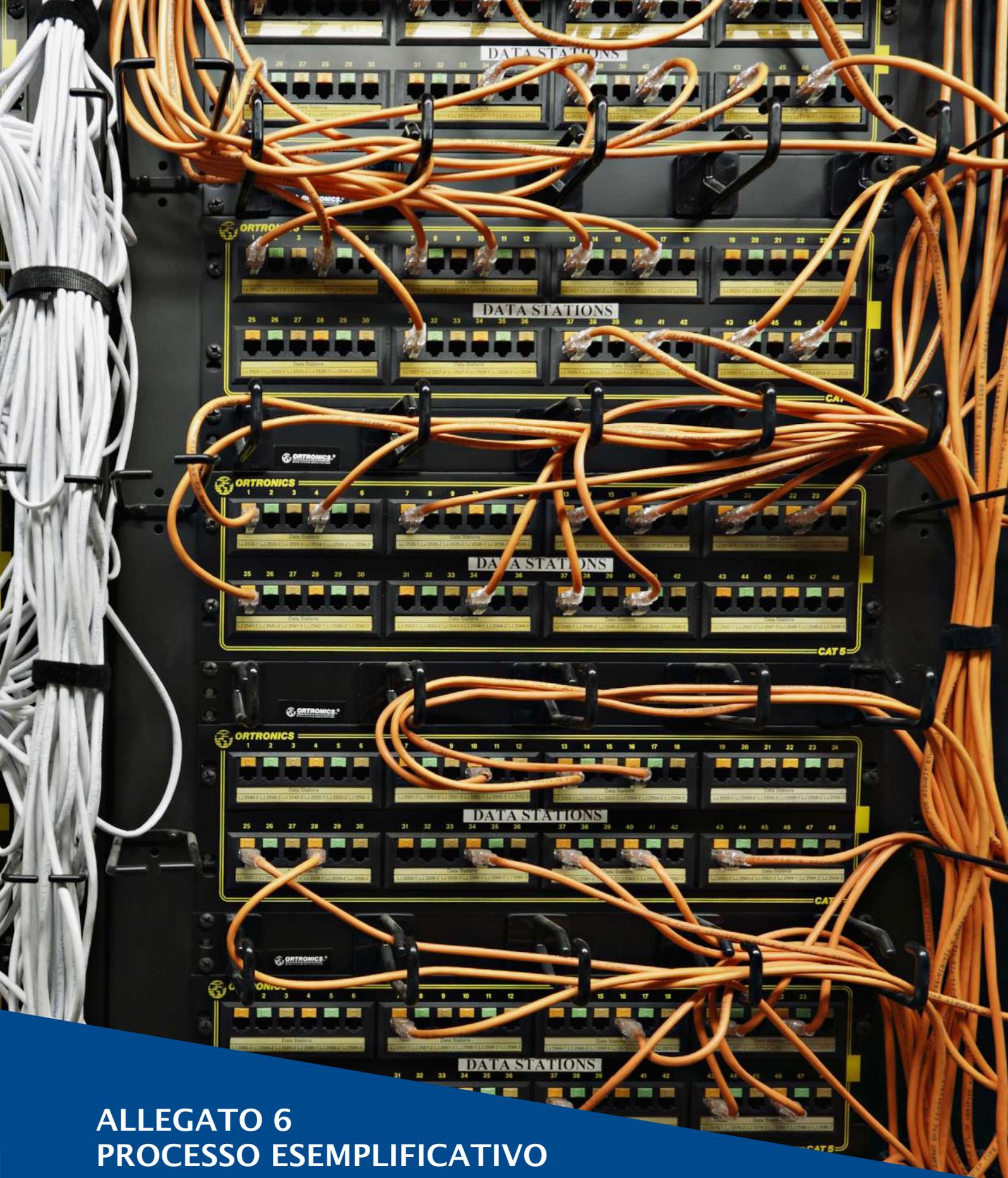
2. Token di moneta elettronica e token collegati ad attività

Il Regolamento MiCAR identifica diverse tipologie di Cripto-attività che potrebbero essere utilizzate per il regolamento delle operazioni on-chain diverse dalla moneta di banca centrale: i token di moneta elettronica (EMT) e i token collegati ad attività (ART).

2.1 I token di moneta elettronica (EMT) sono un tipo di Cripto-attività che mira a mantenere un valore stabile facendo riferimento al valore di una valuta ufficiale. Essi sono considerati moneta elettronica (art. 48, par.2, MiCAR) e sono conseguentemente da considerarsi ricompresi nella nozione di fondi (art. 3, par. 1, n.14, MiCAR). La loro funzione è «molto simile» alla moneta elettronica. Infatti, come la moneta elettronica i token di moneta elettronica sono surrogati elettronici per monete e banconote e sono «plausibilmente» utilizzabili per effettuare pagamenti (considerando 18). I token di moneta elettronica: (i) sono strumenti privati di pagamento, la cui emissione è rimessa all'attività di istituzioni finanziarie private autorizzate (Banche, IMEL); (ii) sono emessi al valore nominale al momento del ricevimento dei fondi; (iii) deve essere assicurato il rimborso al valore nominale; (iv) gli emittenti (e anche i prestatori di servizi per le cripto-attività) non possono concedere interessi o benefici di altra natura per il tempo del possesso di tali strumenti; (v) gli emittenti sono tenuti alla segregazione patrimoniale di parte dei fondi ricevuti per l'emissione dei token di moneta elettronica per assicurarne il rimborso; (vi) il sottostante di riferimento (valore rappresentato dal token) è una valuta ufficiale (moneta avente corso legale) alla cui unità di conto essi si riferiscono. Sono stati ricompresi nell'azione di sorveglianza della BCE (PISA framework).

2.2 I token collegati ad attività (ART) sono un tipo di Cripto-attività che non è un token di moneta elettronica e che mira a mantenere un valore stabile facendo riferimento a un altro valore o diritto o a una combinazione dei due, comprese una o più valute ufficiali. Gli emittenti di ART possono essere enti creditizi o soggetti previamente autorizzati da parte dell'autorità competente dello Stato membro d'origine. Al fine di prevenire i potenziali impatti negativi (effetti di sostituzione monetaria) legati all'ampia diffusione degli ART come mezzo di scambio, il Regolamento MiCAR prevede: (i) un regime di monitoraggio in itinere, con trasmissione dati su base trimestrale ad autorità competente delle transazioni associate a utilizzi come mezzo di scambio (ii) se il numero medio e il valore aggregato medio trimestrali stimati delle operazioni giornaliere associate a usi dell'ART come mezzo di scambio sono superiori, rispettivamente, a un milione di operazioni e a 200.000.000 euro, uno stop a emissione e presentazione di un piano all'autorità competente per tornare «sotto soglia».

La scelta dell'utilizzo come mezzi di scambio dei token di moneta elettronica o dei token collegati ad attività per le operazioni di sottoscrizione e rimborso di quote o azioni di fondi richiede una attenta valutazione anche tenendo conto dei seguenti profili: (i) a differenza degli EMT, gli ART sono utilizzabili come mezzi di pagamento solo entro determinate soglie e sono soggetti a un monitoraggio dell'autorità competente (v. artt. 22-23 MiCAR); (ii) al momento non è nota la valutazione che le Autorità faranno sull'ammissibilità delle due cripto attività, EMT e ART, come mezzo di regolamento in contropartita alla sottoscrizione di quote di fondi.



**ALLEGATO 6
PROCESSO ESEMPLIFICATIVO
DI SOTTOSCRIZIONE E RIMBORSO
DI QUOTE DI FONDI ITALIANI DLT
E PRIME VALUTAZIONI⁹**

Di seguito si individuano possibili modalità di sottoscrizione e rimborso “on-chain” delle quote di un Fondo aperto di diritto italiano DLT, in via non esaustiva e meramente a titolo indicativo, nel presupposto che (i) le operazioni di sottoscrizione e rimborso vengano effettuate per il tramite del Distributore (c.d. modello parzialmente intermediato); (ii) il calcolo del NAV del Fondo e la gestione dei processi di sottoscrizione e rimborso siano esternalizzati dal Gestore ad un soggetto terzo (Depositario), secondo il modello oggi prevalente sul mercato.

I processi sono distinti a seconda della modalità di regolamento delle operazioni utilizzata: regolamento in moneta di banca centrale (wholesale), da un lato, e token di moneta elettronica/ token collegati ad attività, dall'altro.

Per consentire la gestione delle operazioni di sottoscrizione e rimborso di quote del Fondo si prevede l'esecuzione dei seguenti step preliminari

- Il Gestore definisce se (i) emettere quote su un Registro tenuto da un soggetto specializzato iscritto nella sezione 4 dell'Elenco tenuto dalla Consob ovvero da un soggetto iscritto nella sezione 1 dell'Elenco tenuto dalla Consob, ovvero (ii) svolgere l'attività di Responsabile del registro con riferimento alle quote dei propri Fondi Italiani DLT (previa iscrizione nella sezione II dell'Elenco tenuto dalla Consob), eventualmente avvalendosi di Altri Operatori per lo svolgimento di servizi/attività;
- Il Responsabile del registro individua l'infrastruttura tecnologica (DLT) e la soluzione attraverso la quale emettere e gestire le quote digitali del Fondo (c.d. Tokenization Platform);
- Il Gestore individua le modalità di pagamento utilizzabili per le operazioni di sottoscrizione e rimborso on-chain delle quote digitali del Fondo¹⁰;
- Il Gestore fornisce indicazione al Key Custody Provider (KCP) di creare il Wallet del Fondo, intestato al Gestore stesso ed allo specifico Fondo;
- Il Gestore fornisce indicazione al Responsabile del registro di creare lo Smart Contract del Fondo, tenuto conto delle caratteristiche dello specifico prodotto e di quanto suggerito nell'Allegato 4;
- Il Distributore dà indicazione al Key Custody Provider di creare il Wallet dell'investitore (c.d. wallet della posizione)¹¹.

Al termine di queste attività preliminari, il Distributore e il Gestore avranno a disposizione i Wallet sulla DLT su cui saranno emesse e gestite le quote digitali del Fondo (tramite smart contract), mediante cui potrà essere gestita la “proprietà” delle quote del Fondo.

9. I seguenti processi rappresentano un modello esemplificativo che può essere utilizzato come punto di partenza da modificare o aggiornare sulla base delle esigenze specifiche dei singoli operatori e dei modelli prescelti, ad esempio per quanto concerne le scelte di allocazione delle attività tra i diversi attori della catena o di adozione di specifiche soluzioni tecnologiche.

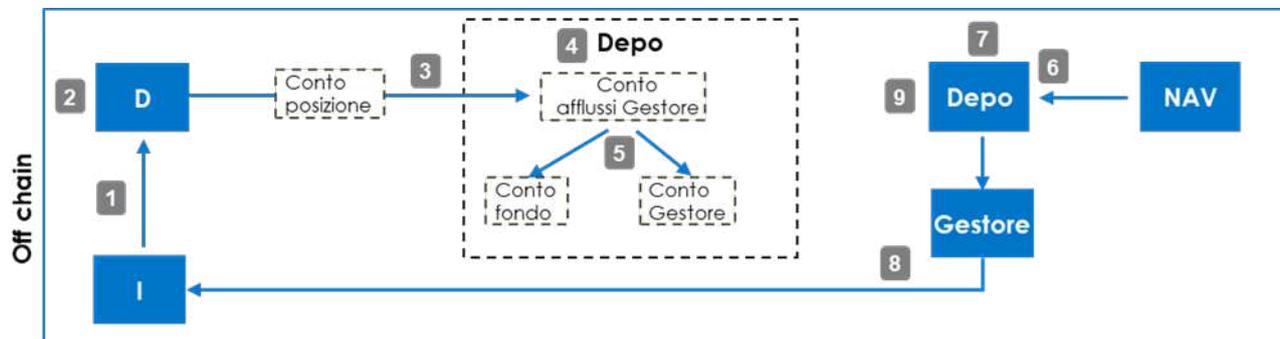
10. Ai fini dell'individuazione delle modalità di pagamento utilizzabili, si rammenta che per il regolamento on-chain in moneta di banca centrale il soggetto rilevante deve essere eleggibile ai fini dell'accesso ai servizi Target.

11. Nel processo esemplificativo presentato di seguito viene considerata la soluzione segregated, in cui il Distributore gestisce un wallet per ogni singolo Investitore.

1. Processo esemplificativo di sottoscrizione e rimborso di quote di Fondi Italiani DLT

1.1 Processo “as is” di sottoscrizione e rimborso di quote di Fondi Italiani

Processo “as is” di sottoscrizione di quote di Fondi Italiani¹²



Data valuta: T+0

1. L'Investitore invia al Distributore l'ordine di sottoscrizione di quote del Fondo.
2. Il Distributore prima di sottoscrivere le quote del Fondo per conto dell'Investitore effettua off-chain il processo di identificazione e di adeguata verifica dell'Investitore, dell'esecutore e del titolare effettivo, al fine di garantire la corretta acquisizione delle informazioni necessarie che andranno poi registrate on-chain sul Registro. Restano fermi gli obblighi in capo ai soggetti destinatari della disciplina antiriciclaggio.
3. Il Distributore trasmette l'importo dell'ordine dal conto della posizione al conto afflussi del Gestore (EoD).

Data valuta: T+1

4. Il Depositario¹³ esegue i controlli di Transfer Agency (e.g. Lotto minimo di acquisto, gg di sottoscrizione etc.).
5. Il Depositario applica i diritti fissi all'importo lordo. L'importo lordo, al netto dei diritti fissi, viene trasferito dal conto afflussi del Gestore al Conto del Fondo (Data NAV). La quota parte della sottoscrizione corrispondente a fees/diritti fissi viene accreditata sul Conto del Gestore (fees).

Data valuta: T+2

6. Il Depositario valorizza le quote al NAV.
7. Il Depositario avvalora l'emissione dei certificati (nominativi o al portatore) o, se l'Investitore non ne richiede la consegna fisica, aggiorna il certificato cumulativo.

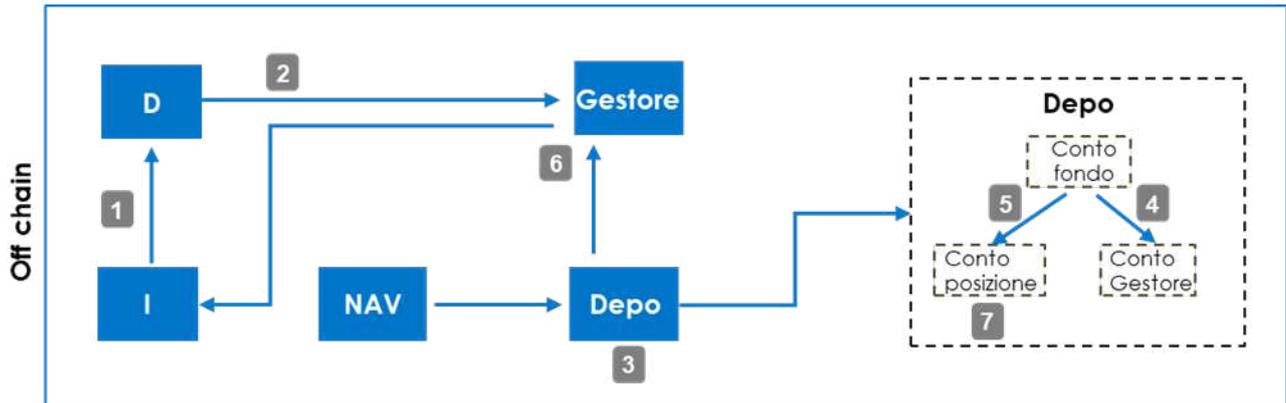
Data valuta: T+3

8. Il Depositario informa il Gestore dell'avvenuta esecuzione dell'ordine, il quale invia la lettera di conferma all'investitore per confermare l'esecuzione dell'ordine.
9. Il Depositario effettua i controlli ex post (ad es. controlli su quote emesse e movimentazioni cash).

12. Le tempistiche di esecuzioni dei controlli possono variare sulla base dell'operatività specifica dei singoli operatori. Questa rappresentazione non considera le specificità dei singoli modelli operativi.

13. Nel modello rappresentato il Depositario svolge anche il ruolo di TA.

Processo “as is” di rimborso di quote di Fondi Italiani



Data valuta: T+0

1. L'investitore invia al Distributore¹⁴ l'ordine di rimborso del numero delle quote del Fondo.

Data valuta: T+1

2. Il Distributore invia per conto dell'Investitore l'ordine di rimborso (in numero quote) al Gestore.

Data valuta: T+2

3. Il Depositario, una volta completati con esito positivo i controlli e avendo calcolato il NAV valorizza le quote e il controvalore di rimborso lordo. Successivamente, effettua il calcolo della fiscalità e calcola il controvalore di rimborso netto.

Data valuta: T+3

4. Il Depositario applica la fiscalità all'importo lordo. La quota parte del rimborso corrispondente alla fiscalità viene accreditata sul Conto del Gestore.

5. Il Depositario esegue il pagamento a favore dell'Investitore nel rispetto di quanto previsto dal regolamento di gestione del Fondo.

6. Il Depositario informa il Gestore dell'avvenuta esecuzione dell'ordine, il quale invia la lettera di conferma all'investitore per confermare l'esecuzione dell'ordine.

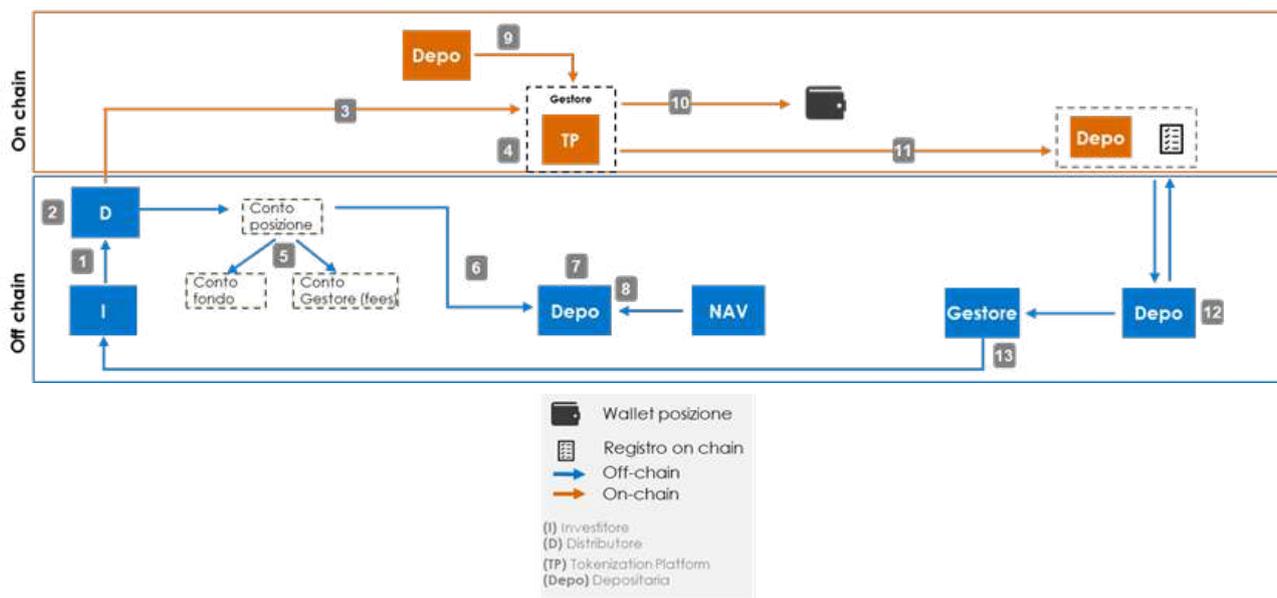
Data valuta: T+4

7. Il controvalore netto è reso disponibile sul conto della posizione dell'investitore

14. Per fini di semplicità illustrativa questo processo non illustra la casistica in cui l'investitore invia l'ordine di rimborso direttamente al Gestore.

1.2 Processo di sottoscrizione e rimborso di quote di Fondi Italiani DLT con regolamento in moneta di banca centrale

Processo di sottoscrizione di quote di Fondi Italiani DLT con regolamento in moneta di banca centrale



Data Valuta: T+0

1. L'Investitore invia al Distributore l'ordine di sottoscrizione di quote del Fondo Italiano DLT.
2. Il Distributore prima di sottoscrivere le quote del Fondo Italiano DLT per conto dell'Investitore effettua off-chain il processo di identificazione e di adeguata verifica dell'Investitore, dell'esecutore e del titolare effettivo, al fine di garantire la corretta acquisizione delle informazioni necessarie che andranno poi registrate on-chain sul Registro. Restano fermi gli obblighi in capo ai soggetti destinatari della disciplina antiriciclaggio.
3. Il Distributore invia per conto dell'Investitore, l'ordine di sottoscrizione, per il tramite della Tokenization Platform, al Gestore.
4. Vengono effettuati i controlli previsti sulla validità dell'ordine per il tramite della Tokenization Platform.
5. Il Distributore effettua il trasferimento della liquidità dal conto della posizione a: a) conto Fondo per l'importo netto delle commissioni; b) conto del Gestore per le commissioni.
6. Il Distributore informa il Depositario del trasferimento della liquidità.
7. Il Depositario esegue i controlli off-chain non svolti dalle logiche insite nello Smart Contract.

Data Valuta: T+1

8. Il Depositario, una volta completati con esito positivo i controlli off-chain, valorizza le quote al NAV.
9. Il Depositario autorizza l'emissione delle quote tramite lo Smart Contract del Fondo.
10. Le quote del Fondo vengono emesse e attribuite al Wallet della posizione.

11. Tutte le transazioni sono registrate sulla blockchain che mantiene un registro immutabile e tracciabile delle attività relative al Fondo tenendo conto di quanto riportato nella Linea Guida n. 13.

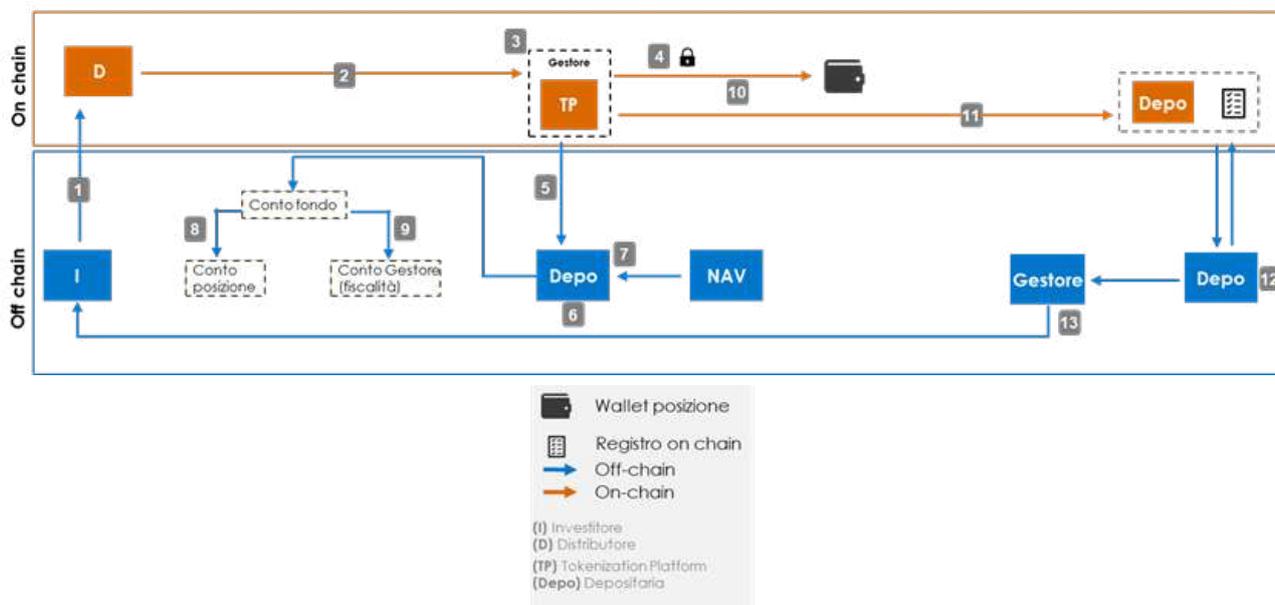
Ex-post

12. Il Depositario effettua i controlli ex post (es. controlli sulle quote digitali).

13. Il Depositario informa il Gestore dell'avvenuta esecuzione dell'ordine, il quale invia la lettera di conferma all'investitore per confermare l'esecuzione dell'ordine.

Si segnala che le tempistiche indicate sono soggette a variazioni in base ai tempi di regolamento delle operazioni di pagamento con moneta di banca centrale.

Processo di rimborso delle quote digitali di Fondi Italiani DLT con regolamento in moneta di banca centrale



Data Valuta T+0

1. L'Investitore invia al Distributore l'ordine di rimborso del numero di quote del Fondo.
2. Il Distributore invia per conto dell'Investitore, l'ordine di rimborso (in numero quote) al Gestore.
3. Lo Smart Contract del Fondo effettua i controlli previsti sulla validità dell'ordine. Tra questi vi possono essere alcuni controlli che riguardano, ad esempio, la capienza del saldo, etc.
4. Il Gestore vincola le quote digitali sul Wallet della posizione tramite la Tokenization Platform, interagendo con la specifica funzione dello Smart Contract.
5. Il Gestore comunica al Depositario l'approvazione dell'ordine di rimborso.
6. Il Depositario esegue i controlli off-chain non svolti dalle logiche insite nello Smart Contract.

Data Valuta T+1

7. Il Depositario, una volta completati con esito positivo i controlli off-chain e avendo calcolato il NAV valorizza le quote e il controvalore di rimborso lordo. Successivamente, effettua off-chain il calcolo della fiscalità e calcola il controvalore di rimborso netto.

Data Valuta T+1/T+2

8. Il Depositario effettua il trasferimento della liquidità dal conto Fondo al conto posizione, relativamente alla parte da rimborsare.
9. Il Depositario effettua il trasferimento della liquidità dal conto Fondo al conto del Gestore, per la parte relativa alla fiscalità.
10. Contestualmente, il Gestore, ricevuto l'input dal Depositario, effettua il burning delle quote digitali per il tramite della Tokenization Platform, interagendo con la funzione corrispondente dello Smart Contract.
11. Tutte le transazioni sono registrate sulla blockchain che mantiene un registro immodificabile e tracciabile delle attività relative al Fondo tenendo conto di quanto riportato nella Linea Guida n. 13.

Ex-post

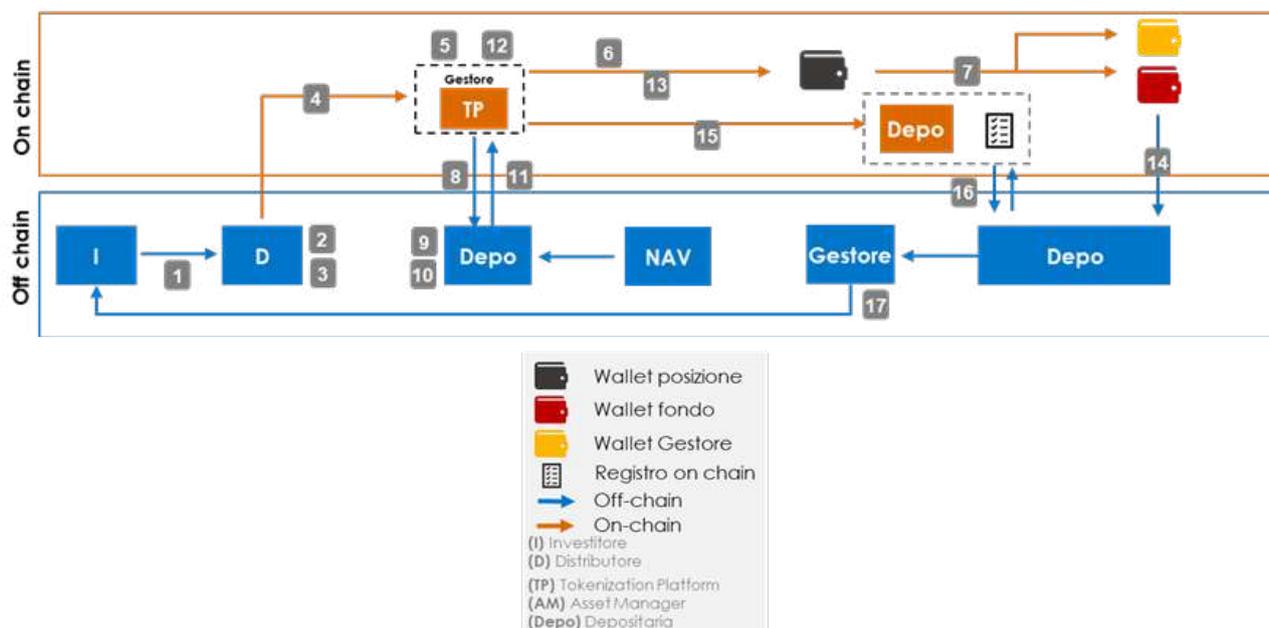
12. Il Depositario effettua i controlli ex post (es. controlli su quote rimborsate, liquidità).
13. Il Depositario informa il Gestore dell'avvenuta esecuzione dell'ordine, il quale invia la lettera di conferma all'investitore per confermare l'esecuzione dell'ordine.

Si segnala che:

- il completamento del processo di rimborso a T+1 oppure a T+2 risente dei vincoli operativi legati alla necessità di costituire la liquidità necessaria al fine di elaborare il rimborso stesso.
- Le tempistiche indicate sono soggette a variazioni in base ai tempi di regolamento delle operazioni di pagamento con moneta di banca centrale.

1.3 Processo di sottoscrizione e rimborso di quote di Fondi Italiani DLT con token di moneta elettronica/ token collegati ad attività¹⁵

Processo di sottoscrizione di quote di Fondi Italiani DLT con token di moneta elettronica/ token collegati ad attività



Data Valuta: T+0

1. L'Investitore invia al Distributore l'ordine di sottoscrizione di quote del Fondo Italiano DLT.
2. Il Distributore prima di sottoscrivere le quote del Fondo Italiano DLT per conto dell'investitore effettua off-chain il processo di identificazione e di adeguata verifica dell'Investitore, dell'esecutore e del titolare effettivo, al fine di garantire la corretta acquisizione delle informazioni necessarie che andranno poi registrate on-chain sul Registro. Restano fermi gli obblighi in capo ai soggetti destinatari della disciplina antiriciclaggio.
3. Il Distributore richiede la conversione da Euro fiat (dal conto corrente dell'investitore) a token di moneta elettronica.
4. Il Distributore invia l'ordine di sottoscrizione per conto dell'Investitore al Gestore.
5. Lo Smart Contract del Fondo effettua i controlli previsti sulla validità dell'ordine. Tra questi vi possono essere alcuni controlli relativi, ad esempio, al lotto minimo di acquisto, ai giorni di sottoscrizione, etc.
6. Il Gestore autorizza, per il tramite della Tokenization Platform, l'ordine ed il trasferimento del token di moneta elettronica dal Wallet della posizione al Wallet del Fondo.
7. Il token di moneta elettronica viene trasferito dal Wallet della posizione al: a) Wallet del Fondo per l'importo netto delle commissioni; b) Wallet Gestore, per le commissioni. I token di moneta elettronica rimangono vincolati in tali Wallet.
8. Il Gestore comunica al Depositario l'approvazione dell'ordine di sottoscrizione.
9. Il Depositario esegue i controlli off-chain non svolti dalle logiche insite nello Smart Contract.
15. Negli esempi che seguono per brevità si richiamano solo i token di moneta elettronica.

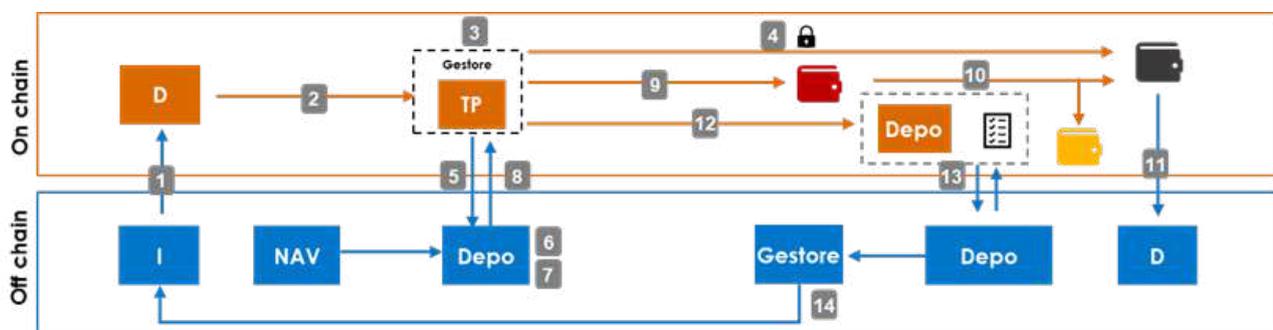
Data Valuta: T+1

10. Il Depositario, una volta completati con esito positivo i controlli off-chain, valorizza direttamente le quote al NAV.
11. Il Depositario richiede lo svincolo dei token di moneta elettronica e l'emissione delle quote digitali (indicandone il numero) al Gestore.
12. Il Gestore tramite la Tokenization Platform, ricevuto l'input dal Depositario, sblocca i token di moneta elettronica ed emette le quote digitali.
13. Le quote digitali emesse vengono accreditate sul Wallet della posizione.
14. I token di moneta elettronica possono essere riscattati in Euro fiat dalla Tokenization Platform su richiesta dell'ente emittente e accreditati nel conto corrente del Fondo tenuto presso il Depositario.
15. Tutte le transazioni sono registrate sulla blockchain che mantiene un registro immutabile e tracciabile delle attività relative al Fondo tenendo conto di quanto riportato nella Linea Guida n. 13.

Ex-post

16. Il Depositario effettua i controlli ex post (eg. controlli su quote emesse, Euro fiat e token di moneta elettronica).
17. Il Depositario informa il Gestore dell'avvenuta esecuzione dell'ordine, il quale invia la lettera di conferma all'investitore per confermare l'esecuzione dell'ordine.

Processo di rimborso delle quote digitali di Fondi Italiani DLT con regolamento in token di moneta elettronica/ token collegati ad attività



Data Valuta T+0

1. L'Investitore invia al Distributore l'ordine di rimborso del numero di quote del Fondo.
2. Il Distributore invia per conto dell'Investitore, l'ordine di rimborso (in numero quote) al Gestore tramite la Tokenization Platform.

3. Lo Smart Contract del Fondo effettua i controlli previsti sulla validità dell'ordine. Tra questi vi possono essere alcuni controlli che riguardano, ad esempio, la capienza del saldo, etc.
4. Il Gestore, pre-autorizza l'ordine e vincola le quote digitali sul Wallet della posizione tramite la Tokenization Platform, interagendo con la specifica funzione dello Smart Contract.
5. Il Gestore comunica al Depositario l'approvazione dell'ordine di rimborso.
6. Il Depositario esegue i controlli off-chain non svolti dalle logiche insite nello Smart Contract.

Data Valuta T+1

7. Il Depositario, una volta completati con esito positivo i controlli off-chain e avendo calcolato il NAV valorizza le quote e il controvalore di rimborso lordo. Successivamente, effettua off-chain il calcolo della fiscalità e calcola il controvalore di rimborso netto.

Data Valuta T+1/T+2

8. Il Depositario richiede il rimborso delle quote (indicandone l'equivalente in token di moneta elettronica) al Gestore tramite la Tokenization Platform.
9. Il Gestore tramite la Tokenization Platform, ricevuto l'input dal Depositario, interagendo con la specifica funzione dello Smart Contract, effettua il burning delle quote digitali e sblocca il trasferimento dei token di moneta elettronica dal Wallet del Fondo.
10. I token di moneta elettronica vengono trasferiti dal Wallet del Fondo al: a) Wallet della posizione, relativamente alla parte da rimborsare; b) Wallet del Gestore per la fiscalità.
11. Gli Euro fiat possono essere riscattati dalla Tokenization Platform, su richiesta dell'ente emittente e accreditati nel conto della posizione tenuto presso il Distributore.
12. Tutte le transazioni sono registrate sulla blockchain che mantiene un registro immutabile e tracciabile delle attività relative al Fondo tenendo conto di quanto riportato nella Linea Guida n. 13.

Ex-post

13. Il Depositario effettua i controlli ex post (eg. controlli su quote rimborsate, Euro fiat e token di moneta elettronica).
14. Il Depositario informa il Gestore dell'avvenuta esecuzione dell'ordine, il quale invia la lettera di conferma all'investitore per confermare l'esecuzione dell'ordine.

Si segnala che il completamento del processo di rimborso a T+1 oppure a T+2 risente dei vincoli operativi legati alla necessità di costituire la liquidità necessaria al fine di elaborare il rimborso stesso.

2. Alcune prime valutazioni

2.1 Benefici generali della tokenizzazione di quote di fondi

Benefici relativi al processo di Sottoscrizione:

- Accorciamento del ciclo di regolamento dell'operazione con disponibilità delle quote al sottoscrittore in anticipo rispetto al processo as-is dovute all'accredito automatico delle quote digitali nel Wallet posizione. Nello specifico, il Gestore per il tramite della Tokenization Platform emette le quote digitali e le assegna al Wallet della posizione

dove le quote sono rese disponibili immediatamente per l'investitore non appena le quote sono valorizzate. Ciò rappresenta un vantaggio rispetto al modello attuale dove le quote sono rese disponibili il giorno successivo alla valorizzazione delle quote.

- Accreditamento del capitale nel Wallet del Fondo in T0 con un anticipo rispetto al processo as-is, per gli ordini inseriti entro il cut off. L'introduzione di Wallet per la gestione di token di moneta elettronica consente il trasferimento immediato dal Wallet posizione al Wallet Fondo, senza necessità di effettuare il trasferimento per il tramite di un conto transitorio, così come nel caso del conto afflussi del Gestore utilizzato nel processo tradizionale.
- Certezza del valore della quota (time to market) con un anticipo rispetto al processo as-is, per gli ordini inseriti entro il cut off. Come descritto al punto precedente, la somma destinata alla sottoscrizione è accreditata sul Wallet Fondo (per poi essere vincolata) in T0, rendendo possibile di prendere come riferimento la data NAV T0.

Benefici relativi al processo di Rimborso:

- Abilitazione del DvP tramite il burning delle quote contestuale al trasferimento dei token di moneta elettronica.
- Riduzione del ciclo di regolamento dell'operazione con disponibilità per l'investitore della liquidità con un anticipo rispetto al processo as-is.
- Certezza del valore della quota (time to market) contestuale all'invio dell'ordine (per gli ordini inseriti entro il cut off) con un anticipo rispetto al processo as-is.

Altri benefici:

- Esecuzione di controlli on-chain: riduzione del perimetro di controlli eseguiti off-chain, a favore dell'inserimento degli stessi on-chain (eg. in caso di scarto dell'operazione, l'immediatezza della restituzione fondi all'investitore ed eventuale azione di rimedio tempestiva).
- Il Registro dei sottoscrittori è on-chain e viene aggiornato automaticamente e contestualmente al completamento di esecuzione degli ordini con una potenziale riduzione dei costi di gestione del registro dei sottoscrittori rispetto ai sistemi legacy.

2.2 Ulteriori considerazioni

- Con riferimento a Fondi chiusi, il processo di sottoscrizione iniziale potrebbe beneficiare pienamente delle opportunità del DvP. In questo caso specifico, infatti, la sottoscrizione iniziale e la conferma del numero delle quote sottoscritte non deve sottostare ai temi di calcolo del NAV e valorizzazione delle quote - che rappresentano un vincolo off-chain alla simultaneità delle transazioni.
- Nel caso di istituzione di Fondi Italiani Digitali (e cioè di Fondi che investono in Digital asset e che allo stesso tempo emettono quote di fondi digitali) si ottengono una serie di possibili vantaggi tra cui:
 - a. il processo per il calcolo del NAV potrebbe essere reso più efficiente;
 - b. l'abilitazione di servizi aggiuntivi (es. staking) in una modalità con price point, fee, complessità operative ridotte;
 - c. i minori costi sul Fondo, poiché si riducono i costi di gestione dei flussi di controllo ed elaborazione dei dati, delegati a DLT.



**ALLEGATO 7
INDICAZIONI SULL'INFORMATIVA PER GLI
INVESTITORI DI FONDI ITALIANI DIGITALI**

Nell'Informativa destinata agli Investitori è necessario includere considerazioni sulla tecnologia che sta alla base di questi strumenti, evidenziando anche i rischi emergenti associati. Si riportano qui di seguito, a titolo esemplificativo e non esaustivo, alcune indicazioni sull'Informativa che dovrebbe essere fornita all'Investitore, tenuto conto del target di clientela considerato.

Che cosa è una Distributed Ledger Technology?

Una Distributed Ledger Technology è una tecnologia che consente la registrazione e conservazione dei dati in specifici database distribuiti nei quali è solo possibile aggiungere informazioni (append-only) secondo regole condivise. Per raggiungere il consenso su un'unica versione del registro incensurabile, in assenza di fiducia e di un ente centrale, viene utilizzata la crittografia e sono impiegati algoritmi di consenso.

Che cosa è una Blockchain?

Una Blockchain è un particolare tipo di DLT il cui nome deriva dalla struttura del registro, ossia una struttura dati che contiene una sequenza di transazioni solitamente raggruppate in blocchi concatenati. Le transazioni da includere e il loro ordine nel blocco vengono stabiliti tramite un meccanismo di consenso al quale può partecipare chiunque (piattaforme permissionless) o solo soggetti che hanno soddisfatto determinate condizioni di accesso (piattaforme permissioned) e che si basa tipicamente su incentivi e disincentivi economici, attuati tramite asset contabilizzati nella Blockchain stessa.

Quali sono i rischi tecnologici di un Fondo Italiano DLT?

La tecnologia del registro distribuito alla base delle quote di un Fondo Italiano DLT può comportare svariati rischi, tra cui:

Rischi tecnologici

- i. la possibilità di difetti tecnici non ancora identificati nella DLT, per esempio nel processo attraverso il quale le transazioni vengono registrate;
- ii. la possibilità che misure di sicurezza crittografiche o altre misure di sicurezza che autenticano le transazioni precedenti per una DLT possano essere compromesse, o "hackerate", il che potrebbe permettere a un attaccante di alterare la DLT e quindi compromettere la capacità di confermare le transazioni registrate;
- iii. la possibilità che nuove tecnologie o servizi inibiscano l'accesso a una DLT;
- iv. il rischio che i nodi partecipanti alla rete DLT potrebbero essere in numero ridotto e che tale fatto si possa ripercuotere negativamente sul livello di decentralizzazione, sicurezza e stabilità della rete stessa;
- v. il rischio di disservizi, anomalie di funzionamento, di inefficienze o vulnerabilità di tecnologie diverse dalle DLT ma strumentali: per la conservazione delle quote in DLT e per l'accesso alle relative informazioni o per l'esercizio dei diritti attribuiti dalle quote (quali, ad esempio, interfacce digitali di accesso o le reti di comunicazione);
- vi. i rischi legati alle particolarità dei protocolli per la formazione del consenso (ad es., proof-of-work o proof-of-stake) che potrebbero influire sulla sicurezza, l'efficienza e la sostenibilità, anche ambientale, della rete DLT;
- vii. il rischio che la tecnologia utilizzata per rappresentare le quote in DLT cambi, in tutto o in parte, durante il ciclo di vita delle quote e sia necessario procedere al trasferimento

degli stessi ad un nuovo protocollo o tecnologia. In particolare, il Fondo, anche a causa della tenuta da parte di soggetti terzi dei registri mediante i quali sono rappresentati le quote DLT oggetto di investimento, potrebbe essere esposto al rischio di perdita o indisponibilità degli strumenti oggetto di investimento a causa di attacchi informatici, errori umani, guasti o altri disservizi tecnici;

- viii. i rischi connessi al fatto che le DLT potrebbero subire variazioni strutturali e di protocollo significative nel tempo, con conseguente impatto negativo sul valore del Fondo e delle relative Quote;
- ix. i rischi legati alle mancanze tecniche o inefficienze della DLT utilizzata per rappresentare le quote DLT possono avere un impatto negativo sul valore delle quote del Fondo così come un mutamento del quadro normativo applicabile a livello nazionale o sovranazionale alle DLT;
- x. i rischi derivati da possibili cambiamenti improvvisi nelle regole operative delle reti blockchain, noti come “fork” o “scissioni”, che potrebbero influire materialmente sui servizi. In particolare, in alcuni casi (c.d. hard fork), tali cambiamenti possono essere tanto radicali da rendere non validi le transazioni e i blocchi precedenti e comportare pertanto per il sottoscrittore il rischio di perdite delle proprie quote o azioni.

Quali sono i rischi legati all’investimento in un Fondo Italiano Cripto?

Il Fondo Italiano Cripto può investire in strumenti finanziari DLT e in Cripto-attività MiCAR (Attività digitali).

Gli strumenti finanziari DLT sono strumenti finanziari emessi su un registro distribuito per la circolazione digitale, ivi compresi gli strumenti finanziari digitali di cui all’articolo 1, comma 1, lettera c) del Decreto Fintech.

Le Cripto-attività MiCAR sono le cripto-attività, diverse dagli strumenti finanziari DLT, rientranti nell’ambito di applicazione del Regolamento (UE) 2023/1114 (Markets in Crypto-Assets Regulation – MiCAR).

L’investimento in strumenti finanziari DLT e in Cripto-attività MiCAR è soggetto al rischio tecnologico derivante dall’utilizzo delle tecnologie a registro distribuito (vedi sopra). In particolare, il Fondo che investe in Attività digitali potrebbe essere esposto al rischio di concentrazione tecnologica se la maggior parte delle Attività digitali in cui è investito il Fondo si basa su uno specifico protocollo o tecnologia.

L’investimento in Cripto-attività MiCAR, seppur attività regolamentate, presenta i seguenti ulteriori rischi:

- i. movimenti estremi dei prezzi: molte cripto-attività sono soggette a movimenti di prezzo improvvisi ed estremi e sono speculative perché il loro prezzo spesso dipende esclusivamente dalla domanda dei consumatori (ad esempio, potrebbero non esserci attività di copertura o altro valore tangibile). Si potrebbe perdere un’enorme quantità o addirittura tutto il denaro investito. I movimenti estremi dei prezzi significano anche che molte cripto-attività non sono adatte come riserva di valore e come mezzo di scambio o pagamento.
- ii. complessità dei prodotti: alcuni prodotti che forniscono esposizione alle Cripto-attività sono molto complessi, talvolta con caratteristiche che possono aumentare l’entità delle perdite in caso di andamenti sfavorevoli dei prezzi. Questi prodotti, data la loro complessità, non sono adatti a molti consumatori.

Avvertenza: Diversi emittenti e prestatori di servizi per le Cripto-attività, incluse le borse valori di Cripto-attività e fornitori di portafogli, hanno subito attacchi informatici e gravi problemi operativi. Molti consumatori hanno perso le loro Cripto-attività o subito perdite sia a causa di tali violazioni e disservizi sia perché hanno perso le chiavi private che forniscono l’accesso alle loro attività.

Bibliografia

- Alternative Investment Management Association (2022), Digital Asset Custody an AIMA Industry Guide*
- Association of National Numbering Agencies e DTI Foundation (2023), ISIN-DTI Guide*
- Association of National Numbering Agencies (2023), Isin Uniform Guidelines Relating To ISO 6166 (8th edition)*
- Assogestioni (2023), Oltre le Criptovalute. Tecnologie a registro distribuito a servizio dell'asset management*
- Banca d'Italia, Università Cattolica del Sacro Cuore, Università Roma Tre (2023), Caratteristiche degli Smart Contract, Documento di Consultazione*
- Banca d'Italia (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*
- Banca d'Italia (2022), Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e Cripto-attività, Roma*
- 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. e 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 Custodian Whitepaper

EBA, European Bank 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

ESMA, European 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, Banca d'Italia

Gruppo di lavoro articolo 29 per la protezione dei dati (2014) - Parere 05/2014 sulle tecniche di anonimizzazione

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. e 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, Documenti di ricerca, Banca d'Italia

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

Ministero dell'economia e delle finanze (2022), Libro Verde sulla competitività dei mercati finanziati italiani a supporto della crescita

Monetary Authority of Singapore e 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, disponibile al seguente 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 Custodian 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

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

Zetsche 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. e El Isa M., (2019) Melon Protocol: a Blockchain Protocol for Digital Asset Management Draft

Chi è Assogestioni

Assogestioni è l'associazione italiana dei gestori del risparmio e rappresenta la maggior parte delle società di gestione italiane e straniere operanti in Italia, oltre a banche e imprese di assicurazione attive nella gestione del risparmio, anche previdenziale.

Le principali finalità dell'associazione consistono nella promozione e nel supporto allo sviluppo dell'industria italiana del risparmio gestito, attraverso la ricerca di condizioni normative e di mercato utili a garantirne la tutela e favorirne la diffusione in Italia. Assogestioni svolge questa attività offrendo ai propri membri consulenza e supporto tecnico su tematiche legali, fiscali e operative. Inoltre, stimola un costante dibattito fra le imprese associate, gli altri operatori del settore finanziario e le istituzioni sui temi del risparmio e dell'investimento, di una sana corporate governance e dell'innovazione regolamentare e operativa dell'industria.

Riconoscimenti

La realizzazione di queste Linee Guida è stata possibile grazie, in primis, ai membri del ComDigit di Assogestioni ed, in particolare, a Giovanni Sandri (BlackRock), Presidente del ComDigit, Edoardo Del Bosco (Generali), Vice Presidente di ComDigit, Roberta D'Apice (Assogestioni), Segretario del ComDigit, Maria Canale De Rossi (Assogestioni), 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).

Uno speciale ringraziamento va poi a coloro che hanno dato un contributo tecnico-scientifico alla redazione delle Linee Guida e, in particolare, a Mauro Panebianco, Andrea Laurenti, Stefano Rossi, Alessia Maria Selenia Moia, Francesco Losso, Andrea Castellaneta, Luca Fumagalli (PwC Italia) e, per l'Osservatorio Fintech & Insurtech del Politecnico di Milano, a Marco Giorgino, Laura Grassi, Claudio Garitta e Jacopo Fracassi.

Desidero infine ringraziare per gli utili commenti ABI, ABI Lab, Societe Generale Securities Services e Metier Securities Services Bnp Paribas SA – Succursale Italia.

Fabio Galli, Direttore Generale, Assogestioni



ASSOGESTIONI

associazione del risparmio gestito