

UNIVERSITÀ
DEGLI STUDI
DI BRESCIA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Corso di Laurea
in INGEGNERIA INFORMATICA

Relazione Finale

REGOLAMENTAZIONE EUROPEA SULLE TECNOLOGIE DI REGISTRO DISTRIBUITO NELLA FINANZA DIGITALE

Relatore: Prof. Signoroni Alberto

Laureando:
Sica Mattia

Anno Accademico 2021/2022

Indice

Introduzione 1
1. Digitalizzazione 7
2. Cripto-Ecosistema 9
2.1 DLT e Blockchain 9
2.2 Portafogli 12
2.3 Asset Digitali 13
2.4 Servizi intrinseci 14
2.4.1 Trasferimento e riserva di valore 14
2.4.2 Mercati paralleli 16
2.5 Servizi Estrinseci 17
2.5.1 Compravendita 17
2.5.2 Custodia 18
2.6 Limiti del quadro europeo 19
2.7 Pacchetto per la Finanza Digitale: 20
3. Markets in Crypto-Assets Regulation 21
3.1 Definizioni 22
3.2 Token 23
3.2.1 WhitePaper 23
3.2.2 Autorizzazione 27
3.3 Fornitori di Servizi 30
3.3.1 Autorizzazione 30
3.3.2 Obblighi e Requisiti 31
3.4 Abusi di Mercato 37
3.5 Autorità Competenti 38
3.5.1 Poteri 38
3.5.2 Sanzioni 39
3.5.3 Collegi di Vigilanza 40
3.5.4 ABE 41
3.6 Progetti di norme tecniche 43
3.7 Relazione finale 44

3.8 Emendamenti....45
4. DLT Pilot Regime....47
4.1 Infrastrutture di mercato....48
4.2 Valori mobiliari DLT....49
4.3 Esenzioni e Misure Compensative....50
4.3.1 MTF DLT....50
4.3.2 SS DLT....51
4.4 Requisiti....52
4.5 Autorizzazioni....53
4.5.1 MTF DLT....53
4.5.2 SS DLT....54
4.6 Collaborazione con le Autorità....55
4.7 Relazione Finale....56
5. Digital Operational Resilience Act....57
5.1 Gestione del rischio....59
5.2 Gestione degli Incidenti....62
5.3 Test di Resilienza....63
5.4 Rischi derivanti da terzi....64
5.4.1 Struttura dei Contratti....65
5.5 Condivisione delle Informazioni....65
5.6 Autorità....66
Conclusione....67
Indice delle immagini....71
Riferimenti....73

Introduzione

Alla base del miglioramento e del progresso delle infrastrutture e dei servizi, c'è sempre stata l'**innovazione**; l'esempio più evidente di questo è la digitalizzazione, che ha **radicalmente trasformato** innumerevoli aspetti del quotidiano, impattando sulla quasi totalità dei settori: l'industria è stata rivoluzionata dall'introduzione della robotica e dell'IoT, l'intrattenimento dalle piattaforme di streaming digitale, le relazioni sociali dai social media e i servizi digitali stessi dalla virtualizzazione e dal cloud; anche il settore finanziario ha beneficiato della digitalizzazione, che ha permesso lo sviluppo di quelli che sono gli odierni sistemi su cui si erigono i mercati finanziari e i processi per il trasferimento di valore.

L'avvento di Bitcoin è stato l'introduzione di un'**innovazione** che ha segnato l'inizio dello **sviluppo delle tecnologie di registro distribuito** e, in particolare, della **blockchain**. Negli anni, la blockchain è evoluta passando dall'essere un *"semplice"* database distribuito contenente transazioni, come Bitcoin, a forme sempre più complesse; su database di questo genere sono infatti stati introdotti meccanismi come virtual machine e smart contracts che hanno permesso lo sviluppo di generazioni evolute di blockchain, ognuna delle quali ha portato con sé un incremento di **scalabilità** e di **interoperabilità**, permettendo così lo sviluppo di prodotti, di applicazioni e di servizi sempre più complessi. Primo tra questi prodotti sono le **criptovalute,** che hanno avuto il merito di attrarre l'**interesse degli investitori** verso le tecnologie e l'ecosistema di registro distribuito. Le criptovalute non sono però l'unico prodotto che è stato sviluppato in tale ambiente, esistono infatti innumerevoli **asset digitali,** cioè forme di rappresentazione digitale di valore, ognuna delle quali con pregi e difetti; tra gli asset digitali si possono annoverare ad esempio: asset finanziari tokenizzati, atti di proprietà digitale come gli NFT e i token di moneta elettronica.

La digitalizzazione del valore, cioè la **tokenizzazione** *[1]* di questo, comporta innumerevoli benefici. Oltre alla semplicità di accesso, i token, in quanto informazione digitale, sono trasferibili a costi estremamente ridotti, in tempi brevissimi e sono peraltro potenzialmente più semplici da monitorare. La tokenizzazione non comporta però solo lati positivi; questa, infatti, non è altro che uno strumento e quindi, il risultato della sua applicazione è una conseguenza diretta dell'obiettivo di chi ne fa uso.

L'attenzione delle istituzioni verso l'ecosistema delle tecnologie di registro distribuito è iniziata fondamentalmente con la crisi delle criptovalute del 2018 e quindi, nel tempo trascorso tra la nascita del Bitcoin e lo sviluppo dei primi, recentissimi approcci regolamentari, si sono potute sviluppare, anarchicamente, una serie di strutture, di sistemi, di processi e modalità che oggi costituiscono di fatto il settore nel suo complesso. La prolungata assenza di forme di vigilanza e di riferimenti regolatori, ha lasciato emergere strutture e sistemi che spesso si sono rivelati inadeguati rispetto ai canoni di sicurezza e di fiducia rigorosamente necessari in un contesto come quello finanziario: truffe, schemi

piramidali, trattamenti fallaci dei dati, carenze infrastrutturali, schemi per il riciclaggio di denaro, evasione fiscale e manipolazione del mercato sono infatti fenomeni comuni nel settore, che risulta quindi un ambiente frammentato e incerto.

Tipicamente i progetti blockchain sono caratterizzati dall'emissione di qualche tipologia di token che può, o meno, essere funzionale all'accesso a un servizio; in qualsiasi caso, tali token devono essere in qualche modo ottenibili e conservabili: queste esigenze vengono soddisfatte da appositi fornitori di servizi, che permettono la negoziazione e la custodia di tali asset digitali. Tali fornitori erogano quindi servizi che sono in qualche modo equivalenti a quelli offerti dalle banche e dalle entità a queste connesse nel sistema finanziario tradizionale. Le opportunità rappresentate dalla tecnologia di registro distribuito, l'elevata affluenza di denaro che ne caratterizza il contesto e la necessità di tutelare i consumatori e la stabilità finanziaria, hanno dunque attirato l'attenzione delle istituzioni e dei governi. L'incertezza dell'odierno contesto DLT va superata attraverso l'adozione di approcci regolatori che favoriscano l'integrazione sia delle istituzioni finanziarie canoniche che delle rispettive modalità di vigilanza e, conseguentemente, delle garanzie che le accompagnano.

A questo proposito, diverse nazioni stanno sviluppando piani legislativi per regolamentare l'ecosistema distribuito nella sua interezza; l'America, ad esempio, sta cercando di adottare tramite la Securities and Exchange Commission (SEC) delle politiche di protezione degli investitori, che stanno però impattando lo sviluppo del mercato dei servizi connessi, stimolando l'emigrazione dei Crypto Assets Service Providers (CASPs) *[2]*.

La Cina, invece, ha adottato un approccio più drastico, introducendo nel 2021 il divieto assoluto di negoziazione degli asset digitali ed escludendo quindi i cittadini cinesi dal mercato; nonostante questa decisione, la Cina sta comunque esplorando la tokenizzazione dello yuan sotto il controllo centralizzato delle sue entità finanziarie *[3]*. Di fatto, l'applicazione delle DLT nei sistemi di moneta garantita dalle banche centrali (CBDC) è una realtà che sta venendo esplorata da quasi tutte le nazioni.

La differenza principale alla base degli approcci regolatori adottati dalle diverse nazioni, riguarda il grado di chiusura o di flessibilità adottato rispetto a quello che è l'attuale, reale ecosistema. In questi termini l'Unione Europea ha sviluppato, all'interno di quello che è il suo framework per la finanza digitale, una serie di regolamentazioni flessibili finalizzate a rendere, nel rispetto dei valori europei, il territorio dell'Unione attrattivo per i CASPs, i cui sistemi di gestione della tokenizzazione e dei token vengono, con lungimiranza, percepiti come il futuro della finanza.

Le regolamentazioni europee relative al settore della tecnologia di registro distribuito rappresentano un precedente a livello globale; queste, sono contenute nel ***pacchetto sulla finanza digitale*** e si innestano all'interno di quei contorni che vengono definiti da regolamentazioni come la NIS, *sulla sicurezza delle reti e dei sistemi informativi all'interno dell'Unione,* il GDPR *sulla protezione dei dati,* la MiFID II *sui mercati degli strumenti finanziari, il regolamento UE sul trasferimento di fondi (TFR)* e altre regolamentazioni connesse ai settori della finanza, dell'informatica e delle telecomunicazioni. Nello specifico, le regolamentazioni sulle DLT e le rispettive infrastrutture sono tre e disciplinano diverse attività ed entità; gli asset digitali vengono infatti distinti in due macrocategorie: le cripto-attività, regolamentate nella proposta di regolamento sui mercati delle cripto-attività (MiCA) e gli asset finanziari tokenizzati, security tokens, regolamentati nel regime pilota per le infrastrutture di mercato DLT (DLT Pilot Regime).

MiCA è una **proposta di regolamento** che si pone l'obiettivo di delineare i contorni delle attività di diverse entità: emittenti di token, fornitori di servizi e autorità competenti. Gli emittenti di token, vengono discriminati sulla base di un'ulteriore distinzione sul tipo di cripto-attività emessa e vengono classificati in: emittenti di token collegati ad attività, emittenti di token di moneta elettronica ed emittenti di token né di attività né di moneta elettronica; MiCA stabilisce i requisiti generali e specifici che ciascuno di questi deve rispettare in termini di informativa, emissione, marketing e collaborazione con le autorità al fine di ottenere un'autorizzazione per svolgere le proprie attività nello spazio dell'Unione. Il meccanismo è il medesimo per i fornitori di servizi, che vengono distinti in base alla tipologia di servizio erogato; vengono definiti obblighi, modalità di cooperazione con le autorità e requisiti, generici e specifici, che devono essere ottemperati al fine del conseguimento di un'autorizzazione alla prestazione di servizio nell'Unione. MiCA, infine, definisce le regole per la definizione delle autorità nazionali competenti nella materia delle cripto-attività e nella vigilanza sulle entità a queste connesse, chiarendo poteri e responsabilità, illustrando le modalità di cooperazione tra le diverse autorità e identificando le gerarchie di controllo.

Il **DLT Pilot Regime** è un **regolamento** entrato **in applicazione dal 23 Marzo 2023**. In qualità di regime pilota, il regolamento è finalizzato alla definizione di un ambiente di test che consenta all'Unione di valutare l'efficacia di tutte quelle procedure e strutture correlate agli asset finanziari tokenizzati; vengono definite le tipologie di valori mobiliari DLT negoziabili e i limiti di capitalizzazione di mercato entro cui tale negoziazione può avvenire. Alla definizione degli asset trattabili segue l'identificazione di tre strutture di mercato: sistemi multilaterali di negoziazione DLT, sistemi di regolamento titoli DLT e una commistione dei due; per tali infrastrutture, il regime pilota prevede, previa l'adozione di misure compensative, la concessione di esenzioni rispetto agli obblighi che la legislazione finanziaria prevede per i classici sistemi multilaterali di negoziazione e di regolamento titoli. Il DLT Pilot Regime introduce quindi un insieme di regole finalizzate all'integrazione dei sistemi DLT nell'ecosistema della finanza classica, attraverso la definizione di meccanismi di autorizzazione basati sulla verifica di una serie di requisiti minimi finalizzati alla tutela dei consumatori e della stabilità finanziaria.

La terza regolamentazione non è specificatamente legata al contesto delle tecnologie di registro distribuito, questa comprende infatti sia i fornitori di servizi di IT e TLC che tutte le entità finanziarie; gli emittenti di token e i fornitori di servizi a questi connessi sono esplicitamente indicati come soggetti alle disposizioni. Il **Digital Operational Resilience Act** è **entrato in vigore il 17 gennaio 2023 e si applicherà dal 17 gennaio 2025**. **DORA** è finalizzata al miglioramento della resilienza degli apparati finanziari europei nel settore dell'informazione e delle telecomunicazioni. Il regolamento impone lo sviluppo di modelli multifase di gestione del rischio, basati su prevenzione e protezione, individuazione, risposta e ripristino; la responsabilità per tali politiche viene estesa agli organi di gestione delle entità interessate dal regolamento, per i quali vengono introdotti una serie di obblighi come la formazione dello staff sui rischi informatici, la revisione delle procedure e il testing dei sistemi e dei dispositivi. Oltre a quanto concerne le politiche di gestione dei rischi, DORA stabilisce le best practices per la gestione degli incidenti connessi alle infrastrutture informatiche e di telecomunicazione nel settore finanziario, riservando particolare attenzione alle modalità di esternalizzazione di funzioni verso fornitori terzi di servizi e ai contenuti dei contratti che ne disciplinano i meccanismi. In aggiunta alle disposizioni che definiscono i contorni della gestione operativa dei rischi e degli incidenti, DORA definisce i poteri e le responsabilità delle autorità cui compete la vigilanza delle diverse entità interessate, ed evidenzia l'importanza di uno scambio di informazioni tra tali entità e le rispettive autorità competenti ed europee, al fine di analizzare attivamente la situazione dell'Unione per continuare ad evolvere i sistemi a garanzia della resilienza digitale europea.

La presente dissertazione si propone quindi di fornire, attraverso un'analisi dell'odierno contesto DLT e dei regolamenti elaborati dall'Unione, una panoramica delle seguenti:

- Attuale ecosistema delle tecnologie di registro distribuito e dei fornitori di servizi a queste associati.
- Contenuti del piano regolatorio adottato dall'Unione in riferimento all'applicazione delle DLT nel contesto finanziario.
- Problematiche finanziarie e informatiche caratterizzanti il settore DLT.

Al fine di:

- Individuare le modalità in cui l'Unione ha operato per salvaguardare lo sviluppo del settore DLT tutelando al contempo i diritti degli utenti.
- Identificare eventuali sfide regolatorie ancora aperte.

L’elaborato è strutturato in cinque capitoli:

1. **Digitalizzazione:** illustra brevemente alcuni esempi di rischi e opportunità associati all’integrazione di nuove tecnologie nella società, al fine di introdurre la posizione adottata dall’UE.

2. **Cripto-Ecosistema:** dedicato alla definizione del contesto DLT, in particolare dell’ecosistema blockchain; viene sviluppata un’analisi dei principali servizi, entità e problematiche che caratterizzano il mercato, si delinea l’emergente architettura. Si identificano i limiti di applicazione della vigente regolamentazione in relazione alle DLT e si introduce il *Pacchetto per la Finanza Digitale*.

3. **Markets in Crypto-Assets Regulation:** Vengono affrontati i contenuti della proposta di regolamento sui mercati delle criptoattività, ad eccezione della materia delle acquisizioni; dalla distinzione delle diverse tipologie di criptoattività, si procede con l’approfondimento di obblighi, requisiti e procedure previsti per l’autorizzazione di emittenti di token e fornitori di servizi nell’UE, a cui segue l’analisi di una varietà di aspetti: disposizioni in materia di abusi di mercato e recenti casistiche rilevanti, progetti di norme tecniche e contenuti della relazione finale per la valutazione d’impatto. Il capitolo termina con una riflessione sui principali aspetti degli emendamenti recentemente introdotti dal Parlamento europeo.

4. **DLT Pilot Regime:** Vengono individuate le infrastrutture di mercato che caratterizzano il settore degli asset finanziari tokenizzati e le tipologie di asset ammessi alla sperimentazione, si analizzano i requisiti e le misure compensative da introdurre nelle infrastrutture di mercato DLT ai fini del conseguimento di autorizzazioni ed esenzioni; si identificano autorità competenti e modalità di collaborazione. Il capitolo si conclude con l’analisi dei contenuti previsti nella relazione per la valutazione d’impatto del regolamento sperimentale.

5. **Digital Operational Resilience Act:** Vengono delineate le procedure di gestione dei rischi e degli incidenti che devono essere adottate dalle entità finanziarie e le modalità per la validazione di queste; si analizzano le procedure previste per la gestione dei rischi rappresentati dalle esternalizzazioni, prestando dettaglio all’analisi dei vincoli contrattuali e alle clausole imprescindibili. Il capitolo si conclude con un excursus sui collegi di vigilanza e con le raccomandazioni dell’Unione sulla condivisione delle informazioni associate alla gestione dei rischi informatici per le infrastrutture finanziarie.

1. Digitalizzazione

La massiva diffusione della tecnologia, coadiuvata dalla progressiva interconnessione di attività e contesti eterogenei, ha condotto l'equilibrio globale ad un sistema multipolare. Una realtà segnata da vaste collaborazioni internazionali, orientate al conseguimento di una posizione di rilievo nel sempre più articolato panorama geopolitico.

La rapidissima digitalizzazione a cui sono state, e ancora sono soggette, le persone, le organizzazioni e le amministrazioni di tutto il mondo, spinge costantemente verso un frenetico superamento delle infrastrutture e dei servizi. Un'evoluzione necessariamente caratterizzata dalla **progressiva iniezione di nuove tecnologie in sistemi già operativi;** questo implica un **approccio multidisciplinare, imprescindibile per lo sviluppo di standard sia tecnici che giuridici,** che garantiscano le proprietà fondamentali quali il corretto funzionamento, la sicurezza e la tutela di tutti i portatori di interessi coinvolti.

Le nuove applicazioni di tecnologie già esistenti e le frontiere aperte dallo sviluppo di tecnologie estremamente avanzate comportano infatti, non solo potenziali enormi benefici, ma anche altrettanto grandi rischi. Minacce che coinvolgono sia infrastrutture e servizi, nazionali e internazionali, sia i diritti fondamentali dei singoli. Si prendano ad esempio in considerazione:

- Le statistiche sul numero di cyber attacchi avvenuti nel 2022 nel mondo *[4]*, in Europa *[5]* e in Italia *[6]*, alcuni dei quali aggravati dalla matrice politica e inseriti in un contesto di "guerra ibrida" legata al conflitto russo-ucraino *[7]*.
- Il massiccio impiego di tecnologie di sorveglianza come ***droni*** *[8]* ***e telecamere domestiche*** *[9]* da parte delle autorità cinesi nell'ambito dell'aggressiva strategia di contenimento del coronavirus.
- L'applicazione dell'intelligenza artificiale per il riconoscimento e la conseguente soppressione dei sovversivi ad Hong-Kong *[10]*.
- L'induzione di pregiudizi in algoritmi di intelligenza artificiale e i possibili conseguenti fenomeni discriminatori associati alla loro applicazione in contesti delicati *[11]*.
- La potenziale violazione della sicurezza computazionale dei correnti sistemi crittografici a chiave pubblica da parte dei computer quantistici *[12]*.
- **L'indisciplinata insorgenza di cripto-attività e i conseguenti rischi, sia economici che informatici, che esse rappresentano per gli investitori, le istituzioni e la stabilità finanziaria** *[13]***.**

La possibilità di incorrere in abusi e attacchi informatici non è, però, motivo sufficiente per pregiudicare lo studio, lo sviluppo e l'implementazione di nuove tecnologie e delle loro applicazioni che possono, in termini di funzionalità ed efficienza, radicalmente trasformare la nostra società elevando la qualità delle sue infrastrutture e dei suoi servizi.

È in questi termini che l'Unione Europea ha emesso il 19 febbraio e il 24 settembre 2020 le *comunicazioni della commissione al parlamento europeo, al consiglio, al comitato economico e sociale europeo e al comitato delle regioni "**Plasmare il futuro digitale dell'Europa"** [14]* ***e "*Strategia in materia di finanza digitale per l'UE"** *[15]***.**

La finalità di queste comunicazioni era quella di ribadire la **necessità di un quadro chiaro che promuovesse interazioni digitali affidabili in tutta la società,** finalizzato al raggiungimento di un'Europa digitalmente forte che potesse perseguire le esigenze del proprio modello sociale nello spazio digitale.

A questo proposito, veniva evidenziata l'importanza della modernizzazione delle regole applicabili ai servizi digitali in tutta l'UE**,** soprattutto al fine di **chiarire le responsabilità dei fornitori di servizi, il cui ruolo sistemico e potere di mercato non doveva, e tutt'oggi non deve, mettere a repentaglio l'equità e l'apertura dei mercati europei.** Particolare attenzione è stata riservata al settore finanziario, dove l'adozione di nuove tecnologie, l'ingresso di nuovi player e lo sviluppo di nuovi servizi, implicano una profonda influenza sulla natura dei rischi per i consumatori, per gli utenti e per la stabilità finanziaria.

In questo contesto, **la finanza europea si è posta l'obiettivo di cogliere le opportunità offerte dalla rivoluzione digitale, attraverso forti operatori di mercato europei che potessero rendere disponibili i benefici del digitale alle imprese e ai consumatori, garantendo al contempo una solida disciplina dei rischi**.

Questa linea politica ha trovato concretezza nella volontà dell'Unione di attuare, entro il 2024, **un quadro esaustivo in grado di sostenere l'utilizzo della tecnologia di registro distribuito (DLT) e delle cripto-attività, in quanto rappresentanti di importanti opportunità per il settore finanziario**.

2. Cripto-Ecosistema

2.1 DLT e Blockchain

Con il termine Distributed Ledger Technologies (*DLT*) si fa riferimento a registri elettronici o "libri mastri" distribuiti su una rete di nodi, i cui dati sono ridondati, verificati e validati mediante l'adozione di diversi protocolli. La gestione di tali registri è di fatto decentralizzata in quanto l'archiviazione è basata su meccanismi utili perché i nodi della rete concordino sull'insieme di transazioni valide.

Con **Blockchain** si fa riferimento ad un particolare tipo di Distributed Ledger, il più diffuso, in cui i dati delle transazioni vengono validate tramite **algoritmi di consenso** *[16]*, raccolti in blocchi collegati e inseriti nel registro.

Le informazioni archiviate, una volta validate e immesse nel registro sono inalterabili; ogni nuova informazione è indissolubilmente legata allo storico delle transazioni precedenti grazie alle proprietà di appropriate funzioni di hash che agiscono come puntatori robusti *[17]*.

Con l'avvento della seconda generazione di Blockchain, in particolare con Ethereum, il paradigma tecnologico è stato espanso dall'introduzione di:

1. Una **VM** turing completa (EVM[1]).
2. **Smart contracts**, porzioni di codice sviluppate secondo **logica IFTTT** inseribili su indirizzi della chain e **con cui è possibile interagire attraverso transazioni**.

L'inserimento di VM e di smart contracts nelle Blockchain, ha permesso lo sviluppo di una **prima generazione di applicazioni decentralizzate (dApp)** che hanno portato alla luce una varietà di **problematiche**:

1. La necessità di **importare dati** puliti e qualitativamente rilevanti da un ambiente esterno all'ambiente on chain, per lo sviluppo di applicativi rilevanti;
2. La mancanza di **standard** per lo sviluppo di token compatibili;
3. L'assenza di sistemi per garantire l'**interoperabilità** tra chain;

Esigenze che, combinate alla progressiva attenzione di cui la blockchain è stata protagonista, hanno condotto allo sviluppo di:

- **Oracoli**: applicazioni utili per interfacciare gli ambienti Off-Chain con quelli On-Chain, il più noto dei quali è Chain-Link (LINK) *[18]*.
- **Bridge**: sistemi basati su smart contracts che permettono il trasferimento di asset tra chain diverse *[19]*.
- **Standard per i token**, come gli standard ERC di Ethereum *[20]*.

[1] *Ethereum Virtual Machine, EVM*

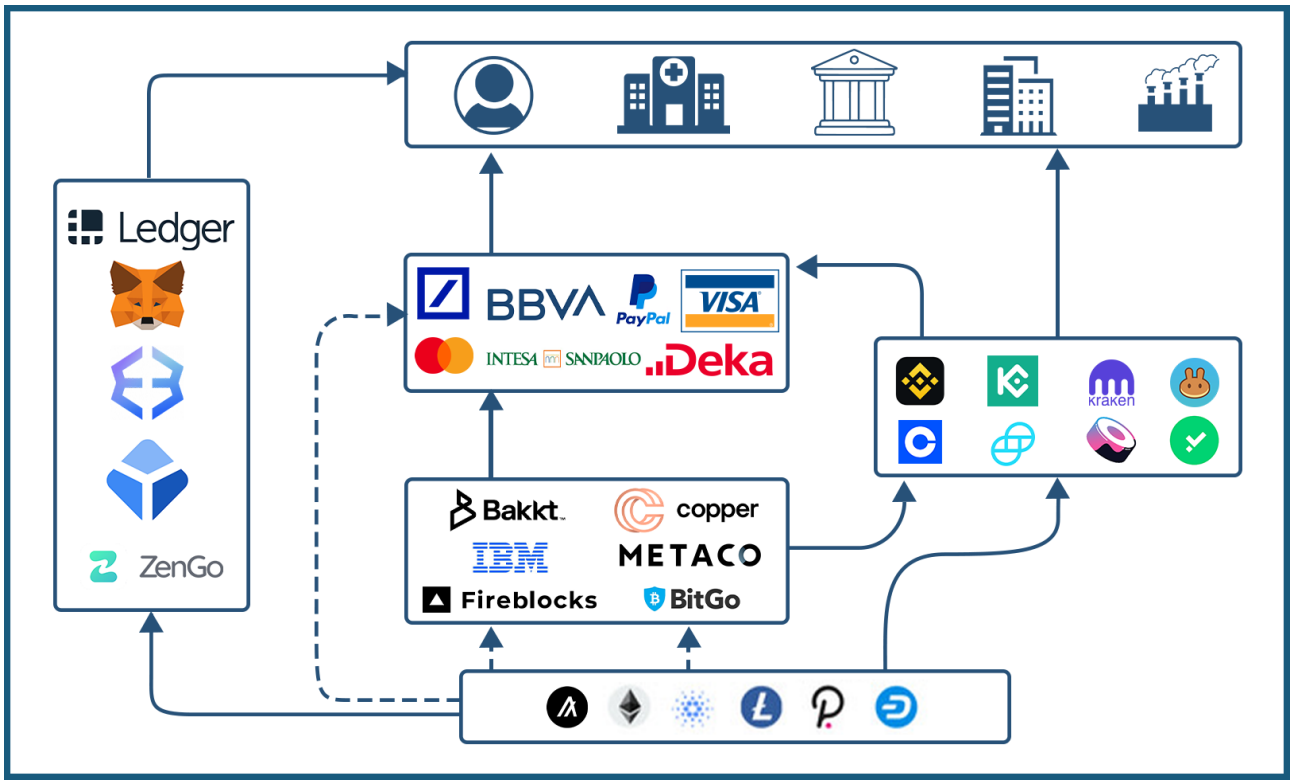


1. Chainlink come interfaccia

L’introduzione di queste innovazioni ha così consentito l'interoperabilità sia tra chain eterogenee, sia tra blockchain ed ecosistema web2; la scalabilità e l’interoperabilità che ne sono conseguite hanno permesso lo sviluppo di progetti sempre più avanzati, come Cardano, Polkadot, Algorand oltreché di una stratificazione di tecnologie e servizi.

L'odierno ecosistema è caratterizzato da una varietà di entità, ed è illustrabile con uno pseudo stack costituito da:

- un layer di basso livello, in cui convergono vari progetti blockchain che offrono l'accesso a virtual machine e a standard che permettono lo sviluppo di prodotti nativi dell'ambiente distribuito;
- un layer intermedio, composto da quei prodotti e da quei servizi che si appoggiano
    - **direttamente sull'ambiente distribuito**, facendo riferimento a codice on chain, come i **custody provider**, gli **exchange** e i **wallet**;
    - **su terze parti**, al fine di sviluppare servizi tramite API che fungono da interfaccia verso la tecnologia distribuita sottostante; esempio di questo potrebbero essere gli istituzionali che si avvalgono dei custody provider.
- un layer di alto livello, rappresentante tutti i clienti.



2. Infrastruttura dell'ecosistema DLT [2]

[2] *Rappresenta le principali categorie e relazioni nell'ecosistema DLT. L'illustrazione non pretende di corrispondere alla realtà: le società sono citate in quanto esponenti di specifiche categorie e non sono necessariamente coinvolte nelle relazioni illustrate*

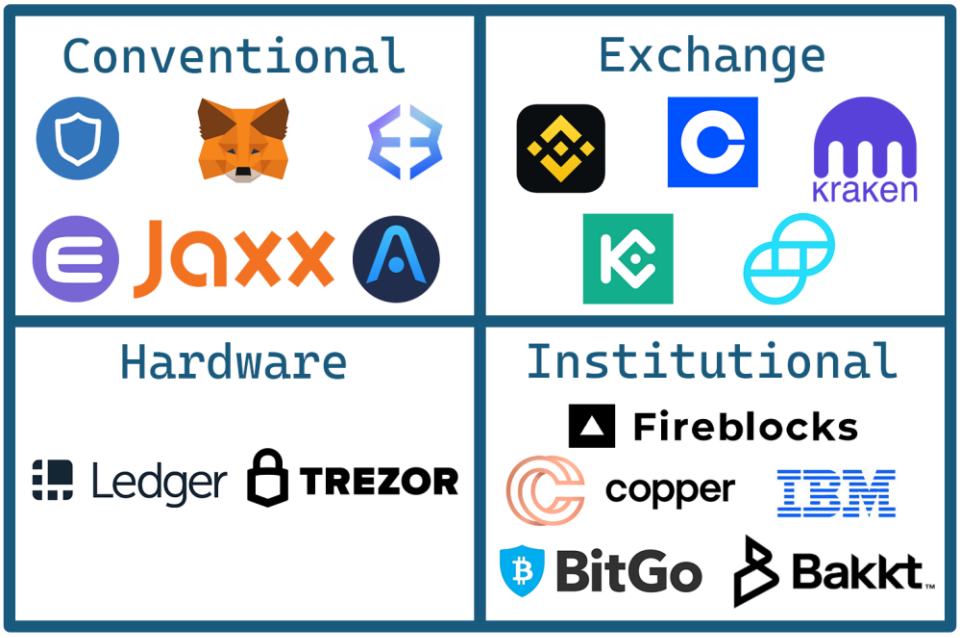
2.2 Portafogli

Un wallet è lo strumento fondamentale per interagire con gli asset digitali. Essere in possesso della chiave privata associata ad un portafoglio permette il controllo degli asset in esso contenuti, mentre la conoscenza di una chiave pubblica rende possibile interagire con il portafoglio a cui questa è associata. Le interazioni possono essere di diverse tipologie e fanno solitamente riferimento ad un indirizzo, cioè a parte dell'hash di una chiave pubblica.

Esistono diverse varianti di wallet, principalmente differenziati in base alla natura fisica (hardware, software) alla connessione in rete (online, offline) alla modalità di fornitura del servizio (applicazione mobile, applicazione web, software dedicato indipendente…) e al responsabile della custodia delle chiavi (se stessi, terza parte).

Ognuno di questi ha diversi punti di forza e debolezza, i più rilevanti dei quali sono:

- Sicurezza: I portafogli online sono per natura più esposti a rischi; la custodia delle chiavi di accesso ai propri asset-digitali da parte di terzi permette di delegare la responsabilità di un servizio ma implica fiducia nella terza parte.
- Accessibilità: I portafogli software online sono molto più agevoli rispetto a quelli offline e hardware, che sono però più sicuri.
- Recupero credenziali: L'autonoma custodia delle proprie chiavi implica, in caso di smarrimento della chiave privata, l'impossibilità di accedere ai propri "asset-digitali *[21]*.



3. Tipologie di portafogli

2.3 Asset Digitali

Si definisca innanzitutto il concetto di token:

“Un’informazione digitale, memorizzata su un registro distribuito, univocamente associata a uno e un solo specifico utente del sistema e rappresentativa di una qualche forma di diritto: la proprietà di un asset, l’accesso a un servizio e così via” [22].

Gli asset digitali possono essere distinti in **tre macroaree**:

- **Token fungibili**: Sinonimo di liquidi; **tutte le criptovalute** sono token fungibili poiché hanno l’obiettivo di funzionare come mezzo di scambio.

  In generale un bene è fungibile se:

  - contiene un valore intrinseco definito e misurabile;
  - è sostituibile facilmente con un bene con caratteristiche simili sul mercato;
  - può, nel lungo termine, diventare un asset di valore;

- **Token non fungibili**: **Unici, non sostituibili, non ripetibili, non divisibili**.

  Gli NFT sono unità di dati archiviati su blockchain che certificano l’unicità di asset digitali sottostanti, di cui costituiscono la rappresentazione nell’ecosistema digitale. Ciascun NFT può differire da un altro per criteri come il soggetto che rappresenta, le caratteristiche tecniche, le applicazioni e il prezzo. Gli NFT sono noti come attestati di proprietà e di autenticità di oggetti d’arte digitale da collezione ma possono, in opportune condizioni, rappresentare l'ownership e l'autenticità di qualsiasi entità, indipendentemente dal fatto che si tratti di un oggetto di un videogioco, di un diploma o dell'atto di proprietà di una casa.

- **Stablecoin**: valuta digitale ancorata a un asset di riferimento.

  Esistono diverse stablecoin ancorate a diversi asset; **tra gli asset sottostanti più comuni, tipicamente ci sono le valute fiat.**

2.4 Servizi intrinseci

La tecnologia blockchain e gli asset digitali, implicano l'esistenza di una serie di servizi intrinseci tra loro molto diversi, indissolubilmente legati alla natura dell'entità a cui si fa riferimento. Di seguito se ne analizzano alcuni tra i più rilevanti:

2.4.1 Trasferimento e riserva di valore

Ai token, generalmente, è associato un valore; questi, rappresentano quindi una forma di riserva di valore; questo implica una serie di problematiche, prima delle quali rappresentata dalla natura tipicamente **pseudoanonima** *[23]* delle blockchain:

essendo gli utenti identificati sulla catena univocamente dalla chiave pubblica associata al loro portafoglio, perché esista quantomeno una minima tutela da problematiche come l'evasione e il riciclaggio, si rende necessaria un'infrastruttura che possa ricondurre i portafogli alle persone fisiche. Quindi, è necessario un layer che possa operare una forma di **Know Your Customer (KYC)** tipica delle infrastrutture bancarie.

Inoltre, risulta evidente la necessità di elaborare un approccio verso quelle blockchain che si dichiarano "totalmente anonime" come Zcash e Monero. Gli Emirati Arabi Uniti, ad esempio, *ne hanno **bandito l'uso** [24]* mentre in Europa, con la MiCA (titolo V, art. 64), queste saranno negoziabili **esclusivamente nel caso in cui gli utenti possano essere identificati e le transazioni tracciate.**

Due asset particolarmente interessanti come riserva di valore sono:

- **Le opere d'arte sotto forma di NFT**:

  Aprono diverse opportunità in termini di garanzie di autenticità, unicità e facilità di trasferimento ma l'arbitrarietà del loro valore e la possibile anonimità dei soggetti coinvolti nelle compravendite espongono a grandi rischi legati al riciclaggio di denaro e all'evasione fiscale.

- **Le stablecoin**: **token ancorati al valore di un asset sottostante**, tipicamente rappresentato da valute fiat come il dollaro americano (BUSD, USDT, USDC) o lo yuan cinese (TCNH); i rischi a queste associati sono connessi ad aspetti quali:

  - La **qualità dei meccanismi per convalidare che la totalità delle attività detenute in custodia dall'emittente di tali stablecoin sia maggiore dell'importo totale delle passività**; quando questi meccanismi sono affidabili sono noti come **Proof of Solvency.**

  - La **qualità del sistema di ancoraggio** al valore fiat di riferimento.

  - Nel caso di stablecoin algoritmiche, la **qualità degli algoritmi** che gestiscono la quantità di stablecoin in circolazione e conseguentemente, l'ancoraggio.

Alcuni casi particolarmente rilevanti nel contesto delle stablecoin sono:

- la recente perdita dell'ancoraggio al dollaro di molte stablecoin come USDC *[25]*, conseguentemente al fallimento della Silicon Valley Bank *[26]*
- il recente caso di fallimento da 42 miliardi di Terra-Luna *[27]* e della stablecoin algoritmica associata UST, che hanno portato all'arresto del fondatore Du Kwon *[28]*.

La natura decentralizzata dei sistemi basati su blockchain non comporta solo rischi ma anche numerosi benefici. L'assenza di intermediari nel trasferimento dei token di moneta elettronica, per esempio, riduce notevolmente le tempistiche rispetto a quelle dei pagamenti transfrontalieri nelle infrastrutture finanziarie classiche.

Le stablecoin, quindi, rappresentano le candidate perfette **per lo sviluppo di sistemi che siano efficienti nel trasferire economicamente e velocemente valore.**

Alcuni esempi di sistemi efficienti nel trasferimento rapido di valore sono **Stellar Lumens (XLM)** che è ampiamente usata in paesi come il Venezuela e la Nigeria **e il sistema sviluppato dall'azienda Ripple**, recentemente protagonista di una *causa legale intentata dalla SEC [29]* rispetto alla natura finanziaria dei suoi token **XRP**.

Al fine di facilitare il trasferimento di denaro real-time a costi ridotti, l'integrazione di questa tipologia di sistemi nell'infrastruttura finanziaria classica è in fase di sperimentazione; alcuni esempi di questo sono i sistemi della Federal Reserve, FedNow e JPM Coin di JP Morgan.

"A permissioned system that serves as a payment rail and deposit account ledger, that allows participating J.P. Morgan clients to transfer US Dollars held on deposit with J.P. Morgan within the system, facilitating the movement of liquidity funding and payments in right time." [30]

Le **Central Bank Digital Currencies** *[31]* (**CBDC**) sono un'altra delle **possibili applicazioni della tokenizzazione della moneta** e rappresentano l'idea di un **sistema di moneta elettronica nazionale o comunitaria, estremamente veloce ed economico, garantito dal sistema di banche centrali**. Le CBDC **rappresentano l'evoluzione del sistema finanziario contemporaneo**.

A questo proposito non mancano le preoccupazioni, con personaggi come Charles Hoskinson, CEO di Cardano, e Srinivasan, CTO di Coinbase, che *"identificano le CBDC come una minaccia alla sovranità personale e gridano al bitcoin come unica forma di possibile dissenso politico nella distopia del Dollar Wall e delle Ponzi Economics". [32]*

Nonostante i timori e i dubbi, permane una realtà: le CBDC rappresentano un approccio più sicuro, più economico, più veloce e meno oneroso di gestione della moneta e, conseguentemente, la prossima rivoluzione delle infrastrutture bancarie e del settore finanziario.

2.4.2 Mercati paralleli

Tra i possibili use-case dei token, sia fungibili che non, c'è quello degli spazi online. **I token sono estremamente efficaci quando combinati con il concetto di collezionabili**[3] *[33]* **tipico dei videogiochi.** Ad esempio, esistono giochi che ricompensano la partecipazione degli utenti con token fungibili spendibili in gioco o con NFT associati ad oggetti di gioco. **Questa applicazione dei token conduce ad un'espansione delle economie parallele tipiche dei giochi on-line** *[34]* **portando allo sviluppo di un sistema di quotazione dei suddetti token, che possono poi essere scambiati sui mercati con altri token o con valuta fiat.** Conseguentemente, si sviluppano **nuove opportunità di guadagno, nuovi possibili sistemi di arbitraggio e nuovi rischi per i consumatori.** Uno dei più noti giochi di questo tipo è Axie Infinity.

Questo tipo di attività non è vincolata all'ambiente videoludico ma rappresenta **una possibilità per qualsiasi spazio virtuale in cui si introducono token**, ne è un esempio il contesto metaverso. Opportunità di business, di gioco e di advertising, conducono soggetti alla costruzione di spazi virtuali attraverso l'uso di token nativi di apposite piattaforme e che, probabilmente, sono stati comprati con valuta fiat su una piattaforma terza. Questo dà luogo ad **instabili economie parallele che espongono ad un serio rischio, quantomeno finanziario, tutti i soggetti coinvolti** *[35]***.** Esempi di token di questo genere possono essere SAND, MANA e altri ancora.

Oltre al mondo del gaming e del metaverso la tokenizzazione è alla base dei sistemi di finanza decentralizzata (DeFi) caratterizzata dall'offerta, tramite applicazioni decentralizzate (dApps) e DLT, di una serie di servizi legati sia alla tecnologia DLT in sé che al contesto finanziario, tra cui:

- rendimenti e interessi attraverso "conti risparmio" in cui vengono depositati token
- negoziazione di asset
- prestiti
- accesso a derivati

In generale, tali mercati paralleli risentono di problematiche comuni legate sia alla natura decentralizzata della tecnologia che all'assenza di sistemi regolatori, alcuni esempi sono:

- la mancanza di un chiaro sistema di quotazione degli asset digitali
- difficoltà di attribuire un valore allo **spazio digitale**
- **rischio di manipolazione del mercato delle varie piattaforme coinvolte**
- **evasione fiscale**
- **riciclaggio di denaro**

[3] Oggetti virtuali conseguibili e/o negoziabili in gioco

2.5 Servizi Estrinseci

2.5.1 Compravendita

I mercati in cui vengono comprati e venduti i token sono tipicamente gli **exchange**, piattaforme che rappresentano la via di accesso agli asset digitali, ai token, alle criptovalute. Gli exchange offrono diversi servizi legati agli asset digitali e tipicamente consentono di:

- Detenere asset digitali.
- Acquistare token con valute fiat.
- Scambiare token con altri token.
- Utilizzare una varietà di strumenti finanziari derivati.

Gli Exchange **rappresentano quindi una piazza su cui vengono quotati token e su cui vengono svolte le operazioni tipiche della borsa, traslate nel mondo degli asset digitali; conseguentemente ne ereditano e mutano sistemi, possibilità e rischi.** Particolarmente rilevanti in questo contesto sono:

1. Il **rischio di forme di insider trading** *[36]* legate alla pregressa conoscenza di quali token saranno resi negoziabili sugli exchange.
2. La **necessità di efficaci sistemi di Proof of Solvency per prevenire bancarotte come nel recente caso dell'exchange FTX di Sam Bankman Fried.**

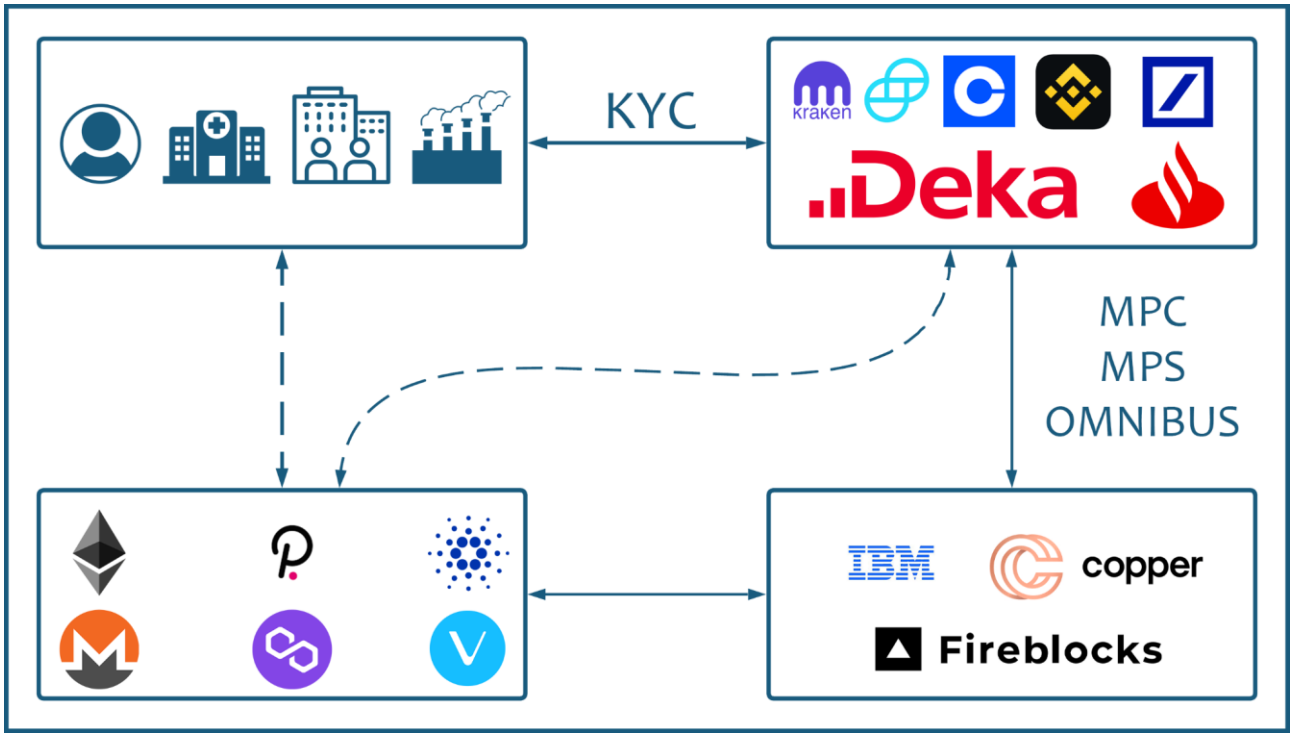
Principalmente **esistono due tipologie di exchange**, distinte in **centralizzati (CEX)** come Binance, Kraken, Coinbase, KuKoin e **decentralizzati (DEX)** come UniSwap, PancakeSwap, SushiSwap. **Un exchange centralizzato (CEX) offre servizi di scambio di asset digitali agli utenti registrati**: il suo servizio principale è quello di far incontrare acquirenti e venditori grazie a un order book. **Un exchange decentralizzato (DEX) utilizza invece smart contract on-chain per gestire i propri servizi. Per accedere a un DEX, è sufficiente avere un wallet e delle criptovalute e non è necessaria una procedura di registrazione e verifica come sui CEX.**

Per i token non fungibili invece, esistono delle piattaforme dedicate come ad esempio Rarible ed OpenSea che offrono varie possibilità, come la detenzione di NFT, la creazione di NFT e di collezioni di NFT, la compravendita di NFT e sistemi di aste di NFT.

2.5.2 Custodia

La custodia di asset ricopre un ruolo di fondamentale importanza all'interno dell'instaurazione di un ecosistema di cripto-attività sostenibile, soprattutto nell'ottica di un'adozione della tecnologia su larga scala. **Dalla modalità di custodia dipendono infatti non solo la sicurezza dei fondi, ma anche i meccanismi di Proof of Solvency, gli auditing, l'agevolezza di sviluppo e conseguentemente la tutela del mercato e di tutti i suoi partecipanti.**

Si stanno rapidamente sviluppando diverse realtà aziendali come Bakkt o FireBlocks, finalizzate all'offerta di disparati servizi di custodia attraverso tecnologie come ***Multi Party Signature (MPS), Multi Party Computation (MPC)*** e Omnibus *[37]*; servizi tipicamente adottati da piattaforme come gli exchange ed eventualmente anche da banche per custodire efficacemente le chiavi dei propri clienti.



4. Relazioni di custodia

2.6 Limiti del quadro europeo

La prima direttiva sui mercati europei degli strumenti finanziari **(MiFID) è entrata in vigore nel novembre 2007, ma durante la crisi finanziaria del 2008 alcune delle sue misure si sono rivelate viziate;** questa ignorava derivati, valute e altre attività. Di conseguenza, **nel 2014 è stato introdotto un quadro giuridico denominato MiFID II (2014/65/UE)** *[38]* per gestire in modo più efficace i mercati finanziari all'interno dell'Unione europea e per rafforzare i diritti degli investitori. **MiFID II ha aggiunto nuovi strumenti finanziari** alle regole MiFID: fondi negoziati in borsa, valute, futures, opzioni, obbligazioni, materie prime, azioni e prodotti extra europei offerti nei paesi dell'UE. **MiFID II è l'attuale normativa sui servizi finanziari in vigore in Europa** e non **copre** solo **una varietà di prodotti** ma anche quasi **tutti gli aspetti del trading e degli investimenti finanziari**, nonché **tutti gli esperti del settore**.

Nel dicembre 2017, dopo l'esplosione della capitalizzazione del mercato delle criptovalute, **la Commissione europea ha incaricato l'ABE e l'ESMA di valutare l'applicabilità e l'adeguatezza del quadro normativo dell'UE per i servizi finanziari alle cripto-attività**. Nel gennaio 2019, dal resoconto **è emerso che** nonostante alcuni cripto-asset possano rientrare nel diritto dell'UE, **la maggior parte delle cripto-attività non rientra nell'ambito di applicazione della legislazione dell'Unione**, le cui disposizioni, tra l'altro, possono impedire l'uso della DLT.

Allo stesso tempo, l'ABE e l'ESMA concordarono che **la maggior parte delle criptovalute non rientravano nella legislazione dell'UE sui servizi finanziari ma solamente in quella contro il riciclaggio di denaro e il finanziamento del terrorismo.**

Nonostante i cripto-assets comportino i rischi finanziari tipici degli strumenti classici, questi non sono quindi soggetti alle necessarie disposizioni in materia di tutela di consumatori, investitori e integrità del mercato; conseguentemente, non esistono norme per i servizi connessi alle cripto-attività, neppure per quanto riguarda la gestione delle piattaforme di negoziazione, il servizio di scambio o la custodia.

A questo proposito, sulla base dell'articolo 114 TFUE, che conferisce alle istituzioni europee la competenza di stabilire le disposizioni appropriate per il ravvicinamento delle legislazioni degli Stati membri che hanno per oggetto l'instaurazione e il funzionamento del mercato interno, la Commissione ha rilasciato quindi un **pacchetto per la finanza digitale***,* una **serie di proposte volte a garantire che la legislazione vigente non ostacoli l'adozione di nuove tecnologie, pur continuando a conseguirne i pertinenti obiettivi normativi** e che riserva particolare attenzione alla materia di quelle che vengono definite **"criptoattività"**.

2.7 Pacchetto per la Finanza Digitale:

Il pacchetto europeo sulla finanza digitale del 24 settembre 2020 vuole essere uno **strumento di modernizzazione completo**. L'UE ha adottato una **serie di strategie normative volte a creare un quadro che consentirà l'armonizzazione normativa dei mercati per le criptovalute, la tokenizzazione delle attività finanziarie tradizionali e l'uso diffuso delle DLT nei servizi finanziari**. Il pacchetto è inoltre predisposto e strutturato nel **rispetto del mercato unico e della tutela dei clienti** e delle imprese oltreché dei valori europei.

Questo è composto da:

1. Una **strategia per la finanza digitale** finalizzata a digitalizzare i servizi finanziari europei stimolando l'innovazione responsabile, soprattutto semplificando l'accesso per i consumatori ai prodotti finanziari digitali e consentendo l'espansione delle start-up finanziarie.
2. Una **strategia per i pagamenti al dettaglio**.
3. **Proposte legislative per un quadro normativo dell'UE sulle criptoattività**, in particolare:
    3.1. **un regolamento sui mercati delle cripto-attività** finalizzato al perseguimento di opportunità in un contesto di stabilità finanziaria e di protezione degli investitori;
    3.2. **un regime pilota per le infrastrutture di mercato volto a consentire la negoziazione e il regolamento di strumenti finanziari sotto forma di cripto-asset**, che consente alle aziende di sperimentare l'applicazione pratica delle norme.
4. Proposte per un quadro normativo dell'UE sulla **resilienza operativa digitale** finalizzate a **imporre a tutte le imprese l'obbligo di garantire di poter far fronte a tutti i tipi di rischi informatici.**

I capitoli seguenti sono dedicati all'analisi integrale dei punti 3.1, 3.2, e 4, rispettivamente:

- Markets in Crypto-Assets Regulation
- DLT Pilot Regime
- Digital Operational Resilience Act

3. Markets in Crypto-Assets Regulation

La proposta di regolamento del parlamento europeo e del consiglio, relativo ai mercati delle cripto-attività, **mira a posizionare l'Europa in prima linea nell'innovazione e nella diffusione della blockchain.** MiCA, sull'applicabilità dell'attuale quadro normativo dell'UE in materia di servizi finanziari alla materia delle cripto-attività e sulle considerazioni dell'ABE[4] e dell'ESMA[5], sulle consultazioni dell'EGBPI[6] e sulle consultazioni dell'opinione pubblica.

Con la MiCA *[39]***, l'UE mira a diventare un ecosistema attraente per i fornitori di servizi di cripto-asset (CASPs) per diventare il fulcro della nuova finanza digitale**, prevenendo al contempo gli abusi di mercato e proteggendo i consumatori da frodi, riciclaggio di denaro, finanziamento del terrorismo e altre attività criminali.

La proposta **riguarda le cripto-attività che non rientrano nella vigente legislazione dell'UE in materia di servizi finanziari (MiFID II), nonché i token di moneta elettronica** e persegue quattro obiettivi:

- Certezza del diritto
- Innovazione
- Tutela dei consumatori, degli investitori e dell'integrità del mercato
- Stabilità finanziaria

MiCA non si applica alle autorità europee come l'ABE, la BCE e l'ESMA, che sono esentate dagli obblighi dei fornitori di servizi e degli emittenti di cripto-attività. Prodotti come le CBDC, conseguentemente, non saranno regolamentati da MiCA.

L'articolo centoventisei del IX titolo della MiCA, **sancisce l'entrata in vigore della proposta di regolamento dal *ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea* e l'applicazione**, a meno delle disposizioni si token collegati e sui token di moneta elettronica che si applicano a decorrere dall'entrata in vigore, **a 18 mesi dopo.**

La pubblicazione in gazzetta ufficiale, inizialmente prevista per febbraio 2023 è stata posticipata alla primavera-estate 2023. L'analisi integrale si basa sul testo della proposta del 2020 a cui, nel corso della stesura dell'elaborato, sono seguiti alcuni emendamenti (12/04/2023) che integrano quanto analizzato senza introdurre modifiche rilevanti al testo; a questi emendamenti verrà dedicata una breve riflessione alla fine del capitolo. La proposta è stata approvata dal Parlamento il 20/04/2023 e sarà discussa dal Consiglio il 16 Maggio 2023, qualora venga approvata anche in questa sede, seguirà la pubblicazione in gazzetta ufficiale.

---

4 *EBA - Autorità bancaria europea (ABE)*

5 *Autorità europea degli strumenti finanziari e dei mercati (ESMA)*

6 *Expert Group on Banking, Payments and Insurance*

3.1 Definizioni

MiCA **identifica come obiettivo della regolamentazione gli obblighi dei fornitori di cripto-attività e dei fornitori di servizi a queste connessi;** vengono delineati come oggetto della proposta i procedimenti di **autorizzazione**, gli **enti** e il sistema di **collaborazioni per la vigilanza** del mercato, le disposizioni a **tutela dei consumatori** e le modalità di gestione delle **relazioni con terze parti**.

Il **terzo articolo** riporta le **definizioni delle entità di riferimento**, alcune delle quali sono imprescindibili per la comprensione di quanto segue e vengono integralmente riportate di seguito:

- ***cripto-attività****: rappresentazione digitale di valore o diritti che possono essere trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga;*
- ***token collegato ad attività****: tipo di cripto-attività che intende mantenere un valore stabile facendo riferimento al valore di diverse monete fiduciarie aventi corso legale, di una o più merci o di una o più cripto-attività, oppure di una combinazione di tali attività;*
- ***token di moneta elettronica****: tipo di cripto-attività il cui scopo principale è quello di essere utilizzato come mezzo di scambio e che mira a mantenere un valore stabile facendo riferimento al valore di una moneta fiduciaria avente corso legale;*
- ***fornitore di servizi per le cripto-attività****: qualsiasi persona la cui occupazione o attività consiste nel prestare a terzi uno o più servizi per le cripto-attività su base professionale;*
- ***servizio per le cripto-attività****: qualsiasi servizio e attività elencati in appresso in relazione a qualsiasi cripto-attività:*
  - ***custodia e amministrazione*** *di cripto-attività per conto di terzi;*
  - ***gestione di una piattaforma di negoziazione*** *di cripto-attività;*
  - ***scambio di cripto-attività con moneta fiduciaria*** *in corso legale;*
  - ***scambio di cripto-attività con*** *altre* ***cripto-attività****;*
  - *esecuzione di ordini di cripto-attività per conto di terzi;*
  - *collocamento di cripto-attività;*
  - *ricezione e trasmissione di ordini di cripto-attività per conto di terzi;*
  - *prestazione di* ***consulenza sulle cripto-attività****;*
- ***collocamento di cripto-attività****: commercializzazione a determinati acquirenti di cripto-attività di nuova emissione o di cripto-attività che sono già emesse ma che non sono ammesse alla negoziazione su una piattaforma di negoziazione di cripto-attività, senza che ciò comporti un'offerta al pubblico o un'offerta ai possessori esistenti delle cripto-attività dell'emittente.*

3.2 Token

Gli **obblighi degli emittenti di token** e i **requisiti** perché questi possano **offrire, vendere o negoziare cripto-attività nell'UE,** vengono trattati nel **II, III e IV titolo** della proposta.

L'**obbligo principale, condiviso dagli emittenti delle diverse tipologie di token**, è la **redazione di un documento informativo fondamentale**, denominato **White Paper**. Nell'articolo quattro del secondo titolo è riportato quanto segue:

"Nessun emittente di cripto-attività diverse dai token collegati ad attività e dai token di moneta elettronica, può operare o rendere negoziabili i suoi token in UE a meno di essere un soggetto giuridico che abbia redatto, notificato e pubblicato sul proprio sito web un White-Paper conforme."

3.2.1 WhitePaper

3.2.1.1 Voci comuni

Il White Paper sulle cripto-attività deve essere **accurato**, **non fuorviante, datato e redatto in almeno una delle lingue ufficiali dell'UE**; non deve inoltre contenere dichiarazioni relative al futuro valore del token a cui fa riferimento.

Per qualsiasi tipologia di token, in un White Paper gli elementi principali sono i seguenti:

- **Descrizione dettagliata dell'emittente**: nome, sede legale, data di registrazione, identificativo della persona giuridica, gruppo societario di appartenenza; **identità, indirizzo, funzione, potenziali conflitti di interesse e storia finanziaria dei membri componenti la governance dell'emittente.**

- **Descrizione dettagliata del progetto e del tipo di asset**: nome del progetto, informazioni sulle persone fisiche o giuridiche coinvolte, **motivi dell'emissione dei criptoasset**, **informazioni sull'organizzazione del progetto**, **descrizione delle milestones** e **uso previsto dei fondi raccolti dall'offerta al pubblico**.

- **Descrizione dettagliata delle caratteristiche dell'offerta pubblica**: numero di cripto-attività che saranno emesse o ammesse al trading e prezzo di emissione della criptovaluta.

- **Descrizione dettagliata dei diritti e degli obblighi connessi** all'asset, nonché le procedure e le condizioni per l'esercizio degli stessi.

- **Informazioni sulle tecnologie e gli standard** per la detenzione, l'archiviazione e il trasferimento degli asset, sulla tecnologia di registro distribuito adottata; **descrizioni dell'algoritmo di consenso**, **dei meccanismi di incentivazione** per garantire le transazioni e **informazioni sui risultati degli audit** della tecnologia implementata.

- **Descrizione dettagliata dei rischi** relativi all'emittente, alle cripto-attività, all'offerta al pubblico e all'attuazione del progetto.
- Dichiarazione di conformità del White Paper e dichiarazione: ***"L'emittente delle cripto-attività è l'unico responsabile del contenuto del presente White Paper, il***

quale non è stato esaminato o approvato da alcuna autorità competente in alcuno Stato membro dell'Unione europea"*.*

- **Sintesi** delle informazioni fondamentali in linguaggio non tecnico, **accompagnata da un'avvertenza** sull'importanza della lettura integrale del documento.

- Inequivocabili **dichiarazioni** equivalenti alle seguenti:
    - "le **cripto-attività possono perdere tutto il loro valore** o parte di esso"
    - "le cripto-attività **possono non essere sempre trasferibili**"
    - "le cripto-attività **possono non essere liquide"**

Gli emittenti di token sono integralmente responsabili del contenuto dei White Paper dei token da loro emessi. Gli articoli quattordici del II titolo, ventidue del III titolo e quarantasette del IV titolo stabiliscono che ***qualora un emittente abbia fornito in un White Paper informazioni inadeguate, il possessore di tali token ha il diritto****, presentando prove attestanti la violazione e l'impatto di questa sulla sua decisione di interagire con i suddetti token,* ***di richiedere un risarcimento*****.**

3.2.1.2 Voci specifiche, Token di attività

Data la natura dei token collegati ad attività, che sono vincolati ad una riserva di valore, la "riserva di attività", questi devono integrare i contenuti fondamentali del White Paper con delle informazioni tra cui:

- La **struttura dei meccanismi e dei dispositivi di governo dell'emittente**.
- L**a riserva di attività,** in particolare relativamente alle **modalità di custodia**, alla **composizione** e alla **politica d'investimento**.
- T**ipo di diritti** che i clienti legati ai beni possono vantare nei confronti della riserva.
- Informazioni dettagliate sui **sistemi che regolano la liquidità dei token**.
- Procedura di trattamento dei reclami.

3.2.1.3 Voci specifiche, Moneta elettronica

Gli emittenti di token di moneta elettronica devono invece integrare le informazioni fondamentali con:

- La **struttura dei meccanismi e dei dispositivi di governo dell'emittente**.
- **Una dettagliata descrizione dei diritti dei fruitori dei token di moneta elettronica**.
- **Esplicite indicazioni relative al diritto al rimborso "*in qualsiasi momento e al valore nominale"*** (art. 46 titolo IV)**.**

3.2.1.4 Modifiche

Nell'eventualità avvengano modifiche o fatti che potrebbero influenzare la decisione di acquisto di un potenziale acquirente o le decisioni di vendita, scambio, MiCA prevede che gli emittenti di token siano obbligati a riportare tali, corredati di data, nel documento fondamentale. L'integrazione delle modifiche nelle informazioni del White Paper deve essere operata senza alterare l'ordine del documento originale e a questa deve seguire una pronta notifica dei clienti, corredata delle giustificazioni e accompagnata da una segnalazione dei cambiamenti alle autorità competenti.

Dagli art. 11, 21, 35, 46 emerge come significativa qualsiasi variazione di: dispositivi di governance, attività di riserva, custodia delle attività di riserva, diritti riconosciuti ai possessori di token, meccanismi di emissione, creazione e distruzione dei token, protocolli per la convalida delle operazioni, funzionamento della DLT sottostante, meccanismi di rimborso, meccanismi a garanzia della liquidità, accordi con terzi e della procedura di trattamento dei reclami.

3.2.1.5 Notifiche

MiCA definisce anche le tempistiche e le modalità con cui devono essere notificati, sia ai clienti che alle autorità competenti, White Paper o eventuali modifiche di questi; queste differiscono in base alla tipologia di token a cui si fa riferimento.

- **Tutti gli emittenti di token, devono obbligatoriamente notificare il White Paper** all'autorità competente del loro Stato membro d'origine prima della pubblicazione, **accompagnando la notifica con un elenco degli eventuali Stati membri ospitanti in cui intendono offrire o negoziare le loro cripto-attività e la data prevista per l'inizio dell'offerta, negoziazione**. Qualora l'autorità competente lo ritenesse necessario, può consultare sia l'ABE che l'ESMA e la BCE ed eventualmente richiedere la **messa in atto di meccanismi a garanzia della tutela dei consumatori e della stabilità finanziaria.**

- **Gli emittenti di token collegati ad attività o di moneta elettronica** sono tenuti alla **notifica di tutte le modifiche al WhitePaper** in quanto **il documento è il contenuto centrale della domanda che questi devono inoltrare per conseguire l'autorizzazione** all'emissione o all'ammissione alla negoziazione delle cripto-attività.

- Entro la data di inizio dell'offerta di una criptoattività, il relativo **WhitePaper deve essere reso di dominio pubblico** sul sito web del rispettivo emittente.

3.2.1.6 Marketing

Le comunicazioni di marketing operate dagli emittenti di token devono essere **chiaramente identificabili, non fuorvianti e coerenti con quanto riportato nel White-Paper, di cui devono riportare la posizione web**. Le comunicazioni di marketing devono contenere chiare indicazioni dell'eventuale assenza di diritti di rimborso e vanno riportate sulla medesima pagina web del White Paper, dove permangono finché i token sono offerti al pubblico. Particolare attenzione viene riservata agli aspetti connessi alle comunicazioni di marketing relative ai token di moneta elettronica; come i WhitePaper, **devono contenere una dichiarazione chiara e inequivocabile attestante che tutti i possessori di token di moneta elettronica beneficiano del diritto al rimborso in qualsiasi momento e al valore nominale da parte dell'emittente.**

Per quanto concerne il ruolo e le responsabilità di personalità influenti, come youtuber, streamer e influencer che sponsorizzano **cripto-attività** che si rivelano poi essere truffe finanziarie o *schemi "Pump and Dump",* la materia è disciplinata nell'articolo 80 della sezione "Abusi di Mercato" del VI titolo. A titolo informativo, seguono alcuni casi americani in cui la controversa condotta di note personalità è attualmente oggetto d'indagine:

- *Elon Musk, il caso Dogecoin e la causa da 258 miliardi di dollari [40]*.
- *La recente citazione a giudizio, in una causa da un miliardo di dollari, di note personalità di youtube che hanno sponsorizzato l'exchange, ormai fallito, FTX [41]*.
- *La recente citazione a giudizio di personalità del mondo dello spettacolo, accusate di aver abusato della loro influenza per realizzare schemi di "Pump and Dump" nella sponsorizzazione del token Safemoon [42].*

3.2.2 Autorizzazione

Con la MiCA, l'UE stabilisce che gli emittenti di criptoattività e i fornitori di servizi connessi, per emettere token o chiedere l'ammissione di questi alla negoziazione, **debbano richiedere l'autorizzazione all'autorità competente del rispettivo Stato membro d'origine**. L'**autorizzazione,** concessa dall'autorità competente, è **valida per tutta l'Unione** e consente all'emittente di emettere o ammettere alla negoziazione in tutto il territorio dell'Unione i token per cui è stato autorizzato.

Come per il White Paper, le modalità di domanda, i contenuti e **le modalità di emissione delle autorizzazioni, sono differenziate in base alla tipologia di token a cui fanno riferimento.** Il caso dei **token diversi da quelli collegati ad attività e diversi dai token di moneta elettronica** è quello più lasco. Nell'**articolo dieci del titolo II** viene stabilito che **la pubblicazione di un White Paper conforme è sufficiente perché la cripto-attività diversa dai token collegati ad attività e dai token di moneta elettronica possa essere offerta in tutta l'Unione** o proposta per l'ammissione alla negoziazione su una piattaforma di negoziazione di cripto-attività. **I requisiti diventano progressivamente più stringenti**; l'**articolo quindici del titolo III** stabilisce infatti l'**impossibilità per gli emittenti di token collegati ad attività, a meno di aver ricevuto un'apposita autorizzazione, di offrire token al pubblico nell'Unione o di chiedere l'ammissione di questi alla negoziazione** su una piattaforma di negoziazione di cripto-attività nell'Unione. **L'Unione ha riservato l'approccio più rigoroso ai token di moneta elettronica,** in quanto questi **potrebbero rappresentare una seria minaccia per la stabilità finanziaria**. *Si pensi all'impatto che potrebbe avere sul piano finanziario internazionale una moneta elettronica transfrontaliera, trasferibile velocemente, garantita e distribuita da un'impresa come Meta ai 3.59 miliardi di utenti [43] presenti sulle sue piattaforme. Non a caso il progetto del token libra-diem di Facebook non è stato rilasciato [44].*

Con la MiCA, l'UE armonizza gli enti emittenti di token di moneta elettronica rispetto al già esistente quadro normativo sull'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica; questi, devono essere **autorizzati come enti creditizi**, cioè ***"imprese la cui attività consiste nel raccogliere depositi o altri fondi rimborsabili dal pubblico e nel concedere crediti per proprio conto"***. Gli emittenti di token di moneta elettronica, per essere autorizzati all'emissione dei loro token o per richiederne l'ammissione alla negoziazione su una piattaforma di trading di criptovalute, devono, oltre ad aver pubblicato White Paper conformi, essere:

1. **Autorizzati come enti creditizi o istituti di moneta elettronica** ai sensi della direttiva sull'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica 2009/110/CE.

2. **Conformi ai requisiti applicabili agli istituti di moneta elettronica** riportati nei titoli II e III della direttiva 2009/110/CE.

3.2.2.1 Struttura

Le specifiche sulle informazioni contenute nella domanda di autorizzazione e i formati, modelli e procedure standard per la domanda di autorizzazione **rimangono in fase di elaborazione da parte dell'ESMA e dell'ABE** che ha però già fornito alcune linee guida. Dal momento che i token diversi dai token collegati ad attività e da quelli di moneta elettronica risultano essere autorizzati d'ufficio in seguito alla pubblicazione di un White Paper conforme e che i token di moneta elettronica debbano, eccetto quanto concerne il White Paper, essere autorizzati ai sensi di un'altra direttiva, il caso più interessante in termini di composizione della domanda di autorizzazione è rappresentato dai token collegati ad attività.

Dall'articolo sedici del titolo lll emerge che **la domanda di autorizzazione** per l'offerta di token debba essere composta da: il **White Paper sulle cripto-attività** per cui si domanda l'autorizzazione, la **struttura**, l'**organizzazione** e l'indirizzo **dell'emittente**; un **programma operativo dettagliato che definisca il modello di business** dell'emittente e un **parere giuridico formale che stabilisca che i token associati all'attività non rientrano tra gli strumenti finanziari, la moneta elettronica, i depositi o i depositi strutturati**.

A cui vanno aggiunti una **descrizione dettagliata dei dispositivi di governance** dell'emittente, l'**identità dei membri degli organi di governo** dell'emittente e una **dimostrazione che le persone al controllo dell'emittente dispongano dei necessari requisiti**.

Particolare rilevanza viene attribuita alle responsabilità delegate alle terze parti e alle informazioni inerenti alla sicurezza e alla resilienza informatica, che non devono mancare:

- Descrizione degli **accordi contrattuali con i terzi**.
- Descrizione della **politica di continuità operativa** dell'emittente.
- Descrizione dei **meccanismi di controllo e delle procedure di gestione del rischio**.
- Descrizione delle **procedure e dei sistemi a tutela della sicurezza, compresa la cyber sicurezza, dell'integrità e della riservatezza delle informazioni.**
- Descrizione delle **procedure di trattamento dei reclami dell'emittente.**

L'attenzione riservata alle terze parti e all'individuazione di chiare catene di responsabilità è una costante della proposta di regolamentazione. Gli articoli 13, 26, 30, 32 e 33, insistono sull'importanza di mantenere i sistemi e i protocolli di accesso nel rispetto delle norme dell'Unione, sulla necessità di politiche che garantiscano la continuità operativa, e sulla necessità di audit. Questi concetti vengono meglio esplorati nel titolo V, riservato agli obblighi dei fornitori di servizi per le cripto-attività (CASPs) e sono strettamente correlati alle direttive per la sicurezza e la resilienza informatica e del settore delle telecomunicazioni contenute nel Digital Operational Resilience Act (DORA).

3.2.2.2 Valutazione

Le domande di autorizzazione vengono inoltrate all'ente competente dello Stato dell'unione designato dall'emittente di cripto-attività; la domanda viene presa in carico e valutata. Nell'eventualità questa soddisfi i requisiti, l'ente competente è tenuto all'inoltro della domanda, accompagnata dalla valutazione, all'EMA, all'ESMA e alla BCE che entro due mesi devono rispondere con un parere non vincolante. Sulla base della valutazione iniziale e del parere non vincolante, l'ente competente determina, entro un mese, se concedere o meno l'autorizzazione e notifica di tutte le autorizzazioni concesse l'EMA, l'ESMA e la BCE.

Nell'eventualità vengano commesse gravi violazioni delle disposizioni, l'autorizzazione rimanga inutilizzata per lungo tempo, l'emittente venga sottoposto a liquidazione ordinata o in generale non sussistano più le condizioni per l'autorizzazione, **l'ente competente revoca l'autorizzazione e notifica della revoca l'EMA, l'ESMA, la BCE e le terze parti con cui l'emittente intrattiene rapporti.**

3.3 Fornitori di Servizi

Il V titolo riguarda i fornitori di servizi connessi alle cripto-attività e comprende le piattaforme di trading per cripto-asset come possono essere gli exchange, i servizi di scambio di cripto-asset con valute fiduciarie in corso legale o con altri cripto-asset, la consulenza finanziaria sulle cripto-attività e la custodia dei cripto-asset.

3.3.1 Autorizzazione

I servizi, per essere a norma con gli articoli 53, 54 e 55 del V titolo della MiCA, devono essere forniti esclusivamente da **persone giuridiche in possesso di un'autorizzazione specifica e con la sede legale in uno Stato membro dell'Unione**. Essere in possesso di un'autorizzazione implica la possibilità di fornire il servizio per cui si è autorizzati in tutta l'Unione.

La domanda di autorizzazione deve essere presentata all'autorità competente dello Stato membro in cui il fornitore di servizi ha la sede legale e deve essere composta da voci come: il nome, la denominazione legale e le denominazioni commerciali del fornitore, l'indirizzo fisico e del sito web, lo statuto, la descrizione della governance, la descrizione dei tipi di servizi per cui si richiede l'autorizzazione e la modalità di commercializzazione di questi. A queste, vanno aggiunte:

- La dimostrazione che i membri dell'organo di gestione di tale emittente **dispongano del tempo, dell'esperienza, della competenza e dei requisiti di onorabilità** necessari e **la prova, per tutti coloro che detengono una quota rilevante** (≥20%) del capitale o dei diritti di voto, **dell'assenza di precedenti penali in diritto commerciale e fallimentare o in materia di servizi finanziari, riciclaggio, terrorismo e obblighi di responsabilità professionale**;
- Una descrizione del meccanismo di controllo interno, della procedura per la **valutazione del rischio e del piano di continuità operativa**;
- Una **descrizione dei sistemi informatici e dei dispositivi di sicurezza** in linguaggio tecnico e non;
- Una descrizione della procedura per la separazione delle cripto-attività e dei fondi del cliente, del **sistema per individuare gli abusi di mercato e delle modalità di gestione dei reclami**;

Inoltre, **nell'eventualità il fornitore di servizi richiedente intenda: garantire la custodia e l'amministrazione delle cripto-attività per conto di terzi, gestire una piattaforma di negoziazione, eseguire ordini di cripto-attività per conto di terzi o ricevere e trasmettere ordini di cripto-attività per conto di terzi,** allora, questo deve fornire rispettivamente: **una descrizione della politica di custodia, una descrizione delle norme operative della piattaforma di negoziazione, una descrizione della politica di esecuzione degli ordini o la dimostrazione che il consulente che agisce per conto del fornitore di servizi richiedente disponga delle competenze appropriate.**

Le richieste di autorizzazione vengono poi sottoposte alle autorità competenti che entro tre mesi dalla ricezione della domanda di autorizzazione emettono un giudizio; l'ESMA viene informata di tutte le autorizzazioni emesse e ne registra i dettagli in un apposito registro. L'articolo 56 del V titolo, stabilisce che nell'eventualità:

- l'autorizzazione non venga utilizzata entro 18 mesi dall'emissione
- l'autorizzazione non venga utilizzata per 9 mesi consecutivi
- avvengano gravi violazioni delle disposizioni
- vengano meno i requisiti entro cui è stata concessa l'autorizzazione

allora, le autorità competenti devono ritirare l'autorizzazione conferita al fornitore di servizi e informare del ritiro l'ESMA e le autorità competenti degli altri paesi in cui il fornitore offre i servizi. **La revoca può riguardare anche l'autorizzazione alla prestazione di uno tra più servizi.** I **fornitori di servizi devono inoltre stabilire, attuare e mantenere adeguate procedure a garanzia di un tempestivo e ordinato trasferimento delle criptoattività e dei fondi dei clienti a un altro fornitore di servizi per le cripto-attività, nell'eventualità venga loro revocata l'autorizzazione alla prestazione dei servizi.**

3.3.2 Obblighi e Requisiti

Il secondo e il terzo capo del quinto titolo, riguardano gli obblighi e i requisiti a cui sono soggetti i fornitori di cripto-attività. I fornitori di servizi hanno l'obbligo di agire in modo onesto, equo e professionale in conformità con i migliori interessi dei loro clienti e potenziali clienti, che devono essere informati con informazioni corrette, chiare e non fuorvianti sulle cripto-attività e sui rischi delle transazioni dei suddetti asset.

3.3.2.1 Requisiti Prudenziali

MiCA stabilisce che i fornitori di servizi connessi alle cripto-attività debbano soddisfare una serie di requisiti prudenziali, il cui importo deve essere quantomeno pari al maggiore tra i requisiti patrimoniali minimi permanenti, che variano tra i 50mila e i 150mila euro a seconda del servizio offerto, o a **un quarto delle spese generali fisse dell'anno precedente**.

Le garanzie prudenziali possono assumere le seguenti forme: fondi propri, una forma di **polizza assicurativa** che copra i territori dell'Unione in cui sono forniti servizi di cripto-attività o una garanzia comparabile; la polizza deve essere **sottoscritta con un'impresa terza autorizzata**, la sua durata iniziale non deve essere inferiore a un anno e il periodo di preavviso per la cancellazione della stessa deve essere di almeno 90 giorni.

La copertura assicurativa deve coprire una varietà di aspetti, tra cui: perdite di documenti, **rilasci di dichiarazioni false o fuorvianti**, atti, errori, **omissioni** che determinino la **violazione di obblighi legali** e regolamentari, oltre ad eventuali violazioni degli obblighi di correttezza e di riservatezza.

MiCA, prevede che la copertura valga anche nell'eventualità emerga l'assenza di appropriate procedure per prevenire i conflitti di interesse o nel caso di perdite dovute a interruzioni dell'operatività, disfunzioni del sistema o grave negligenza nella tutela degli asset dei clienti. La polizza assicurativa sottoscritta deve essere resa pubblica attraverso il sito web del fornitore di servizi.

3.3.2.2 Requisiti di Organizzazione

I requisiti organizzativi, oltre a riguardare onorabilità e competenze della governance, obblighi di competenza del personale assunto e obblighi di istituzione di opportune procedure per il trattamento dei reclami, richiedono **particolare perizia nell'adozione di adeguate misure a garanzia della continuità dei servizi, compresa la resilienza dei sistemi di TIC, che devono essere conformi al Digital Operational Resilience Act (DORA)**. In questo contesto, le procedure che devono essere messe in atto comprendono: meccanismi di controllo interno e di valutazione del rischio, registrazione di tutti i servizi per le cripto-attività offerti e procedure per il monitoraggio degli abusi di mercato.

L'articolo 63, stabilisce i requisiti che devono essere rispettati dai fornitori di servizi che offrono attività di custodia; questi, devono **disporre di adeguati meccanismi per tutelare i diritti di titolarità dei clienti anche in caso di insolvenza del fornitore di servizi** e **devono prevenire l'uso delle cripto-attività di un cliente per conto proprio** a meno di un esplicito consenso. **I fondi dei clienti devono, inoltre, essere depositati presso una banca centrale o un ente creditizio** e in conti distinti da quelli in cui il fornitore detiene i propri.

L'urgenza di una regolamentazione sui fornitori di servizi legati alle criptoattività, soprattutto per quanto concerne le attività di custodia, risulta particolarmente evidente se si analizzano situazioni come la bancarotta dell'exchange FTX avvenuta a novembre 2022.

L'exchange bahamense FTX ha abusato dei fondi dei clienti, utilizzando questi come collaterale per operazioni finanziarie orientate al finanziamento di imprese correlate ad FTX stesso come Alameda Research; per giunta, buona parte delle manovre finanziarie illecite sono state effettuate utilizzando il token nativo di FTX, FTT, il che ha reso più complessa l'analisi delle dinamiche e più grave l'impatto sul mercato delle cripto-attività.

L'attività di blockchain analytics operata da imprese come Coindesk ha smascherato pubblicamente queste **incongruenze di Proof of Reserves e di Proof of Liabilities** e ha conseguentemente condotto alla dichiarazione di bancarotta da parte di più di cento imprese correlate ad FTX, *risultando in una crisi di liquidità di decine di miliardi di dollari [45]*.

Altrettano importanti sono le politiche di prevenzione, gestione e controllo dei conflitti d'interesse tra governance, azionisti, dirigenti, dipendenti e clienti, stabilite nell'articolo 64.

Le fonti, la natura e le procedure messe in atto per la prevenzione dei potenziali conflitti d'interesse devono essere rese pubbliche sul sito web del fornitore di servizi, dove devono essere ben visibili cosicché i clienti possano prendere una decisione consapevole e informata.

3.3.2.3 Requisiti di Esternalizzazione

Nell'eventualità un fornitore di servizio si avvalga dell'**outsourcing di alcune funzionalità**, questa **non deve alterare in alcun modo né i requisiti entro cui è stata concessa l'autorizzazione né gli impegni del fornitore verso i propri clienti**. Il fornitore di servizi **rimane infatti soggetto a tutti gli obblighi contenuti nella MiCA**, in quanto, **l'esternalizzazione non può comportare la delega delle responsabilità del fornitore**. La politica di esternalizzazione deve specificare i diritti e obblighi di tutte le parti coinvolte.

Particolarmente interessante è il contenuto dei paragrafi e, f, g dell'articolo 65 che attestano il dovere di vigilanza e gestione dei rischi del fornitore di servizi verso l'ente esterno e verso i servizi esternalizzati; i fornitori devono infatti, in qualsiasi caso, mantenere un accesso diretto alle informazioni pertinenti e sono responsabili del rispetto delle norme in materia di protezione dei dati da parte dell'ente esterno. ***A questo proposito, il Digital Operational Resilience Act stabilisce i medesimi requisiti per tutte le entità finanziarie.***

È di fondamentale importanza ai fini della prevenzione di situazioni di vendor lock-in, che il piano di esternalizzazione dei servizi preveda una solida ed efficace strategia di uscita.

3.3.2.4 Obblighi Specifici

Gli articoli dal 63 al 67 del terzo capo del titolo V, riguardano gli obblighi connessi ad alcuni servizi specifici quali la custodia di cripto-attività per conto di terzi, la gestione di una piattaforma di negoziazione di criptoattività, lo scambio di cripto-attività con altre cripto-attività, l'esecuzione di ordini per conto di terzi, il collocamento di cripto-attività, la ricezione e la trasmissione di ordini per conto di terzi e la prestazione di consulenza sulle cripto-attività.

3.3.3 Custodia

Il fornitore che intende offrire un servizio di custodia per conto di una terza parte deve obbligatoriamente siglare un accordo sulla natura del servizio prestato che comprenda: le identità delle parti, i sistemi di comunicazioni adoperati tra le parti, il sistema di autenticazione adottato per i clienti, una descrizione dei sistemi di sicurezza implementati, le commissioni previste e la natura del diritto applicabile.

I fornitori di servizi di custodia per terze parti devono:

- istituire e mantenere un registro delle posizioni aperte a nome di tutti i clienti e qualsiasi movimento da loro effettuato.
- fornire in qualsiasi momento e redigere su base trimestrale, in un supporto durevole, un rendiconto del valore, delle transazioni e dei trasferimenti di tutti gli asset detenuti per i propri clienti.
- **stabilire una politica di custodia che garantisca l'impossibilità di perdere le cripto-attività dei clienti o i diritti connessi alle stesse per cause quali frodi, minacce informatiche o negligenza, anche quando la custodia riguardi le chiavi crittografiche di accesso a detti asset.**
- garantire, ove richiesto, la pronta restituzione delle criptoattività o dei mezzi di accesso alle stesse ai loro clienti.

- assicurare che gli asset dei clienti siano detenuti, nella DLT, su indirizzi separati rispetto a quelli in cui sono detenuti gli asset del fornitore del servizio.
- **assumersi la responsabilità nei confronti dei loro clienti della perdita di cripto-attività a seguito di malfunzionamenti o cyber attacchi fino ad un massimo del valore di mercato dei cripto-asset perduti.**

3.3.4 Negoziazione

MiCA, richiede che la gestione di una piattaforma di negoziazione sia soggetta a norme operative finalizzate a: valutare i requisiti e i processi di ammissione alla negoziazione, definire eventuali categorie di esclusione, stabilire procedure e commissioni per l'ammissione, stabilire criteri oggettivi e proporzionati per la partecipazione alle attività di negoziazione, garantire una negoziazione equa e ordinata, mantenere la disponibilità delle cripto-attività per la negoziazione, sospendere la negoziazione e stabilire procedure per regolare le operazioni in cripto-asset e moneta fiduciaria.

Con l'ammissione alla negoziazione, le piattaforme valutano la qualità dell'asset interessato e ne assicurano il rispetto delle norme operative; è importante osservare che **le regole operative stabiliscono che le cripto-attività con funzionalità di anonimizzazione integrate, come Zcash e Monero, non possono essere ammesse alla negoziazione, a meno che i titolari delle cripto-attività e la cronologia delle loro transazioni siano identificabili.**

Anche nel contesto delle piattaforme di negoziazione, MiCA evidenzia, nel **paragrafo 4 dell'articolo 68, l'importanza della resilienza dei sistemi, delle procedure e dei dispositivi, in quanto queste devono sempre garantire continuità operativa e condizioni di negoziazione ordinata, anche in situazioni di mercato critiche.**

3.3.5 Collocamento

I fornitori di servizi per le cripto-attività autorizzati a collocare cripto-asset, prima di concludere un accordo devono fornire all'emittente dettagli sul tipo di collocamento, quindi aspetti come la possibilità di un importo minimo di acquisto, commissioni di transazione, tempi, processi e prezzo associati all'operazione proposta, nonché le informazioni sugli acquirenti destinatari. Le norme sui conflitti di interesse dell'articolo 65 stabiliscono procedure specifiche per prevenire, monitorare, gestire e comunicare eventuali conflitti di interesse derivanti dal collocamento di cripto-attività presso i propri clienti o dalla sovrastima o sottostima del prezzo di collocamento delle cripto-attività.

Il collocamento sregolato, insieme alle Initial Coin Offering (ICO), rappresenta una delle situazioni più problematiche nel settore delle cripto-attività. Spesso, offerte di questo genere risultano in schemi definiti "Pump and Dump" o in situazioni di fortissima speculazione finanziaria che danneggiano gravemente il mercato e conseguentemente la fiducia degli investitori nel settore e nelle DLT. Un caso molto controverso in questi termini, è il progetto Internet Computer (ICP) della Dfinity Foundation: tra il 2017 e il 2021, prima di ammettere ICP alla negoziazione, la Dfinity Foundation ha condotto una serie di collocamenti privati verso il proprio staff, verso Venture Capital e investitori retail a prezzi inferiore al dollaro (*0.03$ per token [46]);* l'ammissione alla negoziazione del token tramite exchange come **Binance** e l'interesse che questo aveva suscitato nel grande pubblico, hanno condotto rapidamente il valore del token a 700$ rendendo ICP, per un breve periodo, dopo Bitcoin ed

Ethereum, il terzo cripto-asset per capitalizzazione. Il token ha poi rapidamente perso valore, ed è arrivato, a marzo 2023, a valere il 99.37% in meno rispetto all'ATH (All Time High).

La poca trasparenza di Dfinity rispetto all'allocazione dei token precedente all'ammissione alla negoziazione di ICP, la perdita del 90% del valore in un mese dall'ammissione alla negoziazione e le segnalazioni dei retail che lamentavano di non riuscire a liquidare i propri asset, hanno spinto diverse aziende del settore ad indagare la situazione attraverso strumenti di chain-analysis *[47]*.

Una di queste, **Arkham**, ha prodotto un ***report*** *[48]* da cui sono emersi 44 indirizzi sospettati di appartenere ad insider e da cui sono stati liquidati sugli exchange, durante il periodo dell'ammissione alla negoziazione, decine di milioni di token ICP per un valore, all'epoca, di oltre 2 miliardi di dollari. *La mancanza di trasparenza sulla distribuzione dei token ICP ha portato all'avvio di un'azione legale collettiva in California.*

Un altro esempio interessante è il token **Refinable**. Refinable, è un token nativo di un marketplace NFT ed era stato sponsorizzato dal noto youtuber **MrBeast** ai suoi 139 milioni di iscritti. Il token è stato ammesso alla negoziazione ad aprile 2021 su exchange decentralizzati, come *PancakeSwap,* al prezzo di 0.033$. Complici l'interesse del grande pubblico e l'incapacità infrastrutturale della piattaforma di negoziazione, che è collassata sotto l'enorme volume di ordini, in poche dozzine di secondi il token è arrivato a valere 9$ per poi perdere rapidamente buona parte del suo valore *[49]*. Il token refinable vale, a marzo 2023, il 99.92% in meno dal suo ATH. Meno della metà del prezzo di lancio.

La questione delle ICOs e dei collocamenti, dovrebbe condurre anche ad una riflessione sugli "sniperbot"; tool che permettono il trading automatizzato e che sono in grado di eseguire operazioni e monitoraggio delle condizioni di mercato a velocità elevatissime; questi, dovrebbero essere soggetti alla vigilanza nel rispetto delle disposizioni contenute nelle regolamentazioni sul *trading ad alta frequenza [50]* **(HFT)** e prevenire i rischi per gli utenti derivanti da *pratiche illecite come spoofing, smoking, front running, stuffing e layering [51]*.

3.3.6 Consulenza

La priorità dei fornitori di servizi di consulenza deve essere quella di garantire la massima compatibilità tra le cripto-attività e le necessità dei propri clienti. A questo titolo, oltre a garantire che i consulenti e coloro che informano i clienti abbiano le competenze necessarie, il fornitore del servizio di consulenza deve operare, all'inizio e ogni due anni, un'opportuna valutazione delle conoscenze, degli obiettivi e della situazione finanziaria dei propri clienti; compresa la capacità di sostenere perdite.

Nell'eventualità le valutazioni operate suggeriscano che i clienti non dispongano di sufficienti conoscenze, il fornitore deve informare i clienti che le cripto-attività, o i servizi ad esse connessi, possono non essere adatti a loro e trasmettere loro un'avvertenza sui rischi associati, che deve esplicitamente indicare chiaramente il rischio di perdita della totalità del denaro; qualora i clienti riconoscano espressamente di aver ricevuto e compreso l'avvertenza o, la valutazione del fornitore di servizi sia risultata positiva, allora il fornitore redige e comunica ai clienti, su un supporto durevole, una relazione che sintetizza la consulenza prestata, in cui specifica le richieste e le esigenze dei clienti.

3.4 Abusi di Mercato

MiCA tratta nel VI titolo *gli atti compiuti da qualsiasi persona relativamente alle cripto-attività ammesse alla negoziazione o per le quali è stata presentata domanda di ammissione alla negoziazione*; la sezione sugli abusi di mercato si sviluppa su due tematiche principali:

- **Divulgazione e abuso di informazioni privilegiate:**

Per informazione privilegiata si intende: *"un'informazione di carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti di "strumenti finanziari" o uno o più "strumenti finanziari", che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti" [52].*

Nel caso in cui possa essere garantita la segretezza delle informazioni privilegiate, queste non devono assolutamente essere divulgate a meno che richiesto dall'esercizio di una specifica professione o funzione. In aggiunta, nessuno in possesso di informazioni privilegiate deve acquistare, vendere o raccomandare, sulla base di queste, investimenti a terzi. Se la segretezza delle informazioni privilegiate non può essere garantita e queste non implicano il rischio di fuorviare o pregiudicare gli interessi del pubblico, allora **gli emittenti sono, invece, tenuti a rivelare le suddette pubblicamente e tempestivamente.**

- **Divieto di manipolazione del mercato:**

A norma dell'articolo 80 sono infatti vietate le seguenti condotte:

- Operazioni che risultano in informazioni fuorvianti in merito all'offerta, alla domanda e al prezzo di una cripto-attività o che ne fissano il prezzo a un livello anormale o artificiale.
- Operazioni che possono incidere sul prezzo di una o più cripto-attività eseguite attraverso strumenti fittizi, inganni o espedienti.
- Diffusione di informazioni che forniscono segnali falsi o fuorvianti sull'offerta, sulla domanda o sul prezzo di una cripto-attività attraverso i media, ***compresa la diffusione di informazioni non confermate****.*
- Acquisizione di una posizione dominante sull'offerta o sulla domanda di una cripto-attività che crei o possa creare condizioni commerciali inique.
- Invio di ordini fasulli o finalizzati ad alterare la percezione della situazione di mercato, wash trading *[53]* e saturazione delle piattaforme di negoziazione.
- Uso dei mezzi di informazione per esprimere pareri su cripto-attività in cui si è precedentemente acquisita posizione, al fine di approfittare degli effetti prodotti da tali pareri sul prezzo, senza avere reso pubblico detto conflitto di interesse.

3.5 Autorità Competenti

MiCA tratta in un titolo a sé stante le autorità competenti, dove ne definisce il sistema di cooperazioni, i poteri e la natura delle sanzioni.

3.5.1 Poteri

Ciascuno stato membro dell'Unione è tenuto a designare una o più autorità competenti per la materia delle criptoattività; di queste, deve esserne designata una come punto di contatto unico con le autorità europee. I minimi requisiti di cui tali enti devono essere dotati, sono definiti nell'articolo 82 e si identificano nei seguenti:

- Possibilità di richiedere o esigere informazioni da chiunque, inclusi coloro che partecipano all'esecuzione delle operazioni e, **nella misura in cui ciò sia consentito dal diritto nazionale, agli operatori di telecomunicazioni**.
- **Possibilità di sospendere**, laddove sussistano dubbi di compliance rispetto alla MiCA, **l'erogazione di un servizio**, di un token o qualora si attestino le suddette violazioni, di vietarne l'erogazione.
- **Possibilità di pubblicare o imporre la pubblicazione di informazioni** sui fornitori di servizi e sugli emittenti di token, a garanzia della tutela dei consumatori e dell'integrità del mercato.
- **Possibilità di trasferire contratti per l'erogazione di servizi ad altri fornitori di servizi.**
- Possibilità di richiedere informazioni a persone sospettate di emettere servizi o token senza autorizzazione e di imporre la cessazione dell'attività.
- Possibilità di imporre modifiche ai White Paper.
- **Possibilità di ispezioni in loco, di accesso e di sequestro di informazioni e dati in qualsiasi forma.**
- Possibilità di chiedere il congelamento o il sequestro di beni e di imporre un divieto temporaneo all'esercizio dell'attività professionale.

L'esercizio di tali poteri non è necessariamente diretto ma può anche manifestarsi sotto forma di collaborazione con altre autorità o attraverso opportune autorità giudiziarie. La collaborazione tra le autorità competenti viene disciplinata negli articoli 83 e 84 che ne definiscono le dinamiche e i ruoli; tali relazioni tra autorità sono coordinate dall'ABE e dall'ESMA (art. 84). **La cooperazione non si limita alle autorità competenti europee** ma può essere estesa sia ad autorità terze che ad autorità di paesi terzi; in qualsiasi caso, questa, **deve però avvenire nel rispetto dei requisiti imposti dal regolamento 2016/679 sulla protezione dei dati (GDPR)**, inoltre, tutte le informazioni scambiate tra le autorità devono essere mantenute riservate e sono soggette al segreto d'ufficio.

3.5.2 Sanzioni

Le segnalazioni di violazioni della MiCA e le persone che le effettuano, sono soggette alla direttiva (UE) 2019/1937 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.

L'articolo 92 definisce **l'obbligo** per tutti gli stati membri di mettere le **autorità competenti** nella condizione di **erogare sanzioni amministrative** e l'**articolo 93 ne definisce la natura**; tutte le violazioni implicano la possibilità di attuare pubbliche dichiarazioni indicanti la persona responsabile e la natura della violazione, ingiunzioni dirette e sanzioni amministrative pecuniarie.

L'entità e la dimensione della sanzione viene definita dalle autorità competenti sulla base di: gravità e durata della violazione, grado di responsabilità e capacità finanziaria del responsabile, dimensione degli utili connessi alla violazione, dimensione delle perdite di terzi connesse alla violazione, grado di cooperazione del responsabile con l'autorità, storico delle violazioni, misure attuate per prevenire le violazioni e conseguenze della violazione sugli interessi dei consumatori. Nel dettaglio, le violazioni possono riguardare:

1. **Omissioni** di notifica, redazione e pubblicazione di un **White Paper** conforme
2. **Comunicazioni di marketing non conformi**
3. **Violazioni dei diritti dei consumatori**, come l'abuso degli asset degli stessi
4. **Inconsistenze** dei protocolli **con gli standard di sicurezza europei**
5. **Inconsistenze** o frode **nelle domande di autorizzazione**
6. **Inconsistenze nei requisiti** prudenziali, organizzativi, di esternalizzazione, specifici
7. **Manipolazioni di mercato**
8. Omessa collaborazione con le autorità

La dimensione delle sanzioni dipende sia dalla natura della violazione che dal contesto di questa ed **è tipicamente connessa al fatturato dell'entità sanzionata**, ad esempio:

- Nel caso di token diversi dai token di attività e dai token di moneta elettronica, le violazioni dei punti sopra elencati possono implicare sanzioni **fino a 5.000.000 di euro o al 3% del fatturato annuo per le persone giuridiche, fino a 700.000 euro altrimenti.**

- Nel caso di token di attività, di moneta elettronica e fornitori di servizi, le violazioni degli obblighi possono comportare una sanzione **fino al 15% del fatturato annuo.**

- Nel caso di abusi di mercato, l'autorità può interdire i membri dell'organo di amministrazione della persona giuridica responsabile o la persona fisica responsabile dalle sue funzioni oltre a imporre **sanzioni amministrative fino a 500.000 euro o al 5% del fatturato annuo per le persone giuridiche, fino a 500.000 altrimenti.**

- Nel caso di omessa collaborazione con le autorità, le sanzioni possono riguardare: la revoca o sospensione dell'autorizzazione, l'interdizione dei responsabili dalle loro funzioni e dalla possibilità di negoziare criptoattività, sanzioni amministrative pecuniarie massime di valore pari ad almeno tre volte l'importo degli utili realizzati a

seguito della violazione, sanzioni fino a 5.000.000 di euro per le persone fisiche e fino a 15.000.000 di euro o al 15% del fatturato per quelle giuridiche.

In seguito all'emissione di una sanzione, le autorità competenti selezionate dagli stati competenti sono tenute alla pubblicazione di questa sul loro sito web, eccetto nel caso in cui tale pubblicazione possa pregiudicare la stabilità dei mercati finanziari o un'indagine in corso; in qualsiasi caso, l'articolo 96 stabilisce che le autorità sono tenute ad informare sia l'ABE che l'ESMA di tutte le sanzioni emesse.

3.5.3 Collegi di Vigilanza

MiCA **pone dei requisiti di vigilanza più stringenti su alcuni token che si distinguono per aspetti come la dimensione della clientela, la capitalizzazione di mercato,** il numero e il valore delle operazioni in tali token, **la rilevanza delle attività transfrontaliere e l'interconnessione con il sistema finanziario**; questi token vengono definiti ***"token significativi".***

L'articolo 98 stabilisce che gli emittenti di token significativi e, in particolare, le attività inerenti ai suddetti, sono sotto la **sorveglianza diretta dell'ABE**, che "*istituisce, gestisce e presiede un collegio consultivo di vigilanza per ciascun emittente di token significativi"* (art. 99 e art. 101). Il consiglio è composto da una varietà di soggetti:

- **ABE**
- **ESMA**
- **BCE**
- **Autorità competente dello Stato membro d'origine** dell'emittente
- **Autorità delle piattaforme di negoziazione e dei fornitori di servizi per le criptoattività interessati**
- *Nel caso di token di attività o di moneta elettronica*, **le autorità competenti degli enti creditizi o dei fornitori di servizi per le criptoattività che garantiscono la custodia** conforme delle attività di riserva o dei fondi ricevuti in cambio dei token di moneta elettronica significativi
- *Nel caso di token di moneta elettronica*, **le autorità competenti degli istituti di pagamento** (più rilevanti) **che forniscono servizi di pagamento in relazione ai token di moneta elettronica significativi**
- Altre autorità di vigilanza pertinenti

Il consiglio viene istituito allo scopo di realizzare un parere consultivo non vincolante per facilitare le funzioni di vigilanza e riguarda una varietà di aspetti legati al contesto delle criptoattività, come: modifiche ai White Paper, piani di liquidazione ordinata, conformità degli emittenti con i requisiti propri dei token di moneta elettronica e dei token di attività ed eventuali proposte di restrizione rispetto a requisiti specifici come quelli sui fondi propri.

3.5.4 ABE

Ai fini di adempiere agli obblighi di sorveglianza sugli emittenti di token significativi, l'ABE **può richiedere qualsiasi informazione pertinente a qualsiasi entità connessa ai suddetti**, in particolare: emittenti stessi, fornitori di liquidità, enti creditizi o fornitori di servizi legati alla custodia di attività di riserva, istituti di pagamento che forniscono servizi connessi ai token di moneta elettronica significativi, qualsiasi persona incaricata della distribuzione dei token e qualsiasi piattaforma di negoziazione.

Una richiesta di informazione da parte dell'ABE deve contenere le seguenti indicazioni minime: la **finalità della richiesta**, le **informazioni richieste**, un **termine entro il quale le informazioni devono essere trasmesse**, l'**importo della sanzione amministrativa pecuniaria prevista nel caso le informazioni risultino essere inesatte**.

Nel caso la richiesta di informazioni non fosse una richiesta semplice ma una "richiesta per decisione"*,* questa deve integrare i contenuti con:

- Le **sanzioni previste per la reiterazione dell'inadempimento**
- Un'indicazione del **diritto all'impugnazione della richiesta dinanzi alla commissione di ricorso dell'ABE e di ottenere il riesame della Corte di giustizia** dell'Unione europea

I funzionari dell'ABE, in possesso di un'autorizzazione scritta che specifica oggetto, finalità d'indagine ed eventuali tempistiche, hanno il diritto di:

- Esaminare qualsiasi tipo di materiale pertinente, su qualsiasi tipo di supporto
- Ottenere copie certificate, dati, estratti di documenti, procedure
- Convocare emittenti o membri degli organi di amministrazione degli stessi, al fine di interrogarli e di registrarne le risposte
- Organizzare audit
- Effettuare ispezioni in loco e apporre sigilli
- ***Richiedere la documentazione relativa al traffico telefonico e al traffico dati***

"Previa, dove necessaria, l'eventuale autorizzazione dell'autorità giudiziaria nazionale. Qualora un'autorità giudiziaria nazionale riceva una domanda di autorizzazione, essa verifica l'autenticità della decisione adottata dall'ABE e se questa risulta proporzionata e non arbitraria o eccessiva" (Art. 105 p. 6)

Le informazioni raccolte vengono poi tempestivamente comunicate al collegio di vigilanza di pertinenza. Nel caso di cooperazione con paesi terzi, il trasferimento dei dati personali in un paese terzo è soggetto al regolamento 2018/1725 ***sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati.***

La **natura delle misure che possono essere attuate dall'ABE nel caso in cui venga attestata una violazione degli obblighi** da parte degli emittenti di token, vengono

formalizzate negli articoli dal 112 al 116. Le possibili misure sanzionatorie sono riassumibili nelle seguenti:

- **Imposizione della cessazione della violazione**
- **Sanzioni pecuniarie amministrative**
- **Sanzioni per la reiterazione**
- **Sospensione dell'offerta al pubblico**
- **Divieto di offerta al pubblico**
- **Sospensione della negoziazione**
- **Divieto di negoziazione**
- **Imposizione della pubblicazione di informazioni**
- **Revoca dell'autorizzazione**

I criteri per valutare la tipologia e la dimensione della sanzione da mettere in atto, rimangono i medesimi adottati nella valutazione operata dalle autorità competenti. Le sanzioni emesse vengono sempre comunicate al pubblico, salvo le eccezioni che potrebbero compromettere indagini in atto o la stabilità finanziaria.

Se l'esercizio delle funzioni di vigilanza da parte dell'ABE rivela indizi che suggeriscono gravi violazioni della MiCA, l'ABE, conseguentemente, incarica dell'indagine un funzionario indipendente; il funzionario ha quindi accesso alle informazioni pertinenti dell'ABE e gode degli stessi diritti dell'ente in materia d'indagine.



5. Gerarchia di vigilanza nelle cripto-attività

3.6 Progetti di norme tecniche

La natura innovativa della proposta di regolamentazione dei mercati delle cripto-attività implica la necessità di eventuali, future integrazioni. MiCA tende a definire obiettivi e modalità di conseguimento di questi ma non fornisce dei chiari protocolli o standard; spesso, nella proposta è riportata infatti la seguente dicitura:

"L'ABE elabora, in stretta cooperazione con l'ESMA, progetti di norme tecniche di regolamentazione per specificare la procedura per [...] L'ABE presenta tali progetti di norme tecniche di regolamentazione alla Commissione entro il [inserire la data corrispondente a 12 mesi dopo l'entrata in vigore]."

Da un'analisi integrale della proposta di regolamento, emerge che l'ABE e l'ESMA dovranno elaborare norme tecniche relative ai seguenti aspetti:

- Modelli standard di White Paper e di approvazione degli stessi
- Strutture standardizzate delle domande di autorizzazione
- Modalità di trattamento dei reclami
- Procedure per l'identificazione e la gestione dei conflitti d'interesse
- Procedure di monitoraggio dei rischi, incluse procedure di controllo interno, di continuità operativa e di auditing
- Procedure per il calcolo dei fondi propri
- Identificazione di s*trumenti finanziari altamente liquidi e con rischio di credito minimo*
- Modalità di garanzia della liquidità dei token
- Modalità di valutazione delle acquisizioni di emittenti e fornitori di servizi
- Procedure, modelli e formati per lo scambio di informazioni tra le autorità
- Modelli per la formalizzazione degli accordi di cooperazione con entità terze
- Condizioni per cui emittenti di token e fornitori di servizi sono da considerare come "più rilevanti"

3.7 Relazione finale

Entro 36 mesi dall'entrata in vigore della MiCA, la Commissione, previa consultazione dell'ABE e dell'ESMA dovrà presentare al Consiglio e al Parlamento una relazione sull'applicazione del regolamento, oltre ad un'eventuale proposta legislativa.

La relazione rappresenta la base di partenza per la verifica dell'efficacia e dell'applicabilità del piano regolatorio europeo; sarà uno specchio della situazione dei mercati delle criptoattività nell'Unione e, pertanto, verrà sviluppata prendendo in considerazione un insieme di voci ritenute fondamentali per l'adattamento rapido e flessibile delle politiche europee, il cui obiettivo rimane il conseguimento di una posizione di leadership e l'estensione spaziale dei valori comunitari. La relazione dovrà pertanto contenere:

- Numero di emissioni di criptoattività, tipo delle criptoattività emesse, capitalizzazione di mercato delle suddette, numero di White Paper e numero di ammissioni alla negoziazione.
- Stime sui numeri di investitori e utilizzatori europei di criptoattività
- Analisi della tipologia, del valore e del numero di frodi, furti e attacchi informatici
- Analisi dei reclami dei consumatori e valutazione del grado di tutela
- Analisi delle autorizzazioni emesse, con annesso dettaglio sulla tipologia di emittente autorizzato, sui volumi di scambio di questi e sulle loro riserve
- Valutazione del mercato delle criptoattività nel suo complesso, comprendente le quote di mercato dei fornitori di servizi e le esperienze delle autorità di vigilanza
- Valutazione del grado di resilienza operativa dei vari player nel mercato
- Valutazione sull'adeguatezza del regolamento, sulla necessità di eventuali integrazioni e sulla possibilità di regimi di equivalenza per fornitori di servizi di criptoattività di paesi terzi
- Valutazione dell'impatto del regolamento sul funzionamento del mercato
- Descrizione dell'evoluzione dei modelli di business e delle tecnologie nel settore
- Analisi del regime sanzionatorio
- Valutazione della cooperazione tra le varie entità coinvolte nella vigilanza
- Valutazione dei costi sostenuti dai fornitori di servizi e dagli emittenti di token per adeguarsi agli obblighi

3.8 Emendamenti

Il testo della *proposta di regolamento del parlamento europeo e del consiglio, relativo ai mercati delle cripto-attività del 24/09/2020* **su cui si basa l'analisi presentata nel presente elaborato***,* è stato discusso ed emendato *[54]* il 12 aprile 2023 e tale versione emendata è stata approvata dal parlamento il 20 aprile 2023. Gli emendamenti non alterano in maniera significativa i contenuti della proposta di regolamento e consistono prevalentemente nell'introduzione di ulteriori definizioni, come la definizione di tecnologia di registro distribuito, e nell'*estensione di alcuni obblighi dei fornitori di servizi e degli emittenti di token ad altre entità, come gli enti creditizi*[7]*.*

Gli aspetti principali degli emendamenti introdotti dal Parlamento alla proposta della Commissione, riguardano gli NFT, le dApps e le considerazioni sull'impatto ambientale delle DLT. In particolare, nei punti introduttivi 10 e 11, si specifica che **gli NFT non ricadono all'interno del dominio della MiCA, con un'eccezione legata a quegli NFT con caratteristiche che possano caratterizzarli in qualche modo come fungibili**, come l'appartenenza a grandi collezioni o la frazionabilità degli stessi. Viene inoltre specificato che **queste considerazioni non precludono la possibilità di classificare NFT come strumenti finanziari**.

In relazione ai servizi decentralizzati, alle dApps e quindi anche alla finanza decentralizzata, nel punto introduttivo 22 si può ritrovare quanto segue:

*"**Qualora i servizi per le cripto-attività siano prestati in modo completamente decentrato senza alcun intermediario, essi non dovrebbero rientrare nell'ambito di applicazione del presente regolamento**. [...] **Qualora le cripto-attività non abbiano un emittente identificabile, esse non dovrebbero rientrare nell'ambito di applicazione dei titoli II, III o IV del presente regolamento.** I prestatori di servizi per le cripto-attività che prestano servizi in relazione a tali criptoattività dovrebbero tuttavia rientrare nell'ambito di applicazione del presente regolamento."*

Per quanto concerne l'impatto ambientale delle tecnologie DLT, il punto introduttivo 7 recita:

*"I meccanismi di consenso utilizzati per la convalida delle operazioni in cripto-attività **potrebbero avere principali impatti negativi sul clima e altri effetti negativi connessi all'ambiente. Tali meccanismi di consenso dovrebbero pertanto prevedere soluzioni più rispettose dell'ambiente e garantire che i principali impatti negativi che essi potrebbero avere sul clima e gli altri effetti negativi connessi all'ambiente siano adeguatamente individuati e comunicati** dagli emittenti di cripto-attività e dai prestatori di servizi per le cripto-attività."*

Il Parlamento impone quindi, con il punto introduttivo 110, l'integrazione all'interno del Whitepaper sulle criptoattività di informazioni *"sui principali impatti negativi sul clima e su altri effetti negativi connessi all'ambiente del meccanismo di consenso utilizzato per emettere la cripto-attività".*

[7] *art.17 del testo emendato*

4. DLT Pilot Regime

Il processo di tokenizzazione delle attività finanziarie può favorire dematerializzazione e disintermediazione della ricchezza, agevolando la prospettiva di un unico mercato globale, in cui il miglioramento delle performance tecnologiche e la flessibilità offerta dai token, possono non solo allargare la platea dei partecipanti al mercato ma anche liberare il mercato dalle limitazioni temporali legate alla finalizzazione delle operazioni finanziarie e dai costosi processi di intermediazione finanziaria *[55]*.

Al contrario della MiCA, che regolamenta quelle cripto-attività che non vengono assimilate a strumenti finanziari, il DLT Pilot Regime mira a promuovere e regolamentare, sotto criteri specifici, i mercati delle cripto-attività che possono essere equiparate a strumenti finanziari come definiti nella MiFID II, **i *Security tokens*** *[56]*.

Dal testo del regolamento:

"Tale regime pilota dovrebbe consentire alle infrastrutture di mercato DLT di essere temporaneamente esentate da alcuni requisiti specifici previsti dalla legislazione dell'Unione in materia di servizi finanziari che altrimenti potrebbero impedire loro di sviluppare soluzioni per la negoziazione e il regolamento delle operazioni in cripto-attività che rientrano nella definizione di strumenti finanziari. Inoltre, il regime pilota dovrebbe consentire all'autorità europea degli strumenti finanziari e dei mercati (ESMA) e alle autorità competenti di acquisire esperienze sulle opportunità e sui rischi specifici derivanti dalle cripto-attività che rientrano nella definizione di strumenti finanziari e dalla tecnologia sottostante. [...] Per conseguire tale obiettivo è opportuno creare un nuovo status dell'Unione per le infrastrutture di mercato DLT." [57]

Come per la MiCA, per il DLT Pilot Regime è previsto un periodo di prova, al termine del quale dovrà essere realizzato un report di analisi sull'impatto dello stesso, al fine di valutare l'efficacia delle misure adottate e le conseguenze di queste sul settore.

Il DLT Pilot Regime è diventato applicabile nel 23 marzo 2023; il report a riguardo dovrà essere realizzato dall'ESMA e consegnato alla Commissione entro cinque anni; la Commissione, dopo tre mesi dalla consegna, dovrà poi presentare un'analisi di questo al Parlamento e al Consiglio che determineranno se:

- estendere il periodo di prova
- rendere il regolamento permanentemente
- applicare delle modifiche al regolamento
- estendere l'applicabilità del regolamento ad altri strumenti

4.1 Infrastrutture di mercato

Il DLT Pilot Regime, al fine di agevolare i mercati degli strumenti finanziari tokenizzati su tecnologia a registro distribuito, introduce e definisce tre infrastrutture di mercato principali:

- Sistemi multilaterali di negoziazione DLT, detti **MTF DLT**

Circuiti di negoziazione gestiti da un'impresa di investimento o da un gestore del mercato **che permettono l'acquisto e la vendita**, **mediante l'incontro di interessi di negoziazione provenienti da una pluralità di soggetti**, di soli **valori mobiliari DLT**[8]; questi possono essere autorizzati a:

  - **assicurare la registrazione iniziale dei valori mobiliari DLT**;
  - **regolare**[9] **le operazioni** in valori mobiliari DLT contro pagamento;
  - **prestare servizi di custodia in relazione ai valori mobiliari DLT** o ai relativi pagamenti e garanzie reali;

- Sistemi di regolamento titoli DLT, detti SS DLT

Un'**infrastruttura di mercato che gestisce**, sulla base di procedure contrattuali e operative, **le diverse fasi successive alla stipula della compravendita tra intermediari**, **consentendo le attività di compensazione e liquidazione fino a pervenire al regolamento finale gestito da un *depositario centrale di titoli***[10] che regola le operazioni in valori mobiliari DLT contro pagamento.

- Sistemi di negoziazione e regolamento DLT, detti TSS DLT

Soggetti che offrono al contempo i servizi di MTF DLT e DLT SS.

8 *categorie di valori, come azioni di società, obbligazioni e altri titoli equivalenti emessi, registrati, trasferiti e stoccati mediante DLT*

9 *completamento di un'operazione su titoli*

10 *persona giuridica che opera un sistema di regolamento titoli*

4.2 Valori mobiliari DLT

Il DLT Pilot Regime non ammette alla negoziazione la totalità degli strumenti finanziari, ma ne seleziona e regolamenta alcuni sotto precise condizioni. Strumenti e condizioni vengono descritti nell'articolo 3 del regolamento.

Possono essere ammessi alla negoziazione su un MTF DLT e registrati da un CSD[11] che gestisce un sistema di regolamento titoli su un registro distribuito, esclusivamente:

- **Azioni** il cui emittente ha una **capitalizzazione di mercato inferiore ai 200 milioni** di euro.
- **Obbligazioni con un'entità di emissione inferiore ai 500 milioni di euro**, *ad esclusione delle obbligazioni sovrane, che non sono ammesse.*

I valori mobiliari DLT registrati su CSD che gestiscono sistemi di regolamento titoli DLT e MTF DLT **non possono eccedere i 2.5 miliardi di euro**. Il monitoraggio del valore di mercato dei suddetti viene effettuato quotidianamente dal CSD o dalla figura di mercato interessata e coincide con il valore di ciascuno strumento registrato, moltiplicato per il numero di valori che coincidono per ISIN[12] e che sono stati regolati quel giorno.

Con cadenza mensile, il gestore dell'infrastruttura di mercato deve presentare all'autorità competente un report che dimostri la compliance dell'attività con i requisiti di volume e di capitalizzazione degli strumenti ammessi alla negoziazione.

Nell'eventualità i valori mobiliari regolati da un'infrastruttura di mercato DLT superino la soglia dei 2.25 miliardi di euro, i gestori dell'infrastruttura di mercato devono attuare una "*procedura di transizione verso un'infrastruttura di mercato tradizionale regolamentata dalla MiFID II o al regolamento N 909/2014 UE. La strategia di transizione deve essere applicabile tempestivamente, mantenuta costantemente aggiornata ed essere condivisa con le autorità competenti e il pubblico" (art. 6 p. 6).*

11 *organizzazione che tiene in custodia titoli finanziari; opera un sistema di regolamento titoli*

12 *codice riconosciuto a livello internazionale per l'identificazione degli strumenti finanziari*

4.3 Esenzioni e Misure Compensative

Le infrastrutture di mercato sarebbero, normalmente, soggette agli obblighi della direttiva 2014/65/UE (MiFID II) e al *regolamento (UE) N. 909/2014* *relativo al miglioramento del regolamento titoli nell'Unione europea e ai depositari centrali di titoli [58]*.

Il DLT Pilot Regime prevede però, la possibilità per i gestori delle infrastrutture di mercato DLT, di richiedere l'esenzione da alcune disposizioni previste per le infrastrutture tradizionali, **a patto che questi ottemperino ad alcune condizioni**, che dipendono dal tipo di infrastruttura DLT.

4.3.1 MTF DLT

Tipicamente, nel contesto finanziario tradizionale

"*A fronte di un'operazione su valori mobiliari eseguita in una sede di negoziazione, i relativi titoli sono registrati in un CSD mediante scrittura contabile entro la data prevista per il regolamento, a meno che non siano già stati precedentemente registrati sotto tale forma."*[13]

I sistemi di negoziazione multilaterali DLT possono invece, previa esplicita richiesta di esenzione, **ammettere alla negoziazione valori mobiliari che non sono registrati presso un CSD**, purché garantiscano alcune condizioni fondamentali:

a. I valori mobiliari siano registrati in un registro distribuito;

b. Il numero di valori mobiliari in circolazione nell'MTF DLT coincida con il numero di valori mobiliari registrati nel registro distribuito in qualsiasi momento;

c. Sia garantita la custodia dei valori mobiliari DLT e dei fondi, delle garanzie per il pagamento di tali titoli;

d. Le operazioni siano regolabili quanto più possibile real-time e non oltre il secondo giorno lavorativo dall'esecuzione delle stesse;

e. Sia assicurato il contestuale pagamento del controvalore in denaro al momento della consegna dei valori mobiliari in moneta della banca centrale o token di moneta elettronica;

f. Siano confermabili con precisione, chiarezza e tempestività tutti i dettagli sulle operazioni effettuate; siano fornite informazioni chiare, precise e tempestive sulla natura delle operazioni di regolamento e sul carattere definitivo di queste;

g. Siano conservate registrazioni tali da rendere possibile la separazione dei valori mobiliari di diversi clienti senza indebito ritardo e in qualsiasi momento;

h. Esista un sistema di prevenzione e protezione dai mancati regolamenti;

13 *art. 3 p. 2 regolamento 909/2014 UE*

4.3.2 SS DLT

Un sistema di regolamento titoli DLT può essere, previa esplicita domanda, esentato da alcune disposizioni previste per i depositi centrali di titoli (CSD) nel regolamento EU 909/2014, in particolare in riferimento alle disposizioni riguardanti:

- Forma dematerializzata[14]
- Ordini di trasferimento[15]
- Conti titoli[16]
- Scritture contabili[17]
- Integrità dell'emissione[18]
- Protezione dei titoli dei partecipanti e di quelli dei loro clienti[19]

Le esenzioni, come nel caso degli MTF DLT, **vengono conferite a patto che gli SS DLT mettano in atto delle misure compensative** che perseguono il soddisfacimento dei medesimi obiettivi delle disposizioni da cui sono esentati. Perché gli SS DLT possano operare nel dominio esentato, devono soddisfare **i seguenti requisiti**:

- I **valori mobiliari devono essere registrati in un registro distribuito**;
- Il **numero di valori mobiliari ammessi deve coincidere con il numero di valori mobiliari registrati** nel registro distribuito;
- **Devono conservare registrazioni** tali da rendere possibile la separazione dei valori mobiliari di diversi clienti senza indebito ritardo e in qualsiasi momento;

Oltre alle esenzioni relative alle disposizioni sopra citate, il regolamento prevede la possibilità di esoneri aggiuntivi, riguardanti: l'estensione e l'esternalizzazione delle attività e dei servizi (art. 19 e 30 della direttiva EU 909/2014), l'ammissione di partecipanti non istituzionali al sistema di regolamento titoli (art. 2 p.19 della direttiva EU 909/2014 e art. 2 lettera f della direttiva 98/26/CE), il regolamento delle operazioni in contanti (art. 40) e sull'interazione con altre strutture di mercato (art. 50 e 53 della direttiva EU 909/2014). Tali esenzioni sono concesse a patto che:

- L'esternalizzazione non gravi sulle capacità di vigilanza e di controllo dei rischi né dell'SS DLT né delle autorità competenti;

---

14 *il fatto che taluni strumenti finanziari esistono soltanto come registrazioni in scritture contabili*

15 *ogni istruzione da parte di un partecipante di trasferire la titolarità o i diritti su uno o più titoli attraverso un libro contabile*

16 *conto sul quale i titoli possono essere accreditati o addebitati*

17 *articolo 3 direttiva EU 909/2014*

18 *articolo 37 direttiva EU 909/2014*

19 *articolo 38 direttiva EU 909/2014*

- I partecipanti al sistema di regolamento titoli godano di buona reputazione e posseggano e dispongano di un livello sufficiente di conoscenza della post-negoziazione e del funzionamento della DLT;
- L' SS DLT assicuri la consegna contro pagamento (DvP[20]), ad esempio per mezzo di token di moneta elettronica;
- L' SS DLT dimostri che l'uso di una DLT è incompatibile con i sistemi esistenti di altri CSD o altre infrastrutture di mercato oppure che la concessione di tale accesso comporterebbe costi sproporzionati

4.4 Requisiti

Il DLT Pilot Regime, in qualità di regime di prova, **prevede che le infrastrutture di mercato DLT ottemperino a una serie di requisiti supplementari**, prevalentemente **orientati alla produzione di informazioni che permettano**, in seguito, **la valutazione dell'impatto del regolamento**; le infrastrutture di mercato DLT devono garantire:

1. **Elaborazione e la pubblicazione di un accurato piano aziendale** che descriva le attività e i servizi, il personale critico, le modalità con cui operano, il tipo di DLT utilizzata, le differenze rispetto alla corrispettiva infrastruttura di mercato tradizionale, i diritti, i requisiti, le responsabilità e gli obblighi del gestore dell'infrastruttura, il diritto applicabile, il meccanismo precontenzioso di risoluzione delle controversie e la giurisdizione per intentare l'azione legale.
2. **Garanzie sui dispositivi e sistemi informatici adottati** e la costante trasparenza, disponibilità, affidabilità e sicurezza dei loro servizi e delle loro attività, **compresa l'affidabilità degli smart contracts utilizzati nella DLT**; a questo proposito, *l'autorità competente deve nominare un revisore indipendente incaricato di effettuare tale verifica" (art.6 p.4).*
3. **Adozione di adeguati dispositivi e sistemi che impediscano, nel caso venga svolta un'attività di custodia dei valori mobiliari, l'accesso non autorizzato** ai fondi dei clienti o alle connesse garanzie reali e che tutti i dispositivi e sistemi adottati a tal fine "*siano protetti dai rischi di accesso non autorizzato, pirateria informatica, degrado, perdita, attacco informatico o furto" (art.6 p.5).*
4. **La condivisione delle regole di funzionamento della DLT da loro gestita**, e quindi delle modalità di: accesso alla tecnologia di registro distribuito utilizzata, di partecipazione dei nodi di validazione, di risoluzione dei potenziali conflitti di interessi e di gestione del rischio.

[20] metodo di regolamento del settore dei titoli che garantisce che il trasferimento dei titoli avvenga solo dopo che è stato effettuato il pagamento

4.5 Autorizzazioni

4.5.1 MTF DLT

Una persona giuridica, **autorizzata ad agire quale impresa di investimento o a gestire un mercato regolamentato**[21] a norma della direttiva 2014/65/UE, può chiedere un'autorizzazione specifica a gestire un MTF DLT.

Una domanda di autorizzazione deve, come nel caso delle autorizzazioni per gli emittenti di token e dei fornitori di servizi, **esplicitare una serie di informazioni ai fini della valutazione per la concessione**; la domanda, indicativamente, deve contenere relative a quanto segue:

- ***Operazioni previste e struttura organizzativa[22]***
- Requisiti applicabili agli investitori e possibili ostacoli alle funzioni di vigilanza
- Informazioni sui requisiti supplementari esposti nella pagina precedente
- **Strategia di transizione verso infrastrutture di mercato tradizionali**
- **Esenzioni richieste, motivazioni per la richiesta** delle esenzioni e **misure compensative** attuate in proposito

Una volta ricevuta la domanda di autorizzazione, le autorità competenti iterano le medesime operazioni che accadono nel contesto MiCA. La domanda viene inoltrata all'ESMA con tutte le informazioni del caso; se l'autorizzazione riguarda un'infrastruttura di mercato che intende operare nell'intero territorio dell'unione, l'ESMA coinvolge le autorità competenti degli stati interessati. Entro tre mesi, l'ESMA pronuncia un parere non vincolante in merito.

Nell'eventualità vengano evidenziati dalla valutazione:

1. **Inadempienza dei requisiti classici di autorizzazione delle infrastrutture di mercato finanziarie[23]**
2. **Inadeguatezza delle misure compensative** adottate ai fini del conseguimento delle esenzioni
3. **Possibilità che le esenzioni richieste siano finalizzate** non all'agevolamento delle infrastrutture DLT nel mercato ma **all'elusione di requisiti giuridici**

Allora l'autorità competente respinge la richiesta di autorizzazione; **altrimenti, l'autorizzazione viene concessa ed è valida per un periodo di 6 anni nel territorio di tutta l'unione**. L'ESMA pubblica sul proprio sito web l'elenco delle autorizzazioni fornite per gli MTF DLT e l'elenco delle esenzioni a questi concesse. Qualsiasi modifica delle attività, dei servizi, delle modalità e in generale del funzionamento dell'MTF DLT deve essere

---

21 *mercati finanziari caratterizzati dalla presenza di una disciplina sull'organizzazione di mercato*

22 *ai sensi dell'art. 7 p.2 MiFID II*

23 *art. 7, 8 e 44 MiFID II*

comunicata alle autorità competenti in modo che possano verificarne la compliance rispetto ai requisiti previsti per l'autorizzazione concessa.

Se dovessero essere rilevati:

- **Vizi nel funzionamento della DLT**, nei servizi o nelle attività dell'MTF
- **Violazioni alle condizioni entro cui sono concesse le esenzioni**
- Registrazione di **valori mobiliari inadeguati**
- **Superamento delle soglie**
- Conseguimento dell'autorizzazione attraverso procedure falsate

Allora, **le autorità competenti revocano la suddetta autorizzazione e le esenzioni a questa connesse.**

4.5.2 SS DLT

Una persona giuridica, **autorizzata ad agire come CSD** a norma del regolamento (UE) n. 909/2014, **può richiedere un'autorizzazione specifica finalizzata alla gestione di un sistema di regolamento titoli DLT**. Anche nel caso dell'SS DLT, la richiesta di autorizzazione deve essere accompagnata da una serie di informazioni concernenti:

- *Le procedure di sospensione*[24]
- Piano aziendale, funzionamento della DLT sottostante, regole del sistema di regolamento, modalità di custodia e dispositivi informatici adottati
- La **strategia di transizione verso un'infrastruttura di mercato tradizionale**
- **Esenzioni richieste**, **motivazioni per la richiesta** delle esenzioni e **misure compensative** attuate in proposito

L'iter di approvazione dell'autorizzazione è il medesimo delle autorizzazioni per infrastrutture MTF DLT; la richiesta di autorizzazione viene trasmessa dall'autorità competente all'ESMA che formula, coinvolgendo gli enti opportuni ed entro tre mesi, un parere non vincolante, sulla base del quale l'autorità competente effettua la decisione.

Nell'eventualità emergano dalla valutazione:

1. Inadempienze rispetto ai requisiti classici di autorizzazione dei sistemi di regolamento titoli[25]
2. Inadeguatezza delle misure compensative adottate ai fini delle esenzioni
3. Dubbi relativi alle finalità delle esenzioni richieste

---

24 art 7 p.9 della direttiva EU 909/2014

25 *art. 17 della direttiva UE 909/2014*

L’autorizzazione non viene concessa. Nel caso in cui la richiesta di autorizzazioni risulti invece completa ed esauriente, questa viene concessa e ha validità su tutto il suolo dell'Unione europea, per una durata massima di 6 anni. Le considerazioni sulla revoca e le modifiche riportate nella sezione dedicata alle autorizzazioni per gli MTF DLT coincidono con quelle per le autorizzazioni dei sistemi di regolamento titoli DLT.

4.6 Collaborazione con le Autorità

Le infrastrutture di mercato DLT devono, in qualità di infrastrutture sperimentali, mantenere una stretta collaborazione con le autorità competenti, non solo a riguardo delle eventuali modifiche delle procedure, dei piani aziendali e delle informazioni sulla base delle quali è stata fornita l’autorizzazione, ma anche, specialmente, in merito ad alcuni aspetti particolari; **le infrastrutture di mercato DLT devono infatti informare tempestivamente e dettagliatamente**

- **Accessi non autorizzati, perdite di dati, malfunzionamenti, attacchi informatici, frodi, furti o qualsiasi tipo di abuso dell’infrastruttura DLT;**
- **Difficoltà operative riscontrate nell’erogazione di qualsiasi servizio legato ai valori mobiliari DLT o alla DLT stessa;**
- **Eventuali nuovi rischi sorti per la tutela dei consumatori e per la stabilità finanziaria;**

Al fine di tutelare gli interessi collettivi, l’autorità competente deve avere il pieno accesso alle informazioni pertinenti e ha il potere, previa consultazione dell’ESMA, di richiedere, fondamentalmente, qualsiasi tipo di misura correttiva ritenuta necessaria.

Per agevolare la vigilanza e lo studio di queste infrastrutture di mercato sperimentali, i gestori delle stesse devono realizzare con cadenza semestrale un report destinato all’autorità competente e all’ESMA che fornisca una visione d’insieme su quanto segue:

- **Tutte le problematiche tecniche e finanziarie riscontrate** nel contesto dell’infrastruttura DLT quindi minacce informatiche, malfunzionamenti, frodi etc…
- **Il numero e il valore di:**
    - **security tokens** registrati e negoziati
    - **operazioni in security tokens**
- Le **difficoltà riscontrate nell’applicazione dell’apparato regolatorio e le misure compensative adottate per ottemperare alle richieste delle autorità**

L’ESMA rimane, come nel contesto della MiCA, l’ente principale responsabile del coordinamento delle autorità competenti e dello sviluppo di una visione d’insieme sulla tecnologia a registro distribuito e sulle modalità di vigilanza di questa.

4.7 Relazione Finale

I contenuti della relazione finale che l'ESMA dovrà realizzare perché la Commissione presenti i risultati del regime pilota al Parlamento e al Consiglio, **sono stabiliti nell'articolo 10 dello stesso; il report dovrà contenere informazioni** sulle infrastrutture di mercato **in merito ai seguenti aspetti**:

- **Funzionamento delle infrastrutture di mercato DLT**, numero e tipologia di queste, tipo di esenzioni richieste e tipo di esenzioni concesse;
- **Numero e valore delle operazioni e dei valori mobiliari DLT** registrati e negoziati;
- **Tipologie di DLT utilizzate, rischi connessi e problematiche di interoperabilità** sorte rispetto all'infrastruttura finanziaria tradizionale;
- **Vantaggi riscontrati in termini di: efficienza, riduzione dei rischi nella catena di negoziazione e post negoziazione, registrazione, custodia, tracciabilità e vigilanza;**
- **Rifiuti, modifiche e revoche delle autorizzazioni**;
- **Cessazioni dell'attività di infrastrutture di mercato DLT**;

5. Digital Operational Resilience Act

Il regolamento europeo relativo alla resilienza operativa digitale per il settore finanziario, DORA *[59]*, è entrato in vigore nel territorio dell'unione il 17 gennaio 2023 e si applicherà dal 17 gennaio 2025.

L'obiettivo di DORA è quello di garantire che in un contesto di crescente dipendenza dalle tecnologie dell'informazione e telecomunicazione, le istituzioni finanziarie gestiscano attivamente i rischi delle operazioni digitali; DORA punta cioè alla **resilienza digitale**, *definita nel regolamento come*:

"La capacità dell'entità finanziaria di creare, assicurare e riesaminare la propria integrità operativa da un punto di vista tecnologico, garantendo, direttamente o indirettamente, tramite il ricorso ai servizi offerti da fornitori terzi di TIC, l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza delle reti e dei sistemi informativi impiegati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità"[26]

Per garantire la resilienza, tutte le istituzioni impattate da DORA **devono stabilire, sviluppare e dimostrare l'efficacia di politiche di gestione dei rischi**. Il regolamento introduce la necessità di un continuo monitoraggio degli strumenti di sicurezza e di telecomunicazione, finalizzato alla minimizzazione dei rischi; **in questi termini, viene attribuita particolare rilevanza al rischio rappresentato dalle terze parti che, con l'introduzione di DORA, deve essere gestito dalle istituzioni in maniera attiva, attraverso clausole contrattuali**, audit, revisioni e ispezioni. Come "rischi", ai sensi dell'articolo 3 del regolamento, si intendono:

"*eventi dolosi o non dolosi, che, qualora concretizzati, potrebbero compromettere la sicurezza della rete e dei sistemi informativi, di eventuali strumenti o processi, della continuazione delle operazioni e dei processi, oppure della fornitura dei servizi, pregiudicando in tal modo l'integrità o la disponibilità dei dati, del software o di eventuali altre componenti dei servizi e delle infrastrutture di TIC, o ancora causando una violazione della riservatezza, un danno alle infrastrutture fisiche di TIC o altri effetti avversi".*

Con DORA, la conoscenza e la competenza verso le minacce e i rischi del patrimonio digitale diventano un obbligo collettivo; la responsabilità per i rischi connessi alle tecnologie, viene infatti estesa agli organi di gestione delle entità finanziarie e ai rispettivi membri, per i quali vengono introdotti una serie di obblighi, come quello di formazione dei dipendenti in merito ai rischi informatici, e sanzioni.

Nell'articolo 4 del regolamento, viene infatti sancito che *"l'organo di gestione definisce, approva, vigila e risponde di tutte quelle disposizione concernenti la gestione dei rischi"*, in particolare, il suddetto organo deve assumersi la responsabilità finale di:

- **definire ruoli e responsabilità connesse alle funzioni di TLC**
- **determinare i livelli appropriati di tolleranza ai rischi**

26 *art.3 DORA*

- **approvare periodicamente e riesaminare la politica di continuità operativa**
- **approvare periodicamente i piani di audit**
- assegnare e riesaminare adeguatamente il bilancio
- **approvare e riesaminare i servizi TLC prestati da terzi**
- **istituire un ruolo specifico per il monitoraggio degli accordi con fornitori terzi di servizi TLC** o designare un dirigente di rango elevato al monitoraggio di questi

DORA si applica a una varietà di entità che costituiscono le unità fondamentali di diversi contesti tra loro in relazione, come quello finanziario, quello assicurativo e quello degli asset digitali; tra queste entità, vi sono **anche i protagonisti principali della MiCA e del DLT Pilot Regime, in particolare:**

- **fornitori di servizi per le cripto-attività**
- **emittenti di cripto-attività**
- **emittenti di token collegati ad attività**
- **emittenti di token collegati ad attività significativi**
- **istituti di moneta elettronica**
- **depositari centrali di titoli**
- **sedi di negoziazione**
- **enti creditizi**
- **istituti di pagamento**
- **fornitori terzi di servizi di TIC.**
- **fornitori di servizi di comunicazione dati**
- **imprese di assicurazione e di riassicurazione**

DORA rappresenta quindi un ulteriore, fondamentale, componente di quello che è il framework digitale europeo per la protezione delle infrastrutture e dei dati e si inserisce a completamento del contesto attualmente segnato dalle:

- **direttiva 2016/1148 (NIS)** recante *misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (in applicazione)*
- **direttiva 2022/2555 (NIS2)** *relativa alle misure per un livello comune elevato di cibersicurezza nell'Unione (in vigore, il regime di applicabilità inizia dal 18 ottobre 2024)*
- **regolamento 2016/679 (GDPR)** *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (in applicazione)*

5.1 Gestione del rischio

DORA impone lo sviluppo di un modello di gestione del rischio multifase analogo ai modelli "Five Functions" NIST *[60]* **(Identify, Protect, Detect, Respond, Recover) e "Three lines of defense" applicato alle TLC**. La gestione multifase prevista, oltre ad una preliminare fase di identificazione dei rischi (art.7), **consiste in tre fasi principali così definite: protezione e prevenzione (art. 8), individuazione (art.9), risposta e ripristino (art.10).**

5.1.1 Prevenzione e Protezione

Il primo paragrafo dell'articolo 8 del regolamento riassume il significato della fase di protezione;

"Allo scopo di proteggere adeguatamente i sistemi di TIC e nella prospettiva di organizzare misure di risposta, le entità finanziarie monitorano e controllano costantemente il funzionamento dei sistemi e degli strumenti di TIC e riducono al minimo l'impatto di tali rischi adottando politiche, procedure e strumenti adeguati alla sicurezza delle TIC."

Il fine della fase di protezione è quindi quello di delineare i contorni entro cui debbano svolgersi le attività dell'istituzione e le caratteristiche di svolgimento delle stesse, al fine di costruire un sistema che rappresenti una solida base di partenza per ridurre le vulnerabilità sia agli attacchi informatici che ai guasti del sistema stesso e che sia strutturato in modo da agevolare lo sviluppo delle strategie di risposta e ripristino. A questo titolo, devono essere adoperate tecnologie ed istituiti processi finalizzati alle seguenti:

- Garantire la **sicurezza dei mezzi di trasmissione**
- **Ridurre i rischi di perdita, corruzione e accesso non autorizzato** ai dati
- **Ridurre i rischi legati ai guasti, al trattamento dei dati e a una gestione amministrativa negligente**
- **Prevenire la fuga di informazioni**
- Elaborare e documentare una politica di sicurezza dell'informazione che specifichi:
    - **norme per la tutela, a livello di TLC, della riservatezza e dell'integrità dei dati** e delle risorse proprie e di quelle dei clienti;
    - **procedure, protocolli, dispositivi e meccanismi adottati per isolare "patrimoni di informazione" vittime di attacchi, in particolare le reti** che devono essere realizzate in modo tale da isolare eventuali compartimenti compromessi;
    - **limiti imposti ai diritti di accesso** sia fisici che virtuali alle informazioni;
    - **politiche di correzione e aggiornamento;**

La protezione consiste quindi nello sviluppo di un sistema che sia progettato tenendo in considerazione tutti i possibili rischi a cui potrebbe essere soggetto e alla conseguente ottimizzazione della struttura, al fine di ridurre sia le possibili vulnerabilità che gli eventuali danni che queste potrebbero causare.

5.1.2 Individuazione

Le istituzioni devono predisporre adeguati meccanismi per l'individuazione tempestiva di attività anomale e di potenziali punti di guasto, *funzioni che vengono tipicamente assolte da un organo denominato Information Security Operation Center (ISOC) la cui funzione principale è lo stretto e costante monitoraggio dell'infrastruttura IT*.

I meccanismi di vigilanza prevedono diversi livelli di controllo, **sistemi di monitoraggio attivo**, **sistemi di controllo automatizzato** *come può essere l'applicazione dell'AI per l'analisi delle vulnerabilità [61]* e **sistemi di soglie per l'allerta tempestiva del personale incaricato alle procedure di risposta** e una varietà di altri sistemi.

5.1.3 Risposta e Ripristino

La messa in atto della politica aziendale di continuità operativa richiede una solida strategia di risposta alle minacce che, vista la natura in continua evoluzione sia degli strumenti tecnologici che dei processi adottati, **richiede al contempo una continua analisi di quanto accade**, a questo proposito, le istituzioni devono:

- **Registrare tutti gli incidenti connessi alle TLC**;
- **Rispondere in maniera rapida ed efficace alle minacce, in particolare agli attacchi informatici, minimizzando i danni e garantendo la continuità delle operazioni;**
- **Attivare piani dedicati all'integrazione di tecnologie, processi e misure contenitive** per scongiurare tali attività malevoli
- **Effettuare stime preliminari sull'impatto, i danni e le perdite connessi agli incidenti**
- **Stabilire e testare annualmente procedure da intraprendere nelle gestioni delle crisi** *(c.d. Piani di Disaster Recovery) [62]* **che devono, inoltre, essere soggette ad audit indipendenti.**
- **Testare periodicamente la resilienza delle funzioni critiche esternalizzate verso terzi**
- **Comunicare i report sugli incidenti alle autorità competenti**

L'articolo 11 di DORA è specificatamente dedicato agli obblighi per le entità finanziarie legati al contesto **disaster recovery** e **quindi ai piani di ripristino e alle politiche di backup**; **i sistemi di backup e ripristino devono appartenere ad un contesto operativo a sé ed essere protetti da qualsiasi accesso non autorizzato o corruzione delle TLC**. Un aspetto assolutamente rilevante in questo contesto è **l'obbligo delle istituzioni finanziarie di assicurarsi che i fornitori terzi di servizi di TIC con cui collaborano, mantengano almeno un sito secondario di trattamento dati dotato di risorse, capacità, funzionalità e personale adeguati a soddisfare le esigenze.**

Tale sito secondario deve rispettare una serie di requisiti, tra cui:

1. **essere ubicato geograficamente a distanza** dal sito primario
2. **essere in grado di garantire la continuità dei servizi critici** in maniera identica al sito primario
3. **essere immediatamente accessibile al personale dell'entità finanziaria** al fine di garantire la continuità dei servizi critici in caso di indisponenza del sito primario.

Le politiche di risposta ad incidenti informatici comprendono anche l'attenta analisi post-evento da parte di personale altamente specializzato (art.12), finalizzata alla messa in atto di miglioramenti in aspetti quali:

- la **tempestività della risposta**
- la **qualità e rapidità dell'analisi forense**
- **l'efficacia nell'attivazione dei vari livelli di sicurezza**
- **l'efficacia della comunicazione nella gestione dell'evento**

L'articolo dodici, "***Apprendimento ed evoluzione"*** **stabilisce inoltre gli obblighi di formazione e di comunicazione; il personale di grado più elevato addetto alle TLC deve comunicare, almeno su base annua, gli esiti delle analisi relative alla Gestione del rischio informatico, corredati da opportune raccomandazioni.**

Oltre a questo, **le entità finanziarie vengono obbligate all'elaborazione di adeguati programmi di sensibilizzazione sulla sicurezza delle TIC e all'erogazione di attività di formazione sulla resilienza operativa digitale che devono manifestarsi sotto forma di moduli obbligatori nei programmi di formazione del personale;** ***tali attività devono riguardare tutti i dipendenti, anche gli alti dirigenti.***

Al fine di mantenere un'infrastruttura adeguata alle crescenti minacce e quindi per sviluppare un framework di procedure sempre più efficaci per la gestione dei rischi connessi alle attività digitali e informatiche, l'ABE, l'ESMA, l'EIOPA[27] e l'ENISA[28] elaborano progetti di norme tecniche legate alle varie procedure e protocolli correntemente attuati. (art. 14)

---

27 *Autorità europea delle assicurazioni e delle pensioni aziendali o professionali (EIOPA)*.

28 *ENISA European Union Agency for Cybersecurity*

5.2 Gestione degli Incidenti

DORA pone dedica gli articoli dal 15 al 20 alle modalità di monitoraggio, classificazione e segnalazione degli incidenti. **L'articolo quindici identifica la procedura generale per la gestione di un incidente, che viene scorporata in tre obiettivi principali**:

1. **Individuazione, registrazione e categorizzazione dell'incidente;**

La classificazione degli incidenti viene operata sulla base di una varietà di parametri definiti nell'art.16, le cui soglie tecniche verranno stabilite in futuro dall'AEV[29]; questi possono essere identificati nelle seguenti voci:

- Numero di utenti e organizzazioni colpite
- Durata dell'incidente e dell'inattività
- Estensione geografica
- Perdite di dati
- Gravità dell'impatto sui sistemi
- Criticità dei servizi colpiti
- Impatto economico

2. **Definizione e assegnazione di ruoli e responsabilità;**
3. **Piani di comunicazione e segnalazione al personale, agli stakeholder e alle autorità;**

L'articolo 17 stabilisce obblighi di segnalazione e tempistiche in cui queste debbano avvenire; la segnalazione di un'incidente alle autorità deve avvenire sotto forma di tre relazioni, una iniziale, una intermedia e una conclusiva. *L'ENISA [63], la BCE e le AVE realizzeranno delle norme tecniche sul contenuto delle suddette segnalazioni*. Sulla base dei dati ricevuti tramite le segnalazioni, le AEV redigeranno annualmente un report indicante *"statistiche di alto livello a supporto delle valutazioni della vulnerabilità e delle minacce connesse alle TIC"*[30].

29 *Il Sistema europeo di vigilanza finanziaria.*

30 *art. 20 DORA*

5.3 Test di Resilienza

DORA, stabilisce anche obblighi, modalità e le tipologie di test che le entità finanziarie sono tenute ad operare, tramite soggetti indipendenti, sui propri sistemi. I test devono riguardare tutti gli applicativi e i sistemi critici di TLC. Tra le tipologie di test richieste dal regolamento si annoverano:

- individuazione e valutazione delle vulnerabilità
- analisi open source
- **valutazioni della sicurezza delle reti**
- analisi delle carenze
- esami della sicurezza fisica
- esami del codice sorgente
- test di compatibilità
- **test basati su scenari**
- test di prestazione
- **test di penetrazione**

Particolare attenzione viene riservata ai test di penetrazione basati su minacce[31] che devono essere effettuati con cadenza quantomeno triennale e **devono riguardare i sistemi reali su cui si basano le funzioni dell'entità finanziaria, anche quelli esternalizzati**.

I risultati dei test vengono trasmessi dall'entità e dai tester indipendenti alle autorità, che emettono un certificato. **Noti esempi di certificazioni legate al contesto della sicurezza dei sistemi informatici sono la certificazione ISO-27001 e la certificazione SOC-II.**

Le **entità finanziarie tenute a svolgere test di penetrazione** e le modalità di questi test **vengono identificate dalle autorità competenti sulla base di** una varietà di aspetti tra cui le **criticità dei servizi forniti**, i **possibili problemi di stabilità finanziaria legati alla loro compromissione** e il **profilo di rischio connesso alle capacità tecnologiche**.

DORA dedica specificatamente ai *tester* l'art. 24 dove ne definisce i requisiti perché possano **operare all'interno dei sistemi delle istituzioni finanziarie**:

- Possesso di un **alto grado di idoneità, reputazione**;
- **Esperienza specifica** nel campo delle minacce, dei test basati su penetrazione o dei test red team;
- **Certificazione** da parte di un ente statale o rispetto di **codici formali di condotta** *Ethical Hackers, White Hats*;

[31] *tecnica di sicurezza informatica utilizzata per identificare ed esaminare le possibili conseguenze derivabili da un'intrusione*

- **Nel caso di tester esterni**, **garanzie indipendenti sulla gestione dei rischi** e siano coperti da un'**assicurazione sui rischi**, anche quelli connessi a negligenza;

5.4 Rischi derivanti da terzi

DORA tratta separatamente, nel quinto capo, la gestione dei rischi derivanti dall'esternalizzazione di servizi e, in generale, dei servizi offerti da terzi:

"Le entità finanziarie trattano i rischi relativi alle TIC derivanti da terzi quali componenti integranti dei rischi relativi alle TIC nel contesto del proprio quadro per la gestione di detti rischi [...] Le entità finanziarie che hanno stipulato accordi contrattuali per l'utilizzo di servizi di TIC per lo svolgimento delle proprie operazioni commerciali rimangono sempre pienamente responsabili del rispetto e dell'adempimento di tutti gli obblighi previsti dal presente regolamento e dalla legislazione applicabile in materia di servizi finanziari"[32]

La **principale misura di prevenzione e di gestione dei rischi** derivanti da terzi viene identificata negli **accordi contrattuali**; le entità finanziarie devono infatti **moderare il legame con i fornitori terzi tramite clausole che prevedano la risoluzione degli accordi contrattuali per l'utilizzazione dei servizi di TIC in circostanze di violazioni, debolezze o difficoltosa vigilanza.**

Tutti i contratti con fornitori terzi di servizi devono essere mantenuti in un registro messo, a disposizione delle autorità competenti; tali contratti, peraltro, devono essere **sottoscritti**:

- **esclusivamente con fornitori di servizi che soddisfano** alti, appropriati e recenti, **standard di sicurezza**;
- **previa un'opportuna valutazione di** una varietà di aspetti:
    - **criticità della funzione esternalizzata**
    - **condizioni di vigilanza**
    - rischio di concentrazione delle TLC
    - **idoneità del fornitore** misurata attraverso procedure quali auditing, ispezioni e revisioni

Fondamentale, in termini di indipendenza delle entità finanziarie dai fornitori di servizi terzi, **è la disponibilità di adeguate strategie di uscita che possano garantire che la possibilità estinguere accordi contrattuali** con tali fornitori, prevenendo situazioni di vendor lock-in e **senza pregiudicare la qualità dei servizi erogati ai clienti.**

[32] *art. 25 DORA*

5.4.1 Struttura dei Contratti

Qualsiasi contratto sottoscritto tra un'entità finanziaria e un fornitore terzo di servizi deve contenere alcune indicazioni fondamentali, specificate nell'articolo 27 relative a:

- **descrizione delle funzioni e dei servizi** che il fornitore deve prestare
- **località in cui si devono svolgere** le funzioni e trattare, conservare i dati
- disposizioni sul **trattamento dei dati personali**
- **obiettivi di prestazione** ai fini del monitoraggio
- termini di preavviso e obblighi di segnalazione
- eventuale **obbligo di assistenza in caso di incidenti** nelle TLC
- **obbligo di attuazione di piani di emergenza**
- **diritto di monitoraggio costante, ispezione, audit**
- diritto di risoluzione
- strategia di uscita e periodo di transizione associato

ABE, ESMA e EIOPA sono designate dalle AEV come **responsabili di quei fornitori di servizi definiti critici per l'infrastruttura finanziaria**, come tali, sono incaricate della valutazione delle norme, degli accordi, delle procedure e dei dispositivi da questi adottati per la sicurezza informatica. **Il grado di criticità dei fornitori di servizi viene stabilito sulla base dell'impatto associato ai servizi erogati**, sulla dimensione delle entità finanziarie dipendenti da questi e sul grado di sostituibilità degli stessi.

5.5 Condivisione delle Informazioni

Al fine di **potenziare la resilienza digitale dell'infrastruttura finanziaria europea**, DORA, stabilisce la **possibilità per le istituzioni finanziarie di istituire meccanismi di condivisione delle informazioni e dei dati relativi alle minacce informatiche** nell'ottica di un miglioramento collettivo delle strategie di difesa, individuazione, mitigazione, risposta e ripristino. La condivisione delle informazioni **deve avvenire all'interno di comunità di entità finanziarie attraverso meccanismi disciplinati da norme di condotta rispettose della protezione dei dati personali**. I meccanismi di condivisione delle informazioni devono quindi definire le condizioni per la partecipazione, specificare gli elementi operativi e i dettagli del coinvolgimento delle autorità.

5.6 Autorità

DORA definisce le autorità competenti alla vigilanza sulle disposizioni in relazione al tipo di entità finanziaria di riferimento, nel rispetto delle già esistenti regolamentazioni.

Nella medesima ottica della collaborazione sul piano europeo per la cibersicurezza (NIS), le AEV, la BCE e il CERS collaborano con tali autorità competenti nell'**istituzione di pratiche finalizzate al miglioramento della consapevolezza situazionale e all'identificazione dei rischi e delle vulnerabilità informatiche.**

Alle autorità competenti deve essere concesso, dai rispettivi stati membri, di esercitare i quantomeno i seguenti poteri:

- **Imposizione della sospensione o della cessazione di qualsiasi pratica ritenuta contraria alle disposizioni** del Digital Operational Resilience Act;
- Adozione di **pene pecuniarie**;
- **Accesso previa autorizzazione delle autorità opportune e ai fini di indagine, alle registrazioni di traffico dati detenute dagli operatori TLC;**
- **Pubblica dichiarazione dell'identità della persona fisica o giuridica che commette violazioni e la natura di tali violazioni;**

Qualora siano previste, dal diritto nazionale degli stati membri, sanzioni penali per le violazioni connesse agli obblighi di gestione del rischio, gestione degli incidenti, test, relazioni con terzi e collaborazione con le autorità, allora gli Stati membri non sono tenuti ad emanare norme relative a sanzioni amministrative.

Conclusione

L'approccio normativo adottato dall'Unione, rende evidente l'interesse che l'Europa nutre verso il conseguimento di una posizione di leadership nelle tecnologie di registro distribuito; interesse manifestato dalla pronta adozione di disposizioni che riducono notevolmente i rischi legati all'incertezza del diritto e all'arbitraggio normativo a cui i CASPs sono attualmente esposti, consentendo così sia lo sviluppo ordinato del mercato che l'analisi dell'evoluzione di questo, nell'ottica di un'integrazione completa con il settore della finanza tradizionale e delle sue regole.

Confrontando l'attuale struttura del settore DLT, in cui si stanno innestando le banche, e le politiche introdotte con il DLT Pilot Regime, emerge chiaramente la volontà dell'Unione di esplorare le potenzialità rappresentate dalla tokenizzazione degli asset finanziari e, al contempo, di introdurre le istituzioni finanziarie all'applicazione di questo tipo di tecnologie, con la probabile prospettiva, considerando anche gli stringenti requisiti per gli emittenti di token di moneta elettronica proposti nella MiCA, dello sviluppo di una moneta elettronica comunitaria. Analizzando le modalità con cui le istituzioni finanziarie si interfacciano verso le tecnologie di registro distribuito, in particolare in riferimento ai custody provider e alle piattaforme di negoziazione, e valutando queste in relazione alla posizione di forza che le disposizioni introdotte sulle esternalizzazioni da DORA e da MiCA garantiscono alle istituzioni finanziarie, l'idea di un prossimo dominio di queste nel settore degli asset digitali si figura come una reale possibilità.

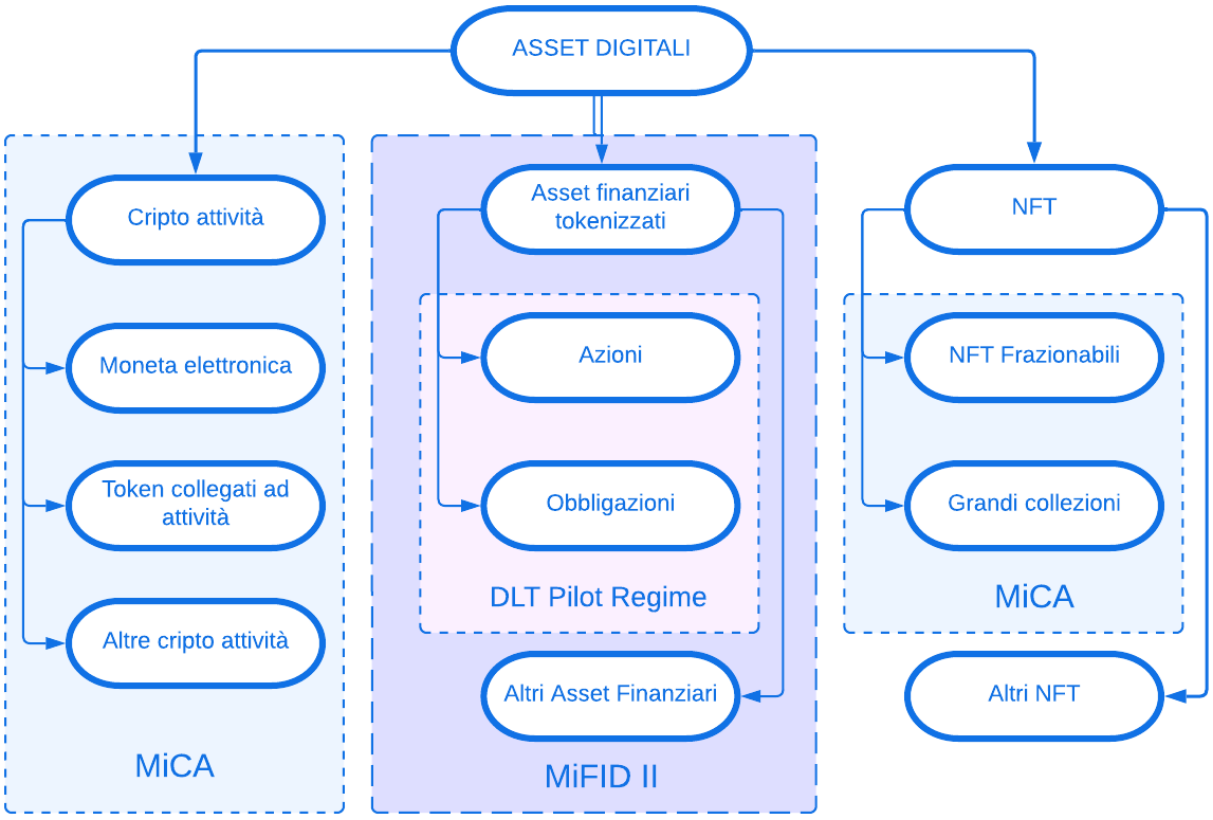
Le disposizioni contenute nell'approccio normativo europeo, arginano con successo le principali minacce del settore; se relazionate con i principali casi negativi avvenuti recentemente nell'ecosistema DLT, cioè la crisi della piattaforma di negoziazione FTX e quella dell'emittente di token Terra Luna, risultano particolarmente rilevanti le disposizioni sugli abusi di mercato e quelle sui fornitori di servizi contenuti nella MiCA, che rappresenta il principale argine normativo rispetto alle minacce per i consumatori e per la stabilità finanziaria, in quanto regolamenta l'insieme delle criptoattività, in cui rientrano anche le criptovalute, e degli emittenti di tali cripto-attività. Il fatto che tale regolamentazione non sia già in vigore rappresenta quindi una carenza a cui l'Europa dovrà porre rimedio quanto prima possibile.

Nonostante l'esaustività dell'apparato regolatorio europeo, in relazione alle DLT nella finanza decentralizzata, questo potrebbe generare delle situazioni conflittuali, le cui soluzioni non sono immediate o addirittura potrebbero non essere possibili.

Ad esempio, non è chiaro né come verranno gestiti i conflitti di classificazione di token che potrebbero rientrare all'interno di diverse categorie, né quale sarà il destino delle valute sviluppate su protocolli decentralizzati anonimi, in quanto, il controllo delle relative transazioni può essere garantito solo nel caso di interfacciamento degli utenti con entità centralizzate e non nel caso di interazioni con portafogli di self-custody o con exchange decentralizzati.

A questo proposito, bisogna considerare che oltre alla possibile insorgenza di conflitti, restano degli aspetti aperti, non chiari o semplicemente non trattati dalle regolamentazioni.

Alcuni aspetti rilevanti che rimangono indefiniti sono: il collocamento dei servizi di finanza decentralizzata, degli NFT e degli exchange decentralizzati; questi infatti non ricadono esplicitamente né all'interno del dominio della MiCA né in quello del DLT Pilot Regime e restano quindi in una zona grigia caratterizzata da incertezza, rischi per i consumatori e arbitraggio normativo. Oltre a questo, il DLT Pilot Regime non comprende una grande quantità di strumenti finanziari, come i derivati e gli ETF, con una diretta conseguenza, quantomeno a livello di tempistiche, sull'emissione di tali strumenti sotto forma di token.



6. Tipi di asset digitali e dominio delle regolamentazioni

Nonostante alcuni aspetti non chiari e potenziali conflitti, che probabilmente verranno emendati in futuro, le regolamentazioni europee risultano essere uno strumento esaustivo e ben ponderato, che riesce a rendere l'Europa attrattiva per i CASPs arginando al contempo la quasi totalità dei rischi rappresentati dal settore e agevolando lo sviluppo di prodotti innovativi e potenzialmente rivoluzionari come le CBDC.

Le tempistiche con cui sta venendo gestito un tale apparato regolatorio e la completezza dello stesso, che rappresenta il primo quadro regolamentare in materia a livello globale, probabilmente porteranno l'Europa ad essere il principale riferimento mondiale delle DLT, garantendo così all'Unione il ruolo di leader nella definizione degli standard della tokenizzazione e quindi, probabilmente, anche del settore finanziario.

Indice delle immagini

1. Chainlink come interfaccia 14
2. Infrastruttura dell'ecosistema DLT 15
3. Tipologie di portafogli 16
4. Relazioni di custodia 22
5. Gerarchie di vigilanza nelle criptoattività 46
6. Tipi di Asset digitali e dominio delle regolamentazioni 71

Riferimenti

[1] Carrière, P. et al. (2023) *Tokenizzazione di azioni e azioni tokens*, Consob. Available at: https://www.consob.it/documents/1912911/1916538/qg25.pdf/0cc70f0f-49ac-7ee4-f8cc-c07f7affbf35
[2] Goswami, R. (2023) *Coinbase sues SEC after months of silence from Federal Regulator*, CNBC. Available at: https://www.cnbc.com/2023/04/24/coinbase-sues-sec-after-months-of-silence-from-federalregulator.html#:~:text=Coinbase%20took%20legal%20action%20against,extended%20to%20the%20crypto%20industry
[3] Raud, M. and MacKinnon, E. (2022) *China's digital currency and blockchain network: Disparate projects or two sides of the same coin?* Stanford.edu. Available at: https://digichina.stanford.edu/work/chinas-digital-currency-and-blockchain-network-disparate-projects-or-two-sides-of-the-same-coin/
[4] Brooks, C. (2022) *Alarming cyber statistics for mid-year 2022 that you need to know*, Forbes. Forbes Magazine. Available at: https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=730cf43d7864
[5] Faggioli, G. (2022) *Crescono Gli attacchi cyber in Italia, Ma Anche le difese: Ecco il Quadro*, Agenda Digitale. Available at: https://www.agendadigitale.eu/sicurezza/cyber-attacchi-minaccia-sempre-piu-reale-anche-in-italia-analisi-e-dati-dellevoluzione/
[6] Ludovico, M. (2023) *Cybersecurity, 2022 annus horribilis: 13mila Attacchi, +138%*. Il Sole 24 ORE. Available at: https://www.ilsole24ore.com/art/cybersecurity-2022-annus-horribilis-13mila-attacchi-138percento-AE2W4pTC
[7] Foschini, G. (2023) *Hacker Russi, quel filo che lega gli attacchi. Matrice politica, sale l'allerta Sulla Sicurezza*, la Repubblica. Available at: https://www.repubblica.it/politica/2023/02/24/news/hacker_russi_attacco_italia_meloni-389223645/
[8] Hanke, S. (2022) *Chengdu, La Città intrappolata Dal Covid: "I Droni Sorvegliano Le Persone in lockdown"*, RaiNews. Available at: https://www.rainews.it/video/2022/09/chengdu-la-citt-intrappolata-dal-covid-i-droni-sorvegliano-le-persone-in-lockdown-05fc152b-342d-44aa-9bd9-54d82bdeb961.html
[9] Di Matteo, G. (2020) *In Cina La videosorveglianza della quarantena arriva Sulla Soglia di Casa, Efficienza o Grande Fratello?* Forbes Italia. Available at: https://forbes.it/2020/04/29/cina-telecamere-videosorveglia-in-casa-per-controllare-la-quarantena/
[10] Pompili, G. (2021) *Pure nella Cina Orwelliana si parla di privacy*, Il Foglio. Available at: https://www.ilfoglio.it/tecnologia/2021/04/24/news/pure-nella-cina-orwelliana-si-parla-di-privacy-2275475/
[11] Giribaldi, D. (2022) *Intelligenza artificiali, Tutti I pregiudizi (bias) che la rendono pericolosa: Ecco I rischi di Discriminazione Algoritmica*, Agenda Digitale. Available at: https://www.agendadigitale.eu/cultura-digitale/intelligenza-artificiale-tutti-i-pregiudizi-bias-che-la-rendono-pericolosa/
[12] Perrone, L. (2022) *Quantum Computing: Gli effetti collaterali per la sicurezza*, ICT Security Magazine. Available at: https://www.ictsecuritymagazine.com/articoli/quantum-computing-gli-effetti-collaterali-per-la-sicurezza/

[13] Falce, V. and Marzialetti, L. (2022) *Criptovalute: Il Pacchetto UE sulla finanza digitale alla prova del mercato*, Agenda Digitale. Available at: https://www.agendadigitale.eu/cittadinanza-digitale/pagamenti-digitali/criptovalute-il-pacchetto-ue-sulla-finanza-digitale-alla-prova-del-mercato/
[14] *Shaping Europe's digital future* - commission.europa.eu (2020) Available at: https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf
[15] *Strategia UE per la finanza digitale* (2020) EUR-Lex. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0591
[16] Paris, C. (2020) *Blockchain, Gli algoritmi del Consenso: Che cosa sono e a cosa servono*, Agenda Digitale. Available at: https://www.agendadigitale.eu/documenti/blockchain-gli-algoritmi-del-consenso-che-cosa-sono-e-a-cosa-servono/
[17] Giuzzi, L. (2020) *Blockchains: from bitcoin to robotics*, Algebra per Codici e Crittografia. Available at: https://luca-giuzzi.unibs.it/corsi/2021-22/Brescia/Algebra_Codici_Crittografia/Notes/slides-blockchain.pdf
[18] *What is a Blockchain Oracle?* (2021) Chainlink. Available at: https://chain.link/education/blockchain-oracles
[19] Moreland, K. (2022) *What's a blockchain bridge?* Ledger. Available at: https://www.ledger.com/academy/whats-a-blockchain-bridge
[20] Ponnan, J. (2023) *Standard token ERC-20*, ethereum.org. Available at: https://ethereum.org/it/developers/docs/standards/tokens/erc-20/
[21] Popper, N. (2021) *Lost passwords lock millionaires out of their bitcoin fortunes*, The New York Times. Available at: https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html
[22] *NFT: Qual è la differenza tra token fungibili e token non fungibili* (2022) Borsa Italiana. Available at: https://www.borsaitaliana.it/notizie/sotto-la-lente/differenza-tra-token-fungibili-e-token-non-fungibili.htm
[23] Rampone, F. (2019) *I Dati Personali in Ambiente Blockchain Tra Anonimato e Pseudonimato*, Associazione Blockchain Italia. Available at: https://associazioneblockchain.it/doc/i-dati-personali-in-ambiente-blockchain-tra-anonimato-e-pseudonimato/
[24] Handagama, S. (2023) *Dubai prohibits privacy coins like Monero under new crypto rules*, CoinDesk. Available at: https://www.coindesk.com/policy/2023/02/08/dubai-prohibits-privacy-coins-under-new-crypto-rules/
[25] Chen, G. (2023) *USDC depegged because of Silicon Valley Bank, but it's not going to default*, Cointelegraph. Available at: https://cointelegraph.com/news/usdc-depegged-but-it-s-not-going-to-default
[26] Flitter, E. and Copeland, R. (2023) *Silicon Valley Bank fails after run on deposits*, The New York Times. Available at: https://www.nytimes.com/2023/03/10/business/silicon-valley-bank-stock.html
[27] Carlini, V. (2023) *La Sec accusa Terra Luna: Investitori ingannati, Miliardi in Fumo*, Il Sole 24 ORE. Available at: https://www.ilsole24ore.com/art/la-sec-accusa-terra-luna-investitori-ingannati-miliardi-fumo-AEK6a7oC
[28] Rociola, A. (2023) *Storia di do Kwon, L'informatico Dietro Il Crac da 40 miliardi di terra-luna arrestato in Montenegro*, la Repubblica. Available at:

https://www.repubblica.it/tecnologia/2023/03/26/news/do_kwon_terra_luna_arresto_storia-393561514/
[29] Sanis, R., Mellor, C. and Henn, P. (2023) *Ripple SEC suit decision: XRP Court ruling timing and details in full*, Capital. Available at: https://capital.com/ripple-sec-suit-decision-timing-xrp-details
[30] *Coin Systems: Onyx by J.P. Morgan* (2023), JPMorgan. Available at: https://www.jpmorgan.com/onyx/coin-system.htm
[31] Leucci, S. (2023) *Central Bank Digital Currency*, European Data Protection Supervisor. Available at: https://edps.europa.eu/press-publications/publications/techsonar/central-bank-digital-currency_en
[32] Wan, S. (2023) *Former Coinbase CTO urges 'get to bitcoin' before CBDC Digital lockdown*, CryptoSlate. Available at: https://cryptoslate.com/former-coinbase-cto-urges-get-to-bitcoin-before-cbdc-digital-lockdown/
[33] V, A. (2020) *Headbands, backpacks and cards: Collectibles in video games*, Medium. Medium. Available at: https://adityava.medium.com/headbands-backpacks-and-cards-collectibles-in-video-games-160529333842
[34] Nejrotti, F. (2015) *Yanis Varoufakis Era già un personaggio quando si occupava di videogiochi*, VICE. Available at: https://www.vice.com/it/article/exjwqp/macro-varoufakis-valve-steam-943
[35] *Money laundering threats to metaverse* (2023) Financial Crime Academy. Available at: https://financialcrimeacademy.org/money-laundering-threats-to-metaverse/
[36] Putnins, T., Johnson, L. and Vinas, E.F. (2022) *Insider trading in crypto markets*, University of Technology Sydney. Available at: https://www.uts.edu.au/news/business-law/insider-trading-crypto-markets
[37] Turbahn, I. (2022) *An overview of multi-signature and multi-party computation*, Dynamic. Available at: https://www.dynamic.xyz/blog/the-evolution-of-multi-signature-and-multi-party-computation
[38] *MiFID II* (2014) EUR-Lex. Available at: https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32014L0065.
[39] *Proposta di regolamento sui Mercati dei Cripto-asset* (2020) EUR-Lex. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593
[40] Martin, K. (2022) *Elon Musk $258B dogecoin lawsuit adds plaintiffs*, Fox Business. Available at: https://www.foxbusiness.com/markets/elon-musk-258b-dogecoin-lawsuit-adds-plaintiffs
[41] Pringle, E. (2023) *Finance youtubers who promoted FTX handed a $1billion lawsuit*, Fortune. Available at: https://fortune.com/2023/03/20/finance-youtubers-who-promoted-ftx-have-now-been-handed-a-1billion-lawsuit/
[42] Sarkar, A. (2022) *Safemoon pump-and-dump lawsuit targets Jake Paul, Soulja Boy and others*, Cointelegraph. Available at: https://cointelegraph.com/news/safemoon-pump-and-dump-lawsuit-targets-jake-paul-soulja-boy-and-others
[43] Shvartsman, D. (2023) *Facebook: The leading social platform of our times*, Investing.com. Available at: https://www.investing.com/academy/statistics/facebook-meta-facts/.
[44] Wright, T. (2020) *G7 will oppose Libra launch until regulations in place*, Cointelegraph. Available at:

https://cointelegraph.com/news/g7-will-block-libra-launch-until-regulations-in-place
[45] Sigalos, M.K. (2022) *Sam Bankman-fried steps down as FTX CEO as his Crypto Exchange Files for bankruptcy*, CNBC. Available at:
https://www.cnbc.com/2022/11/11/sam-bankman-frieds-cryptocurrency-exchange-ftx-files-for-bankruptcy.html
[46] *Internet computer (ICP) ICO - rating, news & details*, CoinCodex. Available at:
https://coincodex.com/ico/internet-computer/
[47] Gondek, C. *What is blockchain analytics, and how does it work?* OriginStamp. Available at:
https://originstamp.com/blog/what-is-blockchain-analytics-and-how-does-it-work/
[48] *ICP Report* (2021) Arkham. Available at:
https://www.arkhamintelligence.com/reports/icp-report
[49] Wan, S. (2021) *MrBeast catches heat for promoting alleged refinable pump and dump scam*, Bitcoin Insider. Available at:
https://www.bitcoininsider.org/article/112223/mrbeast-catches-heat-promoting-alleged-refinable-pump-and-dump-scam
[50] Puorro, A. (2013) *N. 198 – high frequency trading: Una Panoramica*, Banca d'Italia. Available at:
https://www.bancaditalia.it/pubblicazioni/qef/2013-0198/index.html
[51] Caivano, V. et al. (2012) *Il trading ad Alta frequenza*, Consob. Available at:
https://www.consob.it/documents/11973/219968/dp5.pdf/04c93f02-d620-456c-b0a1-868233013f6e
[52] *Glossario finanziario - informazione privilegiata*, Borsa Italiana. Available at:
https://www.borsaitaliana.it/borsa/glossario/informazione-privilegiata.html
[53] Chen, J. (2022) *Wash trading: What it is and how it works, with examples*, Investopedia. Available at:
https://www.investopedia.com/terms/w/washtrading.asp
[54] Berger, S. (2023) *Report on the proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets*, Parlamento europeo. Available at:
https://www.europarl.europa.eu/doceo/document/A-9-2022-0052-AM-002-002_IT.pdf
[55] McGuinness, M. (2022) *Opportunities and challenges of the tokenisation of finance: which role for Central Banks?* European Commission. Available at:
https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_5814
[56] La Sala, E. (2021) *Recenti Sviluppi sull'applicazione di DLT all'emissione di Strumenti Finanziari C.D. securities token*, Allen Overy. Available at:
https://www.allenovery.com/it-it/global/news-and-insights/publications/recent-developments-on-the-application-of-the-dlt-to-the-issuance-of-securities-tokens
[57] *DLT Pilot Regime* (2020) EUR-Lex. Available at:
https://eurlex.europa.eu/legalcontent/IT/TXT/PDF/?uri=CELEX:52020PC0594&from=EN
[58] *Regolamento (UE) n. 909/2014* (2014) EUR-Lex. Available at:
https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32014R0909
[59] *Digital Operational Resilience Act*, EUR-Lex. Available at:
https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554
[60] *The Five Functions* (2023) NIST. Available at:
https://www.nist.gov/cyberframework/online-learning/five-functions
[61] *Ai - how to stop hackers and protect yourself*, BlueFort Security. Available at:
https://www.bluefort.com/news/latest-blogs/ai-how-to-stop-hackers-protect-yourself/
[62] *Che Cos'è un piano di disaster recovery*, IBM. Available at:
https://www.ibm.com/it-it/services/business-continuity/disaster-recovery-plan

[63] *Towards a Trusted and Cyber Secure Europe* (2021) ENISA. Available at: https://www.enisa.europa.eu/about-enisa

A conclusione del lungo percorso che è stato il conseguimento della laurea in ingegneria informatica, è doveroso ringraziare tutti coloro che hanno contribuito a questo successo.

Ringrazio quindi il mio relatore Signoroni Alberto per il prezioso contributo e per la fiducia di cui mi ha investito consentendomi di sviluppare questo testo.

Ringrazio la mia famiglia, per quello che ha saputo insegnarmi e per avermi sempre sostenuto.

Ringrazio Elena e i miei amici, per essermi sempre stati vicini.

Ringrazio Alessandro Marciotti, per il prezioso contributo nella realizzazione delle immagini.

Sica Mattia