

I Crypto-Asset Service Providers (CASP): genesi, sviluppi regolatori e impatti nella Centralized-Decentralized Finance (CeDeFi)

Prof.
Gian Domenico Mosco

SUPERVISOR

Prof.ssa
Mirella Pellegrini

CO-SUPERVISOR

Dott.
Edoardo Tedeschi

CANDIDATE

Prof.
Paolo Savona

CO-SUPERVISOR

*Il segreto del cambiamento è focalizzare tutta la tua energia, non sul combattere il vecchio,
ma sulla costruzione del nuovo*

Socrate

Non sempre cambiare equivale a migliorare, ma per migliorare bisogna cambiare

Winston Churchill

In un mondo che cambia, non c'è maggior rischio che restare fermi

Jacques Chirac

*La tecnologia informatica è sul punto di fornire agli individui e ai
gruppi la capacità di comunicare e interagire tra loro in modo
totalmente anonimo (...). Questi sviluppi modificheranno
completamente la natura della regolamentazione governativa, la
capacità di tassare e controllare le interazioni economiche, la
capacità di tenere segrete le informazioni e modificheranno
persino la natura della fiducia e della reputazione*

Timothy May

ABSTRACT (ENGLISH VERSION)

«Nothing is lasting but change». The statement was formulated by the German writer Ludwig Börne and could be well applied to the financial system, whose structure is constantly transforming. On closer inspection, this is due to a physiological process, determined by the inextricable link between innovation, economic activity and society which has brought visibly increasing improvements throughout history in terms of performance efficiency, refinement of procedures and customization of solutions to meet specific customers-consumers' specific needs. However, it is undeniable how in this sector the technological component - especially of the cryptographic matrix - has gone far beyond merely supporting and enhancing the elements that underpin the complex architecture of Traditional Finance (TradFi). The introduction of DLT Technology, blockchain and smart contracts has reshaped intermediaries, payment systems and trust to the point of building a parallel "crypto financial ecosystem", that is a cryptographic perimeter in which the frame of traditional financial markets has been duplicated. In fact, the mechanism and organizational features trace the classical finance style, and in its structure roughly similar entities, products and services can also be identified. Specifically, digital assets and Crypto-Asset Service Providers (CASPs) are respectively the objects and entities that space within the CeDeFi, a place where Centralized Finance (CeFi) and Decentralized Finance (DeFi), sub-categories of the aforementioned "alternative financial environment", are inextricably linked but for theoretical and academic reasons will be illustrated separate from each other. On the formers, the economic law community has already produced (and is still producing) a large quantity of articles and scholarly texts, confirming that the interest directed towards crypto-assets and Central Bank Digital Currencies (CBDC) has not faded at all; on the latters the same thing cannot be said.

Noting the above, this study focuses on the CASPs with the aim of providing an organic and exhaustive view of them. To do so, the work summarizes the exogenous factors that have fostered their emergence by reconstructing the key episodes that first establish their theorization and then their entry into the law field. Although the legal analysis definitely leans toward a national and European regulatory perspective, the survey also integrates a comparative approach by laying an observational lens on the current regulation of these

intermediaries at a global level.

Furthermore, an overall view of the phenomenon has certainly strengthened the idea of not ignoring the various problems caused by crypto exchange platforms (CEX/DEX) which are gradually gaining relevance and occupying greater space in both academic and institutional debates only after the alarming series of failures that have occurred recently, reaching a negative peak in 2022, annus horribilis for the cryptocurrency market.

Through a scientific-analytical approach, the thesis does not limit itself to chronologically summarizing the most significant failures that have occurred in recent years in the crypto-assets' market, but it strives to essay the degree of interconnectedness between traditional markets and the crypto-economy in order to understand whether and in to what extent this link interferes with financial stability and how it will be necessary to act on a legislative level to avoid falling back into disastrous future crises.

As a corollary to the unraveled reflections, although it must be recognized the EU institutions' capability of realizing an ambitious and complex project such as the Digital Finance Package by guaranteeing greater legal certainty in the crypto-asset markets thanks to MiCA and other European regulations, however, it is not easy to automatically place CASPs in a specific and precise intermediation category.

In conclusion, critical profiles emerge in contexts such as anti- money laundering, taxation, environment, and privacy. Amendments are supposed to be implemented in the future to remove some obstacles that could distort the Digital Single Market.

III

ABSTRACT

«Niente è duraturo come il cambiamento». L'affermazione, formulata dallo scrittore tedesco Ludwig Börne, ben si attaglia anche al sistema finanziario, la cui struttura è in costante trasformazione. A ben considerare, si tratta di un processo che può ritenersi fisiologico giacché determinato dall'indissolubile legame tra innovazione, attività economica e società che nel corso della storia ha apportato miglioramenti visibilmente crescenti in termini di efficienza delle prestazioni, affinamento di procedure e personalizzazione di soluzioni atte a soddisfare specifiche esigenze di clienti-consumatori. È innegabile, tuttavia, come in questo settore la componente tecnologica – specie di matrice crittografica – sia andata ben oltre la mera funzione di supporto e potenziamento degli elementi che vertebrano la complessa architettura della finanza tradizionalmente intesa (*TradFi*). L'introduzione della *DLT Technology*, della *blockchain* e degli *smart contract* ha permesso il rimaneggiamento di intermediari, sistemi di pagamento e fiducia al punto tale da edificare in via parallela un “*crypto financial ecosystem*”, ossia un perimetro crittografico in cui è stata per certi versi duplicata l'intelaiatura dei mercati finanziari tradizionali. Non solo il meccanismo e le fattezze organizzative ricalcano gli stilemi della finanza classica, ma in tale assetto si possono individuare anche entità, prodotti e servizi all'incirca simili dal punto di vista funzionale e della qualificazione giuridico-economica. Nello specifico, *digital asset* e *Crypto-Asset Service Provider (CASP)* sono rispettivamente gli oggetti ed i soggetti che spaziano all'interno della *CeDeFi* (un luogo in cui *Centralized Finance (CeFi)* e *Decentralized Finance (DeFi)*, sottoinsiemi del suesposto “ambiente finanziario alternativo”, sono indissolubilmente connessi ma che per ragioni di natura teorica ed accademica saranno illustrate l'una separata dall'altra). Se sui primi (*digital asset*) la comunità giuseconomica ha già prodotto (e produce tuttora) una quantità corposa di articoli e testi scientifici, confermando come non sia affatto sopito l'interesse rivolto verso le cripto-attività e le *Central Bank Digital Currency (CBDC)*, sui secondi (*CASP*) non può dirsi altrettanto. Constatato quanto descritto sopra, il presente studio s'incentra sui cd. prestatori di servizi per le cripto-attività con l'obiettivo di fornirne una visione organica ed il più possibile esaustiva. Per fare ciò, il lavoro riepiloga i fattori esogeni che ne hanno favorito la nascita e ricostruisce, dapprima, gli episodi-chiave da cui prende abbrivio la loro astratta teorizzazione e,

successivamente, il loro ingresso nella sfera del diritto vivente. Sebbene l'analisi giuridica propenda decisamente per una prospettiva regolatoria nazionale ed europea, l'indagine non manca di integrare un approccio comparato posando una lente d'osservazione sullo stato di normazione di questi intermediari a livello globale. Per di più, l'adozione di uno sguardo complessivo del fenomeno ha certamente rafforzato l'idea di non ignorare ad oltranza le diverse problematiche provocate dalle *crypto exchange platform (CEX/DEX)* che stanno gradualmente assumendo rilevanza ed occupando maggiore spazio nei dibattiti sia accademici che istituzionali solo dopo l'allarmante serie di fallimenti verificatisi di recente, toccando in negativo il picco nel 2022, *annus horribilis* per il mercato criptovalutario. Accedendo ad un approccio scientifico-analitico, l'elaborato non si limita in tale contesto a riassumere cronologicamente i fallimenti più significativi legati al mondo degli *asset* crittografici avvenuti negli ultimi anni, ma si sforza di saggiare il grado di interconnessione tra mercati tradizionali e *crypto-economy* così da comprendere se e in che misura questo legame interferisce sulla stabilità finanziaria e come bisognerà eventualmente agire sul piano della regolamentazione per non ricadere in disastrose crisi future. A corollario delle riflessioni dipanate, l'indagine induce a constatare come, sebbene vada riconosciuta alle istituzioni unionali la capacità di concretizzare un progetto ambizioso e complesso come il *Digital Finance Package* garantendo al mercato dei *crypto-asset* una maggiore certezza del diritto grazie al *MiCA* e ad altre normative europee, non risulti però agevole collocare automaticamente i *CASP* in una specifica e precisa categoria d'intermediazione. Conclusivamente e per completezza di trattazione, più di un cenno si impone verso i profili di criticità registrati in determinati contesti quali l'antiriciclaggio, la tassazione, l'ambiente e la *privacy* che meriterebbero di essere in futuro emendati al fine di rimuovere alcuni ostacoli che potrebbero falsare il Mercato Unico Digitale.

Indice

NOTE INTRODUTTIVE E DI PREMESSA	1
I. LA “FINANZIARIZZAZIONE” DEL SISTEMA <i>CRYPTO</i> E PUNTI DI CONTATTO CON LA FINANZA TRADIZIONALE.....	5
1. L'avvento dell'informatica e della digitalizzazione come fattore di rottura con il passato. Lo sdoppiamento della <i>TradFi</i> in “ <i>crypto financial system</i> ”	5
2. <i>DeFi</i> , <i>CeFi</i> e <i>CeDeFi</i> : una rapida perlustrazione del perimetro crittografico e disamina delle relative terminologie	16
3. Interconnessione tra sistema finanziario e crypto-mondo: criticità connesse a uno sviluppo deregolamentato del mercato	24
II. PRODOTTI ED OPERATORI TRA <i>CEFI</i> E <i>DEFI</i>.....	37
SEZIONE 1. I DIGITAL ASSET: TECNOLOGIE DI BASE E VARIE TASSONOMIE	38
1. Le <i>crypto technology</i> : le tecnologie di base per le crypto-attività	38
1.1. Distributed Ledger Technology (DLT) e blockchain: lineamenti essenziali.....	38
1.2. I Smart contract come principale meccanismo di disintermediazione nel Web3	43
2. La famiglia dei <i>digital asset</i> : <i>crypto-asset</i> e <i>CBDC</i>	46
2.1. I <i>crypto-asset</i> : alla ricerca di una tassonomia condivisa	48
2.2. Central Bank Digital Currency (CBDC): possibile allargamento della strumentazione dei <i>CASP</i> ?	54
SEZIONE 2. I <i>CRYPTO-ASSET SERVICE PROVIDER (CASP)</i>: CONFIGURAZIONE GIURIDICA, PROFILI REGOLATORI E RELATIVI ONERI.....	62
1. Finanza tradizionale e finanza decentralizzata: il paradigma regolatorio delle crypto-attività	62
2. Le esigenze alla base di una rinnovata regolamentazione sovranazionale delle crypto-attività	68
3. La genesi dei <i>CASP</i> : quali profili regolatori oltre i <i>VASP</i> ?	79
3.1. Il quadro normativo italiano in materia di <i>VASP</i> : il nuovo ruolo dell'Organismo Agenti e Mediatori (OAM) dopo il DM 13 gennaio 2022	79
3.2. Da <i>VASP</i> a <i>CASP</i> : una novità formale o sostanziale?	84
4. Inquadramento generale dei <i>CASP</i> : la disciplina <i>MiCA</i>	86
4.1. Premesse: le logiche del bilanciamento tra le istanze regolatorie e le dinamiche di un mercato a-territoriale	86
4.2. Ambito di applicazione del Regolamento <i>MiCA</i>	89
4.3. La definizione normativa di “ <i>CASP</i> ”	93
4.4. Autorizzazioni e condizioni di esercizio per i prestatori di servizi per le crypto-attività.....	94
5. Analisi empirica: scenari attuali e sviluppi futuri sul panorama dei <i>CASP</i>	103
6. Verso una conclusione: <i>CASP</i> come nuovi operatori finanziari?	113
III. L'IMPATTO DELLE CRYPTO-ATTIVITÀ E DEI <i>CASP</i>: SPECIFICI AMBITI DI ATTENZIONE PERIMETRATI DAL <i>MICA</i> E ALTRE NORMATIVE EUROPEE	118
SEZIONE 1. ANTIRICICLAGGIO E LOTTA AL FINANZIAMENTO AL TERRORISMO: LA DIMENSIONE NATIVA DEI <i>CASP</i>	120
1. Analisi del fenomeno: i rischi del riciclaggio nella <i>DeFi</i>	120
2. Focus sulle metodiche tradizionali dell'attività di riciclaggio	124
3. Variabili evolutive del riciclaggio: dal <i>cyber-laundering</i> al <i>crypto-laundering</i>	127
4. Crypto-attività e rischio di riciclaggio	131
5. Il ruolo dello pseudo-anonimato	135
6. La <i>blockchain</i> ed il finanziamento al terrorismo	141
7. Usi illeciti di <i>NFT</i> per finalità di riciclaggio e finanziamento al terrorismo.....	146
8. Il quadro giuridico di contrasto al riciclaggio (<i>AML</i>) e al finanziamento del terrorismo (<i>CFT</i>)	149
8.1. Le avvertenze del Gruppo d'Azione Finanziaria Internazionale (GAFI)	149
8.2. Crypto-asset e normativa antiriciclaggio: dalla IV Direttiva <i>AMLD</i> alle successive V e VI e al loro recepimento	155
SEZIONE 2. TASSAZIONE: COME I <i>CASP</i> DOVRANNO GESTIRE IL TRATTAMENTO FISCALE DELLE CRYPTO-ATTIVITÀ.....	167
1. Introduzione su tassazione in Italia e in Europa	167

2. La disciplina fiscale delle cripto-attività in Italia: l'imposta sul reddito delle persone fisiche (Irpef)	172
3. L'imposta sui redditi delle società (IRES)	186
3.1. Il trattamento contabile delle cripto-attività	187
3.2. La tassazione delle cripto-attività nell'ambito del reddito d'impresa	191
4. Altri redditi	193
5. L'imposta sul valore aggiunto (IVA)	194
5.1. Cripto-attività e servizi connessi	195
5.2. Utility token e Hybrid token	197
5.3. Non Fungible Token (NFT)	198
6. Gli obblighi di monitoraggio fiscale	198
7. Rideterminazione del valore delle cripto-attività	199
8. Regularizzazione delle cripto-attività	200
9. Criticità emergenti e potenziali soluzioni	200
SEZIONE 3. AMBIENTE: DELUCIDAZIONI E SPUNTI NORMATIVI A FRONTE DEL DISPENDIO ENERGETICO GENERATO DA CASP E DIGITAL ASSET	207
1. Ambiente, cripto-attività e CBDC: un nesso problematico	207
2. Tendenze evolutive del mercato criptovalutario e potenziali soluzioni al problema della pesante impronta ambientale ed energetica del <i>mining</i>	218
SEZIONE 4. PRIVACY: UNA NUOVA FONTE DI ONERI CHE I CASP DOVRANNO CONSIDERARE IN FUTURO?	233
1. Considerazioni preliminari: i termini del rapporto tra privacy e finanza digitale	233
2. Le modalità di trattamento del dato bancario: normativa in vigore e prospettive di sviluppo	243
3. Regolamento DORA – <i>Digital Operational Resilience Act</i> : le nuove frontiere della tutela della <i>privacy</i> nel settore finanziario	252
4. <i>Privacy</i> e valuta digitale: il concetto della anonimizzazione delle transazioni e i profili di rischio	257
5. <i>Privacy</i> e CBDC: verso la regolamentazione della valuta digitale. Quali (nuovi) impatti sulla riservatezza delle persone fisiche?	260
RIFLESSIONI CONCLUSIVE	264
FONTI E ULTERIORI RIFERIMENTI	275

La *crypto-economy* è un ecosistema che, al sopraggiungere di determinate novità, richiede di essere aggiornato. Tale circostanza, unitamente ad altre concause, induce la comunità giuseconomica a mantenere sempre alto l'interesse nelle vicende innovative che circolano in questo settore. Muovendo da questi presupposti, l'indagine si colloca nella branca della finanza digitale, sistematizzando ed approfondendo il tema dei cd. "fornitori di servizi per le crypto-attività" che, tra i vari acronimi esistenti per riferirsi a tali soggetti, nel corso dell'elaborato verranno stringatamente denominati *CASP* secondo la nomenclatura dettata dal *Markets in Crypto-Assets Regulation* (noto come Regolamento *MiCA* o semplicemente *MiCA*).

Il **primo capitolo** cercherà di descrivere nel modo più chiaro possibile la trasformazione tecnologica che ha travolto il sistema finanziario tradizionale (*TradFi*) a livello strutturale negli ultimi quindici anni. L'avvento del fenomeno *FinTech* ha sì permesso agli intermediari bancari e finanziari di perfezionare procedure e servizi ed incrementare la propria operatività, ma al contempo ha consentito ad intermediari più snelli e "geneticamente digitalizzati" di irrompere nel settore. Per di più, con l'introduzione delle *crypto technology*, la *TradFi* ha subito una sorta di sdoppiamento, vedendosi replicare molte delle sue componenti e prerogative classiche in una dimensione separata e succedanea ("crypto financial system"), suddivisibile in *Centralized Finance (CeFi)* e *Decentralized Finance (DeFi)*. È proprio sul crinale di questi sottogruppi che si collocano i *CASP* (prevalentemente nella forma di *exchange platform* e *digital wallet custodian*) e i servizi da loro erogati.

In primis, appare interessante scandagliare la natura "duale" (centralizzata e decentralizzata) che connota questi intermediari. Bisognerebbe pertanto chiedersi se (e solo in caso positivo anche *quomodo*) questo duplice raggio d'azione generi delle problematiche in termini di stabilità finanziaria. Per fare ciò, si analizzeranno i profili di interconnessione tra mercato *crypto* e quello bancario-finanziario, osservando i fallimenti più eclatanti avvenuti di recente. Una concreta risposta a tali interrogativi potrebbe certamente aiutare a comprendere verso che direzione muoversi da un punto di vista normativo, mitigando così le probabilità che collassi come quelli della nota società *FTX* (punta dell'*iceberg* di un problema ben più esteso)

si ripetano in futuro.

Nel **secondo capitolo** l'area di osservazione si restringerà occupandosi esclusivamente di prodotti e soggetti che navigano nell'ecosistema *crypto* tra *CeFi* e *DeFi*. Con riferimento ai profili oggettivi, si passeranno sinteticamente in rassegna le fondamentali tecnologie di base ravvisabili nella *Distributed Ledger Technology*, *blockchain* e *smart contract*. In maniera altrettanto succinta si descriveranno rapidamente *crypto-asset* e *Central Bank Digital Currency (CBDC)*, ossia le principali sub-categorie di *digital asset*, il cui utilizzo ha destato l'attenzione di numerose giurisdizioni e istituzioni di vario livello, sollevando eterogenee riflessioni. Da un lato, si registrano sfide di inquadramento giuridico e soprattutto di carattere tassonomico in svariate ramificazioni del diritto, esercitando una certa pressione su *framework* nazionali e non solo; dall'altro lato, invece, la sovranità monetaria, in un'epoca dominata dalla dematerializzazione, reagisce attraverso una propria moneta digitale dinanzi alla minacciosa presenza di attori privati, dotati di sistemi di pagamento immediato ed altri strumenti sempre più attraenti agli occhi dei consumatori digitali.

Una volta ricomposte organicamente le tecnologie basilari ed i prodotti alla base delle cripto-attività, ci si addenterà nell'indagine giuridica sui *CASP*, tentando di sciogliere il seguente nodo: possono tali *provider* considerarsi una categoria a sé di soggetti mediatori? In altri termini, siamo in presenza di soggetti aventi una propria e precisa identità al punto tale da differenziarsi dai soggetti bancari e finanziari e costituire una nuova *species* nel panorama dell'intermediazione? Eventualmente, qualora questa circostanza trasparisse, sarà necessario in seconda battuta chiarire quanto questa separazione rispetto ai classici attori sia sfumata.

Progredendo con l'analisi giuridica, non possono non sottolinearsi i notevoli sforzi realizzati dalle istituzioni sovranazionali per garantire la certezza del diritto nell'ambito delle cripto-attività o una migliore tutela di consumatori ed investitori in questo settore. Ebbene, è d'uopo chiedersi se il complesso delle norme europee circoscriventi l'*habitat* dei *CASP* e delle cripto-attività sia riuscito a regolamentare esaurientemente tutti i possibili profili di criticità. E nell'eventualità che qualcosa sia sfuggito, si tenterà di convertire il potenziale *vulnus* individuato in spunti di riflessione o suggerimenti condivisibili sul piano legislativo.

Per soddisfare tale obiettivo, nel **terzo capitolo** si indirizzerà uno sguardo particolarmente attento a materie come l'antiriciclaggio, la tassazione e l'ambiente. Queste specifiche aree

d'osservazione non sono casuali, ma sono piuttosto accomunate dal fatto di essere tutte segnalate (certe con maggiore evidenza, altre meno ma comunque intravedibili) dalla normativa *MiCA*. E in ciascuno di questi ambiti tematici, gli operatori devono necessariamente soddisfare requisiti o adempiere obblighi, sia diretti che indiretti. Pertanto, l'analisi giuridica verterà inizialmente sulle prospettive in cui la normazione appare più fitta (antiriciclaggio), addentrandosi successivamente negli ambiti meno esplorati ma degni di essere approfonditi (tassazione ed ambiente).

A integrazione di quanto anzidetto, è innegabile la particolare rilevanza che la protezione dei dati personali ha assunto nella società odierna. Ciò non si manifesta solo con i tentativi di rafforzamento della resilienza digitale in ambito finanziario promossi dal Regolamento *DORA*. Quest'ultimo atto normativo costituisce un piccolo tassello di un mosaico ben più grande. L'obiettivo delle istituzioni unionali nei prossimi anni, invero, è implementare una vera e propria strategia europea di cybersicurezza. Il rapido susseguirsi di una crisi pandemica, prima, e di una vera e propria "stagione" bellica, poi, hanno certamente contribuito all'accrescimento quantitativo degli attacchi *cyber* con un livello di sofisticazione sempre più alto. Per questi motivi, il presente lavoro non risulterebbe completo se, assieme alle aree sopra declinate, non si comprendesse anche il tema della *privacy* come ulteriore lente d'osservazione dei *Crypto-Asset Service Provider*. Infatti, nonostante questi soggetti non siano generalmente obbligati a trattare le informazioni dei clienti relative al trasferimento di *crypto-asset* come dati personali ai sensi delle leggi sulla protezione dei dati applicabili (es. *GDPR*), è ragionevole ritenere che in futuro i numerosi oneri già dettati dal *MiCA* si allarghino anche su questo fronte.

Per quanto attiene invece alla **metodologia**, l'approccio adottato è fondato su un'analisi sia giuridica che empirica. Nel primo caso, si è proceduto ad esaminare in maniera rigorosa l'istituto giuridico dei *CASP*, dapprima effettuando cenni generali e di contesto sulle loro origini nonché formulando le opportune domande di ricerca. Dopodiché, si è cercato di sciogliere i nodi problematici preposti attraverso ricostruzioni, riflessioni logico-giuridiche ed argomentazioni alla luce delle normative rilevanti di settore.

Nel secondo caso, vi è una nutrita serie di dati raccolti tramite ricerche in lingua italiana e inglese (in via prevalente) durante l'attività dottorale, ricomprendendo non solo quelli

condivisi da istituzioni e/o entità internazionali ritenute affidabili (es. autorità di settore, *think-tank*, società di consulenza, ecc.), ma anche quelli personalmente messi a punto. Su quest'ultimo versante, si tratta in sintesi di dati concernenti la regolamentazione dei *CASP* in tutte le giurisdizioni del mondo. I criteri selezionati e (laddove possibile) compilati sono i seguenti:

1. Nome del Paese/Giurisdizione;
2. Continente/Area Geografica
3. È presente una regolamentazione *CASP*? O quantomeno si è riusciti a ricomprendere tali soggetti in normative pre-esistenti? (Sì, no, in corso/c'è intenzione)
 - 3.1) Se no, perché?
 - 3.2) Se sì, come sono denominati?
4. Laddove possibile, qual è la terminologia utilizzata per definire le cripto-attività?
5. A prescindere dalla presenza di una normativa *ad hoc*, è comunque prevista un'autorità di vigilanza su soggetti che erogano servizi per le cripto-attività?
6. Altro (curiosità/peculiarità da segnalare).

Al fine di rendere visivamente apprezzabile il lavoro svolto, i risultati di questa analisi verranno riportati in forma di rappresentazioni grafiche. Tale attività analitica si è rivelata sin da subito utile, permettendo di comprendere il loro stato di normazione, mettere ordine sulle denominazioni che abbondano attorno a queste nuove figure a livello globale nonché di cogliere numerose sfumature che variano a seconda delle impostazioni legislative stabilite da ogni singola giurisdizione del mondo.

I. LA “FINANZIARIZZAZIONE” DEL SISTEMA CRYPTO E PUNTI DI CONTATTO CON LA FINANZA TRADIZIONALE

1. L’avvento dell’informatica e della digitalizzazione come fattore di rottura con il passato. Lo sdoppiamento della *TradFi* in “*crypto financial system*”

Lo sviluppo e il successo economico di un Paese dipendono in buona misura dalla solidità del proprio sistema finanziario¹. Scendendo nel dettaglio, in un recente studio proveniente dalla *Bank of International Settlement (BIS)*² si afferma nitidamente come crescita e stabilità economica passino attraverso alcune attività-chiave come *«l’allocazione delle risorse per il loro uso più produttivo, lo spostamento di capitali da agenti con eccedenze a quelli con deficit e la fornitura di mezzi efficienti per spostare la ricchezza nel tempo e negli Stati»*³. Ciò lascia intendere che l’importanza di un sistema finanziario risiede, quanto meno in via principale, nella sua capacità di fornire prodotti per il credito e il risparmio, di trasformare quest’ultimo in investimenti nonché di gestire la volatilità e il rischio correlati. Per di più, la complessa architettura del sistema finanziario non potrebbe sorreggersi robustamente senza una salda interconnessione tra le sue componenti essenziali: intermediari, sistemi di pagamento e fiducia. Analizzando rapidamente questo trittico, si consideri che *«il sistema finanziario statunitense, e analogamente la maggior parte degli altri Paesi, si è tradizionalmente affidato a un insieme di intermediari come banche, broker, borse, ecc. collegati da sistemi di pagamento. Questi intermediari fungono da nodi centralizzati che proteggono l’accesso al sistema finanziario e forniscono ai clienti servizi essenziali come la*

¹ [Consob, Il Sistema Finanziario attuale: una stilizzazione, Educazione Finanziaria, 2023](#). Essenzialmente ciò si traduce, almeno nelle economie moderne, nel soddisfacimento di almeno tre funzioni: la funzione monetaria; la funzione allocativa delle risorse; la funzione di gestione dei rischi connessi agli investimenti effettuati.

² La Banca dei Regolamenti Internazionali (BRI), nata nel 1930, ha sede a Basilea in Svizzera ed è spesso chiamata la "Banca Centrale per le Banche Centrali". Difatti, fornisce servizi bancari a istituzioni come la Banca Centrale Europea e la Federal Reserve. Questi servizi includono conti per depositi e titoli fruttiferi, transazioni in oro e valuta, servizi di gestione patrimoniale e fornitura di prestiti garantiti a breve termine. La BRI non gestisce transazioni né fornisce prestiti ai governi, né affari con aziende o consumatori, bensì incoraggia la cooperazione tra le Banche Centrali. Il Comitato di Basilea per la vigilanza bancaria (BCBS) è un forum internazionale strettamente associato per la regolamentazione finanziaria. È uno dei numerosi comitati e associazioni internazionali governati in modo indipendente con sede presso la sede della BRI e supportato dal suo segretariato. Vds. [Hayes A., Bank for International Settlements: Overview, History, 2022](#).

³ [Makarov I., Schoar A., Cryptocurrencies and Decentralized Finance \(DeFi\), BIS Working Papers no. 1061 – Monetary and Economic Department, 2022](#).

tenuta dei registri, la verifica delle transazioni, il regolamento, la liquidità e la sicurezza. Questa architettura implica che gli intermediari svolgano molte delle funzioni fondamentali del sistema e contribuiscano anche all'attuazione degli obiettivi normativi, come la rendicontazione fiscale, le leggi antiriciclaggio o la tutela dei consumatori»⁴.

Procedendo al secondo punto, se dovessimo paragonare il sistema finanziario a un corpo umano, i «*sistemi di pagamento sono le arterie che trasportano la linfa vitale della finanza*»⁵. L'affermazione non sorprende se si considera che il concetto di scambio e l'evoluzione dei mercati sono andati sempre di pari passo nel corso della storia economica. È proprio attraverso l'incessante perfezionamento degli strumenti e delle procedure preposti a trasferire denaro tra soggetti che viene garantita l'efficienza, la sicurezza e la stabilità dell'intera filiera finanziaria⁶.

In chiusura, si passa alla costruzione e mantenimento della fiducia. Tale sentimento, se ben consolidato all'interno del rapporto intermediari-consumatori, apre le porte a un circolo virtuoso. Com'è intuibile, se il fornitore di servizi finanziari si dimostra affidabile nel suo ruolo, probabilmente riuscirà non solo a far perdurare il rapporto fiduciario con i propri clienti ma questi ultimi potrebbero ribadire il proprio apprezzamento richiedendo l'erogazione degli stessi servizi, se non addirittura di nuovi⁷. Ciò vale, in maniera analoga, per quanto attiene ai rapporti tra gli stessi intermediari e/o istituzioni. Estraendo le parole di Prasad, infatti «*è la fiducia nelle Banche Centrali che mantiene il denaro sostenibile. Allo stesso modo, quando si tratta di creare denaro interno, l'attività bancaria commerciale, è costruita su una base di fiducia, rafforzata da processi di regolamentazione supervisionati da istituzioni governative.*

⁴ Cfr. [Makarov I., Schoar A., *Cryptocurrencies and Decentralized Finance \(DeFi\)*, BIS Working Papers no. 1061 – Monetary and Economic Department, 2022.](#)

⁵ Prasad, E. A., *The future of money. How the digital revolution is transforming currencies and finance*, Harvard University Press, 2021, p. 45.

⁶ Si tratta di un concetto assorbito dal sistema finanziario e che traspare con forza soprattutto dopo aver preso visione del rapporto pubblicato dal Fondo Monetario Internazionale, secondo cui un sistema di pagamento ha rilevanza potenzialmente sistemica se è in grado di innescare o trasmettere turbative nel sistema finanziario nazionale o internazionale. [Khiaonarong T. et al., *Operational Resilience in Digital Payments: Experiences and Issues*, IMF eLibrary, 2021.](#)

⁷ [Van Esterik-Plasmeijer P.W.J. e Van Raaij F., *Banking system trust, bank trust and bank loyalty*, *International Journal of Bank marketing* 35\(1\), 2017, pp. 97—111.](#) Come specificano correttamente gli autori nel loro contributo, «*la fiducia facilita le transazioni con i clienti. I clienti non devono preoccuparsi della cura dei loro interessi personali, dei loro risparmi presso la banca e dei prodotti finanziari che hanno acquistato o intendono acquistare dalla banca, tra cui polizze assicurative e mutui. Con un alto livello di fiducia, i clienti si sentono sicuri che i loro interessi siano ben serviti dalla banca. In un certo senso, un alto livello di fiducia è un cuscinetto contro le esperienze negative che possono verificarsi tra i clienti.*

Alcuni dei principali sviluppi della finanza moderna riflettono l'importanza di mantenere la fiducia attraverso gli intermediari finanziari e senza affidarsi a stampelle come le garanzie che sostengono i sistemi bancari e di pagamento tradizionali»⁸. Da questa angolazione, si potrebbe concepire la fiducia come un lubrificante senza il quale le dinamiche tra intermediari sarebbero connotate da quotidiane frizioni e, similmente, la circolazione del denaro e la fluidità delle transazioni risulterebbero farraginosi, andando a scapito della stabilità finanziaria generale.

Il quadro sinora delineato ci permette di cristallizzare lo spirito essenziale della *Traditional Finance* (o *TradFi*)⁹, un paradigma in cui convenzionalmente si ripone fiducia (volontaria od obbligatoria) verso regolatori, banche e istituzioni statali o sovranazionali che gestiscono tutte le informazioni in registri chiusi e centralizzati¹⁰. Traspone però dal pensiero di Khanna che l'uomo è da diverso tempo nel vortice di un'irreversibile mutazione dettata dalla tecnologia. E nella stessa misura, non sfuggono a questo destino l'economia, il lavoro, la sanità, l'educazione e tutto il complesso delle istituzioni e delle strutture sociali¹¹. Il rapporto pressoché simbiotico che ci lega con la "tèchne" digitale «sta oltrepassando il livello puramente strumentale per entrare nella sfera esistenziale»¹², tanto da definire l'epoca che stiamo vivendo, non più esclusivamente tecnologica, bensì sarebbe più corretto dire socio-tecnologica. Stiamo di fatto avanzando verso un mondo ibrido. Come un moderno Re Mida, la computerizzazione ha pervaso ogni aspetto della vita umana con il suo "tocco". E la quarta rivoluzione industriale, difatti, si è dimostrata inarrestabile. Le tecnologie sviluppate nell'ultimo quindicennio si sono diffuse con una sinora inedita rapidità e hanno contribuito

⁸ Cfr. Prasad. E. A., *The future of money. How the digital revolution is transforming currencies and finance*, Harvard University Press, 2021.

⁹ [AA.VV. TradFi and DeFi: Key difference, Hedera, 2023](#): «Il sistema finanziario tradizionale si basa su punti centrali che consentono e regolano la negoziazione, il prestito e la gestione di asset e strumenti finanziari. La TradFi è fiorita perché funziona. Tra le sue numerose caratteristiche vi sono i solidi requisiti normativi che danno alle imprese la sicurezza necessaria per assumere rischi, garantendo al contempo la protezione dei consumatori. [...] Le entità centralizzate, come banche, società di investimento e agenzie governative, sono fondamentali per l'infrastruttura TradFi. Queste entità sviluppano e commercializzano prodotti e servizi finanziari. Sono anche responsabili della gestione del rischio attraverso la regolamentazione dei mercati finanziari e la fornitura di assicurazioni. Affinché una struttura centralizzata abbia successo, i cittadini devono fidarsi dell'ente che gestisce i loro fondi. Le agenzie governative spesso collaborano con enti non governativi per garantire la protezione dei fondi dei cittadini».

¹⁰ [Capaccioli S., Introduzione alle criptovalute e bitcoin, Coinlex, 2020.](#)

¹¹ Cfr. Khanna A. et al., *L'età ibrida. Il potere della tecnologia nella competizione globale*, Codice Edizioni, 2013.

¹² *Ibidem*.

alla radicale trasformazione - soprattutto di matrice tecnica - di numerosi settori produttivi. Quelli afferenti rispettivamente al mondo monetario, bancario e finanziario non fanno eccezione. A tal proposito, l'impiego di nuove tecnologie nel campo dell'intermediazione bancaria e finanziaria¹³ ha un apposito termine, ormai largamente utilizzato nel panorama internazionale, noto come “*FinTech*” (*Financial Tecnology*)¹⁴ o “Tecnofinanza”¹⁵.

L'impatto di questo assemblaggio¹⁶ si è dimostrato sin da subito dirompente poiché fornisce

¹³ In generale, in tema di *FinTech* v. AA.VV., *Diritto del Fintech*, a cura di Cian M., Sandei C., Cedam, 2020; AA.VV., *FinTech*, a cura di Fimmanò F. e Falcone F., Edizioni Scientifiche Italiane, 2019; AA.VV., *FinTech*, a cura di Paracampo M.T., Giappichelli Editore, 2021; AA.VV., *Fintech: i confini dell'innovazione nella finanza*, a cura di Natale A., Giuffrè, 2022; Abriani N. e Schneider G., *Diritto delle imprese e intelligenza artificiale. Dalla FinTech alla CorpTech*, Il Mulino, 2021; [Blandini A., *Diritto dell'innovazione*, Cedam, 2022](#), p. 435 e ss..

¹⁴ Volendo puntualizzare, l'avvento e l'evoluzione delle tecnologie dell'informazione e della comunicazione (*information and communication technology*, o “ICT”), favorite dai recenti progressi della crittografia e dalle evoluzioni della rete *internet*, hanno determinato un cambiamento radicale nel settore finanziario e bancario, all'interno del quale - sulla scia del più generale processo che sta dando vita alla *digital economy* - è germogliato un nuovo fenomeno noto come “*FinTech*” (*Financial Tecnology*). La formula “*FinTech*” come intuibile nasce dalla contrazione dei termini *Finance* (*Fin*) e *Technology* (*Tech*) e si riferisce all'innovazione finanziaria resa possibile dall'evoluzione tecnologica. In ordine a tale fenomeno, la dottrina parla di “quarta” rivoluzione digitale che succede a quelle già registratesi a partire dagli anni '80 (AA.VV., *Fintech: diritti, concorrenza, regole*, a cura di Finocchiaro G., Falce V., Zanichelli Editore, 2019, p. 1 e ss.). Ai fini più prettamente giuridici si potrebbe avanzare una preliminare definizione giuridica di *FinTech* nei termini indicati nel decreto 30 aprile 2021, n. 100, recante il regolamento sulla disciplina del Comitato e della sperimentazione *FinTech*. Segnatamente, secondo l'art. 1, comma 1, lett. c) dello stesso decreto per *FinTech* si intendono «le attività volte al perseguimento, mediante nuove tecnologie, dell'innovazione di servizi e di prodotti nei settori bancario, finanziario, assicurativo».

¹⁵ [Servizio Studi, *FinTech, Dossier della Camera dei Deputati*, 2022](#). Il documento redatto dal Servizio Studi della Camera dei Deputati riporta le considerazioni dello IOSCO (*International Organization of Securities Commission*), ossia l'Organizzazione Internazionale delle autorità di vigilanza dei mercati finanziari, che individua 8 macro-aree nelle quali il fenomeno *FinTech* si sviluppa: «i) pagamenti; ii) assicurazioni (*InsurTech*); iii) pianificazione finanziaria; iv) *crowdfunding*; v) investimenti e trading; vi) *blockchain*; vii) ricerca ed analisi delle informazioni; viii) sicurezza». Tra questi spicca per l'appunto la tecnologia *blockchain*, considerata potenzialmente la più dirompente in quanto estremamente flessibile e versatile nel suo utilizzo, non solo nel ramo finanziario.

¹⁶ Delineando anche gli aspetti più complessi, come da tempo segnalato dalla dottrina, il fenomeno *FinTech* mette a dura prova i fondamenti giuridici affermatasi nel tempo, con particolare riferimento ai seguenti principi:

- principio di stretta territorialità;
- principio di tipicità delle attività svolte;
- principio del “passaporto” per gli operatori;
- principio della gerarchia delle fonti.

Ad acuire le problematicità è il rapido diffondersi nel settore finanziario della nuova tecnologia basata sui registri distribuiti (e in particolare della *blockchain*) che potrebbero ridurre o eliminare la necessità di intermediari o processi centralizzati tradizionalmente coinvolti nella fornitura di servizi finanziari. Tale decentralizzazione, come osservato dal *Financial Stability Board* assume generalmente una delle tre forme generali: i) la decentralizzazione del processo decisionale, ii) dell'assunzione di rischi e/o iii) della tenuta dei registri. Per ulteriori approfondimenti, si consigliano le seguenti letture: Pitruzzella G., *FinTech e i nuovi scenari competitivi nel settore finanziario-credizio e assicurativo*, Mensile dell'Associazione Bancaria Italiana, 2018. Per ulteriori approfondimenti vds. Lynn T. (a cura di), *Disrupting Finance: Fintech and Strategy in 21st century*, Palgrave – McMillan, 2018; v. anche Tanda M. e Schena C., *Fintech, Bigtech and Banks: Digitalisation and Its Impact*

un mezzo di supporto per gli intermediari tradizionali e dischiude enormi possibilità in termini di accesso ai finanziamenti, efficienza operativa, riduzione dei costi e maggiore competitività¹⁷, generando per certi versi una “TradFi 2.0”, in cui le proprietà tipiche del sistema finanziario tradizionale non sono state intaccate o snaturate¹⁸. Al contrario, vi è stato un notevole irrobustimento e potenziamento delle *performance* sia di *incumbents*¹⁹ che di *new entries*, entrambi riconducibili ad un paradigma pressoché centralizzato. È in questo contesto che, in ottica di semi-discontinuità, si frappongono le *crypto technology*²⁰, ossia «nuove tecnologie, favorite dai progressi della crittografia - ovvero dell'applicazione di metodi che servono per rendere un messaggio comprensibile/intelligibile solo a persone autorizzate a leggerlo - e dalle evoluzioni della rete Internet, apportando un cambiamento radicale nell'economia globale»²¹.

In concomitanza con tali sviluppi e a seguito della Grande Recessione (o *Global Financial Crisis, GFC*), la rete infrastrutturale finanziaria si manifesta in tutta la sua fragilità sistemica scatenando nella popolazione mondiale un generalizzato clima di sconcerto e sfiducia verso l'apparato creditizio, all'epoca difficile da risollevare. Con tempismo pressoché sincronico, nei primi giorni del 2009 affiorano concretamente dalla visione di Satoshi Nakamoto novità

on *Banking Business Model*, Palgrave – McMillan, 2019; La Sala G.P., *Intermediazione, disintermediazione e nuova intermediazione*, in Cian M., Sandei C., *Il diritto del Fintech*, Cedam 2020; [Egmont Group, FIU – FinTech Cooperation and Associated Cybercrime Typologies and Risks, 2022](#).

¹⁷ Una delle cause principali della pluralizzazione del settore è identificata nell'abbassamento delle barriere concorrenziali in favore dei nuovi soggetti, in linea con la direttiva PSD2. In altri termini, dato che nuovi operatori integrati si focalizzano soltanto su specifici segmenti della filiera, l'effetto più significativo delle tecnologie finanziarie è che queste stanno frantumando la catena del valore del mercato bancario, consentendo l'erogazione di servizi *ad hoc* e cuciti su misura per qualsiasi tipo di clientela. D'altro canto, per coloro che adottano una prospettiva critica su questa trasformazione, ciò ha senz'altro consentito a nuovi attori parabancari di agire al di fuori delle regole - ad esempio di vigilanza prudenziale e di requisiti di capitale - generalmente applicabili agli attori tradizionali. In questa prospettiva composita, la *FinTech* sembra rappresentare dunque un settore a sé stante, che pone problemi di regolamentazione, di concorrenza e di vigilanza autonomi.

¹⁸ Sebbene tra non molte pagine si introdurrà l'idea sostanziale della *Decentralized Finance (DeFi)*, preme in questa sede precisare che il fenomeno *Fintech* spazia attraverso innumerevoli dimensioni e segmenti di mercato. Pertanto, nonostante la natura dirompente della *Financial Technology*, «la *DeFi* si distingue anche dal termine generico di "Fintech". Anche se le innovazioni *Fintech* introducono nuove tecnologie nei servizi finanziari, [...] esse si basano ancora su un modello di intermediari centralizzati». Cfr. [Makarov I., Schoar A., Cryptocurrencies and Decentralized Finance \(DeFi\), BIS Working Papers no. 1061 – Monetary and Economic Department, 2022](#).

¹⁹ Con tale termine ci si riferisce agli operatori storici del settore bancario e finanziario, solitamente di grandi dimensioni.

²⁰ Narayanan A. et al., *Bitcoin and cryptocurrency Technologies: a comprehensive introduction*, Princeton University Press, 2016.

²¹ [Luca G., Criptovalute, La piazza d'Italia, 2023](#).

come la *blockchain* e il *bitcoin* che, assieme ad altre applicazioni, gettano le basi per edificare una sorta di “*crypto financial system*”, ossia un perimetro crittografico in cui l’intelaiatura dei mercati finanziari tradizionali è stata per certi versi duplicata. Non solo il meccanismo e le fattezze organizzative ricalcano gli stilemi della finanza classica, ma in tale assetto si possono individuare anche entità, prodotti e servizi all’incirca simili. Per comprendere i motivi per cui tra questi due paradigmi vi siano delle forti similitudini, ma non un’esatta corrispondenza, si passerà nuovamente in rassegna il *tris* di elementi citati precedentemente²². Osservando meglio, una volta venuti a contatto con la tecnologia decentrata, ci si accorge come le componenti di questa triade mutino pelle o subiscano addirittura un cambiamento in senso ontologico. Ne è un esempio lampante il tema della fiducia. Per colmare le asimmetrie informative e acquistare/vendere determinati prodotti nel mercato, nella *TradFi* il cliente si affida solitamente alle qualità consulenziali e operative del soggetto di mediazione²³. Il rapporto consumatore-intermediario si fonda pertanto su «un’aspettativa generalizzata di come l’istituto finanziario si comporterà in futuro. Questa aspettativa generalizzata di comportamento può derivare da convinzioni di comportamento accettabile o da norme, oppure può basarsi su precedenti esperienze con l’istituto finanziario»²⁴. Il legame fiduciario tradizionale impone di per sé di dipendere dall’operato di terzi, obbligando i clienti a identificarne uno adatto alle proprie esigenze e specificità nonché confidare nella loro capacità di agire in modo professionale o assumersi le proprie responsabilità in merito ai servizi promessi. Nel contesto dell’economia digitale questa circostanza ha tutt’altro sapore dal momento che la fiducia sposta il proprio baricentro. Il consumatore-utente non si rimette più alle peculiarità soggettive e comportamentali dell’intermediario, ma fa affidamento alle qualità tecnico-oggettive della *blockchain*, basato

²² Ossia intermediari, sistemi di pagamento e fiducia (che nella seconda analisi verranno riproposti in senso inverso rispetto a come originariamente impostato, cioè fiducia, sistemi di pagamento e intermediari).

²³ Satoshi Nakamoto mette in luce i difetti di questa convenzione asserendo che «il problema alla base delle valute convenzionali è dovuto alla quantità di fiducia necessaria per far funzionare il sistema. Dobbiamo fidarci del fatto che le banche non svalutino la moneta, ma purtroppo la storia è piena di momenti in cui questa fiducia non è stata rispettata. Dobbiamo fidarci del fatto che le banche conservano i nostri soldi, ma spesso sono scoppiate bolle legate al credito bancario, e solo una frazione dei soldi era effettivamente in possesso della banca. Dobbiamo riporre in queste istituzioni la nostra fiducia in termini di privacy, e fidarci del fatto che i ladri d’identità non svuotino i nostri conti correnti». [Buso R., Criptovalute e blockchain, regolamentazione ed evoluzione, Luiss, 2021.](#)

²⁴ [Van der Crujssen C. et al., Trust in Financial Institutions: A Survey, DeNederlandscheBank paper, 2020.](#)

su modelli e meccanismi automatizzati²⁵. Da qui, la nota frase “*Code is Law*” acquisisce un significato più profondo: la fiducia nella terzietà soggettiva²⁶ si tramuta in fiducia nell’incorruttibilità²⁷ della catena a blocchi, nei codici che ne governano il funzionamento nonché in una *governance* decentralizzata, che si regge su sistemi che «consentono di raggiungere un consenso sulle modifiche di un regime distribuito in assenza di un ente centrale datore di fiducia»²⁸.

Venendo ora ai sistemi di pagamento, la crescente complessità di tali fenomeni è stata messa in luce all’Unità di Informazione Finanziaria (UIF) nel proprio rapporto annuale per 2018²⁹, laddove viene evidenziato come l’avvento delle tecnologie *FinTech* abbia modificato radicalmente il mercato dei servizi. Mentre in passato i servizi di pagamento in moneta legale erano offerti in larga prevalenza dal sistema bancario³⁰, gradualmente si sono affermati altri soggetti, come gli istituti di pagamento e gli istituti di moneta elettronica, che si differenziano

²⁵ Garavaglia esprime molto bene questo passaggio affermando come «la tecnologia dei registri distribuiti (*Distributed Ledger Technology – DLT*) consente di replicare le informazioni presso una molteplicità di soggetti, ognuno dei quali ha visibilità dell’intera storia informativa che caratterizza un processo. Ciascuno di essi, dunque, ha la possibilità di farsi una propria ragione dei dati, degli eventi e delle transazioni che su tale registro distribuito si sono registrate: Per ognuno è possibile concorrere (o competere) al raggiungimento di un consenso finale su quella storia, applicando delle regole comuni che si è deciso di accettare e adottare proprio perché proposte e condivise in una logica decentralizzata (ossia frutto di una *governance* decentralizzata): un consenso distribuito basato su controlli altrettanto distribuiti, cui una pluralità perviene nel rispetto di regole condivise e decise in accordo decentralizzato». Vds. Garavaglia R., *Conoscere la blockchain for dummies*, Hoepli, 2022.

²⁶ Spesso impersonificato da professionisti o figure di rilievo come notai, giudici, arbitri e via discorrendo.

²⁷ Per molto tempo i principali sostenitori di una visione decentralizzata del sistema finanziario hanno fatto leva su questo punto, evidenziando come l’uso della *blockchain* garantisca transazioni immediate e sicure. Sebbene l’affermazione possa ritenersi generalmente valida, la nostra contemporaneità ci ha ormai fatto comprendere come la tecnologia proceda speditamente, facendo salti di qualità importanti in brevi lassi di tempo. Già oggi, attraverso apparecchiature con una notevole potenza di calcolo e velocità, è possibile corrompere la tecnologia *blockchain*. Questo evento, tuttavia, potrebbe presentarsi con maggiore frequenza e normalità con l’affermarsi della potenza di calcolo quantistica e dei *quantum bit* (noti anche come *qubit*). Per maggiori chiarimenti, si veda Cavicchioli M., *USA: i computer quantistici metteranno a rischio bitcoin*, *The Cryptonomist*, 2022.

²⁸ Garavaglia R., *Conoscere la blockchain for dummies*, Hoepli, 2022. In altre parole, le *DLT* sono connotate dall’assenza di un ente centrale, sostituito invece da un’organizzazione che non prevede gerarchizzazioni o verticismi e dove i processi decisionali sono assunti in modo orizzontale, dando titolo a chiunque a partecipare al processo di validazione.

²⁹ Vds. [Banca d’Italia, Rapporto Annuale 2018. Unità di Informazione Finanziaria per l’Italia, 2018.](#)

³⁰ Più di recente, nel report annuale per il 2022 [Banca d’Italia, Rapporto Annuale 2022. Unità di Informazione Finanziaria per l’Italia, 2022](#), l’UIF ha evidenziato che «sul fronte delle valute virtuali, il cui trend segnaletico è in progressiva crescita, i sospetti più ricorrenti attengono all’origine dei fondi utilizzati per l’acquisto degli asset, spesso correlati a possibili illeciti fiscali, frodi informatiche o episodi di ransomware. Sono state rilevate ipotesi di truffe nel trading online e di investimenti eseguiti dalle vittime dei raggiri presso piattaforme estere, sovente non autorizzate, a seguito di contatti telefonici insistenti o tramite l’intermediazione di sedicenti consulenti finanziari; l’investimento in valute virtuali è generalmente offerto applicando basse commissioni, in virtù di presunte partnership con i principali exchange».

dagli istituti bancari per un'operatività limitata, costi ridotti e struttura organizzativa semplificata³¹. Siffatta struttura del mercato dei servizi di pagamento, consolidatasi con l'avvento del *FinTech*³², sta tuttavia nuovamente modificandosi, mediante l'utilizzo intensivo delle tecnologie dell'informazione (*Cloud Computing, Internet of Things, Big Data e Intelligenza Artificiale*), oramai interconnesse ed integrate con le *DLT*. È indubbio, infatti, come i vantaggi apportati dalla *blockchain* assicurino una maggiore tutela di *privacy* e dati, riduzione dei costi ed una semplificazione delle transazioni transfrontaliere in modo veloce, accessibile e trasparente³³. Da questo punto di vista si è certamente innestato un rimodellamento dei pagamenti sia al dettaglio (*retail*) che all'ingrosso (*wholesale*)³⁴, dalle valute digitali delle banche centrali (*CBDC*) basate su *blockchain* e dai cd. *stablecoin*, alla resilienza operativa e alle nuove offerte di finanza incorporata³⁵.

Sintetizzando al massimo, l'importazione delle *crypto technology* nel sistema finanziario se da un lato ha sconvolto l'essenza originaria del concetto di fiducia, nel caso dei pagamenti a mutare sono soprattutto i metodi con cui ci relazioniamo ad essi e come li mettiamo in atto³⁶. A conferma di ciò, come asserito dall'Ufficio Rapporti con l'Unione Europea della Camera dei Deputati nel 2021, «nell'ultimo decennio (...) la maggior parte delle innovazioni nel settore dei pagamenti si è concentrata sul miglioramento delle interfacce con i clienti (ad

³¹ Cfr. [Giammatteo M., Cash use and money laundering: An application to Italian data at bank-municipality level, Quaderni dell'antiriciclaggio, 13, 2019](#), che sottolinea come «in epoca recente il settore degli strumenti di pagamento è stato interessato da cambiamenti radicali».

³² Nel modello di mercato dei servizi di pagamento guidato dal *FinTech* i metadati rappresentano la principale fonte di creazione di valore aggiunto e, conseguentemente, possono essere rappresentativi di attività di riciclaggio. A ciò si deve aggiungere che, la partecipazione di più soggetti alla fornitura del servizio può determinare la dispersione del patrimonio informativo, finora prevalentemente concentrato presso il sistema bancario, e delle responsabilità di prevenzione dei rischi di riciclaggio.

³³ [AA.VV., Cos'è la Blockchain e cosa cambia per i sistemi di pagamento digitale?, Worldline, 2021](#).

³⁴ [U.S. Department of the Treasury, The Future of Money and Payments. Report pursuant to Section 4 \(b\) of Executive Order 14067, 2022](#). «In generale, i consumatori e le imprese utilizzano sistemi di pagamento "al dettaglio", mentre le banche e le altre istituzioni finanziarie accedono a sistemi di pagamento "all'ingrosso". I sistemi di pagamento al dettaglio elaborano volumi elevati di transazioni di valore inferiore per conto di consumatori e imprese e possono non regolare istantaneamente (cioè in tempo reale). I sistemi di pagamento all'ingrosso supportano transazioni di valore più elevato per istituzioni finanziarie e agenzie governative e possono utilizzare una forma di regolamento in tempo reale o continuo. Una stessa forma di denaro può utilizzare più di un sistema di pagamento; ad esempio, il denaro delle banche private (cioè i depositi) può essere trasferito utilizzando assegni, sistemi di compensazione automatica (ACH) o carte di debito».

³⁵ [Clifford Chance, Payment trends 2023, Report, 2023](#).

³⁶ «Nel contesto della Quarta Rivoluzione industriale, tecnologie come l'Intelligenza Artificiale (IA) e la *DLT* stanno contribuendo non solo alle nostre discussioni sulle funzioni relative al denaro, ma anche al modo in cui interagiamo con esse». Chishti S. et al., *Il manuale della PayTech. Guida ai pagamenti digitali per imprenditori, manager e operatori della finanza*, Apogeo, 2021.

esempio le applicazioni mobili) o delle soluzioni front-end, senza modificare in modo sostanziale gli strumenti di pagamento utilizzati (carte, bonifici bancari, ecc.); recentemente, tuttavia, sono emerse alcune tendenze significative: l'atto del pagamento è diventato meno visibile e sempre più dematerializzato e disintermediato e le grandi imprese tecnologiche sono diventate attive nel settore dei pagamenti»³⁷.

Questa percezione risalta anche agli occhi di chi non è particolarmente avvezzo alle tendenze tecnologiche del momento. I mezzi di trasferimento del denaro e le transazioni stesse sono stati resi invisibili³⁸ in quanto gran parte delle nostre attività quotidiane (specie quelle che coinvolgono le spese o lo scambio di soldi) sono sottoposte ad un processo di “piattaformizzazione”³⁹, ossia vengono convogliate ed automatizzate in specifici *markeplace* o nelle cd. *Super-app*⁴⁰. In altri casi, si preferisce adottare approcci di pagamento comodi e veloci tramite lo sfruttamento di dispositivi mobili (*smartphones*), di opportune apparecchiature indossabili (*wearable devices*)⁴¹ e/o di determinate parti del corpo necessarie ad accedere all'*account*⁴² personale. In merito alla portata innovativa dei pagamenti, Fracassi e Ruggieri evidenziano come a livello globale, a seconda del contesto geografico che si vuole prendere ad esame, determinate tendenze prevalgano maggiormente rispetto ad altre. In

³⁷ [Camera dei Deputati, Pacchetto di finanza digitale, Ufficio Rapporti con l'Unione Europea, 2021.](#)

³⁸ Cfr. Chischti S. et al., *Il manuale della PayTech. Guida ai pagamenti digitali per imprenditori, manager e operatori della finanza*, Apogeo, 2021.

³⁹ Per uno spunto sul tema vds. Malaguti, M. C., *Fintech e piattaforme digitali nel settore finanziario tra concorrenza e regolazione*, in Salce V. e Finocchiaro G. (a cura di), *Fintech: diritti, concorrenza, regole*, 2019, pag. 55-82.

⁴⁰ È il caso di *AliPay* e *WeChat*, ma questa tendenza è già in atto per giganti tecnologici come *Meta*, *Google* o *Amazon* (riferendosi rispettivamente a *MetaPay*, *GooglePay* e *AmazonGo*), ma anche altri attori intendono ampliare la propria gamma di servizi come *Snapchat*, *Twitter* e *Revolut*. Per maggiori dettagli sul tema: Chischti S. et al., *Il manuale della PayTech. Guida ai pagamenti digitali per imprenditori, manager e operatori della finanza*, Apogeo, 2021; [Fracassi J. e Ruggieri M., Lo scenario internazionale del mondo dei pagamenti: evoluzioni e trend, Webinar promosso da Osservatori.net del Politecnico di Milano, 2023.](#)

⁴¹ Gli orologi (o *smartwatches*) costituiscono la versione più nota, insieme a cinture, anelli e occhiali. Anche, la diffusione della tecnologia delle *Application Programming Interfaces (API)* ha consentito lo sviluppo di applicazioni per accedere ai conti bancari e alle relative informazioni.

⁴² Sono all'ordine del giorno metodi di accesso basati su impronte digitali o su riconoscimento facciale. Tuttavia, nell'orizzonte della finanza digitale si ricorrerà a *chip* sottopelle o al trattamento dei dati biometrici. Un esempio calzante è riscontrabile nelle ambizioni del progetto *Worldcoin*, gestito da *OpenAI* (creatore della nota Intelligenza Artificiale *ChatGPT*). Come si vedrà più avanti nei temi relativi alla *privacy*, l'idea consiste nel legare la criptovaluta *WLD* «a un'identità digitale verificata attraverso acquisizione e trattamento di dati biometrici con l'intenzione, come dichiarato nel loro *whitepaper*, di distinguere gli esseri umani dalle intelligenze artificiali. Ciò rappresenta solo la punta dell'iceberg: l'ambizione è infatti di favorire processi democratici globali e fornire una potenziale strada verso un *Universal Basic Income (UBI)* finanziato dall'*IA*». Per ulteriori chiarimenti si rimanda alla seguente lettura: [Niola F., Worldcoin: le sfide normative su identità biometriche e criptovalute, Agenda Digitale, 2023.](#)

ambito europeo si registra una maggiore inclinazione verso i seguenti fenomeni: *open banking*⁴³, *buy now pay later (BNPL)* e *digital identity*⁴⁴.

Relativamente ai mediatori, infine, il discorso si fa più articolato. Il cambiamento apportato dai registri distribuiti ha decisamente impattato sull'operatività degli intermediari finanziari, e più in generale nella dialettica tra finanza tradizionale e decentralizzata, originando alcuni effetti⁴⁵:

1. **riduzione della necessità di intermediazione.** Gli utenti finali possono accedere ad una vasta gamma di servizi e gestirli in maniera autonoma e diretta;
2. **riduzione dei costi.** Le transazioni realizzate nei circuiti bancari comportano spese significative come commissioni, oneri di servizio e costi di gestione. Transitando nella sfera decentralizzata, si eliminano (o quantomeno riducono) drasticamente queste spese, rendendole convenienti nonché preferibili per gli utilizzatori;
3. **aumento della trasparenza.** Le transazioni basate sulla tecnologia *blockchain* sono per natura trasparenti ed immutabili. Questo fornisce una maggiore chiarezza e non fa che accrescere la fiducia dei consumatori nel sistema;
4. **accessibilità semplificata e maggiore inclusione finanziaria.** Si registrano innovazioni che stanno aprendo le porte del sistema finanziario a persone *cd. unbanked* che per molteplici ragioni sono state relegate ai margini della società e di

⁴³ Va ammesso come su questo fronte il motivo dei progressi sinora compiuti (almeno in ambito europeo) va ricercato nell'impulso dato dalla *Payment Services Directive (PSD2)*, snodo normativo rilevante che ha promosso il concetto di *open banking* sin dal 2016 nonché l'abbassamento delle barriere per l'ingresso al mercato da parte di nuovi operatori. Dopo gli effetti positivi generati dalla *PSD2*, le istituzioni europee hanno recentemente salutato con favore l'avvio dell'iter legislativo della Direttiva *PSD3*, con l'intento di mettere ordine nell'intero ecosistema *FinTech*, affollato in questi anni da numerose novità. Correttivi saranno introdotti il settore «adeguatamente attrezzato per la continua trasformazione digitale». [Garavaglia R., PSD3 e Fida, ecco il nuovo corso europeo su pagamenti e finanza digitali, Agenda Digitale, 2023.](#)

⁴⁴ Cfr. [Fracassi J. e Ruggieri M., Lo scenario internazionale del mondo dei pagamenti: evoluzioni e trend, Webinar promosso da Osservatori.net del Politecnico di Milano, 2023.](#) Di estremo interesse da quanto traspare dallo stesso studio la tendenza nel continente nordamericano verso i *cd. smart object payment* in cui è possibile abilitare in una *smart car* una serie di servizi aggiuntivi (tra cui quelli afferenti alla sfera dei pagamenti) resa possibile dalla interconnessione con l'ambiente circostante e dallo scambio di dati con esso.

⁴⁵ Come riassume incisivamente Minenna, «i vantaggi offerti dalla DeFi sono notevoli: assenza o riduzione delle barriere all'ingresso, anonimato, maggiore rapidità di esecuzione dei contratti, riduzione dei costi di transazione, estrema varietà delle applicazioni disponibili». Vds. [Minenna M., DeFi: come funziona la finanza prêt-à-porter basata sulla blockchain, Il Sole 24 Ore, 2022.](#)

conseguenza escluse dall'accesso a prestiti (es. *credit score* bassi⁴⁶ o un buono *status* socioeconomico non consentono l'apertura di un conto corrente o l'attivazione di un mutuo). Il *kit* necessario per diventare invece parte di questo sistema consiste in poche cose: il possesso di un dispositivo tecnologico (*PC, smartphone, tablet*), una connessione *internet* e perlomeno una minima disponibilità economica per partecipare ad attività finanziarie;

5. **nuove opportunità di business:** molti attori tradizionali stanno esplorando il potenziale espresso dalla *DeFi*, con l'intento di integrarvisi. Alcune banche hanno iniziato a fornire servizi supportati da *blockchain* ed hanno adottato nuove architetture aziendali che ne incorporano alcuni elementi.

Nonostante le origini disintermedie e decentralizzate, all'interno di questa nicchia crittografica sono fioriti anche giovani operatori riconducibili alla finanza cd. centralizzata che, adottando nuovi modelli di *business*, processi o prodotti (o riadattando quelli già conosciuti in chiave digitale)⁴⁷, hanno saputo intercettare, recepire e quindi soddisfare esigenze specifiche espresse da investitori interessati al cripto-mondo. L'apprezzamento di questo *trend* è comprovato dai volumi di mercato rilevanti e consistenti, aggirandosi a svariati miliardi di dollari, non definibili con precisione a causa delle continue oscillazioni di valore⁴⁸. Nel volgere lo sguardo verso l'altra faccia della medaglia, una criticità evidente di questa trasformazione viene segnalata dalla Banca d'Italia, spiegando che la diffusione della *Distributed Ledger Technology (DLT)* «abilita modelli “diffusi” e “disintermediati” che i paradigmi tradizionali di regolamentazione e controllo, basati su attività e soggetti tipizzati non sono più da soli sufficienti a comprendere e governare. Negli scenari di finanza decentralizzata, ad esempio, le regole e la governance delle piattaforme sono affidate a

⁴⁶ Tedeschi E., *Credit scoring: la valutazione del merito creditizio nell'era dell'IA, degli Alternative Data e dei Digital Footprints*, Vol. 256455, La via europea per l'Intelligenza artificiale. Atti Convegno del progetto Dottorale di Alta Formazione in Scienze Giuridiche – Venezia, 25-26 novembre 2021, 2022.

⁴⁷ [AA. VV., Financial Data Aggregation e Account Information Services. Questioni regolamentari e profili di business, Quaderni FinTech Consob, 2019.](#)

⁴⁸ L'impetuosa crescita di volumi delle cripto-attività ha interessato anche il fenomeno *DeFi* come certificato dal boom del *Total Value Locked (TVL)*, ossia il totale ammontare del valore depositato nei protocolli della *DeFi* che nel quadriennio 2017-2021 ha raggiunto la cifra di \$260 miliardi. Cfr. [Fondazione Finanza etica, Criptovalute e tecnologia blockchain. Capire la finanza, n.26, 2022.](#) Inoltre, [Minenna M., DeFi: come funziona la finanza prêt-à-porter basata sulla blockchain, Il Sole 24 Ore, 2022](#) pone in evidenza l'altrettanto straordinaria crescita nel numero di utenti della *DeFi* che nel 2022 ha raggiunto 4,5 milioni di utenti giornalieri.

espressioni algoritmiche, i cd. “smart contract”, elaborate da “sviluppatori” che si collocano oltre il perimetro tradizionale di osservazione e intervento delle autorità pubbliche; in questi moderni ecosistemi digitali, è la piattaforma tecnologica che connette una pluralità di soggetti a prescindere dai loro vincoli contrattuali che, invece, nel mondo analogico tracciavano il confine delle relazioni ammesse e regolate»⁴⁹. Queste osservazioni anticipano tematiche che verranno affrontate nel terzo paragrafo, la cui lettura richiede preliminarmente la comprensione dell’*habitat* in cui operano i fornitori di cripto-attività.

2. DeFi, CeFi e CeDeFi: una rapida perlustrazione del perimetro crittografico e disamina delle relative terminologie

La pervasività dei programmi informatici e automatizzati ha permeato la struttura finanziaria *standard*, plasmando elementi quali fiducia, pagamenti e intermediari.

TradFi vs CeFi vs DeFi			
	TRADFI	CEFI	DEFI
Infrastructure	Centralized	Centralized	Decentralized
Accessibility	Low to Moderate (often requires bank accounts or credit checks)	Moderate (need to comply with platform requirements)	High (anyone with internet and a crypto wallet can access)
Regulation	Highly regulated	Partially regulated (varies by country)	Unregulated
Risks	Low risk, often FDIC insured	Centralized risks	Smart contract risks
Transaction Speed	Slow	Moderate to fast	Fast
KYC	Yes	Mostly yes	No

tastycrypto.

Figura 1 – Fonte: [Antonovici A., TradFi vs CeFi vs DeFi: Here's how they differ, TastyCrypto, 2023.](#)

⁴⁹ [Pascale R., Finanza digitale: prospettive e opportunità per le imprese, Presentazione Banca d'Italia – Servizio Strumenti e Servizi di pagamento al dettaglio, 2023.](#)

Nell'addentrarci nei meandri del “*crypto financial system*”, è opportuno specificare che tale ecosistema può teoricamente suddividersi in due sottoinsiemi denominati *Decentralized Finance (DeFi)* e *Centralized Finance (CeFi)* che, al pari di quanto sopra rilevato in rapporto alla *TradFi*, meritano di essere rispettivamente analizzati in modo da fotografare l'intero assetto crittografico⁵⁰ nonché avere una panoramica completa dei rapporti e delle differenze concettuali che intercorrono tra questi paradigmi, come mostrato nella Figura 1.

Prendendo abbrivio dalla *Decentralized Finance*, essa può definirsi come un «*ecosistema finanziario competitivo, contendibile, componibile e non custodiale costruito su una tecnologia che non richiede un'organizzazione centrale per operare e che non ha una rete di sicurezza. Consiste in protocolli finanziari - implementati come "contratti intelligenti" - in esecuzione su una rete di computer per gestire automaticamente le transazioni finanziarie. Implementato sulla base della DLT, non richiede banche o altri intermediari centralizzati tradizionali. L'ecosistema sottostante è competitivo, in quanto i nuovi intermediari - minatori o validatori - competono per elaborare e regolare le transazioni. Gli utenti possono scegliere tra diversi protocolli finanziari; questi sono contendibili, in quanto chiunque può diventare un intermediario o implementare un protocollo o persino avviare un nuovo libro mastro; componibili, in quanto servizi complessi possono essere assemblati da protocolli di base; e non custodiali, in quanto gli utenti possono mantenere la custodia diretta dei loro beni quando accedono ai servizi finanziari. La DeFi non è dotata di alcuna rete di sicurezza, in quanto non è protetta da comportamenti criminali o frodi da parte degli investitori e le transazioni errate non possono essere annullate*»⁵¹.

Questa immagine ampia e densa di dettagli pone in luce il ruolo sostanziale ricoperto dalle *Decentralized Autonomous Organization (DAO)*⁵² e dalle applicazioni decentralizzate,

⁵⁰ [Antonovici A., TradFi vs CeFi vs DeFi: Here's how they differ, TastyCrypto, 2023.](#)

⁵¹ [Auer R. et al., The Technology of Decentralized Finance \(DeFi\), BIS Working Papers No 1066, 2023.](#)

⁵² [Gorman B., What Is a Decentralized Autonomous Organization \(DAO\)?, Avast, 2023](#) spiega che DAO significa letteralmente “organizzazione autonoma decentralizzata”, la cui peculiarità consiste nel decentralizzare «i processi di gestione utilizzando smart contract e dando a ogni membro di un'organizzazione un voto su come viene gestita. Tutti i voti sono registrati sulla blockchain, garantendo la trasparenza. Le DAO sono spesso menzionate nel contesto delle criptovalute, ma in futuro molti tipi diversi di organizzazioni potrebbero operare come DAO. Un altro nome per una DAO è DAC (decentralized autonomous corporations). Entrambi questi tipi di organizzazione sono diversi dalle organizzazioni autonome distribuite, nonostante le somiglianze nel nome».

dette *DApp*⁵³ o protocolli, che creano una rete finanziaria *peer-to-peer* sulla *blockchain* per effettuare molteplici attività (pagamenti, prestiti, scambi, depositi, *staking*⁵⁴, investimenti, *yield farming*⁵⁵, ecc.) in modo diretto tramite *smart contract*, ovvero *software* auto-esecutivi costruiti *ad hoc* in base al programma che gli sviluppatori desiderano o devono implementare. Attualmente, riportando la catalogazione prodotta da Boiardi⁵⁶, possono annoverarsi determinate tipologie di piattaforme decentralizzate nei seguenti ambiti:

- 1) ***Lending e Borrowing***. In questo ambito vi è una distinzione interna tra piattaforme “di prestito” che possono emettere *stablecoin* attraverso collaterale⁵⁷ e altre⁵⁸ che svolgono le medesime attività sfruttando *crypto-asset* emessi da terzi;
- 2) ***Decentralized Exchange (DEX)***⁵⁹. Si tratta di piattaforme decentrate che facilitano lo scambio o la conversione programmatica di *crypto-asset*;

Per ulteriori approfondimenti, [Colosimo B. e Corbò A., DAO: Decentralized Autonomous Organization: cos'è, finalità e prospettive giuridiche, Agenda Digitale, 2022.](#)

⁵³ Le *DApp* (acronimo di “*Decentralized Applications*”), o applicazioni decentralizzate, sono un tipo di applicazione il cui funzionamento si basa su una rete decentralizzata di nodi che interagiscono tra loro.

⁵⁴ È un meccanismo in base al quale è possibile ottenere delle ricompense sotto forma di criptovalute.

⁵⁵ Come spiegato su *CoinMarketCap*, si tratta di un'operazione molto popolare nel settore *DeFi* tanto da contribuire all'incremento della sua capitalizzazione di mercato da \$500 milioni a \$10 miliardi nel 2020. In sintesi, «*lo yield farming è la pratica di staking o prestito di criptovalute al fine di generare rendimenti elevati o ricompense sotto forma di criptovaluta aggiuntiva. (...) In breve, i protocolli di yield farming incentivano i fornitori di liquidità (Liquidity Providers) a vincolare i propri asset crittografici in un pool di liquidità basato su contratti intelligenti. Questi incentivi possono essere una percentuale delle commissioni di transazione, interessi da parte dei finanziatori o un token di governance. Questi rendimenti sono espressi come rendimento percentuale annuo.*» [Vermaak W., What is Yeld Farming, CoinMarketCap, 2022.](#)

⁵⁶ [Boiardi L., DeFi: tutto sulla finanza decentralizzata, The Crypto Gateway, 2023.](#)

⁵⁷ È il caso di *MakerDAO*, un protocollo che consente agli utenti di ottenere prestiti, utilizzando *Ethereum*⁵⁷ come “valuta” collaterale. Il protocollo funziona attraverso uno *smart contract* ed utilizza un sistema di governance decentralizzato per prendere decisioni riguardo alle modifiche del sistema.

⁵⁸ È il caso delle piattaforme *AAVE* o *Compund*.

⁵⁹ Come precisa [Auer R. et al., The Technology of Decentralized Finance \(DeFi\), BIS Working Papers No 1066, 2023](#) «*la loro progettazione può seguire due modelli principali: le order book DEX come 0x ed EtherDelta, che sfruttano lo stesso modello implementato nelle piattaforme di trading centralizzate, e AMM-based DEX (o Automated Market Maker-based DEX) (...) diversamente dagli scambi tradizionali (e decentralizzati) basati su “order book”, in cui la scoperta dei prezzi dipende dal meccanismo di abbinamento degli ordini di acquisto e vendita piazzati dai trader, i DEX basati su AMM sfruttano un peer-to -pool mechanism: per ciascuna coppia di trading supportata, uno smart contract specifico per protocollo raggruppa le riserve di cryptoasset fornite da molti singoli fornitori di liquidità, agendo di fatto come un Automated Market Maker (AMM), e le operazioni in entrata vengono eseguite contro questi pool.*» Esempi di *AMM-based DEX* sono *PancakeSwap* e *Uniswap*. Quest'ultimo consente agli utenti di scambiare criptovalute direttamente tra loro attraverso uno *smart contract*, eliminando la necessità di veicolare le transazioni per mezzo di un *exchange* tradizionale. Gli utenti possono fornire liquidità al protocollo e ricevere in cambio una quota delle commissioni di transazione generate dagli scambi effettuati sulla piattaforma. Questo modello decentralizzato ha reso *Uniswap* uno dei protocolli *DeFi*

- 3) **Combo Farming**⁶⁰. In pratica, aggregatori di piattaforme che permettono di aumentare il rendimento degli *asset*;
- 4) **Derivates**⁶¹. *DApp* che emettono e facilitano la negoziazione dei contratti/prodotti derivati (copie) di altri *asset* come azioni, materie prime, immobili o altre *crypto*;
- 5) **Assicurazioni**. Piattaforme che permettono di assicurare i fondi depositati siano esse all'interno di *smart contract*, di altre piattaforme o altro.

Per converso, anche se la decentralizzazione offre maggiore trasparenza, possibilità di controllo agli utenti e rendimenti alti, persistono ancora potenziali rischi⁶² dettati dall'incertezza di recuperare fondi persi a seguito di errori o frodi (e dalla difficoltà di individuare il soggetto cui imputare l'eventuale responsabilità) nonché la possibilità di dipendere da *smart contract* difettosi o vulnerabili⁶³.

Andando oltre le criticità, tra le prospettive segnalate da esperti del settore vi è l'integrazione della *DeFi* nelle attività già esistenti. Molti intermediari – anche classici – hanno già iniziato ad esplorare questa possibilità, creando *partnership* e collaborazioni con progetti

più apprezzati ed ha contribuito a una sua maggiore adozione. Per ulteriori approfondimenti, vds. [Sasi-Brodesky A. e Nassr I. K., DeFi liquidations: volatility and liquidity – OECD Working Papers on Finance, Insurance and Private Pensions No. 48, 2023.](#)

⁶⁰ Si citano, a titolo d'esempio, *Beefy Finance* e *Yearn Finance*. Si tratta di *yeld farm* (o aggregatori) che «monitorano rendimenti e interessi delle piattaforme e, combinandoli fra loro, trovano le migliori condizioni sul mercato». [Boiardi L., DeFi: tutto sulla finanza decentralizzata, The Crypto Gateway, 2023.](#)

⁶¹ [Auer R. et al., The Technology of Decentralized Finance \(DeFi\), BIS Working Papers No 1066, 2023:](#) «per tracciare il prezzo degli *asset* sottostanti, questi protocolli *DeFi* sfruttano gli Oracoli, ovvero *smart contract* che fungono da servizio ponte tra una *DLT* e il mondo esterno, consentendo di recuperare dati del mondo reale, off-chain. Mentre gli investitori finanziari centralizzati si affidano a intermediari che accettano e regolano gli ordini, i protocolli derivati *DeFi* li sostituiscono con *smart contract* che emettono strumenti finanziari a determinate condizioni automatizzate, previa fornitura di garanzie collaterali come protezione contro i rischi».

⁶² Il tema della *Decentralized Finance* meriterebbe di essere esplorato con dovizia di sfumature e in spazi appositamente dedicati, specie in relazione ai rischi che essa genera. Stando alla revisione della letteratura scientifica in questo ambito, Peterson nota che «attualmente, nella letteratura sulla finanza decentralizzata mancano studi critici. Gran parte degli studi esistenti sulla *DeFi* hanno una visione positiva della *DeFi* e concludono che la *DeFi* trasformerà la finanza tradizionale in modo eccezionale. Tenendo presente che le innovazioni tecnologiche portano con sé problemi alla società, è importante alterare l'ottimismo della *DeFi* con un po' di pessimismo, per trovare una soluzione che funzioni al meglio per la società. Sono necessari studi di ricerca critici che identifichino i nuovi rischi e problemi della *DeFi* che sono dannosi per il benessere delle persone nella società, in modo da poterli affrontare». [Peterson K. O., Decentralized finance research and developments around the world, J Bank Financ Technol. 2022.](#)

⁶³ Tra i più noti vi sono il *rug Pull*; *bug* di *smart contract*; *flash loan attack*; *impermanent loss*; truffe di vario genere (*scam*). [Boiardi L., DeFi: tutto sulla finanza decentralizzata, The Crypto Gateway, 2023.](#)

decentralizzati già avviati⁶⁴. Ad esempio, alcune istituzioni finanziarie hanno iniziato ad offrire servizi di prestito secondo logiche decentrate ai propri clienti, permettendo loro di guadagnare interessi sui depositi in *crypto-asset*. Tuttavia, l'integrazione della *DeFi* presenta anche alcune sfide. Una delle principali, se non la più importante, è la regolamentazione del settore. Attualmente, la *DeFi* è una zona grigia dal punto di vista normativo, poiché non è ancora stato definito come si debba affrontare questa novità⁶⁵ e gli intermediari tradizionali devono navigare tra regole e normative complesse per garantire che le transazioni sulla *DeFi* siano conformi alle leggi finanziarie esistenti⁶⁶. Perciò, l'approccio a questo settore per un intermediario tradizionale necessita di investimenti in soluzioni di sicurezza e misure per proteggere i propri clienti dai rischi associati alla stessa decentralizzazione⁶⁷.

Senza confondersi con la *TradFi*⁶⁸ – anche se apparentemente simile – trasferiamoci al concetto di *CeFi*, ossia un mercato creatosi autonomamente in risposta alla crescente domanda di interazione con le cripto-attività. Difatti, anche se il “*crypto financial system*” poggia su basi decentralizzate e disintermedie, la necessità di scambiare *digital asset* ha comportato lo spuntare di *centralized exchange (CEX)* che supportassero i clienti soprattutto nelle attività di *trading*. Come si vedrà in seguito, i soggetti appena citati sono noti per aver generato non pochi problemi sul piano della stabilità finanziaria in determinate giurisdizioni – specie nel contesto statunitense – a causa della loro mancata regolamentazione o complicazioni nel trattenere l'area di competenza in cui le Autorità di vigilanza potessero esercitare i propri poteri.

Malgrado ciò, le realtà esistenti in questo settore non si riducono unicamente nei *crypto*

⁶⁴ D'altro canto, vantaggi come la trasparenza, la velocità e l'accesso globale, sono tutti elementi in grado di aumentare il divario concorrenziale e competere direttamente con gli intermediari finanziari tradizionali. A tal riguardo, negli ultimi anni, con l'avvento della *DeFi* sono sorti numerosi intermediari che, sono in grado di offrire agli utenti molti servizi analoghi a quelli offerti da un operatore tradizionale, con tassi di interesse anche più competitivi.

⁶⁵ Com'è noto, il Regolamento *MiCA* rimane scoperto su questo ambito.

⁶⁶ Intervento durante il Seminario inaugurale della Scuola estiva dell'Università di Cagliari di [Savona P., Rischi, regolamentazione e stabilità finanziaria: senza una modifica dell'architettura istituzionale continueremo a inseguire l'obiettivo senza evitare che le crisi di singoli operatori si tramutino in rischi sistemici, 2023.](#)

⁶⁷ [Savona P., Alcune riflessioni sul progresso scientifico e tecnologico al servizio della finanza, Lectio alla Banca di Piacenza, 2022.](#)

⁶⁸ «La *CeFi* presenta analogie con la *TradFi* in termini di approccio, poiché anch'esso si basa su intermediari centralizzati. Tuttavia, questo ecosistema opera con criptovalute basate sulla blockchain, che i governi non emettono. *CeFi* è considerata *off-chain*». Cfr. [Antonovici A., TradFi vs CeFi vs DeFi: Here's how they differ, 2023.](#)

exchange platform, punta dell'*iceberg* di una categoria ben più ampia⁶⁹. Difatti, per poter accedere all'ecosistema crittografico è d'obbligo possedere un *digital wallet* in cui depositare specifici *crypto-asset*⁷⁰. Per coloro che sul piano informatico non sono sufficientemente abili nel gestire in maniera autonoma le proprie ricchezze dematerializzate, il rischio di essere derubati tramite *hacking* o di smarrire accidentalmente la "*seed phrase*" (una frase di recupero) è decisamente alto. Su questo versante, mentre alcuni *service provider* hanno maturato nel proprio arsenale procedure atte contestualmente a possedere e controllare le cripto-attività degli utenti (*custodial services*), altre figure si sono invece specializzate nella detenzione delle chiavi crittografiche private degli utenti fondamentali per accedere al relativo portafoglio (*non-custodial services*)⁷¹. Nell'uno o nell'altro caso si sta discorrendo comunque di *digital wallet custodian*, soggetti di pari notorietà rispetto ai suddetti *CEX*. Il ventaglio di attori *CeFi* si potrebbe in via teorica estendere ulteriormente ricomprendendo in questo gruppo anche *crypto ATM*⁷², *crypto hedge fund*, *miner/validator*⁷³ ed anche sviluppatori di applicazioni decentralizzate. Il minimo comune denominatore che lega tutti questi soggetti sembra individuarsi in una più evidente gestione umana che non demanda precipuamente il controllo e l'esecuzione di determinati servizi ad un *software*⁷⁴. Va però detto che in merito a quest'ultimo punto il terreno comincia a farsi scivoloso dato che il

⁶⁹ A tal proposito, nella ricerca di [Strategy&, European Crypto Survey, 2022](#) si afferma che «*nel complesso, il panorama dei fornitori è piuttosto frammentato – i crypto exchange internazionali di criptovalute sono in testa: Coinbase, Binance e Crypto.com particolarmente noti e con un elevato tasso di utilizzo. I Neo-brokers sono al secondo posto: Oltre ai crypto exchange di criptovalute, TradeRepublic, eToro e Bitpanda detengono una quota di mercato rilevante - le banche non svolgono quasi alcun ruolo, ad eccezione di Revolut*».

⁷⁰ La gestione del portafoglio digitale non è idealmente dissimile da quella di un comune portafoglio fisico in cui inseriamo/conserviamo il nostro denaro contante, sebbene l'*habitat* digitale comporti l'adozione di alcune accortezze che la dimensione fisica invece non contempla.

⁷¹ [Di Noia C., The new frontiers of digital finance – Decentralised Finance \(DeFi\), Conferenza Consob, 2023.](#)

⁷² [Frankenfield J., Bitcoin ATM: definition, fees, and locations, Investopedia, 2021.](#) «Un Bitcoin ATM è un chiosco collegato a Internet che consente ai clienti di acquistare bitcoin e/o altre criptovalute con denaro contante depositato. Un bancomat bitcoin non è la stessa cosa di uno sportello automatico (ATM) che consente ai clienti delle banche di prelevare, depositare o trasferire fisicamente i fondi sul proprio conto corrente. I bancomat bitcoin producono piuttosto transazioni basate sulla blockchain che inviano le criptovalute al portafoglio digitale dell'utente, spesso tramite l'uso di un codice QR».

⁷³ La differenza sta nel tipo di meccanismo di validazione di transazioni utilizzato: mentre i *miner* operano nell'ambito della *Proof-of-Work*; invece, i *validator* (detti anche *minter* o *forger*) sono coloro che trattano la *Proof-of-Stake*.

⁷⁴ Volendo osservare il fenomeno da una prospettiva inversa, i regimi *CeFi* e *DeFi* si affidano all'operatività dei protocolli e degli *smart contract*; tuttavia, la loro differenza si sostanzia nell'uso che ne fanno. Mentre in ambito *CeFi* si è soliti «*utilizzare i contratti intelligenti in misura limitata in alcune aree*», invece in ambito *DeFi* viene fatto «*ampio uso di contratti intelligenti, la cui codifica controlla il funzionamento dell'applicazione DeFi*». [Deloitte, DeFi deciphered: Navigating disruption within financial services, 2023.](#)

fattore umano appare necessariamente presente anche in contesti *DeFi*, seppure in misura marginale.

Giunti a questo punto, va fatta una doverosa precisazione. Nella presente trattazione si è inteso discorrere (e si discorrerà) distintamente di *Decentralized Finance (DeFi)* e *Centralized Finance (CeFi)* per fornire una migliore rappresentazione teorica e concettuale delle singole categorie che ruotano attorno e dentro l'ecosistema *crypto*. In aggiunta a ciò, buona parte di scritti accademici e *dossier* prodotti da autorevoli istituzioni nazionali, sovranazionali ed internazionali è ricorsa a questa distinzione⁷⁵. Tuttavia, vi è una problematica di fondo. Oltre all'insita difficoltà di ricostruire la tassonomia dei prodotti *crypto* in un contesto saturo di acronimi e inglesismi vari talvolta usati come sinonimi, chi desidera approfondire queste tematiche afferenti alla finanza digitale tra le altre cose rischia di incorrere nell'equivoco che esista un paradigma completamente decentralizzato (nel gergo tecnico si usa l'espressione "*Full-DeFi*"). Invero, una visione fondata su servizi finanziari interamente automatizzati e autogestiti non sembra avere reale fondamento – non per ora almeno – se non in un mondo ideale. Le ragioni sono riconducibili sia a pragmatiche logiche di mercato sia per concrete questioni di carattere tecnico-gestionale. A tal proposito, incisivo e chiarificatore appare quanto condiviso da Anker-Sørensen e Zetzsche, secondo i quali più che di *DeFi* sarebbe invece appropriato parlare di "*Fake-DeFi*", cioè «un'applicazione decentralizzata nella quale gli innovatori o i fornitori di servizi detengono diritti di governance, o l'equivalente tecnico dei diritti di governance, con cui possono modificare i fondamenti della rete decentralizzata. Le ragioni della Fake-DeFi sono in parte legali e normative, ma in gran parte la Fake-DeFi è insita nella logica di mercato: gli innovatori vogliono capitalizzare le loro invenzioni. Realizzare profitti in una rete completamente decentralizzata è incredibilmente difficile. Di conseguenza, gli innovatori si rivolgono all'alternativa meno difficile di creare reti e servizi solo reti e servizi parzialmente centralizzati sui quali detengono vari gradi di controllo. Il Fake-DeFi rimarrà il modello di business più diffuso anche se la legge e la regolamentazione fornissero certezza giuridica e

⁷⁵ Ad esempio, sul rapporto *CeFi/DeFi* si leggano le seguenti pubblicazioni: [OCSE, Institutionalisation of crypto-assets and Defi-TradFi interconnectedness, OECD Publishing, 2022](#); [OCSE, Lessons from the Crypto Winter. DeFi versus CeFi, OECD Business and Finance Policy Papers, 2023](#); [Fondo Monetario Internazionale, The money Revolution. Crypto, CBDCs and the future of finance, IMF Magazine, 2022](#).

normativa e una supervisione agevole di una rete transfrontaliera e completamente decentralizzata. La Fake-DeFi richiede una risposta normativa. Le autorità di regolamentazione incaricate di affrontare la Fake-DeFi come fenomeno diffuso sono incoraggiate a rivedere le leggi e i regolamenti relativi ai diritti di governance e alle modalità di controllo. Le regole sulla solidità dei principali azionisti e dei titolari effettivi, sull'idoneità e sulla correttezza delle persone-chiave, sull'organizzazione e sulle modalità di controllo, sui requisiti personali, organizzativi e prudenziali degli azionisti dominanti, così come le definizioni di gruppi di servizi finanziari devono essere riconsiderate per rispecchiare i diritti di governance come modalità di controllo tecnico, piuttosto che giuridico»⁷⁶. Il commento appena condiviso porta a sviluppare determinate riflessioni. In primis, la «piena decentralizzazione è un mito»⁷⁷ (o «un'illusione»⁷⁸ per dirla con le parole di Aramonte). Si potrebbe perciò avanzare la ragionevole ipotesi secondo cui, oltre a rappresentare teoricamente una dimensione a sé, la DeFi vada attualmente intesa come un pezzo inscindibile del “*crypto financial system*”. E i *player* (emergenti e non) che vi abitano ne sono un riflesso: incorporando e/o avvalendosi di soluzioni decentralizzate per aumentare la propria appetibilità sul mercato e rivolgersi a un maggiore bacino di utenti, tali *provider* possono strutturalmente definirsi soggetti centralizzati-decentralizzati. Vista in quest'ottica, ecco che l'espressione *CeDeFi*⁷⁹ (*Centralized-Decentralized Finance*) sembra meglio descrivere il paradigma del “*crypto financial system*”, in cui gli approcci e le peculiarità di *CeFi* e *DeFi* si mescolano, sintetizzando le migliori funzionalità di entrambe. Comunque, al di là di ogni supposizione, quanto sinora riportato ha consentito di attraversare tutti gli *step* necessari per delimitare paradigmi così estesi quali il sistema finanziario tradizionale e il “*crypto financial system*”. Nel prossimo paragrafo si ripercorreranno i fallimenti più dibattuti in tema di *Crypto-Asset Service Provider (CASP)*, cercando di capire se – ed eventualmente in che misura – i due succitati mondi sono interconnessi.

⁷⁶ [Anker-Sørensen L. e Zetsche D.A., *From Centralized Finance to Decentralized Finance. The issue of “Fake-DeFi”*, SSRN, 2021.](#)

⁷⁷ [Zetsche D.A., *Keynote Speech, Presentazione Conferenza “The regulation on Markets in Crypto-Assets \(MiCA\). The future of Blockchain Technology in Europe”*, Bocconi, 2023.](#)

⁷⁸ [Aramonte et al., *DeFi risks and decentralisation illusion*, BIS Quarterly Review, 2021.](#)

⁷⁹ Il termine è di recente coniazione e diffuso nei contesti specializzati, ma potrebbe presto prendere piede nei documenti istituzionali. Ne è un esempio la Banca di Francia. Vds. [Banca di Francia, “Decentralised” or “disintermediated” finance: what regulatory response?](#), Discussion Paper, 2023.

3. Interconnessione tra sistema finanziario e crypto-mondo: criticità connesse a uno sviluppo deregolamentato del mercato

Il vorticoso e inarrestabile progresso tecnologico ha avuto un impatto rivoluzionario sull'economia mondiale, dando vita a quella che viene comunemente indicata come "economia digitale", ossia «un'economia basata sulle tecnologie digitali (a volte chiamata economia di Internet) (...) sempre più intrecciata con l'economia tradizionale rendendo meno chiare le differenze tra loro»⁸⁰.

Come è stato accennato in precedenza, la DeFi ricomprende una vasta ed eterogenea serie di servizi finanziari *peer-to-peer* eseguiti da entità prive di vertici e/o organizzazioni gerarchiche in stile piramidale⁸¹. Valorizzando quest'ultimo profilo, non sfugge come il sistema finanziario tradizionale e la finanza decentralizzata siano formalmente in aperto contrasto. Se il primo è soggetto alla regolamentazione statale e amministrativa e presidiato da Autorità spesso indipendenti, il cui funzionamento richiede l'intervento necessario di terze figure professionali, il secondo invece esautora gli intermediari e i "guardiani", concedendo "potere" agli utenti che, in piena autonomia, possono "partecipare"⁸² e in alcuni casi "gestire" le attività che avvengono al suo interno⁸³. Inoltre, il fenomeno criptovalutario ha oramai una valenza economico-patrimoniale che consente di identificare diverse fattispecie rispetto alle quali il diritto in generale non può assolutamente rimanere estraneo.

Muovendo da questi presupposti che non sono di certo passati inosservati, ragionevoli preoccupazioni sono seguite sia in merito ai prodotti che ai soggetti *crypto*. Ad esempio, un primo campanello d'allarme è rinvenibile negli avvertimenti diffusi dalle autorità europee che hanno segnalato i rischi derivanti dagli investimenti in *crypto-asset*, come nel caso della *European Supervisory Authority System (EBA, ESMA⁸⁴, EIOPA)*, che ha più

⁸⁰ [Commissione Europea, Commission Expert Group on taxation of the Digital Economy - general issues – working paper, Bruxelles, 2013.](#)

⁸¹ [Morini G., Criptoaluta: digitalizzazione di valore e finanza decentralizzata. Tra regolamentazione ed elusione, Il caso.it, 2023, p. 12.](#)

⁸² La decentralizzazione permette un più diretto coinvolgimento degli utenti, attraverso la costituzione di comunità diffuse ed interconnesse mediante tecnologie DLT.

⁸³ I protocolli di finanza decentralizzata consentono la disintermediazione dei pagamenti e degli investimenti.

⁸⁴ [Securities and Markets Stakeholder Group \(MSG\), Advice to ESMA – Own Initiative Report on Initial Coin Offerings and Crypto-Assets, 2018, p. 7.](#) Ad esempio nel 2018, in uno specifico rapporto l'ESMA ha evidenziato

volte ribadito le problematiche scaturite dai *crypto-asset* e dai relativi operatori di mercato⁸⁵. Più di recente, il Comitato europeo per il rischio sistemico (*European Systemic Risk Board, ESRB*) ha redatto un *report* in cui vengono condivise le implicazioni del *crypto market* sull'infrastruttura finanziaria, suggerendo alcuni spunti volti a rafforzare la regolamentazione sull'argomento così da affrontare i rischi derivanti dai *crypto-asset* e dalla *DeFi*⁸⁶. I fenomeni in questione, infatti, pur portando con sé rilevanti opportunità, si rivelano una minaccia per la tutela degli investitori⁸⁷, l'integrità del mercato e la stabilità finanziaria⁸⁸. A complicare ulteriormente il quadro vi è la difficoltà di regolamentare fenomeni contraddistinti da una rapidità di evoluzione mai vista, in grado di rendere superate anche le più recenti regolamentazioni⁸⁹. In via analoga, la Banca d'Italia ha da tempo denunciato i rischi di una diffusione incontrollata e deregolamentata del fenomeno *crypto*⁹⁰, anche in ragione di elementi come «*l'elevata crescita del numero e del valore delle cripto-attività; l'estrema volatilità delle quotazioni; i ricorrenti episodi di crisi di operatori e schemi della specie, dovuti a truffe, a incidenti informatici o a difetti di fondo, che hanno comportato anche di recente ingenti perdite per i soggetti coinvolti; la forte opacità degli scambi e degli assetti proprietari di gran parte di questi schemi; in molti casi, l'elevatissima volatilità del loro prezzo*»⁹¹. Se si volge lo sguardo a livello globale, dunque,

come in quel periodo numerose *ICOs* si sono rivelate una truffa, con evidenti ripercussioni negative per gli investitori.

⁸⁵ [EBA-ESMA-EIOPA, *Crypto-assets: ESAs remind consumer about risks*, 2021.](#)

⁸⁶ [ESRB, *Crypto-assets and decentralised finance*, 2023.](#)

⁸⁷ [Consob e Banca d'Italia, *Consob e Banca d'Italia mettono in guardia contro i rischi insiti nelle cripto-attività. Comunicazione pubblica*, 2021.](#) «In assenza di un quadro regolamentare di riferimento, infatti, l'operatività in cripto-attività può presentare rischi di diversa natura, tra cui: la scarsa disponibilità di informazioni in merito alle modalità di determinazione dei prezzi; la volatilità delle quotazioni; la complessità delle tecnologie sottostanti; l'assenza di tutele legali e contrattuali, di obblighi informativi da parte degli operatori e di specifiche forme di supervisione su tali operatori nonché di regole a salvaguardia delle somme impiegate. A ciò si aggiungono i rischi di perdite causate da malfunzionamenti, attacchi informatici o lo smarrimento delle credenziali di accesso ai portafogli elettronici».

⁸⁸ Oltre ai rischi connessi propriamente al mercato finanziario occorre ricordare a che i rischi collegati alla criminalità ed all'utilizzo delle cripto-attività nell'ambito delle attività di riciclaggio.

⁸⁹ La rapidità con le quali evolve l'attuale tecnologia pone interrogative anche di tecnica legislative favorendo tendenzialmente un approccio regolatorio possibilmente flessibile cosicché il Legislatore non sia costretto ogni volta a rincorrere le novità con notevoli ritardi, ma riesca invece a stare al passo con i tempi.

⁹⁰ Banca d'Italia e Consob hanno più volte informato gli investitori *retail* «sugli elevati rischi connessi con l'operatività in cripto-attività (*crypto-asset*) che possono comportare la perdita integrale delle somme di denaro utilizzate». [Consob e Banca d'Italia, *Consob e Banca d'Italia mettono in guardia contro i rischi insiti nelle cripto-attività. Comunicazione pubblica*, 2021.](#)

⁹¹ [Banca d'Italia, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività*, 2022.](#)

non si può non notare come l'insorgere delle problematiche sopra richiamate abbia scatenato reazioni differenti in ogni singola giurisdizione del mondo. Volendo ridurre la questione all'osso, ciascun Paese ha dovuto attuare una delle tre possibili linee d'azione per affrontare i rischi delle crypto-attività⁹²:

1. **Divieto.** Il divieto rappresenta certamente un metodo adatto a chi intende risolvere il problema alla radice, come è avvenuto in Cina ed in altri Paesi dove le attività *crypto* sono state bannate;
2. **Regolazione.** D'inverso, la regolamentazione appare essere la strada più intuitiva ma la più ardua in termini di attuazione. Si tratta di un processo che almeno nell'Unione Europea ha richiesto molto tempo. Si sta facendo chiaramente riferimento al *MiCA*, Regolamento di recente approvazione⁹³ volto a disciplinare il mercato finanziario delle crypto-attività a livello comunitario, con lo scopo principale di armonizzare il *framework* giuridico degli Stati membri. In particolare, il provvedimento intende introdurre sia regole comuni per l'emissione e l'offerta al pubblico di crypto-attività non riconducibili a strumenti finanziari (quali definiti nell'art. 4, paragrafo 1, punto 15, della Direttiva 2014/65/UE), sia norme per la prestazione di servizi ad esse collegati, come, ad esempio quello di *trading*⁹⁴. Rispetto al suo ambito applicativo vengono da più parti sollevati dubbi in ordine alla sua estensione ai servizi comunemente noti come finanza decentralizzata⁹⁵, tantoché pare poter ritenere che i servizi completamente decentralizzati forniti senza intermediari siano esclusi dal suo campo di applicazione;

⁹² [Aquilina M. et al., Addressing the risks in crypto: laying out the options, BIS Bulletin n. 66, 2023.](#)

⁹³ Il Regolamento 2023/1114/UE c.d. *MiCA* è stato approvato il 16 maggio scorso da parte dell'Ecofin e pubblicato nella Gazzetta ufficiale dell'Unione europea il 9 giugno 2023.

⁹⁴ In assenza di un quadro generale dell'Unione per i mercati delle crypto-attività, il *MiCA* ambisce ad offrire un quadro armonizzato e specificatamente dedicato ai mercati delle crypto-attività a livello unionale, sopperendo all'assenza di disciplina in tale ambito ed evitando al contempo il rischio di frammentazione del mercato unico.

⁹⁵ [Minenna M., DeFi: come funziona la finanza prêt-à-porter basata sulla blockchain, Il Sole 24 Ore, 2022.](#) il quale solleva dubbi sull'applicabilità delle norme sulla fornitura di servizi di scambio di *crypto-asset* completamente decentralizzati o sul funzionamento di piattaforme di *trading* per *crypto-asset* (gli *exchange* decentralizzati o *DEX*).

3. **Contenimento.** Si tratta di una vasta zona grigia di molteplici approcci più o meno protendenti verso una delle due estremità, spaziando dall'ignorare completamente il fenomeno criptovalutario, tollerarlo oppure ingabbiarlo in schemi normativi preesistenti. Gli Stati Uniti d'America hanno declinato questa terza via nella non-interferenza con l'innovazione tecnologica, reputando il proprio sistema normativo sufficientemente solido per gestire i prodotti crittografici e soprattutto i relativi intermediari⁹⁶.

Su quest'ultimo punto, i vari fallimenti e collassi finanziari avvenuti negli ultimi anni sembrano comunicare tutt'altro. Volendo fare una sintesi cronologica, meritano di essere annoverati i seguenti eventi di mercato⁹⁷ e/o operatori:

- 1) **Aprile/maggio 2014: Mt. GOX.** Nel quadriennio 2010-2014 *Mt. GOX* costituiva il più grande *exchange* di *bitcoin*, da cui passava il 70% delle transazioni di *bitcoin* nel mondo⁹⁸. Le ragioni che di fatto arrestarono l'ascesa di questo *CASP* possono essere identificate in un impressionante *hackeraggio* di 850.000 *bitcoin*, all'epoca con un controvalore di oltre \$400 milioni. Nonostante l'evento in questione abbia compiuto quasi dieci anni, si tratta di uno dei primi rilevanti scossoni avvenuti ai danni di un prestatore di servizi per le crypto-attività. Altra peculiarità che caratterizza questo *crypto service provider* è nel fatto di essere ricorso al “*Chapter 15*”, «norma cugina del più noto “*Chapter 11*”, per intendersi quello usato da *Enron* a *Worldcom*, introdotto per facilitare la gestione di un fallimento che ha avuto luogo fuori dagli Stati Uniti ma che coinvolge anche cittadini americani»⁹⁹. I fornitori *crypto* di seguito elencati hanno tutti invece invocato una procedura fallimentare “*Chapter 11*”, con la possibilità di

⁹⁶ «Non c'è motivo di trattare il mercato delle criptovalute in modo diverso dal resto dei mercati solo perché utilizza una tecnologia diversa. I recenti eventi dimostrano perché è fondamentale che le società di criptovalute rispettino le leggi sui titoli». Si tratta di una frase di Gary Gensler, presidente della SEC in cui riporta esaurientemente il suo pensiero in un articolo del [Gensler G., The SEC Treats Crypto Like the Rest of the Capital Markets, Wall Street Journal, 2022.](#)

⁹⁷ [Coinbase, 2023 Crypto Market Outlook, 2022.](#)

⁹⁸ Miccoli C., *Bitcoin e crypto-valute. La guida per tutti*, Vallardi, 2022.

⁹⁹ [Sideri M., Bitcoin, Mt. Gox chiede il “Chapter 15”, Corriere della Sera, 2014.](#)

riorganizzare e ristrutturare l'intero assetto aziendale senza chiudere del tutto i battenti¹⁰⁰.

2) Maggio 2022: collasso dell'ecosistema *crypto Terra (LUNA)* e *Terra USD (UST)*.

Sebbene non costituisca propriamente un *provider*, col senno di poi il collasso dell'ecosistema *Terra* ha giocato un ruolo fondamentale nella sequela di fallimenti avvenuti di lì a poco nell'ambito *CeFi*, rendendo il quadro causa-effetto dei vari crolli complessivamente più nitido. Per gli esperti del settore è stata la riprova di come le *stablecoin* non siano veramente così stabili come il loro nome professa. Prima del suo crollo, *Terra USD (UST)* era la quarta *stablecoin* più grande dietro *Tether (USDT)*, *USD Coin (USDC)* e *Binance USD (BUSD)*, con una capitalizzazione di mercato pari a \$18 miliardi. L'ecosistema *Terra* non era nient'altro che un protocollo che «*si basava su un sistema a due monete, che non era completamente sostenuto da garanzie tradizionali (ad esempio valuta fiat o oro)*»¹⁰¹: la *stablecoin* algoritmica *UST* e il *crypto-asset LUNA*. Il collasso sembrerebbe essere stato provocato da un'azione di *short selling* sul valore di quest'ultima. In altri termini, determinate persone hanno “scommesso” sul crollo del prezzo della *crypto LUNA*, dopo aver scovato una falla nel meccanismo di funzionamento della *stablecoin UST*¹⁰².

3) Giugno/luglio 2022: fallimenti di *Three Arrows Capital (o 3AC)*, *Celsius Network* e *Voyager Digital*.

Le parole di Forbes riassumono perfettamente questo periodo in cui «*il tracollo di Luna ha avuto un impatto sull'intero mercato delle criptovalute, che all'epoca era già altamente volatile e in difficoltà. Si stima che il crollo di LUNA abbia finito per far crollare il prezzo del bitcoin e causare una perdita stimata di 300 miliardi di dollari di valore in tutto lo spazio delle criptovalute. I leader delle criptovalute*

¹⁰⁰ L'avvio della procedura consente di poter nuovamente tornare ad operare sul mercato dopo aver soddisfatto tutti i criteri necessari dettati dal “Chapter 11”. Ne sono un esempio *American Airlines*, *General Motors*, *Hertz* o *Marvel*.

¹⁰¹ «Essendo più specifico, il protocollo *LUNA-UST* si basava su due concetti principali. In primo luogo, il protocollo ha stabilizzato i prezzi *UST* assicurando che la sua offerta e la sua domanda fossero in equilibrio attraverso l'arbitraggio, cioè contraendo (o espandendo) il pool *UST* utilizzando il pool *LUNA* come counterweight. In secondo luogo, attraverso il modulo di mercato algoritmico del protocollo *Terra*, gli arbitraggisti sono stati autorizzati a scambiare 1 dollaro di *LUNA* per 1 *UST* e viceversa, indipendentemente dai prezzi *LUNA* e *UST*». Briola A. et al., *Anatomy of a Stablecoin's failure: The Terra-Luna case*, *Finance Research Letters* Volume 51, 2023.

¹⁰² [Carbone F., Terra LUNA e UST: tutto sul drammatico crollo dello stablecoin, Fintastico, 2022.](#)

Voyager e Celsius hanno presentato istanza di fallimento. Three Arrows Capital (3AC) è stato costretto alla liquidazione»¹⁰³.

- 4) **Novembre/dicembre 2022: fallimenti di FTX, Alameda Research, BlockFi e Core Scientific Group.** Fra tutti i recenti casi di fallimento quello di FTX (tra i più noti *exchange* in circolazione insieme a *Binance* e *Coinbase*) rappresenta il momento più eclatante finora toccato dal mercato CEX. Sul piano reputazionale, la gravità dell'evento è tale da equipararlo ad una sorta di *Lehman Brothers* nel panorama *crypto*¹⁰⁴. Nonostante le funzionalità tecniche e operative fossero generalmente apprezzate, FTX «aveva delle fondamenta finanziarie davvero poco solide. Infatti, purtroppo il board aveva deciso di utilizzare i fondi depositati dai loro clienti per finanziare spese ed investimenti della loro società. In questo modo non avevano più in cassa sufficienti riserve per coprire l'intero valore complessivo dei fondi che i loro clienti conservavano sui wallet dell'exchange. Oltretutto tra le spese e gli investimenti finanziati in questo modo ce n'erano diversi infruttiferi, o addirittura che generavano perdite. Ad esempio, la consociata Alameda Research, che si occupava di trading e di investimenti, aveva ottenuto molti fondi da FTX, attinti presumibilmente dai depositi dei clienti, ed alcuni di questi li aveva persi in operazioni di mercato non andate a buon fine». Di conseguenza, Alameda Research e BlockFi hanno risentito fortemente dell'episodio in quanto strettamente connesse con FTX: la prima è una società sorella andata in bancarotta perché non disponeva di molti strumenti volti alla gestione del rischio o le capacità professionali in grado di contenere le perdite¹⁰⁵; la seconda è incorsa prima in problemi di liquidità, poi ha dovuto dichiarare l'insolvenza a causa dei crediti “in pancia” che deteneva verso FTX ed altre controparti. Infine, vi è Core Scientific Group, colosso del *crypto mining* «che ha dovuto far ricorso al Chapter 11

¹⁰³ [Forbes, What Really Happened To LUNA Crypto?, 2023.](#)

¹⁰⁴ Tra gli innumerevoli contributi, vds. [Carlini V., Cripto-crack: intrecci sui titoli e contratti automatici, così dilaga il contagio, Il Sole 24 Ore, 2023;](#) [Lops V., Cripto, cresce la voragine di Ftx. In fumo oltre 30 miliardi di dollari, Il Sole 24 Ore, 2022;](#) [Rociola A. Storia del più grande crac della storia delle criptovalute. Cosa è successo a Ftx, la Repubblica, 2022.](#) Per una più approfondita analisi si rimanda a [Arner D.W. et al., The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023, University of Hong Kong Faculty of Law Research Paper n. 19, 2023.](#)

¹⁰⁵ [Pannone A., Il fallimento di Alameda è un rischio per Tether? Ecco quanto ne sappiamo, The Cryptonomist, 2023.](#)

non per truffe o malagestione ma per il costo dell'energia volato alle stelle nel corso dell'anno e per il crollo del valore del bitcoin che ha reso non più sufficientemente remunerativo il business»¹⁰⁶.

- 5) **Gennaio 2023: Genesis Global HoldCo.** Sotto il controllo del *Digital Currency Group (DCG)*, Genesis è l'azienda di *crypto-trading* che, colpita dal crollo di *3AC* e *FTX*, ha cessato tutte le operazioni di *trading*. La bancarotta è stata successivamente dichiarata insieme a due sue sussidiarie, presentando una passività strutturalmente più grave di quella di *FTX* in termini di esposizioni che ammonterebbero a \$3,4 miliardi¹⁰⁷.
- 6) **Marzo 2023: Silicon Valley Bank (SVB), Silvergate Bank, Signature Bank e First Republic Bank.** In questa finestra temporale l'opinione pubblica finanziaria si è concentrata sulla crisi delle banche regionali statunitensi. Nell'arco di poco tempo, tre istituti bancari noti al settore come *crypto-friendly* «sono entrati in liquidazione volontaria o sono stati messi in amministrazione controllata dalle autorità di regolamentazione statunitensi: Silvergate ha annunciato l'intenzione di procedere alla liquidazione volontaria l'8 marzo, in un modo che si prevede ordinato, e di restituire interamente il capitale ai depositanti; Silicon Valley Bank (SVB), la 16a banca statunitense, è stata chiusa e messa in amministrazione controllata dalla FDIC il 12 marzo, rendendo il fallimento bancario da 209 miliardi di dollari il secondo più grande nella storia degli Stati Uniti; la Signature Bank New York (SBNY) è stata chiusa il 12 marzo, come annunciato dalla Federal Reserve»¹⁰⁸. Tali disastri hanno provocato una corsa agli sportelli (*bank run*), determinando l'insolvenza di *First Republic Bank*. Tutti questi incidenti hanno dimostrato quanto possa essere pericoloso per il settore bancario avere un piano aziendale che si basa fortemente sui prodotti crittografici, specie senza tenere conto dell'importanza dei requisiti prudenziali necessari in tali frangenti.

L'illustrazione degli eventi pur succintamente elencati fa risaltare l'eterogeneità delle variabili che hanno scatenato i fallimenti dei vari *exchange*: resilienza digitale poco

¹⁰⁶ [Chicco M., Le 9 crisi più nere delle criptovalute del 2022, Wired, 2022.](#)

¹⁰⁷ [AA.VV., Criptovalute, crolla anche il colosso Genesis. Peggio di Ftx: buco da 3,4 miliardi, Open, 2023.](#)

¹⁰⁸ [Cancelli E., Silvergate, Silicon Valley Bank e Signature Bank: che succede a Bitcoin?, Crypto.it, 2023.](#)

sviluppata a fronte di attacchi cibernetici; costi energetici insostenibili; tecniche aggressive poste in essere dagli investitori; dipendenti con *know-how* non all'altezza della situazione; modelli di *business* non solidi; scarsa applicazione dei criteri prudenziali; depositi non assicurati; forte esposizione ad *asset* particolarmente rischiosi; incauta e/o negligente gestione societaria; problemi di liquidità; insolvenza e via discorrendo. Arner e colleghi riuniscono questo ventaglio di criticità sotto il nome di “*financialization of crypto*”, rimarcando con tale espressione che «*le criptovalute non sono né speciali né immuni e sono arrivate a presentare tutti i problemi classici della finanza tradizionale. Con l'evoluzione dell'ecosistema delle criptovalute, sono emersi i fallimenti del mercato e le esternalità della finanza tradizionale*».

Date	Platform	Assets diverted	Method
Jul 05	Mt. Gox	\$ 473 000 000	Inside job / bad business conduct
Jan 18	Coincheck	\$ 534 000 000	Inadequate security
Feb 21	CreamFinance	\$ 38 000 000	Flash loan attack
Mrz 21	PAID Network	\$ 7 000 000	Compromised private keys
Aug 21	CreamFinance	\$ 25 000 000	Flash loan attack
Aug 21	Poly Network	\$ 611 000 000	Software bug
Oct 21	CreamFinance	\$ 130 000 000	Flash loan attack
Oct 21	Compound	\$ 150 000 000	Software bug
Nov 21	bZx Protocol	\$ 55 000 000	Compromised private keys
Dec 21	Bitmart	\$ 196 000 000	Stolen private keys
Dec 21	VulcanForged	\$ 140 000 000	Stolen private keys
Dec 21	BadgerDAO	\$ 120 000 000	Governance attack
Feb 22	Wormhole	\$ 325 000 000	Bridge exploit
Feb 22	Qubit Finance (X-Bridge)	\$ 40 000 000	Bridge exploit
Mrz 22	Ronin Network	\$ 625 000 000	Stolen private keys
Apr 22	Beanstalk	\$ 182 000 000	Governance attack
Aug 22	Nomad Bridge	\$ 190 000 000	Software bug
Sep 22	Wintermute	\$ 162 000 000	Software bug
Okt 22	Binance	\$ 570 000 000	Bridge exploit
Nov 22	FTX	\$ 477 000 000	Inside job / bad business conduct

Figura 2 – Fonte: [Arner D. W. et al., *The financialization of Crypto: lessons from FTX and the Crypto Winter of 2022-2023*, University of Hong Kong Faculty of Law Research Paper No. 2023/19, 2023.](#)

La Figura 2, composta dai succitati autori, riporta ulteriori esempi di piattaforme *exchange* gravemente colpiti, mettendo in luce il controvalore degli *asset* rubati o persi.

A integrazione di quanto sinora osservato, il lavoro di Aquilina ed altri autori nel Bollettino n. 66 del BIS dichiara senza troppi giri di parole che, «*dopo il fallimento di alcune importanti società di criptovalute, affrontare i rischi dei mercati delle criptovalute è diventata una questione politica più urgente. I mercati dei crypto-asset hanno già attraversato boom e disastri in passato, e finora i fallimenti non hanno portato a un contagio più ampio che ha minacciato la stabilità finanziaria. L'ecosistema crittografico e le funzioni di "finanza ombra" che esso svolge, attraverso entità finanziarie centralizzate (CeFi) e protocolli di finanza decentralizzata (DeFi), condividono molte delle vulnerabilità note della finanza tradizionale (TradFi). Ma diversi fattori esacerbano i rischi standard. Si tratta di un'elevata leva finanziaria, di disallineamenti di liquidità e di scadenze e di sostanziali asimmetrie informative. Le risposte politiche dovrebbero considerare come affrontare queste fonti di rischio in modo appropriato, data la natura senza confini delle criptovalute*»¹⁰⁹

Nel confrontare peraltro le pubblicazioni di diverse entità di rilievo come la Banca dei Regolamenti Internazionali (*Bank of International Settlement, BIS*), il Consiglio per la Stabilità Finanziaria (*Financial Stability Board, FSB*), il Fondo Monetario Internazionale (*International Monetary Fund, IMF*), l'OCSE (*Organization for Economic Co-operation and Development, OECD*), lo *European Systemic Risk Board (ESRB)* o ancora la *Banque de France*, è emerso che tutte convergono su un punto¹¹⁰: il legame che intercorre tra economia reale, finanza tradizionale e mercato *crypto* esiste, ma al momento risulta limitato e meno preoccupante di quello che i vari fallimenti verificatisi recentemente fanno sembrare.

Assodata l'esistenza del rapporto tra *TradFi* e “*crypto financial system*” e misuratane la consistenza, il passo successivo è ora capire in che modo si struttura. Ebbene, a tal riguardo, si intravedono dei punti di contatto che tengono insieme la finanza decentralizzata con il mondo reale:

¹⁰⁹ [Aquilina M. et al., Addressing the risks in crypto: laying out the options, BIS Bulletin n. 66, 2023.](#)

¹¹⁰ [Fondo Monetario Internazionale-FSB, IMF-FSB Synthesis Paper: Policies for Crypto-Assets, 2023; ESRB, Crypto-assets and decentralised finance, 2023; Banca di Francia, “Decentralised” or “disintermediated” finance: what regulatory response?, Discussion Paper, 2023; BRI, The crypto ecosystem: key elements and risks. Report submitted to the G20 Finance Ministers and Central Bank Governors, 2023; Iyer R. e Popescu A., New Evidence on Spillovers Between Crypto Assets and Financial Markets, IMF Working paper, 2023; Fondo Monetario Internazionale, Global Financial Stability Report. Safeguarding Financial Stability amid High Inflation and Geopolitical Risks, 2023; OCSE, Institutionalisation of crypto-assets and Defi-TradFi interconnectedness, OECD Publishing, 2022.](#)

- 1) **Consumatori retail.** La principale porta d'ingresso è data dai singoli investitori e risparmiatori, i quali pur non avendo un'educazione finanziaria solida alle spalle il più delle volte si affacciano a un mondo altamente rischioso e speculativo come quello delle cripto-attività incorrendo talvolta, attraverso la mediazione dei suddetti *provider*, a ingenti perdite di denaro e truffe. Molti attori istituzionali accendono periodicamente un faro su questa problematica, avvisando sostanzialmente i consumatori che tali operazioni «non sono adatte per la maggior parte dei consumatori al dettaglio come investimento o mezzo di pagamento o scambio»¹¹¹ e che peraltro «dovrebbero prestare attenzione ai rischi di pubblicità ingannevole, anche attraverso i social media e gli influencer, ed essere particolarmente cauti nei confronti dei rendimenti rapidi o elevati promessi, specialmente quelli che sembrano troppo allettanti per essere veri»;
- 2) **Le stablecoin**¹¹². Per far fronte alla volatilità dei prezzi, molti utenti *retail* utilizzano questo specifico prodotto come garanzia per i prestiti in *crypto-asset*. In altri termini, si opta per una strategia di copertura basata su partecipazioni in *stablecoin* senza doverli riconvertire in valuta ufficiale. Inversamente, le società emittenti sono diventati attori principali di questo mercato nel 2021. Per entrambi questi motivi, le *stablecoin* sono una parte critica da arginare. La perdita di parità (*depeg*) di una *stablecoin* (rispetto alla valuta

¹¹¹ [Aliperto D., Criptomonete, faro delle Autorità di vigilanza Ue: "Subito le regole", NetworkDigital 360, 2022.](#)

¹¹² [Fondo Monetario Internazionale, Regulating the Crypto Ecosystem: The Case of Stablecoins and Arrangements, 2022.](#) «La crescente interdipendenza delle criptovalute con la finanza convenzionale e l'economia reale potrebbe rappresentare un pericolo per la sovranità monetaria. La disponibilità di *stablecoin*, in particolare, potrebbe rendere più facile la sostituzione delle valute locali con quelle basate sulle criptovalute, un processo noto come "criptoizzazione". I detentori di valute fiat nazionali potrebbero convertirsi a valute alternative in periodi di instabilità macroeconomica e di tassi di cambio in calo, aumentando la pressione sulla valuta nazionale. Tali azioni potrebbero avere effetti a lungo termine sulla stabilità monetaria e finanziaria complessiva di queste nazioni, privando le autorità monetarie nazionali della loro sovranità monetaria e allontanando i finanziamenti per le istituzioni finanziarie regionali. Indubbiamente, la possibilità di una sostituzione valutaria è sempre presente ed è responsabilità di ogni giurisdizione gestirla in modo appropriato. Tuttavia, poiché le monete stabili e le criptovalute rendono la sostituzione della valuta molto più semplice nella realtà, la loro esistenza può aumentare significativamente la probabilità che tali scenari si concretizzino. La minaccia alla sovranità monetaria potrebbe aumentare in modo significativo se le grandi aziende tecnologiche decidessero di emettere *stablecoin* per capitalizzare il ciclo auto-rinforzante dati-rete-attività che consente loro di trarre vantaggio dagli effetti di rete in costante espansione. Le criptovalute e il sistema finanziario consolidato possono essere collegati in entrambe le direzioni. Ad esempio, diverse *stablecoin* hanno perso il loro peg a seguito delle turbolenze bancarie del marzo 2023. USDCoin ha perso il suo peg dopo aver rivelato che una parte consistente della sua riserva di contanti era depositata presso la Silicon Valley Bank. Mentre alcune *stablecoin* sono state scambiate a premio, altre che utilizzavano l'USDCoin come asset di riserva non hanno raggiunto la parità».

a cui è presumibilmente agganciata) può minare la stabilità di molte applicazioni, come hanno dimostrato gli effetti a catena del crollo di Terra-Luna. Al di fuori dell'ecosistema, le *stablecoin* sono il principale vettore potenziale attraverso il quale gli *shock* possono essere trasmessi dalla *DeFi* ai settori più tradizionali della finanza¹¹³;

- 3) **Esposizioni bancarie**¹¹⁴. Come nel caso di *Silvergate Bank* e *Signature Bank*, le banche (o istituzioni finanziarie che potrebbero essere attratte dai profitti potenzialmente elevati degli investimenti in cripto-attività quali *hedge fund* e gestori patrimoniali) possono potenzialmente impegnarsi nel settore *crypto* offrendo diverse tipologie di servizi quali erogazione del credito alle controparti che hanno un'esposizione su questi *asset* oppure prestazione di servizi di custodia. Tuttavia, data la posizione delle banche come spina dorsale del sistema monetario, i rischi legati al nesso banche/*crypto* non si riducono solo alle esposizioni (dirette e indirette), ma anche a possibili esternalità negative che si verificano quando gli istituti creditizi convogliano fondi nell'ecosistema criptovalutario.

¹¹³ [Centre for International Governance Innovation, Digitalization of Payments and Currency. Key Takeaways from a Third Virtual Workshop with Canadian and International Experts on the Digitalization of Money. Conference Report, 2023.](#) Il documento in questione discorre della questione dal punto di vista del diritto canadese, ma in realtà le osservazioni fatte rilevano anche sul piano internazionale. «Una discussione ricorrente nello spazio normativo delle *stablecoin* e delle criptovalute è se le *stablecoin* debbano essere trattate come titoli o strumenti di pagamento. Mentre le autorità di regolamentazione dei titoli in diversi Paesi, tra cui il Canada, si sono mosse per far rientrare i prodotti di criptovaluta nelle loro competenze, i partecipanti temono che la sola vigilanza sui titoli possa essere insufficiente per affrontare i rischi macroprudenziali che le *stablecoin* potrebbero rappresentare per il più ampio sistema finanziario. Tra le questioni da affrontare vi sono i requisiti per la composizione dei mix di attività sottostanti alle *stablecoin* e la misura in cui gli emittenti di *stablecoin* dovrebbero essere trattati come istituti di deposito. Sostenendo un approccio relativamente neutrale agli strumenti per la regolamentazione delle *stablecoin*, i partecipanti hanno proposto un quadro di riferimento "stesso rischio, stessa attività, stessa regolamentazione" sulla base del trattamento esistente in Canada per gli istituti di deposito. I partecipanti hanno anche osservato che il trade-off sicurezza-valuta può essere in ultima analisi modellato dalle autorità di regolamentazione e che esiste il potenziale per sbloccare un valore reale con le *stablecoin* limitando la loro capacità di servire come depositi di valore e spingendo invece verso i loro potenziali usi solo come mezzo di pagamento. Le *stablecoin* sollevano la questione se dovremmo deviare dal percorso normativo ampiamente intrapreso fino ad oggi e diventare a nostro agio con i circuiti di pagamento decentralizzati. I partecipanti hanno notato l'ulteriore ironia del fatto che, nonostante l'obiettivo dichiarato delle *stablecoins* di offrire un percorso verso la finanza decentralizzata, il futuro a lungo termine delle *stablecoins* sembra essere più probabilmente quello in cui le grandi autorità centralizzate mantengono un ruolo di primo piano nell'emissione di valuta».

¹¹⁴ Non è inaspettato che i *crypto-asset* continuino a essere un veicolo prevalentemente autoreferenziale utilizzato per la speculazione. In realtà, uno dei fattori principali delle connessioni attuali è la necessità per le criptovalute di confrontarsi con la finanza tradizionale per mantenere la propria crescita. Tuttavia, nonostante gli eventi dell'ultimo anno, gli investitori istituzionali e le persone comuni sono ancora interessati alle criptovalute. Pertanto, non si può escludere che queste connessioni si rafforzino. La connessione tra le criptovalute e il settore bancario principale è la più significativa di queste relazioni.

Considerando le innumerevoli criticità possibili (es. di volatilità, operativo, di riciclaggio e di finanziamento del terrorismo, reputazionale), è quanto mai urgente ridurre al minimo indispensabile tali rischi. Secondo il supervisore finanziario giapponese (corrispondente alla nostra Consob), la valutazione dell'acquisizione, della detenzione e della cessione di criptovalute da parte delle istituzioni finanziarie tradizionali si dovrebbe concentrare principalmente sull'adeguatezza di (i) identificazione e mitigazione dei rischi in base alle caratteristiche delle criptovalute; (ii) misure di *AML/CFT*; (iii) misure per assicurare la solidità finanziaria; e (iv) controllo della *cybersecurity*¹¹⁵;

- 4) **La tokenizzazione dei crediti su beni fisici**¹¹⁶. Tokenizzare¹¹⁷ azioni o immobili è un altro modo in cui la finanza tradizionale e le criptovalute potrebbero intrecciarsi maggiormente, specie in considerazione del ruolo assunto dalla tecnologia *blockchain* nella cd. “*next web revolution*” (*Web3*). L'afflusso di nuovo denaro in questi *asset* tokenizzati potrebbe portare alla crescita delle criptovalute stesse. Inoltre, l'intrecciarsi delle operazioni dei partecipanti a questi due ecosistemi potrebbe condurre a una rete più intricata di connessioni tra finanza tradizionale e criptovalute.

Gli elementi raccolti fanno ritenere che quanto dedotto nella prima domanda di ricerca in sede di apertura della tesi sia stato correttamente percepito. Alla luce di quanto osservato sinora, i punti di contatto tra *TradFi* e *CeDeFi* nonché la natura “duale” (centralizzata-

¹¹⁵ [Amaya T., Vice Minister for International Affairs, Financial Services Agency Japan, *Regulating the crypto assets landscape in Japan, 2023*.](#)

¹¹⁶ Il fenomeno in realtà è ben più ampio e rientra sotto la denominazione di «*tokenizzazione di asset, intesa come rappresentazione di asset reali sotto forma di token digitali emessi sulla blockchain, che ne rappresentano il valore economico intrinseco e i diritti di possesso*». [Banca d'Italia et al., *Caratteristiche degli Smart Contract, 2023*.](#)

¹¹⁷ Il tema merita di essere ulteriormente approfondito in sedi specializzate, ma basti sapere che in queste righe si dischiude il concetto di “*tokenomics*”, «*fusione di due termini, token ed economics, ovvero tutto l'insieme di decisioni che ruotano attorno alla creazione e alla circolazione di un token, che altro non è che la rappresentazione in digitale di un progetto, o di un'idea, o di un'attività. Quando si sta lanciando un token occorre definire tutte le regole all'inizio, o almeno questo è l'ideale, come per esempio: valore, distribuzione su quale blockchain, diritti e incentivi, fee legati alla vendita primaria o eventualmente secondaria se si tratta di un NFT, supply limitata o no, e con quale roadmap temporale. Queste sono tutte informazioni chiave, che servono a compratori di qualsiasi progetto nel Web3*». Pagano F. e Soldavini P., *Il capitale decentralizzato: Blockchain, NFT, Metaverso*, Il Sole 24 Ore, 2022. Per ulteriori dettagli sul concetto di tokenizzazione vds. [BRI, *Blueprint for the future monetary system: improving the old, enabling the new, BIS Annual Economic Report, 2023*.](#)

decentralizzata) che connota i *CASP* possono nuocere alla stabilità finanziaria in quanto fanno perno su questi punti di contatto menzionati poc'anzi. I fallimenti avvenuti Oltremare, la cui cassa di risonanza mediatica ha certamente risvegliato a livello sistemico una questione fino ad allora rimasta sopita, sono la cartina al tornasole dell'interconnessione tra questi mondi. L'approccio normativo statunitense si è basato finora su leggi finanziarie preesistenti senza creare un quadro specifico per i fornitori di crypto-attività. D'inverso, seppur consapevoli della drammaticità degli episodi crypto-finanziari nel contesto americano, i Paesi europei non sono stati assorbiti da un "terremoto crittografico" di tale portata. Probabilmente ciò è riconducibile all'implementazione preventiva di regolamenti specifici per i *CASP* secondo le raccomandazioni del GAFI¹¹⁸. Inoltre, l'introduzione del *MiCA* consentirà di aggiungere ulteriori presidi, imponendo maggiori oneri a tali soggetti. In conclusione, attualmente i rischi di contagio tra "*crypto financial system*" e *TradFi* si assestano ancora a un livello basso, ma soppesando le dichiarazioni delle autorevoli entità più volte menzionate nelle pagine che precedono, tenderà ad aumentare in futuro. In base a questo ragionamento, l'accelerazione nella regolamentazione di strutturate politiche sui *CASP* potrebbe essere il passo-chiave per ridurre, o quanto meno contrastare, i contagi che sono oggettivamente emersi nella realtà finanziaria. Dunque, per puntare a una maggiore stabilità a livello infrastrutturale e sistemico, appare necessario trovare una normativa armonizzata a livello internazionale che spinga le giurisdizioni nazionali ad accelerare al più presto uno specifico regime di legge disciplinante i fornitori di crypto-attività.

¹¹⁸ «Costituito nel 1989 in occasione del Vertice dei capi di stato e di governo del G7 tenutosi a Parigi, il Gruppo d'Azione Finanziaria Internazionale (GAFI, o Financial Action Task Force) è un organismo intergovernativo che promuove strategie di contrasto al riciclaggio dei capitali di origine illecita e, dal 2001, anche di prevenzione del finanziamento al terrorismo. Nel 2008, il mandato del GAFI/FATF è stato esteso al contrasto del finanziamento della proliferazione di armi di distruzione di massa (Counter Proliferation Financing/CPF). In occasione del trentesimo anniversario del GAFI, il 12 aprile 2019, a Washington D.C. i Ministri dei Paesi membri hanno conferito al FATF/GAFI il nuovo mandato, per la prima volta a tempo indeterminato in considerazione della rilevanza che l'organismo ha assunto per la salvaguardia dell'integrità e della trasparenza del sistema finanziario internazionale. Compito del GAFI è elaborare gli standard AML/CFT - le cosiddette raccomandazioni - riconosciuti su scala globale per il contrasto delle attività finanziarie illecite. Gli Standard AML/CFT del GAFI/FATF sono compendati in 40 Raccomandazioni aggiornate periodicamente». [MEF, Attività del Gruppo d'azione finanziaria \(GAFI/FATF\), Dipartimento del Tesoro, 2022](#). Come si vedrà nel prosieguo dell'elaborato, è proprio grazie alla lungimiranza di questa entità intergovernativa che sono state le prime definizioni di criptovaluta (definendola "*virtual asset*" già nel 2014) o sono state delineate le prime pubblicazioni in cui si discorreva di prestatori di crypto-attività sotto il nome di *Virtual Asset Service Provider (VASP)*.

II. PRODOTTI ED OPERATORI TRA *CEFI* E *DEFI*

Prima di iniziare è necessario porre delle premesse. Dopo aver descritto e confrontato rispettivamente il sistema finanziario tradizionale (*TradFi*) e il “*crypto financial system*”, il secondo capitolo si addenterà con maggiore profondità nel perimetro crittografico.

Come riferito nelle note di introduzione che hanno dato abbrivio al presente lavoro, la letteratura scientifica riferita alle tecnologie di base e ai prodotti crittografici è pressoché sconfinata. Tuttavia, una tesi vertente sui *CASP* non può distaccarsi dal tema della cripto-attività, oggetto dei servizi da loro erogati. Volendo pertanto adottare un approccio pragmatico in cui ciascun elemento appartenente al “*crypto financial system*” viene presentato in maniera rigorosamente ordinata, il secondo capitolo si suddividerà in due sezioni:

1. **Prodotti.** Nel corso della prima sezione verranno sviscerati celermente i *digital asset* attualmente esistenti: *crypto-asset* e *CBDC*. Con riferimento ai primi, si metteranno in luce le difficoltà che si stanno registrando sul piano definitorio e tassonomico; con riferimento ai secondi, si illustreranno le principali ragioni alla base della loro adozione e le diverse tipologie di *design* che i singoli Stati stanno prendendo in considerazione per l'emissione delle proprie valute digitali;
2. **Soggetti.** Nella seconda sezione invece si entrerà nel cuore del discorso, operando un'analisi giuridica sia dei *CASP* che delle cripto-attività alla luce del Regolamento *MiCA*, nonché integrando un'indagine personalmente condotta per misurare a livello globale lo stato di regolazione di questi soggetti.

1. Le *crypto technology*: le tecnologie di base per le cripto-attività

1.1. *Distributed Ledger Technology (DLT) e blockchain: lineamenti essenziali*

La tecnologia posta alla base del funzionamento delle cripto-attività in generale è rappresentata dalla già menzionata *DLT*, ossia un insieme di dispositivi informatici connessi tra loro all'interno di una rete *peer-to-peer*¹¹⁹ in cui i partecipanti condividono la responsabilità della custodia, della conservazione e dell'aggiornamento di un registro informatico¹²⁰. La soluzione tecnologica a registro distribuito ha essenzialmente dato slancio all'implementazione di molteplici programmi, «ciascuno dei quali caratterizzato da modelli operativi e funzionali (*permissioned* o *permissionless*¹²¹; *centralized* o *decentralized*), da algoritmi, (*consensus algorithms* operanti col modello *proof-of-work* o *proof-of-stake*, al fine di validare e registrare le transazioni) protocolli

¹¹⁹ «Si tratta di un'architettura di calcolo distribuito, ovvero una struttura informatica nella quale più computer interagiscono tra loro. I nodi (ovvero ciascun dispositivo che riesca a comunicare con gli altri facenti parte di una stessa rete) si dicono "equivalenti" perché sono contemporaneamente sia server che client, hanno pari livello gerarchico e si coordinano senza necessità di identità centrali». [Blockchain Revolution, Glossario, BlueChain, 2023.](#)

¹²⁰ Così, letteralmente si esprime AA.VV., *Fintech. I confini dell'innovazione nella Finanza*, a cura di Natale A., 2022, p. 15.

¹²¹ Con specifico riguardo ai modelli di *governance*, si fa generalmente riferimento a due tipologie di *DLT*:

- il ***permissionless ledger***, che è a schema aperto e non necessita di alcuna autorizzazione per poter accedere alla rete, eseguire transazioni o partecipare alla verifica e creazione di nuovi blocchi (modello *Bitcoin* o *Ethereum*). L'obiettivo è quello di consentire ad ogni utente di aggiornare i dati sul *ledger* e di avere la disponibilità di tutte le copie immutabili di ogni operazione. Questo modello di *blockchain* inibisce qualsiasi forma di censura, poiché impedisce di cancellare o modificare una transazione, una volta acquisito il consenso necessario tra tutti i nodi partecipanti. Nelle *DLT permissionless*, e in particolare in quelle basate su meccanismi di consenso "*Proof-of-Work*", si configura un sistema di *governance* che scaturisce non tanto da meccanismi di delega e di verifica del rispetto delle regole, quanto da automatismi e da meccanismi economici endogeni che conducono al raggiungimento di un consenso fra attori che non comunicano direttamente tra loro;
- il ***permissioned ledger***, che è invece controllabile e gestito da un numero limitato di utenti. In questo caso il meccanismo del consenso è del tipo *Proof-of-Authority (PoA)*, che presuppone l'esistenza di nodi speciali che assumono un ruolo di coordinamento, svolgendo di fatto il ruolo di *trusted third parties*. Questi nodi validano le transazioni inserite grazie a meccanismi di firma crittografica.
- il ***DLT hybrid***, che «combina gli elementi essenziali delle *DLT permissionless* e *permissioned*. In genere le transazioni e le registrazioni in una *DLT hybrid* non sono rese pubbliche, ma possono essere verificate quando necessario, ad esempio attraverso uno specifico *smart contract*. Le informazioni riservate sono tenute all'interno della rete, ma sono comunque verificabili. Anche se un'autorità centrale può presiedere la *DLT hybrid*, non ne può alterare le transazioni». [Assogestioni, Oltre le criptovalute. Tecnologie a registro distribuito a servizio dell'asset management, 2022.](#)

informatici/crittografici e modelli di digital wallet¹²² anche molto diversi tra loro»¹²³.

La sub-categoria più nota è costituita dalla *blockchain*, «un libro mastro (“ledger”) digitale, decentralizzato e distribuito su un network, strutturato come una catena di registri (“i blocchi”), responsabili dell’archiviazione dei dati (dalle transazioni di valore a intere applicazioni digitali). È possibile aggiungere nuovi blocchi di informazioni, ma non è invece possibile la modifica o la rimozione di blocchi precedentemente aggiunti alla catena. In questo ecosistema, la crittografia e i protocolli di consenso garantiscono sicurezza e immutabilità. Il risultato è un sistema aperto, neutrale, affidabile e sicuro, dove la nostra capacità di utilizzare e di avere fiducia nel sistema non dipendono dalle intenzioni di nessun individuo o istituzione. La blockchain è molto più di un’infrastruttura di pagamento, di un sistema di monitoraggio della supply chain o di un gestore di identità digitale. È un sistema con le potenzialità per portare un nuovo livello di fiducia nelle applicazioni, introducendo un cambio di paradigma nelle modalità con cui esse vengono realizzate e dandoci l’opportunità di innovare liberamente»¹²⁴. Senza pretesa di esaustività, la definizione sopra articolata di permette di disvelare le più significative caratteristiche della *blockchain*:

- **Decentralizzazione.** L’assenza di un singolo soggetto provvisto di potere gestorio, di validare, modificare, alterare o cancellare i dati e le transazioni registrate;
- **Disintermediazione.** La piena autonomia delle proprie operazioni senza rivolgersi ad un terzo¹²⁵;

¹²² Pezzuto A., *Cripto-attività: classificazione, caratteristiche e prospettive di regolamentazione*, *Magistra banca e Finanza*, 2022. «La custodia dei token implica la necessità che gli utenti dispongano di portafogli digitali (o wallet), portafogli che possono raggrupparsi in quattro categorie:

- **hot custodial wallet**, connesso ad internet e gestito da un terzo che detiene le chiavi private dell’utente e a cui quest’ultimo può accedere mediante forme di crittografia;
- **hot non custodial wallet**, pure connesso ad internet, in cui l’utente mantiene il controllo delle proprie chiavi private;
- **cold hardware wallet**, un dispositivo fisico che può essere collegato a un personal computer;
- **cold paper wallet**, fogli di carta su cui sono registrati l’indirizzo digitale e la chiave privata».

¹²³ Carrière P., *La “cripto-arte” e i non-fungible tokens (NFT): tentativi di inquadramento giuridico*, *Diritto Bancario*, 2021. Per un ulteriore approfondimento si veda *Politecnico di Milano, La blockchain spiegata in maniera semplice: significato e applicazioni*, blog.osservatori.net.

¹²⁴ Chiap G. et al., *Blockchain. Tecnologia e applicazioni per il business*, Hoepli, 2021.

¹²⁵ La *blockchain* consente infatti di perfezionare transazioni economiche e finanziarie anche utilizzando wallet decentralizzati, gestiti direttamente dagli utenti, senza l’intervento di soggetti operanti in mercati regolamentati e obbligati a fornire informazioni alle Autorità giudiziarie, di vigilanza e fiscali.

- **Pseudonomizzazione dei partecipanti.** La possibilità di nascondere i dati personali. Questo tecnicamente consente di fare a meno dell'intervento di un operatore professionale per la detenzione di *asset* digitali e l'effettuazione di transazioni regolate in cripto-attività, quali ad esempio l'acquisto di beni o servizi pagati utilizzando *stablecoin*, l'investimento in *security token* e *NFT*, oppure la sottoscrizione di prestiti su una piattaforma *DeFi*¹²⁶;
- **Crittografia avanzata.** I dati salvati sulla *blockchain* sono schermati attraverso tecniche avanzate di crittografia, in modo da garantire la loro fruizione solo ai legittimi proprietari del dato stesso. Vi sono due principali strumenti di crittografia utilizzati nella *blockchain* per dissimulare le transazioni: chiavi di crittografia¹²⁷ e le funzioni *hash*¹²⁸. Questo sistema genera una forte fiducia negli utenti, rassicurati dal fatto che i propri messaggi (transazioni) possono essere letti esclusivamente dal destinatario degli stessi. Inoltre, non è necessario che i due soggetti si conoscano fisicamente, ma basta che ciascuno conosca l'*account* di registrazione all'interno della *blockchain*¹²⁹;

¹²⁶ Cfr. Antonacchio F., *Web3 ed economia decentralizzata nuove sfide fiscali*, *Il fisco*, n. 39, 2022, p. 3753 e ss.

¹²⁷ Una delle applicazioni più note e usate di questa tecnica è la crittografia asimmetrica (o “a chiave pubblica”), la *PGP* (*Pretty Good Privacy*), che venne distribuita dal suo sviluppatore, Phil Zimmerman, come *software* libero nel 1991. La prima forma di crittografia sviluppata era di tipo simmetrico, anche nota come crittografia a chiave privata. Questa prevede che, per occultare un messaggio e renderlo leggibile solo per il destinatario, il mittente debba procedere alla sua cifratura. Esistono molti cifrari ed operano con una modalità per cui mittente e destinatario possiedano la medesima chiave, indispensabile sia per cifrare sia per decifrare. Va da sé che nel campo della comunicazione a distanza, mittente e destinatario scambiano anche la chiave con il rischio di essere intercettati. La crittografia a chiave pubblica, nota come crittografia asimmetrica, consente di risolvere questo problema: esiste, infatti, una coppia di chiavi (*keypair*), di cui una funge come chiave privata e l'altra come chiave pubblica. La prima chiave viene generata casualmente e da essa si ricava la chiave pubblica, attraverso una funzione unidirezionale, che non consente di far derivare la prima dalla seconda. In questo modo, se si intende inviare un messaggio cifrato, è sufficiente conoscere la chiave pubblica del destinatario e solo quest'ultimo avrà la possibilità di decifrare il messaggio utilizzando la propria chiave privata. Questo tipo di crittografia è impiegata, oltre che per lo scambio di messaggi cifrati, anche per l'attivazione di algoritmi di firma digitale.

¹²⁸ In sostanza, le informazioni transitano da un nodo ad un altro, secondo uno schema che richiama una concatenazione di blocchi (contenenti più transazioni validate), uno dopo l'altro, dove il blocco corrente contiene il codice *hash* di quello precedente, formando, così, una catena immutabile di blocchi. L'*hash* è una funzione algoritmica informatica non invertibile che prende come *input* una stringa di dati di lunghezza arbitraria e li trasforma in una stringa binaria di dimensione fissa e predeterminata, che rappresenta l'impronta del messaggio (o valore di *hash*). Il sistema *bitcoin* usa principalmente SHA-256 (*secure hash algorithm*) elaborato dal *National Security Agency* (*NSA*, Agenzia per la Sicurezza Nazionale), organismo governativo degli Stati Uniti d'America che si occupa di sicurezza nazionale, e pubblicato dal *NIST*, ossia dal *National Institute Of Standards and Technology*.

¹²⁹ Questo sistema è stato ideato, in origine, per prevenire il problema della “doppia spesa”, rischio insito in un sistema di scambi che è privo di un terzo (intermediario) che si ponga come garante ed assolva alle funzioni di

- **Immutabilità.** Su questo punto spesso sorge l'erronea convinzione secondo cui il legame di *hashing* tra i blocchi garantisca l'immutabilità della catena. Ciò è inesatto in quanto l'*hashing* ha la mera funzione di rendere evidente per tutti i nodi partecipanti l'avvenuta modifica delle transazioni, includendo con ciò anche una potenziale manomissione. Per dirla con parole più semplici, «*manomettere una blockchain è facile, far accettare la blockchain manomessa al resto del network è difficile. L'immutabilità non risiede nella struttura di una blockchain ma nel protocollo di consenso*»¹³⁰;
- **Merkle Tree.** Al fine di garantire l'integrità dell'intera catena, la *blockchain* impiega una specifica struttura di dati (*data architecture*) chiamata "*Merkle Tree*". Questa è costruita su più blocchi, ciascuno dei quali è composto da un "*Merkle Tree*". Alla base del *Merkle Tree* sono allocate le transazioni; al livello superiore si trovano i loro corrispondenti valori di *hash*, che vengono "*ri-hashati*" in altri livelli superiori fino a raggiungere il *top hash*, noto come "*Merkle root*", che fornisce la prova della validità di tutte le transazioni aggiunte all'albero (e quindi al blocco). Ciascun blocco è collegato a quello precedente da un ulteriore *hash*, che garantisce l'integrità del blocco N e del blocco N-1;
- **Meccanismi di validazione del consenso.** Si tratta di un meccanismo attraverso il quale si assicura che le informazioni inserite nei blocchi siano corrette e coerenti con le regole

verifica e validazione delle transazioni. Il commercio elettronico, ad esempio, nasce come sistema in cui, al di là del mezzo impiegato (il *web*), è assicurato un sistema fiduciario ove istituzioni terze si pongono come garanti delle transazioni assicurando che all'incremento di un dato valore nel portafoglio del venditore corrisponda la diminuzione di un pari valore nel portafoglio dell'acquirente. Il sistema, tuttavia, non è perfetto, poiché gli intermediari non hanno la capacità di assicurare che il precedente proprietario non abbia speso due volte la stessa valuta e, di conseguenza, di assicurare che le transazioni siano totalmente irreversibili. In pratica, la soluzione individuata con la *blockchain* impedisce la presenza di doppie transazioni semplicemente rendendo pubblici tutti gli scambi avvenuti in precedenza, grazie all'utilizzo di *server* a marcatura temporale distribuiti su reti *peer-to-peer*, in grado di generare la prova dell'ordine cronologico delle transazioni: ogni marcatura temporale comprende quella precedente nel suo *hash* e ogni marcatura successiva rafforza quelle precedenti, formando una vera e propria catena in cui sono registrate e contabilizzate tutte le operazioni svolte in *bitcoin*. I dati della catena sono, in questo modo, conservati in ogni computer-nodo del sistema e tutte le transazioni risultano unite in una serie di blocchi interconnessi ed immutabili, secondo una logica che non contempla compromissioni del dato storico, se non attraverso la creazione di un diverso blocco totalmente avulso dal sistema, facilmente individuabile dagli altri utenti che non ne permetterebbero l'accettazione. In tale ottica, è possibile definire tecnicamente i *crypto-asset* come dei valori di natura digitale che prendono vita da una catena di firme digitali che si fonda su uno schema crittografico basato sull'interdipendenza delle chiavi pubbliche-private (la cosiddetta "firma digitale") e sulla produzione di codici *hash* irreversibili. Attraverso questa catena ciascun proprietario trasferisce gli asset al proprietario successivo, attraverso transazioni che sono tracciabili sulla *blockchain*.

¹³⁰ Chiap G. et al., *Blockchain. Tecnologia e applicazioni per il business*, Hoepli, 2021.

stabilite dal protocollo. Ciò consente alle informazioni di essere condivise tra due nodi senza la necessità di ricorrere preventivamente ad una entità centrale perché la validi. Sebbene esistano numerose tipologie e modalità di validare transazioni¹³¹, tra le più blasonate da annoverare in regime di *blockchain* vi sono il *Proof-of-Work (PoW)*¹³² e il *Proof-of-Stake (PoS)*¹³³.

Complessivamente, per tutti i motivi esposti sopra, gli aspetti di sicurezza insiti nel meccanismo con il quale le transazioni vengono eseguite all'interno della *blockchain*, la resilienza della catena stessa, assieme ad un certo grado di anonimità con cui gli utenti possono prendere parte, hanno negli anni incentivato una fetta di utenza ad utilizzare la più diffusa e popolare applicazione della *blockchain* come strumento per l'esercizio di attività classiche della *TradFi* (scambio, pagamento, conservazione, ecc.).

A ben pensarci, se da un lato i diversi ordinamenti si sono mossi sin dall'inizio in modo misurato e diffidente nei confronti delle cripto-attività, dall'altro hanno mostrato molta più apertura e dinamismo con riferimento allo sviluppo e alle potenzialità offerte dalla *blockchain*. Del resto, si tratta di una tecnologia versatile e applicabile in progetti che spaziano dal *Fintech* all'*Insurtech*, dalla sanità all'agroalimentare, dal turismo al *design* e che riguardano anche settori molto avanzati, come l'Intelligenza Artificiale (IA) o il *Machine Learning (ML)* o addirittura avveniristici, come lo spazio, l'ingegneria genetica e la biologia sintetica. Ciò dimostra che, nonostante la notorietà della *blockchain* legata in via assorbente ai *crypto-asset* (che con essi è nata e si è sviluppata), la contabilità decentrata si presta a diventare una tecnologia diffusa e dalle smisurate possibilità di utilizzo, cambiando il modo di organizzare le relazioni sociali ed economiche nonché introducendo nuovi schemi di gestione, conservazione e condivisione delle informazioni e dei dati. In altri termini, la

¹³¹ A titolo d'esempio si annoverano meccanismi quali la *Delegated Proof-of-Stake (DPoS)*; *Proof of Space and Time* (anche conosciuto come *Proof-of-Capacity, PoC*); *Proof-of-Weight*; *Proof-of-Authority* (noto anche come *Proof-of-Reputation*); *Practical Byzantine Fault Tolerance*; *Unique Node List*; *Direct Acyclic Graph (DAG)*.

¹³² La *blockchain* di *Bitcoin* si basa ad esempio sul meccanismo di consenso *Proof-of-Work (PoW)*. In sostanza, ciascun nodo chiamato a validare la transazione deve dimostrare di aver risolto un puzzle crittografico, per la soluzione del quale è necessaria una grande capacità computazionale. Questa modalità di validazione dei blocchi è però da molti ritenuta altamente dispendiosa in termini energetici.

¹³³ Esistono anche altri metodi per il conseguimento di un consenso distribuito, oltre a quello previsto nella *blockchain* di *Bitcoin*. Altri *crypto-asset* utilizzano, ad esempio, la *proof of stake* (la *Peercoin* è stata la prima).

tecnologia legata alla *blockchain* offre la possibilità di superare le logiche tradizionali fondate su reti centralizzate che hanno determinato un'eccessiva concentrazione della *governance* dei servizi disponibili su *Internet*, restituendo agli utenti il potere di gestire in autonomia processi organizzativi sia a livello di impresa sia a livello sociale. Prendendo consapevolezza di tali caratteristiche, le istituzioni europee si sono largamente occupate di dare maggiore risalto a questa strumentazione, la cui trattazione normativa (segnatamente inserita nel *DLT Pilot Regime* nell'ambito del *Digital Finance Package*) verrà meglio esposta nella successiva sezione. Tuttavia, almeno da un punto di vista nazionale, è possibile anticipare che il Legislatore italiano ha dedicato spazio a tale strumento nel proprio ordinamento per mezzo dell'art. 8-ter, co. 1 del D.L. n. 135/2018 ("Decreto Semplificazioni"), convertito con modificazioni dalla L. n. 12/2019, aprendo di fatto all'uso delle tecnologie a registro distribuito e delle loro applicazioni (inclusendo quindi anche gli *smart contract*) nonché configurando un quadro normativo dei loro effetti giuridici¹³⁴.

1.2. I Smart contract come principale meccanismo di disintermediazione nel Web3

Sulla scorta del precedente paragrafo, abbiamo visto come la tecnologia basata sulla *blockchain* sia praticamente divenuta un tassello fondamentale del cd. *Web3*¹³⁵, la terza

¹³⁴ L'art. 8-ter, co. 1 così recita: «*si definiscono "tecnologie basate su registri distribuiti" le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetture decentralizzate su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili*».

¹³⁵ «*Anche se ci appare sempre lo stesso, il web ha vissuto varie epoche. In particolare, si parla di tre forme distinte del web, ognuna definita da ciò che gli utenti potevano fare online, sia in termini di interazione con siti e servizi già esistenti sia di creazioni di contenuti. Per questo, considerando l'ordine cronologico di arrivo si parla di:*

- ***Web 1.0***, in riferimento alla prima interazione del web, quando la maggioranza degli utenti poteva solamente accedere all'informazione online attraverso siti statici. Pochi attori avevano la possibilità di pubblicare.
- ***Web 2.0*** ha invece aperto le porte alla creazione e condivisione dei propri contenuti online per tutti. L'espressione si riferisce alla prima grande rivoluzione del web. Quella in cui i creatori diventano "content creator" oltre che meri utilizzatori passivi della rete. Uno scenario accelerato dall'arrivo di piattaforme come Facebook, Twitter, Youtube, LinkedIn, TikTok. In tali applicazioni, i contenuti creati dagli utenti, le loro interazioni, i gusti, le preferenze, ed in ultima analisi le loro identità online, non sono di proprietà degli utenti stessi, ma dei colossi che controllano le piattaforme utilizzate.
- La *blockchain*, insieme ad altre tecnologie, potrebbe essere alla base della Next Web Revolution ossia il ***Web3***, una sorta di spazio decentralizzato che per alcuni sarà la naturale evoluzione dell'attuale web, in gran parte decentralizzato e dominato dalle Big Tech. Per fare un esempio, pensiamo allo username di un'app che utilizziamo oggi. Benché ognuno sia libero di scegliere l'identificativo che preferisce tra quelli ammessi. Non è detto che possa usare anche quel nome anche su Instagram. Insomma, quel nome in realtà

generazione del web. Discorrendo di *DLT* e *blockchain*, non si può non imbattersi nell'espressione *smart contract*, che all'origine della sua diffusione ha provocato numerosi malintesi poiché tradotto erroneamente e semplicisticamente come “contratto intelligente”. In termini meno intuitivi, come riporta Deloitte, si tratta di «*protocolli di transazione computerizzati che eseguono automaticamente i termini di un contratto, rendendolo essenzialmente auto-esecutivo. Mentre un contratto tipico utilizza un linguaggio per stabilire eventi o azioni legalmente rilevanti secondo i termini dell'accordo, un contratto intelligente stabilisce eventi attraverso linee di codice che vengono eseguite quando vengono soddisfatte condizioni predeterminate*»¹³⁶. Il codice consente l'esecuzione tra le parti senza la necessità

non è di proprietà dell'utente, che infatti non può disporre liberamente al di fuori della piattaforma di riferimento. Inoltre, Twitter o qualsiasi altro servizio centralizzato potrebbe in qualsiasi momento revocare l'uso dello username. E la stessa cosa accade con gli altri attributi della realtà online. attributi della nostra personalità online. Non è quindi l'utilizzatore del servizio online a detenere il controllo dei propri dati, ma è il titolare della piattaforma che ospita l'utente stesso. E si tratta di un contesto che il Web3 promette di ribaltare completamente, questo perché la terza generazione del web permette di divenire effettivamente proprietari dei propri contenuti e degli attributi che compongono la loro identità online.

Volendo sintetizzare, possiamo dire che nel Web 1.0 gli utenti leggevano contenuti online tramite siti web, nel Web 2.0 ne possono fruire e soprattutto scrivere/creare/pubblicare tramite post, mentre nel Web3 si aggiunge la componente del possesso delle informazioni digitali tramite token. L'opportunità di “possedere” contenuti, informazioni, attributi della propria identità è un fattore di forte impatto che apre la strada ad una possibile rivoluzione della struttura tecnologica, economica e sociale delle applicazioni web. Un panorama che già oggi mostra le sue potenzialità e che è destinato a svilupparsi ulteriormente nel prossimo futuro». Informazioni ricavate [Portale V., Cos'è il Web3 e come funziona: guida al web 3.0, Osservatori.net digital innovation, 2023](#) e più in generale dai webinar degli Osservatori.net digital innovation. Per ulteriori approfondimenti, vds.: [A16zcrypto, State of Crypto, 2023](#); [Allen D. W. E. e Potts J., Web3 toolkits: A user innovation theory of crypto development, Journal of Open Innovation: Technology, Market and Complexity 9, 2023](#); [Parlour C.A., An introduction to Web3 with implications for financial services, Federal Reserve Bank of Atlanta's Policy Hub, 2023](#).

¹³⁶ Parola L. et al., *Blockchain e smart contract: questioni giuridiche aperte*, Contratti, 2018. «*A differenza di una catena di controllo semplice che registra solo le transazioni, lo smart contract aggiunge un codice autoeseguibile con un ulteriore grado di complessità e di organizzazione. I protocolli verificano ed eseguono le clausole del contratto e monitorano l'esecuzione dello stesso. La tecnologia blockchain permette, quindi, per così dire, la self enforceability del contratto: vengono cioè eseguiti automaticamente i termini e le condizioni dello stesso al verificarsi degli eventi predeterminati dalle parti e iscritti nel codice. Gli smart contract si basano, come un diagramma di flusso, sulla logica “if this then that”: una volta soddisfatte le condizioni descritte nel codice si attivano automaticamente delle specifiche azioni che non possono essere interrotte. Infatti, dato che il libro mastro di blockchain è immutabile, il codice - e così il contratto al quale esso si riferisce - può solo essere cancellato o modificato seguendo i termini definiti dal codice stesso. Pertanto, a differenza dei contratti tradizionali, che offrono la possibilità di adempiere le prestazioni come stabilito nel contratto stesso o di rendersi inadempienti ed andare incontro alle relative conseguenze (ad esempio, sospensione della controprestazione, risoluzione per inadempimento, ecc.), tale opzione non è disponibile in uno smart contract dove l'adempimento del contratto è, per così dire, automatizzato e subordinato unicamente al verificarsi di determinati eventi sottratti alla volontà delle parti. Gli smart contract, in altri termini, non possono rimanere inadempienti: lo loro è una esecuzione a prova di manomissione, tamper proof. L'adempimento “automatico” di uno smart contract è euritmico alle teorie “non negoziali” che sottolineano l'irrilevanza dell'animus solvendi nell'inquadramento del concetto di adempimento.*

di un'autorità centrale, di un sistema legale o di un meccanismo di applicazione esterno. Queste condizioni predeterminate e i programmi di supporto sono memorizzati su una blockchain distribuita e decentralizzata ed eseguiti in parallelo attraverso una rete progettata per convalidare e verificare la corretta esecuzione di qualsiasi operazione, garantendo la tracciabilità e l'irreversibilità delle transazioni. Sebbene la velocità di elaborazione dei contratti intelligenti sia ancora piuttosto inefficiente rispetto all'informatica centralizzata tradizionale, i contratti intelligenti offrono anche diversi vantaggi. Ad esempio, gli smart contract offrono un elevato grado di fiducia, in quanto vengono sempre eseguiti secondo i termini specificati e consentono a chiunque di verificare le modifiche in modo indipendente. Inoltre, mentre le applicazioni tradizionali basate su server non consentono all'utente di osservare la logica interna dell'applicazione o di controllare l'ambiente di esecuzione, gli smart contract permettono all'utente di fare entrambe le cose. Se implementati in modo sicuro, gli smart contract sono altamente trasparenti e riducono al minimo il rischio di manipolazioni e interventi arbitrari. Sono flessibili, in quanto consentono al programmatore di sviluppare un set di istruzioni su misura, attraverso il codice, adattato al risultato specifico desiderato. Possono anche immagazzinare e gestire gli asset di criptovaluta, assumendo così il ruolo di custodi, con criteri del tutto personalizzabili su come, quando e a chi possono essere rilasciati. Ciò consente una grande varietà di applicazioni innovative»¹³⁷. Tutte le suesposte proprietà mettono in risalto il reale valore di questa specifica tecnologia, senza la quale CeFi e DeFi non avrebbero assunto le sembianze odierne. Inoltre, per quanto sia pacifico considerare lo smart contract come principale meccanismo di disintermediazione del Web3, ciò non significa che abbia irreversibilmente disintermediato tutti i servizi finanziari, ma ha lasciato la discrezionalità di poterne fare più o meno richiesta. Difatti, ad essere precisi, «poiché tutte le parti possono essere certi dei

Riassumendo, è possibile descrivere lo smart contract come un contratto:

- **digitale:** le clausole contrattuali sono incorporate nel software sotto forma di codice;
- **autoeseguibile:** l'adempimento, essendo governato dagli input previsti nel codice, prescinde non solo dall'animus solvendi del debitore, ma finanche dal comportamento delle parti; e
- **irrevocabile:** una volta iniziato, il processo di esecuzione non può essere fermato o modificato».

Per ulteriori approfondimenti sul tema, specie in merito alla differenza tra “Smart Contract code” e “Smart legal contract”, si riporta una recente pubblicazione di [Banca d'Italia et al., Caratteristiche degli Smart Contract, 2023](#).

¹³⁷ [Deloitte, DeFi deciphered: Navigating disruption within financial services, 2023](#).

*dettagli del contratto e sapere che sarà seguito automaticamente, ha reso non più necessario un livello aggiuntivo (o terza parte) per garantire la fiducia nel sistema»¹³⁸. Infine, per quanto concerne invece i dettagli normativi, come riferito sulle DLT, la definizione nazionale di *smart contract* può individuarsi nell'art. 8-ter, co. 2 del D.L. 135/2018, descrivendolo come «un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto».*

2. La famiglia dei digital asset: crypto-asset e CBDC

Sin dalla nascita del *bitcoin* e dal successivo sviluppo di *altcoin*¹³⁹, accademici ed esperti giuristi si sono sforzati di ricondurre il fenomeno criptovalutario in determinate categorie giuridiche. Dottrina e giurisprudenza hanno certamente fatto passi in avanti sul piano interpretativo ma, come notifica il Fondo Monetario Internazionale (FMI), ad oggi «non esistono ancora definizioni¹⁴⁰, classificazioni o tassonomie coerenti a livello globale degli asset crittografici»¹⁴¹. Assodato ciò, scattare in questa sede una fotografia dei prodotti che hanno nel tempo affollato la galassia *crypto* può rivelarsi utile non solo ai fini di una

¹³⁸ [Schneepf N. et al., Introduzione a Web3: Guida, Oracle, 2023.](#)

¹³⁹ [Tedeschi E., Le Altcoin quali solide alternative al Bitcoin, 2022.](#) Il termine “altcoin” viene utilizzato per riferirsi

¹⁴⁰ Questo spiega anche la ragione per la quale nel corso di questa tesi non ci si imbatte in un'unica terminologia – ancorché vi sia una personale propensione verso espressioni come “digital asset”, “crypto-asset” o “cripto-attività” – ma si impiegheranno termini non totalmente appropriati sul piano tecnico, ma tollerati in quanto ricorrenti sul piano giuridico e/o accademico come “virtual asset” o “criptovalute”.

¹⁴¹ [Fondo Monetario Internazionale, Elements of effective policies for crypto assets, IMF Policy Paper, 2023.](#) In realtà, la questione appare evidente agli occhi di altre organizzazioni ed entità di rilievo, come ad esempio la Banca dei Regolamenti Internazionali (*Bank of International Settlement*) che rimarca il fatto che molte Autorità «utilizzano termini, definizioni e tassonomie diverse, che di solito dipendono dalla prospettiva in cui questi asset vengono analizzati (ad esempio tecnica, funzionale, legale). Ad esempio, termini come asset digitali, crypto-asset, asset virtuali o crypto token sono spesso utilizzati in modo intercambiabile». Ciò comporta, come notano ulteriormente Ocampo e altri ricercatori, «che qualsiasi analisi delle misure politiche in questo settore è complicata da incoerenze tra le varie giurisdizioni per quanto riguarda la classificazione delle attività considerate per definire se un attore è un fornitore di servizi a fini normativi». Per ulteriori approfondimenti si riporta l'articolo appena citato: [Ocampo D.G. et al., Crypto, Tokens and DeFi: navigating the regulatory landscape, FSI Insights on policy implementation No 49, 2023.](#)

maggior chiarezza terminologica o di una migliore comprensione del rapporto *genus/species* che intercorre tra i vari *asset*, ma anche per acquisire maggiore speditezza e capacità di orientamento nelle attività di ricerca afferenti a questi temi. Il raggiungimento di tale obiettivo richiede innanzitutto di individuare un termine-ombrello che possa “catturare” il maggior numero di categorie possibili. Inutile dire che anche su questo fronte aleggi ancora incertezza. Tuttavia, a seguito di svariate letture di settore, negli ultimi anni solo due espressioni sono riuscite a emergere con maggiore forza rispetto alle altre sia nel contesto normativo europeo che nelle pubblicazioni di autorità internazionali: “*digital asset*” e “*crypto-asset*”. Seppure trattati delle volte come sinonimi, in realtà la prima sembra avere una portata applicativa maggiore rispetto alla seconda poiché ricomprende anche le *Central Bank Digital Currency (CBDC)*.

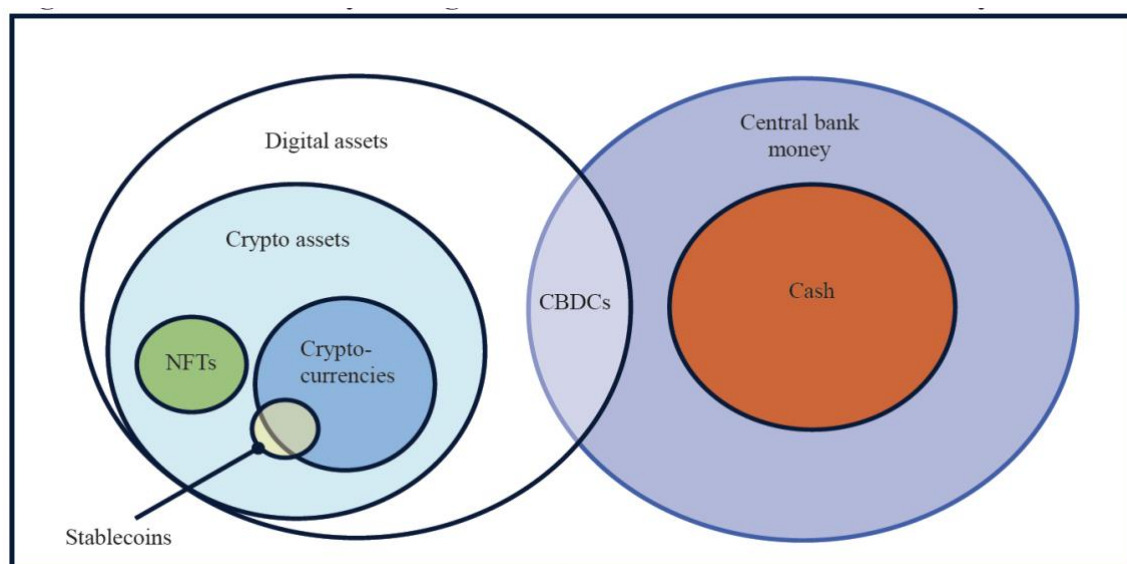


Figura 3 – Fonte: [AA.VV., Chapter 8. Digital Assets: Relearning Economic Principles, Economic report of the President, 2023.](#)

Inoltre, Assogestioni dà un’ampia e interessante definizione di *digital asset*, descrivendolo come una «*rappresentazione di un’unità elementare di informazione che può essere utilizzata in sistemi DLT-based. I digital asset sono ospitati all’interno di un ambiente digitale e memorizzati su una piattaforma blockchain che ne traccia le movimentazioni e i cambi di proprietà. I digital asset possono rappresentare beni di diversa natura, da un*

oggetto fisico a beni immateriali, come la moneta, i brevetti, i diritti d'autore»¹⁴². Trasferendo i concetti a livello visivo, questa visione appare confermata da un'immagine tratta dalla documentazione pubblicata dagli uffici governativi statunitensi (Figura 3). Nella sua semplicità, a parere di chi scrive, la mappatura proposta risulta esaustiva ed essenzialmente valida, ancorché generica e priva di ufficialità a livello internazionale e può essere usata come base per le considerazioni che verranno poste più avanti.

2.1. I crypto-asset: alla ricerca di una tassonomia condivisa

Come desumibile dalla figura appena richiamata, la famiglia dei *digital asset* si suddivide principalmente in due macrocategorie: *crypto-asset*¹⁴³ (anche denominate come cripto-attività) e *Central Bank Digital Currency (CBDC)*. Se i secondi (che verranno trattati nel secondo sotto-paragrafo) possono ritenersi un fenomeno recente, abbastanza coeso e formalmente omogeneo, lo stesso non può valere per i primi giacché nel tempo sin dal 2009 si sono sedimentate diverse applicazioni, ognuna con una propria funzione o segno distintivo. Prima dell'approdo del *MiCA*, la dottrina si è sin da subito gettata a capofitto nell'individuazione di un'appropriata categoria giuridica dove poter collocare i *crypto-asset*. C'è chi li ha definiti (e ancora li definisce) come una forma di moneta digitale non regolamentata, chi invece ritiene che svolgesse solo una parte delle tre classiche funzioni della moneta¹⁴⁴, chi addirittura invoca l'idea di una “non-moneta”¹⁴⁵, chi invece la equipara

¹⁴² Definizione ripresa da [Assogestioni, Oltre le criptovalute. Tecnologie a registro distribuito a servizio dell'asset management, 2022.](#)

¹⁴³ Volendo rapidamente descriverli, si prenderà in prestito la definizione di Auer e altri autori, chiamandoli «*asset digitali che utilizzano primitive crittografiche e tecnologie DLT e che rappresentano una risorsa economica o un valore per qualcuno*». [Auer R. et al., The Technology of Decentralized Finance \(DeFi\), BIS Working Papers No 1066, 2023.](#)

¹⁴⁴ Mezzo di scambio, riserva di valore e unità di misura. Per approfondire i profili storici ed evolutivi che hanno determinato nel tempo la formulazione di questa triade vds. De Bonis R. e Vangelisti, M.I., *Moneta. Dai buoi di Omero ai Bitcoin*, Il Mulino, 2019.

¹⁴⁵ Ulteriore problematica che hanno incontrato i regolatori, soprattutto in origine, era legata al fatto che persistevano differenti correnti di pensiero sulla stessa natura dei *crypto-asset* che all'atto pratico andavano ad incidere sulla possibilità o meno di sottoporre le relative transazioni alla normativa antiriciclaggio. In tal senso, l'Italia e più in generale l'Europa hanno svolto un ruolo pionieristico nel cercare di regolamentare gli aspetti connessi agli adempimenti antiriciclaggio e alla tassabilità delle operazioni di “incrocio” tra moneta reale ed asset virtuale, muovendo da un assunto, secondo il quale, nonostante l'utilizzo equivoco dei termini “criptovaluta” o “criptomoneta”, ci troviamo di fronte ad una “non-moneta”, che rappresenta pur sempre l'espressione digitale di un valore suscettibile di una valutazione economica da parte di coloro che ne accettano la negoziazione. Tuttavia, anche quest'ultima teoria sembra stridere alla luce di recenti accadimenti quali

a una moneta elettronica,¹⁴⁶ fino ad arrivare a ipotesi più sofisticate come sistemi di pagamento, strumenti di investimento, beni in senso civilistico¹⁴⁷, beni rifugio¹⁴⁸,

l'adozione del *bitcoin* come moneta avente valore legale da parte di El Salvador e della Repubblica Centrafricana.

¹⁴⁶ Prima della *MiCA*, i concetti di moneta elettronica e criptovaluta non erano affatto sovrapponibili, potendo esprimere al massimo, quale punto di contatto, la forma digitale degli strumenti e delle piattaforme a loro connessi. Le monete elettroniche, infatti, costituiscono un surrogato digitale di monete aventi corso legale, memorizzate su un dispositivo elettronico, come una carta a microprocessore o una memoria di elaboratore, e generalmente destinate ad effettuare pagamenti di importo limitato. La più evidente differenza stava nel fatto che prima dell'approdo del *MiCA* per i *crypto-asset* non esisteva una specifica ed organica regolamentazione, tanto che sfuggiva la possibilità di darne una qualificazione giuridica; invece, le monete elettroniche risultavano ampiamente normate nei diversi ordinamenti. Ne derivava che gli emittenti moneta virtuale non erano soggetti alla disciplina prudenziale e di sorveglianza cui sono invece sottoposti gli emittenti di moneta elettronica, ai quali invece è dedicata una apposita regolamentazione. In particolare, le monete elettroniche sono state disciplinate dall'Unione Europea in un primo momento con la direttiva del Parlamento europeo e del Consiglio 2000/46/CE 18 settembre 2000 (recepita in Italia con Legge 1° marzo 2002, n. 39), poi abrogata e sostituita dalla direttiva del Parlamento europeo e del Consiglio 2009/110/CE del 16 settembre 2009 (recepita in Italia con D. Lgs. 16 aprile 2012, n. 45). L'art. 2 di quest'ultima direttiva definisce la moneta elettronica come «*il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento ... e che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica*». La moneta elettronica, pertanto, incorpora un diritto di credito vantato dal titolare nei confronti dell'istituto emittente. Più in particolare, i criteri utilizzati dalla direttiva per identificare una moneta elettronica sono la conservazione elettronica, la disposizione di fondi in quantità non inferiore al valore monetario emesso, la comune e diffusa accettazione quale mezzo di pagamento.

A differenza del "titolo di credito" rappresentato dalla moneta elettronica, le criptovalute esprimono un valore che non dipende da alcuna Autorità finanziaria esterna/centrale, non facendo riferimento ad alcuna valuta corrente con valore legale, salvo dover procedere ad ulteriori operazioni di conversione. Ulteriore differenza sta nel requisito della disponibilità della provvista di denaro a monte dello scambio, che non sussiste per le criptovalute, anche in considerazione dell'attività di *mining* che consente di generare la stessa moneta in assenza di alcun sottostante. Nei sistemi di moneta elettronica il legame con le monete tradizionali sottostanti ha un fondamento legale, in quanto la stessa è assistita dalla garanzia di costante rimborsabilità. L'art. 11 della Direttiva prevede, in particolare, che gli emittenti di moneta elettronica rilascino la moneta elettronica al valore nominale e dietro ricevimento di fondi e che, su richiesta del detentore della moneta elettronica, gli emittenti rimborsino, in qualsiasi momento e al valore nominale, il valore monetario della moneta elettronica detenuta. Per i *Bitcoin* l'unità di conto è puramente virtuale, priva di un valore legale, e la loro emissione non avviene dietro rimessa di moneta legale, né sussistono condizioni di costante rimborsabilità.

Punti di contatto con la moneta elettronica sono, quindi, veramente limitati e riferibili ai citati requisiti della conservazione con modalità elettroniche ed alla comune e diffusa accettazione dello strumento quale mezzo di pagamento, peraltro meno nitida per le criptovalute (se consideriamo la più ristretta base di consenso).

¹⁴⁷ [Sartori N., *Le valute virtuali e il trattamento fiscale dei proventi a esse connessi*, Università degli Studi di Milano-Bicocca, 2023.](#)

¹⁴⁸ Più recentemente, molti analisti hanno evidenziato come non sono solo l'oro, lo *yen*, il franco svizzero o il *bund* tedesco beneficino della volatilità delle Borse mondiali, ma, paradossalmente, anche determinate cripto-attività, che crescono quando i mercati tradizionali sono in tensione, come un qualsiasi "bene rifugio". [Arnoldi B., *Bitcoin è un bene rifugio come oro e diamanti? Parlano gli esperti*, Everyeye.it, 2023.](#)

*commodity*¹⁴⁹, *security*¹⁵⁰ o più in generale strumenti finanziari¹⁵¹ e via scorrendo. Altrettanti sforzi sono stati profusi in merito alla ricerca di definizioni esaustive, ma il risultato ottenuto non sembra aver messo ordine sul tema, bensì l'opposto¹⁵². Inoltre, la mancanza di uniformità sembra dipendere principalmente dal contesto (ad esempio, tecnico o legale) e dai quadri giuridici¹⁵³. Non deve inoltre stupire come questa frammentarietà

¹⁴⁹ [Adami A., Bitcoin ed Ethereum classificate come commodity: la sentenza definitiva di un tribunale di New York, The Cryptonomist, 2023.](#) «Secondo un giudice di New York sia Bitcoin che Ethereum, le prime due criptovalute per capitalizzazione di mercato, possono essere considerate commodity per via della loro natura decentralizzata. A stabilirlo è stato lo stesso giudice che si occupa della causa SEC vs Coinbase, che con l'ultima affermazione sta orientando il dibattito pubblico in riferimento alla presunta violazione dell'exchange delle leggi sui titoli statunitensi».

¹⁵⁰ [Fior T., Gary Gensler salva solo Bitcoin: tutte le crypto sono security, Cryptofacili, 2023.](#)

¹⁵¹ La ricostruzione normativa che giustifica tale interpretazione verrà riportata per motivi di carattere organizzativo nella sezione successiva.

¹⁵² [Monetario Internazionale, Virtual Assets and anti-money laundering and combating the financing of terrorism \(1\) – Some legal and practical considerations, 2021.](#) Ad esempio, a detta del Fondo Monetario Internazionale, «sebbene il GAFI abbia definito chiaramente i Virtual Assets come «una rappresentazione digitale di valore che può essere scambiata o trasferita digitalmente e può essere utilizzata per scopi di pagamento o di investimento», diverse altre terminologie sono frequentemente utilizzate in contesti diversi per coprire asset simili. Tuttavia, non hanno una definizione concordata a livello internazionale. Ecco alcuni esempi:

i) crypto-asset. Il FMI, in alcune delle sue pubblicazioni più recenti, fa riferimento ai crypto-asset, che definisce come «rappresentazioni digitali del valore, rese possibili dai progressi della crittografia e della tecnologia dei ledger distribuiti»;

ii) criptovalute. Molti altri si riferiscono alle criptovalute generalmente intese come «beni digitali progettati per funzionare come mezzo di scambio in cui i record di proprietà delle singole monete sono memorizzati in un libro mastro esistente nella forma di un database computerizzato che utilizza una forte crittografia per proteggere i record delle transazioni, per controllare la creazione di monete aggiuntive e per verificare il trasferimento della proprietà delle monete. In genere non esiste in forma fisica (come la carta-moneta) e non è emessa da un'autorità centrale»;

iii) stablecoin e global stablecoin. Il Financial Stability Board considera le stablecoin come «un tipo di crypto-asset che mira a mantenere un valore stabile rispetto a un'attività specifica, o a un pool o paniere di attività». Le cosiddette GSC includono iniziative, come Diem (in precedenza Libra), costruite su una base di clienti esistente ampia e/o transfrontaliera, che hanno il potenziale di scalare rapidamente per raggiungere un'impronta globale o un'altra impronta sostanziale. Il GAFI ritiene che il termine «stablecoin» non sia una chiara categoria legale o tecnica, ma sia principalmente un termine di marketing utilizzato dai promotori di tali monete. Per evitare di avallare involontariamente le loro affermazioni, il GAFI si riferisce ad esse come «cosiddette stablecoin». Le monete indicate come «global stablecoin» nei rapporti del G20 e in altri rapporti sono denominate «cosiddette stablecoin con il potenziale per un'adozione di massa» ai fini del GAFI per lo stesso motivo».

¹⁵³ La terminologia utilizzata per descriverle varia moltissimo nelle diverse giurisdizioni. A tal proposito si riportano dati contenuti all'interno dell'indagine personalmente condotta: **virtual asset** (adottata dalla maggior parte dei Paesi che hanno recepito le raccomandazioni AML/CFT del GAFI); **crypto-asset** (Giappone, Indonesia, Regno Unito, UE, Uzbekistan); **digital asset** (Antigua e Barbuda, Bahamas, Bermuda, Francia, Thailandia, Malesia, Nigeria); **digital currency** (Argentina, Australia, Kazakistan, Russia); **digital crypto currency** (Comore); **digital token** (Albania, Bielorussia); **virtual currency** (Austria, Bulgaria, Canada, Finlandia, Guatemala, Lituania, Norvegia, Polonia, Romania, Slovacchia, Slovenia, Spagna, Taiwan); **virtual digital asset** (India); **utility token** (Anguilla). Da questa angolazione, il mondo del diritto potrebbe assimilarsi ad una torre di Babele, dove ognuno parla una lingua composta da propri «originali» vocaboli, cosicché «ci saranno tante

traspaia anche dalle classificazioni. Soffermandoci su quest'ultimo aspetto, difficilmente ci si imbatte in studi in cui tutte queste divergenze vengono raccolte sotto un unico sguardo d'insieme, dando così la possibilità di scorgere le reali interrelazioni tra i vari *crypto-asset*. Se da un lato è indubbio che radunare in modo schematico tutte le tipologie esistenti non sia un compito agevole, tuttavia, al pari degli istituti giuridici, anche i *digital asset* possono essere classificati in molteplici modalità a seconda del criterio-base previamente selezionato. Una prima possibile distinzione potrebbe essere fatta in base alla loro struttura di *governance*, con la divisione principale tra quelli centralizzati e quelli decentralizzati, come rappresentato dalla Figura 4.

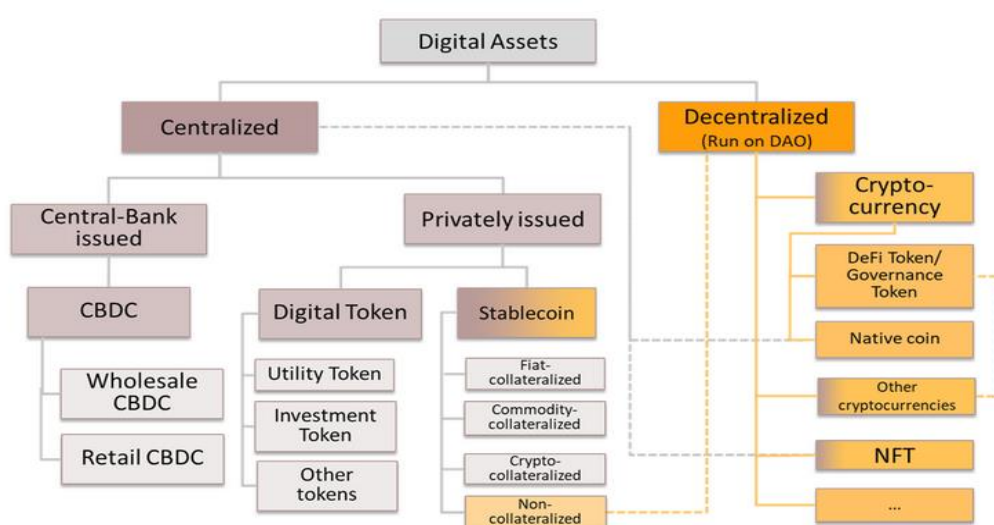


Figura 4 – Fonte: [Krungsri Research, Digital Asset \(Part 1\) “When Thais are drawn towards digital assets”, 2023.](#)

Estraendo le parole della *Krungsri Research*, «si definiscono asset digitali centralizzati quelli per i quali un'autorità centrale controlla l'emissione o il valore dell'asset. Questi possono

lingue quanti sono i giuristi e ciascuno dedicherà la maggior parte dei propri studi a rintracciare le differenze tra la propria lingua e quella di altri». Ferrajoli L., Teoria assiomatica del diritto. Parte generale, 1970, p. 2, il cui studio sul linguaggio giuridico è finalizzato all'elaborazione di una teoria «del tutto indipendente dai valori politici che di fatto informano il sistema giuridico teorizzato» al fine di consentire al medesimo di esplicitare quegli stessi valori e di «svelarne le antinomie» con l'obiettivo di «richiamare il giurista alla responsabilità sociale del suo lavoro, rendendolo consapevole della convenzionalità delle sue assunzioni... (omissis)...sollecitandone l'impegno non solo scientifico, ma anche civile e politico, in una loro fondazione argomentata coerente e controllata», p. 10.

essere ulteriormente suddivisi in base al tipo di autorità emittente. Gli asset digitali emessi privatamente includono i token digitali e le stablecoin, mentre gli asset emessi dalle banche centrali sono attualmente limitati alle valute digitali delle banche centrali, o CBDC. Al contrario, gli asset digitali decentralizzati sono emessi senza che il volume o il valore dell'asset sia controllato dall'emittente. Sono generalmente strutturati come organizzazioni autonome decentralizzate (DAO) e possono essere suddivisi in diverse categorie principali, come criptovalute, NFT e altri tipi di asset digitali. Tuttavia, a prescindere dal tipo di struttura di governance che può essere in vigore per determinati asset digitali, il mercato di questi ultimi è globale e senza confini, e quindi l'estrema volatilità che gli asset digitali possono sperimentare ha il potenziale per colpire gli investitori in ogni angolo del mondo»¹⁵⁴. Se si vuole invece scendere maggiormente nel dettaglio, la Figura 5 permette di visionare altre accreditate modalità di suddivisione dei *crypto-asset*. Più in generale, il pregio di questa immagine sta nella sua capacità di contenere molteplici schematizzazioni in una, a seconda della prospettiva da cui li si intende osservare. Tra le più note da segnalare vi sono le classificazioni basate su:

- **token nativi/non-nativi**¹⁵⁵: mentre i primi si sostanziano in una ristretta categoria di *token* aventi una propria *blockchain* autonoma e indipendente in cui circolare¹⁵⁶, i *token* non nativi invece si appoggiano a reti *blockchain* già esistenti¹⁵⁷;

¹⁵⁴ «Per questo motivo, sono cresciuti i timori per la crescita a rotta di collo che ha gonfiato il mercato in modo massiccio negli ultimi anni. Molte organizzazioni hanno espresso preoccupazione per la rapida espansione della minaccia che ciò rappresenta per la stabilità finanziaria. I suggerimenti per una migliore gestione e supervisione degli asset digitali sono stati avanzati, tra l'altro, in occasione delle riunioni del Comitato di Basilea per la vigilanza bancaria (BCBS), del Financial Security Board (FSB) e dell'International Organization of Securities Commissions (IOSCO). La regolare segnalazione della volatilità del mercato e il conseguente rischio di enormi perdite per gli investitori hanno incoraggiato le autorità a riconoscere l'importanza di porre dei firewall per evitare che il contagio dai mercati degli asset digitali si ripercuota su altre parti del settore finanziario. È quindi essenziale che la supervisione regolamentare si metta al passo e tenga il passo con la dinamica di rapido sviluppo che ha caratterizzato lo spazio degli asset digitali. Detto questo, le autorità di regolamentazione dovranno anche bilanciare l'esigenza di garantire la sicurezza del sistema finanziario con la necessità di mantenere uno spazio entro il quale il settore possa continuare a prosperare e innovare». [Krungsri Research, Digital Asset \(Part 1\) "When Thais are drawn towards digital assets", 2023.](#)

¹⁵⁵ In altri contesti, questa differenziazione viene attuata utilizzando terminologie lievemente diverse, ossia *coin* (o *token* nativi) e *token* (o *token* non nativi).

¹⁵⁶ È il caso dei *bitcoin* nella rete *Bitcoin*, *ether* nella rete *Ethereum*; *algorand* nella rete *Algorand*; *ADA* nella rete *Cardano*, e così via.

¹⁵⁷ Ne sono un esempio *Uniswap (UNI)* o *ChainLink (LINK)* che circolano sulla rete di *Ethereum*.

- **fungibili/infungibili:** come vedremo più avanti, le disposizioni del *MiCA* possono applicarsi solo in caso di fungibilità dell'*asset*. Pertanto, debbono escludersi dal suo ambito di competenza i cd. *Non-Fungible Token (NFT)*¹⁵⁸, unità digitali registrate sulla *blockchain* che certificano l'autenticità di un determinato bene, che può essere detenuto e scambiato facilmente. I *token* fungibili¹⁵⁹ invece sono intrinsecamente indistinguibili e possono essere usati per molteplici scopi¹⁶⁰.
- **Privacy-focused/transparent:** in base a questa distinzione vi sono *asset* con cui è possibile realizzare transazioni anonime (*ZCash* o *Monero*) o trasparenti (*bitcoin*).

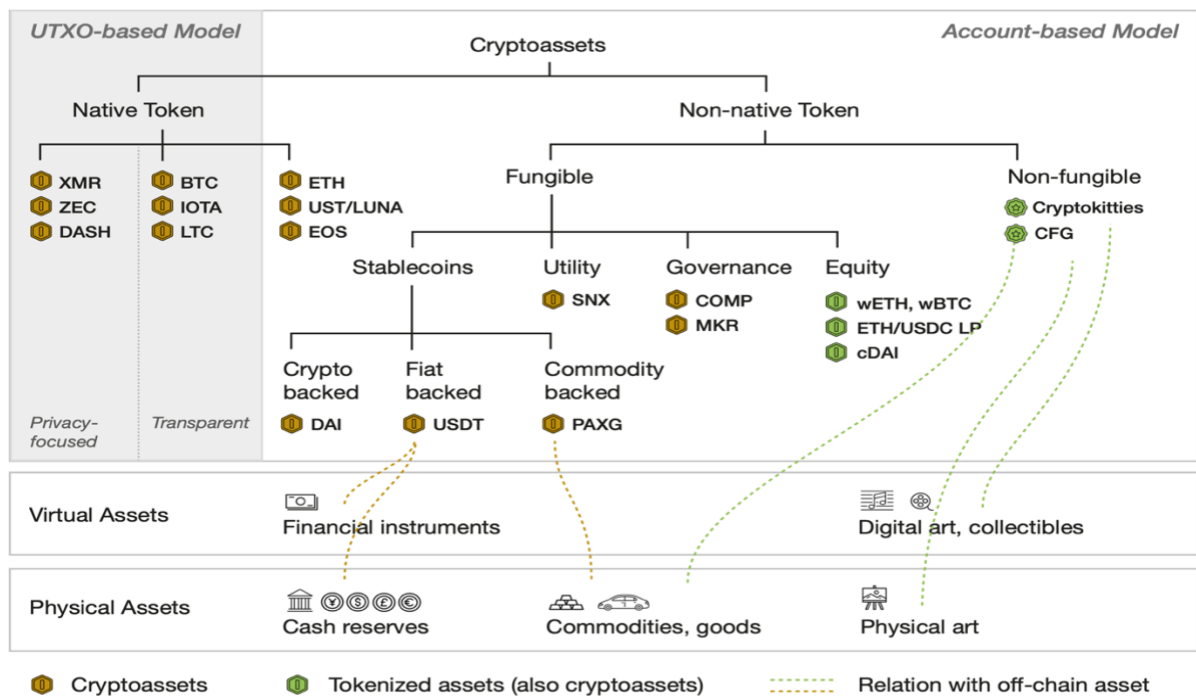


Figura 5 – Fonte: [Auer R. et al., The Technology of Decentralized Finance \(DeFi\), BIS Working Papers No 1066, 2023.](#)

Parimenti con la *DLT* e le altre *crypto technology*, dinanzi alle svariate possibilità di suddividere le crypto-attività, il Legislatore europeo attraverso il *MiCA* ha voluto imprimere

¹⁵⁸ L'estrema notorietà dei *NFT* nel 2021 ha permesso di introdurre il concetto di "scarsità digitale". Per ulteriori approfondimenti sul tema vds.

¹⁵⁹ [Auer R. et al., The Technology of Decentralized Finance \(DeFi\), BIS Working Papers No 1066, 2023.](#)

¹⁶⁰ Tra i più diffusi si annoverano i) *utility token*; ii) *security token*; iii) *payment token*.

la propria prospettiva anche su questo aspetto, stabilendo una personale tassonomia che verrà illustrata nella sezione a seguire, unitamente all'analisi giuridica dei *CASP*.

2.2. Central Bank Digital Currency (CBDC): possibile allargamento della strumentazione dei CASP?

Il paragrafo in esame integra la seconda macrocategoria prospettata nella Figura 3: la *Central Bank Digital Currency (CBDC)*. Si tratta, in sintesi, di una vera e propria valuta digitale di Stato giacché annoverabile come passività diretta di una Banca Centrale che ha assunto «una forma digitale di moneta della Banca Centrale diversa dai saldi dei tradizionali conti di riserva o di regolamento»¹⁶¹.

Di primo acchito, può apparire stridente discorrere di valute digitali emesse da Banche Centrali all'interno di una tesi vertente sui fornitori di crypto-attività. A ben pensarci, però, il nesso non pecca di asimmetria. Al contrario, a parere di chi scrive, la versione digitale delle valute *fiat* non solo potrebbe essere vista come una potenziale estensione della strumentazione dei *provider*, i quali sono dotati della tecnologia necessaria per poter applicare buona parte degli stessi servizi che già erogano in regime di *crypto-asset*, ma almeno in teoria costituisce l'anello di congiunzione tra *TradFi* e *CeFi*, annichilendo le relative differenze concettuali tra queste dimensioni. È di questa idea anche Antonovici, il quale afferma che la dimensione «*CeFi può sovrapporsi al TradFi quando è coinvolto il denaro fiat*»¹⁶².

Andando ora a rintracciare rapidamente gli aspetti salienti della sua ascesa, l'ideazione di tale mezzo innovativo è sorta come spontanea reazione istituzionale in opposizione all'adozione crescente dei *crypto-asset* nell'ultimo quindicennio. Segnatamente, è possibile ricostruire in maniera semplificata i passaggi essenziali che hanno portato all'introduzione delle *CBDC*:

- **Nascita del *bitcoin*.** Come già richiamato nel primo capitolo, a seguito della Grande Recessione (o *Global Financial Crisis*), la rete infrastrutturale finanziaria si manifesta in

¹⁶¹ [World Economic Forum, Central Bank Digital Currency. Global Interoperability Principles, White Paper, 2023.](#)

¹⁶² [Antonovici A., TradFi vs CeFi vs DeFi: Here's how they differ, TastyCrypto, 2023.](#)

tutta la sua fragilità sistemica scatenando nella popolazione mondiale un generalizzato clima di sconcerto e sfiducia verso l'apparato creditizio, all'epoca difficile da risollevare. Con tempismo pressoché sincronico, nei primi giorni del 2009 affiorano concretamente dalla visione di Satoshi Nakamoto novità come la *blockchain* e il *bitcoin* che, assieme ad altre applicazioni, propongono una nuova modalità di concepire i servizi finanziari, facendo affidamento all'incorruttibilità di codici e programmi crittografati, unitamente a transazioni immediate e basate su una gestione decentralizzata;

- **Problema della volatilità del *bitcoin* e successiva introduzione delle cd. *stablecoin*.**

Nel corso degli anni successivi ci si rende conto che buona parte degli *asset* come il *bitcoin* siano caratterizzate da un'estrema volatilità, sollevando i primi dubbi in merito a un loro utilizzo sicuro come mezzo di scambio. La ricerca di un'alternativa che possa mantenere i vantaggi poc'anzi richiamati, integrando al contempo una maggiore stabilità, porta all'affiorare delle cd. *stablecoin*, ossia *crypto-asset* con un valore economico non fluttuante giacché ancorate (*pegged*) a un bene stabile. La modalità più semplice per garantire questa circostanza consiste nel sorreggere il valore delle *stablecoin* per mezzo di valute *fiat* (*fiat-collateralized stablecoin*). Facendo ciò, le *stablecoin* sono «supportate dalla piena fiducia e dal credito dell'emittente di fiat, il cui valore viene garantito dalla banca centrale di quella nazione»¹⁶³. Col tempo si instaurano forme di ancoraggio sempre più sofisticate basate su prodotti crittografici (*crypto-collateralized stablecoin*), materie prime (*commodity stablecoin*) fino all'utilizzo di modelli decentralizzati basati su algoritmi (*algorithmic stablecoin*, come nel caso di Terra/LUNA)¹⁶⁴.

- **Progetto *Diem* (ex *Libra*): minaccia delle “monete” digitali private.** Sulla scorta di quanto detto sopra, presto si fa largo tra i soggetti privati l'idea di emettere una propria moneta digitale. Ne è un esempio *Libra*¹⁶⁵ (poi convertitosi nel progetto *Diem*) di *Facebook* (ora *Meta*). Superata l'euforia iniziale e spuntate problematiche di vario

¹⁶³ [Sephron C., Come le stablecoin rimangono stabili, spiegato semplicemente, CoinTelegraph, 2021.](#)

¹⁶⁴ [Carbone F., Terra LUNA e UST: tutto sul drammatico crollo dello stablecoin, Fintastico, 2022.](#)

¹⁶⁵ Lo scopo di *Libra* è quello di creare una valuta accettata universalmente e che permetta ad una platea illimitata di utenti di accedere a servizi finanziari a basso costo. Più in particolare, «l'obiettivo di *Libra Blockchain* è quello di fungere da solida base per i servizi finanziari, inclusa una nuova valuta globale, in grado di soddisfare le esigenze finanziarie quotidiane di miliardi di persone».

genere, nessuna delle due iniziative riesce mai a decollare ed essere effettivamente lanciata sul mercato, concludendosi alla fine con un nulla di fatto. Al di là dell'insuccesso registratosi, l'annuncio di *Libra/Diem* non manca di suscitare clamore (e conseguente timore) tra gli addetti ai lavori e gli esponenti politici di tutto il mondo. Hughes all'epoca evidenziava come l'influenza di *Facebook* non avesse eguali nel settore privato, superando persino quella dello stesso governo americano; questo perché combinando la sua rete con quella di *WhatsApp* e di *Instagram* (entrambe di sua proprietà) era capace di determinare, attraverso degli algoritmi, «*chi vede che cosa*». Se poi a ciò si aggiunge che *Meta* supera il PIL di intere nazioni, l'intenzione di dotarsi di una propria “moneta”¹⁶⁶ appariva una mossa in aperta competizione con gli Stati sovrani. In quest'ottica, la vera rivoluzione non sarebbe più la creazione del *bitcoin* (asset decentralizzato) ma quella di una moneta privata (dal sapore haeyekiano)¹⁶⁷ in grado di imporsi su di una platea di utenti/consumatori/investitori di oltre 2 miliardi di persone, superando potenzialmente la diffusione di valute come il dollaro o l'euro. Come scriveva sempre Chris Hughes dalle pagine del *Financial Times*¹⁶⁸, «*quello che i sostenitori della Libra chiamano “decentralizzazione” grazie alla blockchain è in realtà uno spostamento di potere dalle Banche Centrali dei paesi in via di sviluppo verso le multinazionali*».

- **Consequente reazione delle Banche Centrali.** Nonostante l'esito disastroso di *Libra/Diem*, «*le Banche Centrali non sono di certo rimaste immobili dinanzi a questo importante cambiamento*»¹⁶⁹, correndo ai ripari mediante una nuova forma di moneta diversa da quella cd. elettronica, indissolubilmente legata alla Banca che la emette. Da qui, l'ideazione delle *Central Bank Digital Currencies*. Tuttora, come testimonia il *tracker* di *Atlantic Council*¹⁷⁰, ciascun Paese si trova in una determinata fase del ciclo di produzione delle CBDC: vi sono molti Paesi che si trovano sia in fase ancora esplorativa e di ricerca che in fase di sviluppo/progettazione (tra questi anche l'Unione Europea che recentemente ha presentato una proposta di Regolamento sull'Euro Digitale, che si

¹⁶⁶ Attraverso un'infrastruttura *DLT permissioned*, che, a differenza della *blockchain* distribuita, si basa su strumenti di *governance* centralizzati.

¹⁶⁷ Von Hayek F. A. *La denazionalizzazione della moneta*, Rubbettino, 2018.

¹⁶⁸ Cfr. [Hughes C., Facebook co-founder: Libra coin would shift power into the wrong hands. Regulators should not underestimate the digital currency's disruptive potential, Financial Times, 2019.](#)

¹⁶⁹ [PWC, Central Bank Digital Currency, 2023.](#)

¹⁷⁰ [Atlantic Council, Central Bank Digital Currency Tracker, 2023.](#)

inserisce all'interno del c.d. *Single Currency Package*¹⁷¹), altri ancora invece sono in circostanze avanzate giacché stanno testando progetti pilota o hanno già lanciato una propria valuta digitale¹⁷².

A titolo di completezza, la ricostruzione appena proposta, per quanto veritiera, mette in luce solo l'aspetto politico-istituzionale della questione. In realtà, le ragioni che hanno spinto determinate autorità governative a progettare (o quanto meno valutare seriamente la possibilità di creare) una propria valuta digitale sono molteplici e non si esauriscono meramente nella strenua difesa della propria sovranità monetaria. Si tratta di un'osservazione peraltro avvalorata dalle parole dell'attuale Direttrice Generale del Fondo Monetario Internazionale, Kristalina Georgieva, la quale afferma che *«non esiste un caso universale per le CBDC perché ogni economia è diversa. In alcuni casi, una CBDC può essere un percorso importante per l'inclusione finanziaria, ad esempio quando la geografia è un ostacolo alla banca fisica. In altri casi, una CBDC potrebbe fornire un supporto essenziale in caso di fallimento di altri strumenti di pagamento. Uno di questi casi è stato quello in cui la Banca Centrale dei Caraibi Orientali ha esteso il suo progetto pilota di CBDC alle aree colpite da un'eruzione vulcanica lo scorso anno. Le Banche Centrali dovrebbero quindi adattare i piani alle loro specifiche circostanze ed esigenze»*¹⁷³.

¹⁷¹ Si tratta di un «“pacchetto” di norme avente l'obiettivo di “fare in modo che i cittadini e le imprese possano continuare ad accedere alle banconote e alle monete in euro, utilizzandole per i pagamenti in tutta la zona euro, e per definire il quadro relativo a un possibile nuovo formato digitale dell'euro” e contenente anche una proposta di regolamento sul corso legale del contante in euro. Secondo gli obiettivi della Commissione, il “pacchetto moneta unica”, garantirà ai cittadini e alle imprese di poter utilizzare una forma di “moneta digitale” che possa essere ampiamente accettata, economica e sicura. I pagamenti in forma elettronica sono, infatti, oggi possibili solo grazie alla necessaria intermediazione di enti privati (istituti di credito, di pagamento e di moneta elettronica) e non, quindi, tramite la spendita di moneta emessa e distribuita dalla Banca Centrale Europea (BCE), così come avviene per quella “cartacea”. La Proposta di Regolamento sull'euro digitale mira proprio a superare questo “gap” istituendo uno strumento di pagamento informatico “di Stato” che si pone in diretta concorrenza con i sistemi di pagamento elettronici già offerti dal settore privato». [Furnari S.L. e Schettini D., Euro digitale: primi commenti alla Proposta di Regolamento. Tra innovazione tecnologia e adozione di massa, 2023.](#)

¹⁷² È il caso della Nigeria che ha lanciato la sua *eNaira* nell'ottobre 2021 o della *Eastern Caribbean Central Bank* (Banca centrale dei Caraibi orientali), la quale alcuni mesi prima (marzo 2021) ha emesso la *DCash*.

¹⁷³ Georgieva K., *The Future of Money: Gearing up for Central Bank Digital Currency*, International Monetary Fund (IMF), 2022.

Al riguardo, lo studio del *World Economic Forum* racchiude le motivazioni¹⁷⁴, intrecciate tra loro, alla base dell'emissione di una propria *CBDC* che possono così riepilogarsi:

- **Innovazione, efficienza e sicurezza dei pagamenti:** al pari dei prodotti *crypto*, le *CBDC* dimostrano di essere altrettanto affidabili sul versante dei pagamenti. Difatti, l'obiettivo è offrire transazioni più rapide e sicure, riducendo la dipendenza dagli intermediari tradizionali e minimizzando i tempi di regolamento. Dietro questi evidenti vantaggi, vi sono però delle sfide da affrontare, *in primis* la salvaguardia della *privacy* degli utenti e della protezione dei dati (es. garantendo l'anonimato o lo pseudonimato, bilanciando al contempo le esigenze di trasparenza e supervisione normativa). Per farlo sarà necessario costruire programmi e sistemi resilienti e proteggerli dalle minacce informatiche attraverso misure volte a garantire e preservare la fiducia dei consumatori nello strumento di pagamento (es. protocolli di crittografia e autenticazione);
- **Inclusione finanziaria:** la digitalizzazione dei sistemi di pagamento e delle monete, oltre a costituire un passaggio rilevante per le giurisdizioni intenzionate a tenere il passo con i progressi tecnologici globali, rappresenta un mezzo potente per promuovere l'inclusione finanziaria, attraendo segmenti di popolazione *unbanked* al fine di coinvolgerli nell'accesso a servizi finanziari e altre opzioni di pagamento digitale a prezzi accessibili;
- **Maggiore controllo della politica monetaria con potenziali ripercussioni positive sul piano della stabilità economica e della compliance:** l'adozione di *crypto technology* in forma centralizzata può drasticamente migliorare la messa in atto della politica monetaria nonché la stabilità economica di un Paese. Inoltre, sebbene il modello di sorveglianza cinese rappresenti un chiaro caso estremizzato, il controllo delle transazioni delle *CBDC* potrebbe inficiare positivamente in merito all'attività di monitoraggio delle autorità di vigilanza, con benefici in termini di conformità normativa e tutela dell'integrità finanziaria;

¹⁷⁴ [World Economic Forum, Central Bank Digital Currency. Global Interoperability Principles, White Paper, 2023.](#)

- **Motivi geopolitici e geoeconomici:** l'interesse per le valute digitali può essere dettato anche da questioni strategiche di vario tipo. A titolo di esempio, possono offrire una minore dipendenza da sistemi di pagamento stranieri o mitigare i rischi geopolitici associati a interruzioni, sanzioni o tensioni politiche che coinvolgono tali sistemi, così da aumentare la propria resilienza finanziaria e ridurre la propria vulnerabilità alle pressioni esterne. Altra funzione è quella di facilitare transazioni transfrontaliere più rapide, efficienti e a basso costo. Più in generale, l'adozione delle *CBDC* può influenzare le scelte dei Paesi in materia di alleanze e *partnership* finanziarie e rimodellare le dinamiche geopolitiche e le strutture di potere, portando potenzialmente a riallineamenti nei sistemi economici e finanziari globali.

Ovviamente, in merito all'elenco appena stilato, *«è importante notare che, sebbene queste priorità si allineino a livello globale, gli approcci specifici, le strategie di attuazione e l'enfasi su ciascuna priorità possono variare a seconda dei contesti economici, culturali e normativi delle diverse regioni»*¹⁷⁵.

Da ultimo, indipendentemente dalle finalità perseguite e dopo aver superato le prime fasi di *assessment*, le Banche Centrali sono chiamate ad affrontare una sfida tecnico-giuridica consistente nella scelta del modello di emissione della *CBDC*. Difatti, come già indirettamente accennato nella Figura 4, le *CBDC* *«possono essere destinate all'uso all'ingrosso (wholesale) - cioè solo per le transazioni tra istituzioni finanziarie - o al dettaglio (retail), cioè aperte al pubblico in generale. Le CBDC all'ingrosso consentono nuove modalità per mettere il denaro della banca centrale a disposizione delle istituzioni finanziarie regolamentate. Le CBDC al dettaglio differiscono fondamentalmente dall'attuale moneta elettronica nelle mani delle famiglie e delle imprese non finanziarie, che costituisce una passività per le istituzioni finanziarie. Le CBDC al dettaglio, come il contante, sono un credito diretto nei confronti della banca centrale»*¹⁷⁶.

¹⁷⁵ [World Economic Forum, Central Bank Digital Currency. Global Interoperability Principles, White Paper, 2023.](#)

¹⁷⁶ [Auer et al., Rise of the Central Bank Digital Currencies, International Journal of Central Banking, 2023.](#)

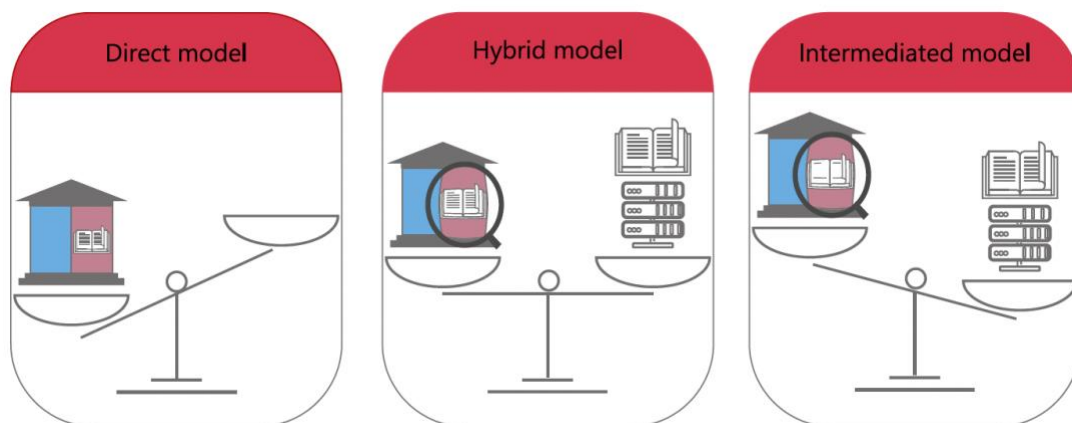


Figura 6 – Fonte: [Auer R. e Böhme R., *Central bank digital currency: the quest for minimally invasive technology*, BIS Working Papers n. 948, 2021.](#)

In altri termini, schematizzando le teorie di Auer e Böhme, la Figura 6 mostra le tre possibili modalità di comporre una CBDC:

- **«Direct model (modello diretto).** Secondo questo modello, la Banca Centrale emette e gestisce direttamente la CBDC. Ha il controllo completo dell'intero processo, compresa l'emissione, la distribuzione e il rimborso. La banca centrale mantiene il libro mastro digitale e garantisce la sicurezza e l'integrità della CBDC. I privati e le imprese possono detenere conti CBDC direttamente presso la banca centrale, senza dover ricorrere a intermediari finanziari tradizionali;
- **Two-Tier CBDC Model (modello CBDC a due livelli).** Nel modello a due livelli, la Banca Centrale collabora con le banche commerciali o altri intermediari finanziari per la distribuzione e l'accessibilità delle CBDC. La banca centrale emette le CBDC agli intermediari, che a loro volta forniscono servizi di CBDC al pubblico. Gli intermediari fungono da collegamento tra la banca centrale e gli utenti, offrendo conti, servizi di pagamento e altre funzionalità relative alla CBDC. Questo modello sfrutta l'infrastruttura finanziaria esistente mantenendo il controllo della banca centrale;

- **Hybrid Model (modello ibrido).** *Il modello ibrido combina elementi sia del modello diretto che di quello a due livelli. Consente l'emissione e la gestione diretta delle CBDC da parte della Banca Centrale, pur coinvolgendo gli intermediari per alcuni aspetti. In questo modello, la banca centrale può fornire conti CBDC direttamente al pubblico, come nel modello diretto. Tuttavia, può anche collaborare con gli intermediari per servizi o funzionalità specifiche, come l'assistenza ai clienti, l'onboarding o l'elaborazione delle transazioni. Il modello ibrido mira a trovare un equilibrio tra il controllo della banca centrale e lo sfruttamento delle istituzioni finanziarie esistenti»¹⁷⁷.*

¹⁷⁷ [Chandra A., CBDC: Design Principles, Medium, 2020.](#) Per una lettura più dettagliata sulle CBDC si veda [BRI, Central bank digital currencies, 2018](#) (vds. anche commento di [Paesani P., Bitcoin di Stato? Il caso della moneta digitale di Banca Centrale, 2018](#)). Con riferimento al rapporto tra token-based system e CBDC, si veda [Kahn C. M., Rivadeneyra F. e Wong T. N., Should the central bank issue e-money?, 2018](#); [Auer R. e Claessens S., Regulating Cryptocurrencies: Assessing Market Reactions, 2018](#); [Aquilina M. et al., Addressing the Risks in Crypto: Laying out the Options, 2023.](#)

SEZIONE 2. I CRYPTO-ASSET SERVICE PROVIDER (CASP): CONFIGURAZIONE GIURIDICA, PROFILI REGOLATORI E RELATIVI ONERI

1. Finanza tradizionale e finanza decentralizzata: il paradigma regolatorio delle cripto-attività

Sulla scorta delle problematiche sinora illustrate, è possibile comprendere i motivi per cui soprattutto a livello europeo e nazionale i primi aspetti legati al fenomeno dei *crypto-asset* presi in considerazione dal Legislatore perseguano finalità di natura pubblicistica e siano connessi con l'esigenza di impedire l'utilizzo illecito di detti strumenti, specialmente, come si avrà modo di approfondire oltre, in ottica di contrasto al riciclaggio ed al finanziamento del terrorismo¹⁷⁸. Di recente, si è assistito ad una più seria presa di coscienza sulla necessità di interventi organici tesi a regolamentare in modo esteso l'ecosistema delle cripto-attività e, più in generale, le innovazioni repentinamente sviluppatesi in ambito *CeDeFi*, per due ordini di ragioni: la prima discende dalla constatazione che tali settori appaiono via via connotati da sempre maggiori interconnessioni con la *TradFi*, circostanza che preoccupa non poco per gli scenari che potrebbero aprirsi in caso di ulteriori fallimenti/crisi del sistema *crypto* visti nel primo capitolo; la seconda è invece connessa con l'impellente necessità di creare un solido sistema di tutele per gli investitori, esposti a tentativi di frode o a rischi di improvvisi *default* di operatori di settore.

Il percorso europeo, che ha portato ad un primo *framework* regolamentare, è stato piuttosto articolato¹⁷⁹ e si è sviluppato attraverso diversi momenti con il coinvolgimento di tutte le Autorità unionali e nazionali competenti in materia, in un contesto allargato a livello globale

¹⁷⁸ Tale evidenza è esplicitata nel quarto considerato del Regolamento 2023/1114/UE relativo ai mercati delle cripto-attività, c.d. Regolamento *MiCA*, nel quale si afferma che «*attualmente non esistono norme, ad eccezione di quelle in materia di antiriciclaggio, in relazione alla prestazione di servizi connessi a tali cripto-attività non regolamentate, anche per quanto riguarda il funzionamento delle piattaforme di negoziazione di cripto-attività, lo scambio di cripto-attività con fondi o altre cripto-attività e la prestazione di custodia e amministrazione di cripto-attività per conto dei clienti. L'assenza di tali norme fa sì che i possessori di tali cripto-attività siano esposti a rischi, in particolare nei settori non disciplinati dalle norme in materia di tutela dei consumatori. L'assenza di tali norme può anche comportare rischi sostanziali per l'integrità del mercato, anche in termini di abuso di mercato e di criminalità finanziaria. Per far fronte a questi rischi, alcuni Stati membri hanno introdotto norme specifiche per tutte le cripto-attività che non rientrano nell'ambito di applicazione degli atti legislativi dell'Unione in materia di servizi finanziari o per un sottoinsieme di esse e altri Stati membri stanno valutando l'opportunità di legiferare nel settore delle cripto-attività*».

¹⁷⁹ Cfr. Paracampo M.T., *I prestatori di servizi per le cripto-attività. Tra mifidizzazione della MiCA e tokenizzazione della Mifid*, Giappichelli, 2023, p.2 e ss.

secondo un approccio coordinato anche a livello G20, sotto la cui egida operano il *Financial Stability Board (FSB)*¹⁸⁰, il Fondo monetario internazionale (*FMI*)¹⁸¹ e la Banca dei Regolamenti Internazionali (*Bank of International of Settlement*), che si pongono l'obiettivo di delineare la *policy* macroprudenziale in un'ottica quanto più allargata ed accettata. Di recente, proprio su richiesta della presidenza indiana del G20, FMI e FSB hanno pubblicato un documento congiunto che espone «raccomandazioni politiche e normative avanzate», quale guida rivolta alle varie giurisdizioni per affrontare i rischi per la

¹⁸⁰ Il *Financial Stability Board (FSB)* è stato istituito in occasione del summit del Gruppo dei Venti (G-20) tenuto a Londra nell'aprile 2009, come evoluzione del già esistente *Financial Stability Forum (FSF)*, allo scopo di promuovere la stabilità del sistema finanziario internazionale, migliorare il funzionamento dei mercati finanziari e ridurre il rischio sistemico, attraverso lo scambio di informazioni e la cooperazione internazionale tra le Autorità di vigilanza, le Banche Centrali, le principali organizzazioni sovranazionali. Nel documento [*FSB, Decentralised financial technologies. Report on financial stability, regulatory and governance implications, 2019*](#) è analizzata la questione del decentramento dei servizi finanziari in relazione alla possibilità di superare la figura dell'intermediario finanziario o dei processi accentrati, tipici della configurazione classica dei servizi finanziari. L'applicazione di tecnologie finanziarie decentralizzate, secondo il FSB, potrebbe costituire uno fra gli strumenti più adatti a favorire la stabilità finanziaria, dando vita ad un sistema effettivamente decentralizzato. Il *paper* guarda, infatti, in prospettiva alle “*decentralised financial technology*”, riconoscendo il pregio di facilitare l'allontanamento da autorità certificatrici centrali e, contestualmente, decentralizzare la registrazione delle informazioni, ad esempio per il tramite della nota tecnologia a registri distribuiti ed il processo di asseveramento del dato, il cd. “*meccanismo del consenso*”: «la tecnologia sta anche facilitando il decentramento dell'assunzione di rischi e del processo decisionale. Ad esempio, i prestiti e le assicurazioni peer-to-peer stanno spostando i rischi di credito e di altro tipo da una singola entità (ad esempio una banca o un assicuratore) a singoli risparmiatori (o a gruppi di essi)». Allo stesso tempo, tuttavia, potrebbero verificarsi dei rischi per la stabilità del sistema, dando origine a concentrazioni proprietarie in relazione ad infrastrutture chiave, oltre che situazioni critiche rispetto alla protezione dei consumatori ed alla fiducia del pubblico in tutto il sistema finanziario. Più di recente. Più di recente, il FSB ha pubblicato un documento, in consultazione, intitolato [*FSB, Regulation, supervision and oversight of crypto-asset activities and markets: consultative document, Consultative document, 2023*](#). Le conclusioni sono state accolte nel *report* [*FSB, Global Regulatory Framework for Crypto-Asset Activities. Umbrella public note to accompany final framework, 2023*](#) che contiene due distinte serie di raccomandazioni rivolte alle autorità di regolamentazione, vigilanza e controllo.

¹⁸¹ Il Fondo Monetario Internazionale - FMI (*International Monetary Fund - IMF*) è un'organizzazione internazionale pubblica a carattere universale composta dai governi nazionali di 189 Paesi e insieme al gruppo della Banca Mondiale fa parte delle organizzazioni internazionali dette di Bretton Woods. Il Fondo monetario non è stato meno attivo nell'esprimere le proprie considerazioni sul fenomeno dei *crypto-asset*. In particolare, risale al mese di aprile 2019 il seminario dal titolo “*Money and Payments in the Digital Age*”, nell'ambito del quale i partecipanti si sono cimentati nel raccogliere le diverse visioni sul futuro del sistema finanziario in relazione all'emergere dei nuovi strumenti tecnologici. Sembra interessante segnalare come, in quell'occasione, sia stato affermato che «la fiducia, non la tecnologia, è il vero ostacolo». La *policy* del FMI, più di recente, è stata riportata in diversi *report* (vds. [*Fondo Monetario Internazionale, Elements of effective policies for Crypto Assets, IMF Policy Paper, 2023*](#); [*Bains P. et al., Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets, 2022*](#); [*Bains P. et al., Regulating the Crypto Ecosystem: The Case of Stablecoins and Arrangements, 2022*](#)).

stabilità macroeconomica e finanziaria insiti nelle *crypto-asset*, comprese le attività connesse con le *stablecoin*, e nella finanza *DeFi*¹⁸².

In Europa l'*ESMA*¹⁸³, l'*EBA*¹⁸⁴ e l'*EIOPA*¹⁸⁵, le tre Autorità europee di vigilanza nel settore finanziario, bancario e assicurativo, si sono occupate di *crypto-asset* rilasciando a più riprese degli avvisi per i consumatori e gli investitori circa i rischi legati all'acquisto e/o alla detenzione delle cripto-attività. Le suddette istituzioni, in estrema sintesi, ritengono preoccupante il crescere del numero dei risparmiatori che acquista cripto-attività, spesso con l'aspettativa di vederne continuamente aumentare il valore, senza essere in alcun modo consapevoli dell'elevato rischio di perdere il denaro investito. In particolare, l'*ESMA* ha rilasciato, nel novembre del 2017, due avvisi sulle *Initial Coin Offerings*, mentre l'*EBA* ha pubblicato diversi *alert* e pareri sui *crypto-asset* datati dicembre 2013, luglio 2014 e agosto 2016. Entrambe sono tornate periodicamente, anche in tempi più recenti, aggiornando le proprie posizioni puntualmente recepite nelle avvertenze della Banca d'Italia¹⁸⁶.

¹⁸² Cfr. [Fondo Monetario Internazionale-FSB, IMF-FSB Synthesis Paper: Policies for Crypto-Assets, 2023](#). Il documento si sofferma anche sui rischi in materia di antiriciclaggio e finanziamento al terrorismo affermando, in particolare «a causa della loro pretesa natura pseudonima, della velocità, della portata globale e dell'evidenza di una debole implementazione dei pertinenti requisiti AML/CFT, i *crypto-asset* possono essere attraenti per i criminali, aumentando i rischi per l'integrità finanziaria. I *crypto-asset* possono essere utilizzati impropriamente per commettere una serie di reati (ad esempio, ransomware, frodi, evasione fiscale, riciclaggio di denaro, finanziamento della proliferazione di armi di distruzione di massa e finanziamento del terrorismo)». Di qui la raccomandazione secondo cui «le giurisdizioni dovrebbero applicare gli standard GAFI nel settore degli asset virtuali per proteggere i loro sistemi finanziari e l'economia globale dalle minacce di riciclaggio di denaro, di finanziamento del terrorismo e di proliferazione delle armi di distruzione di massa».

¹⁸³ L'*European Securities and Markets Authority (ESMA)* è un organismo di vigilanza europeo istituito dal Regolamento 1095/2010/UE del 24 novembre 2010, che ha il compito di sorvegliare il mercato finanziario europeo. Ad essa partecipano tutte le autorità di vigilanza bancaria dell'Unione europea. L'Autorità sostituisce il *Committee of European Securities Regulators (CESR)*.

¹⁸⁴ L'*European Banking Authority (EBA)* è un organismo di vigilanza europeo che, ai sensi dell'art. 9 del Regolamento 1093/2010/UE del 24 novembre 2010, ha il compito di monitorare le attività finanziarie nuove ed adottare orientamenti e raccomandazioni volti a promuovere la sicurezza e la solidità dei mercati e la convergenza delle prassi. Ad essa partecipano tutte le autorità di vigilanza bancaria dell'Unione europea. L'Autorità sostituisce il *Committee of European Banking Supervisors (CEBS)*.

¹⁸⁵ L'*European Insurance and Occupational Pensions Authority (EIOPA)* è un organismo dell'Unione europea, istituito con Regolamento 1094/2010/UE del 24 novembre 2010, che ha compiti di vigilanza nel mercato assicurativo europeo. Ad essa partecipano tutte le autorità di vigilanza assicurativa dell'Unione europea. L'Autorità sostituisce il *Committee of European Insurance and Occupational Pensions Supervisors (CEIOPS)*.

¹⁸⁶ L'ultimo intervento si deve all'[ESMA, ESMA highlights the risks arising from the provision of unregulated products and/or services by investment firms, Statement, 2023](#). In tale contesto, appare di particolare interesse la pubblicazione dell'EBA del 2014, che è stato forse il primo intervento in cui un'Autorità di vigilanza ha ritenuto indispensabile addivenire ad una regolamentazione integrata del fenomeno a livello europeo, «che riservi l'operatività in valute digitali a soggetti autorizzati e definisca, tra l'altro, requisiti in materia di capitale e governance dei partecipanti al mercato e segregazione dei conti della clientela». La Banca d'Italia, nella Comunicazione del 30 gennaio 2015, ha messo per la prima volta in luce gli elementi di criticità in materia di

A fronte di questi primi richiami, che hanno visto come protagoniste le tre Autorità di vigilanza, il percorso verso un più compiuto *framework* regolamentare si è articolato attraverso ulteriori tappe, che hanno preso le mosse dalla Comunicazione della Commissione Europea dell'8 marzo 2018 che enunciava la sua *policy* nel settore delle tecnologie finanziarie al Parlamento Europeo, al Consiglio, alla Banca Centrale Europea, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni¹⁸⁷. Segnatamente, nel suo *FinTech Action Plan* la Commissione evidenzia come gli approcci possibili alla materia siano due e si sostanzino in:

- uno “*status quo approach*”, improntato sulla possibilità di regolare la maggior parte dei modelli di *business* innovativi con le attuali regole UE e, quindi, con gli istituti tipici del *TradFi*;
- un “*revolutionary approach*”, fondato invece sull'opportunità di una regolamentazione *ad hoc* del fenomeno – secondo nuovi paradigmi e nuove regole di linguaggio - sulla constatazione che molte delle innovazioni sviluppatesi in ambito *DeFi* non appaiono rientrare nel campo di applicazione del vigente quadro normativo europeo.

Per entrambi gli approcci, tuttavia, requisito imprescindibile è che la Comunità internazionale intervenga tempestivamente attraverso un quadro di regole chiare che muovano verso modelli di coordinamento e di convergenza dei *framework* normativi domestici. In realtà, tutt'altro che tempestivo può essere letto il comportamento (di tipo *bottom up*) che molte Organizzazioni internazionali ed Autorità di vigilanza sovranazionali, comprese le istituzioni

crypto-asset prendendo le mosse proprio dal *report* dell'EBA da ultimo citato. Anche il Rapporto UIF per l'anno 2014, che analizza il fenomeno dell'acquisto e vendita di *crypto-asset* in relazione a problemi di tracciabilità delle operazioni, prende spunto dal predetto parere EBA. L'Unità, in particolare, ha rilevato di aver attenzionato il tema dei rischi di riciclaggio connessi all'utilizzo delle cripto-attività, anche attraverso la partecipazione ad un progetto curato dall'*Operational Working Group* di Egmont (*Virtual Currencies and Money Laundering*), «che mira a favorire la condivisione di conoscenze ed esperienze tra le FIU partecipanti, stimolare la collaborazione internazionale nella materia e definire appositi “red flag” che possano agevolare gli operatori nell'individuazione di operazioni sospette».

¹⁸⁷ Cfr. [Commissione europea, Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo, COM\(2018\) 109 final, 2018](#). Il *report*, che segue di poco le pubblicazioni dell'ESMA, dell'EIOPA e dell'EBA, è teso a mappare i diversi approcci tenuti dalle Autorità nazionali e, in particolare, a verificare l'uso dei principi di proporzionalità e di flessibilità in sede di autorizzazione delle attività *FinTech*, nonché nell'applicazione della legislazione sui servizi finanziari (cfr. [Paracampo M. T., FinTech, modelli di business innovativi e regimi di autorizzazione: il responso delle Autorità europee, 2019](#)).

europee, hanno tenuto negli anni in cui si affacciava la rivoluzione delle *DLT*. Infatti, i *policy maker* internazionali hanno assunto un atteggiamento attendista avviando un'attività di iniziale osservazione dei modelli di normazione statali, non “calando dall'alto” una propria regolamentazione, ma aspettando che le normative nazionali via via in emanazione si consolidassero, in modo da individuare possibili linee di convergenza/armonizzazione. Il risultato di questo atteggiamento si è tradotto nell'adozione, da parte di alcuni Stati membri, di regole su misura in contrasto tra loro e/o di difficile allineamento, se non attraverso l'introduzione di un unico quadro normativo di riferimento. A mero titolo esemplificativo, la possibilità di “tokenizzare” *asset*, prodotti e servizi, soprattutto in attività di *crowdfunding* e di finanza *peer-to-peer* (generalmente connesse con l'avvio o l'espansione di *start-up* tipo *ICO*), ha indotto taluni Stati membri ad introdurre regimi speciali ed ha spinto altri ad includere tali attività finanziarie nel quadro normativo europeo esistente (*MiFID II*, *PSD2* e *AIMFD*)¹⁸⁸. Su tali premesse la Commissione Europea, il 24 settembre 2020 ha adottato un pacchetto per la finanza digitale (*Digital Finance Package*) composto da quattro proposte

¹⁸⁸ La direttiva *MiFID* o *Markets in financial instruments directive* (2004/39/EC) ha disciplinato dal 31 gennaio 2007 al 2 gennaio 2018 i mercati finanziari dell'Unione Europea. Dal 3 gennaio 2018 è entrata in vigore in tutta l'Unione la nuova direttiva *MiFID II* (2014/65/EU) che, insieme alla *MiFIR* o *Markets in financial instruments regulation* (Regolamento 600/2014/UE) ha preso il posto della precedente regolamentazione europea. Inoltre, il 13 gennaio 2018 è entrata in vigore la Direttiva 2015/2366/UE (cd. *PSD2*), che ha abrogato la prima Direttiva in materia di servizi di pagamento (i.e. Direttiva 2007/64/CE o *PSD1*) che ha introdotto un quadro giuridico armonizzato per la creazione di un mercato interno dei pagamenti a livello europeo. La *PSD2* ha dunque introdotto rilevanti novità con l'obiettivo ultimo di promuovere una maggiore concorrenza, efficienza ed innovazione nel mercato dei servizi di pagamento rafforzando al contempo la tutela degli utilizzatori dei servizi di pagamento, la trasparenza e la sicurezza dei pagamenti elettronici. Il quadro si completa con la Direttiva 2011/61/UE del Parlamento europeo e del Consiglio sui Gestori di Fondi di Investimento Alternativi (cd. Direttiva *AIFMD*) adottata l'8 giugno 2011, che è il risultato della volontà politica del G20 per introdurre un controllo regolamentare più stringente sul rischio sistemico che può derivare dalle attività dei soggetti che operano nel settore dei fondi di investimento cosiddetti “alternativi”, ossia di quei fondi di investimento diversi rispetto ai fondi disciplinati dalla Direttiva 2009/65/CE in materia di Organismi di Investimento Collettivo in Valori Mobiliari (OICVM).

di regolamento¹⁸⁹: i primi due sono dedicati alle cripto-attività (il *MiCA* o *MiCAR*¹⁹⁰ - *Markets in Crypto-Assets regulation* e il *DLT Pilot Regime* - regime pilota per le infrastrutture di mercato dei capitali basate su tecnologia *DLT*), il terzo (il *DORA* - *Digital Operation Resilience*) è dedicato alla sicurezza nel settore finanziario, mentre il quarto reca delle proposte di modifica alle principali fonti normative della legislazione finanziaria europea.

A titolo di completezza, sul panorama internazionale si segnalano le iniziative portate avanti dal governo del Regno Unito che prevede di implementare presto la propria regolamentazione e che a tal fine ha pubblicato nel febbraio 2023 un documento in consultazione¹⁹¹. Anche negli Stati Uniti, dove ancora non esistono normative specifiche sulle cripto-attività, il governo intende intervenire sulla base di un ordine esecutivo del marzo 2022. Fino ad ora i *crypto-asset* sono stati regolamentati negli USA tramite interventi degli organismi di controllo (soprattutto la *Securities and Exchange Commission [SEC]* e la *Commodities Futures Trading Commission [CFTC]*), che hanno adottato un approccio tipo

¹⁸⁹ Cfr. [Commissione Europea, Strategia in materia di finanza digitale per l'UE, COM\(2020\)591 final, 24 settembre 2020](#). Gli orientamenti del pacchetto di misure sono illustrati in due comunicazioni: la strategia in materia di finanza digitale (COM(2020)591), che prefigura due interventi entro il 2024, nell'ottica di promuovere il potenziale della finanza digitale in termini di innovazione e concorrenza, al contempo riducendo i rischi che ne derivano (connessi alla cyber-sicurezza, alla protezione di dati, consumatori e investitori e all'integrità del mercato); la strategia in materia di pagamenti al dettaglio (COM(2020)592), che prospetta l'adozione di azioni volte a promuovere i pagamenti istantanei e le soluzioni di pagamento in tutta l'UE. Nel quadro della strategia in materia di finanza digitale sono stati adottati due gruppi di proposte legislative:

- il primo gruppo introduce una regolamentazione a livello europeo dell'offerta di cripto-attività, qualificabili come rappresentazioni digitali di valori o di diritti che possono essere trasferiti o memorizzati elettronicamente attraverso una tecnologia che supporta la registrazione distribuita di dati cifrati. In tale ambito, sono state articolate due proposte di regolamento, il *MiCA* (COM(2020)593) e il Regolamento relativo ad un Regime Pilota *DLT* (COM(2020)594);
- il secondo gruppo di proposte introduce per le entità finanziarie un'ulteriore armonizzazione delle principali prescrizioni sulla resilienza operativa digitale, al fine di introdurre regole in materia di gestione dei rischi delle tecnologie *ICT* e segnalazione di incidenti ad esse connessi (proposta di Regolamento *DORA* (COM(2020)595), nonché di modificare le norme vigenti in materia di servizi finanziari, al fine di adeguarle al nuovo Regolamento *DORA*, e di aggiornare la definizione di "strumento finanziario" includendo gli strumenti emessi utilizzando la tecnologia *DLT* (proposta di direttiva COM(2020)596).

Con riferimento a tali proposte, si segnala la definitiva approvazione e pubblicazione del Regolamento 2022/858/UE del Parlamento Europeo e del Consiglio del 30 maggio 2022 relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito e del Regolamento 2022/2554/UE pubblicato in Gazzetta ufficiale dell'Unione Europea il 27 dicembre 2022 (c.d. "*DORA*"). Il Regolamento *MiCA* 2023/1114 è stato invece approvato dal Consiglio in data 16 maggio 2023.

¹⁹⁰ Il Regolamento è conosciuto in entrambe le versioni dell'acronimo. Per comodità di trattazione, ad eccezione di eventuali citazioni dottrinali che saranno opportunamente evidenziate si precisa sin d'ora che nel prosieguo ci si riferirà alla normativa come *MiCA*.

¹⁹¹ Cfr. [HM Treasury, Future financial services regulatory regime for cryptoassets: Consultation and call for evidence, 2023](#).

“*regulation by enforcement*”.

2. Le esigenze alla base di una rinnovata regolamentazione sovranazionale delle crypto-attività

Alla luce delle considerazioni sopra esposte, appare di tutta evidenza come le innovazioni prodotte dall’era digitale in materia di servizi finanziari abbiano reso quanto mai necessario un adeguamento sia della legislazione che degli scenari economici tradizionali così da modellare gli ordinamenti giuridici in una misura che sia performante per le sfide del futuro. La stessa Unione Europea ha più volte mostrato il forte interesse allo sviluppo e alla promozione di «*tecnologie trasformative nel settore finanziario, compresa la diffusione della tecnologia a registro distribuito (DLT)*»¹⁹². D’altronde, nell’ambito delle reti decentralizzate circolano crypto-attività in grado di inserirsi sui mercati e di conseguenza di partecipare alla raccolta di capitale, a mezzo di meccanismi da taluni ritenuti stimolo ad innovativi processi di sviluppo. Il Regolatore europeo si è mosso tenendo in debita considerazione la complessità dei fenomeni associati alla *DLT* che, in maniera repentina, hanno introdotto un nuovo paradigma nel mondo finanziario, basato su tre dimensioni fortemente interconnesse¹⁹³:

- **tecnologica**, attraverso l’introduzione di un’infrastruttura di mercato distribuita, che consente di trasferire valore o diritti, senza l’intermediazione di un’autorità fiduciaria centralizzata, attraverso modelli di *governance* costruiti attorno ad un concetto di fiducia suddivisa tra tutti gli utenti¹⁹⁴;
- **quella legata alla rappresentazione digitale del valore**, con l’emissione di *token* che possono essere privi di una attività sottostante o rappresentare digitalmente strumenti finanziari o altre attività¹⁹⁵;

¹⁹² Cfr. *Considerando* n. 1 al Regolamento 2023/1114/UE del Parlamento Europeo e del Consiglio del 31 maggio 2023 relativo ai mercati delle crypto-attività e che modifica i Regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le Direttive 2013/36/UE e (UE) 2019/1937.

¹⁹³ Cfr. [Siani G., La regolamentazione delle nuove tecnologie basate sulla Distributed ledger technology – DLT, tra tutela del mercato e rischi di sistema, Università Luiss Guido Carli di Roma Guardia di Finanza – Scuola di Polizia Economico-Finanziaria, 2022.](#)

¹⁹⁴ Vds. [Parlamento Europeo, Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione \(2017/2772\(RSP\)\), 2018.](#)

¹⁹⁵ Avendo premura di chiarire ulteriormente il concetto di “tokenizzazione”, questa può essere definita come la rappresentazione di attività tradizionali - ad es. strumenti finanziari, un paniere di garanzie e *asset*, ecc. - su

- **quella connessa con l'ingresso sul mercato di una vasta tipologia di nuovi soggetti privati** (i “*Crypto-Asset Service Provider*” (*CASP*) secondo la terminologia *MiCA*), diversi dagli intermediari tradizionali che, tuttavia, coesistono con questi ultimi¹⁹⁶.

Il *MiCA Regulation* si innesta in tale contesto e rappresenta il primo *framework* armonizzato, teso a favorire la creazione e lo sviluppo dei mercati di cripto-attività non regolamentati dalle vigenti normative con l'obiettivo di riconoscere un ruolo centrale alle banche e agli altri intermediari finanziari vigilati chiamati a svolgere «una varietà di possibili funzioni all'interno degli ecosistemi di cripto-attività, contribuendo al loro funzionamento, supportando e facilitando il trasferimento dei token, la custodia, le interazioni con i titolari e i movimenti in entrata e in uscita dall'ecosistema»¹⁹⁷.

In particolare, il Regolamento si rivolge agli emittenti, offerenti e prestatori di servizi in *crypto-asset*, tra cui gli *exchange*, le piattaforme di *trading* e i fornitori di *wallet*, contiene specifiche misure contro la manipolazione del mercato e per prevenire il riciclaggio di denaro, il finanziamento del terrorismo e altre attività criminali.

Va ammesso come non sia semplice per il Regolatore considerare tutte le implicazioni e le variabili che un simile sistema possa comportare, anche e soprattutto in ottica di sviluppi futuri. In tale prospettiva, la regolamentazione - pur parziale come è quella del *MiCA* - ha cercato di tenerne conto garantendo alcune condizioni fondamentali:

una *DLT*. Più precisamente, la tokenizzazione consiste nella conversione dei diritti di un bene in un *token* digitale registrato su una *DLT*, dove il bene reale e il *token* sono collegati da *smart contract*. Uno dei primi esempi di tokenizzazione nel settore del *capital market* è stata l'emissione di “bond-i” da parte della Banca Mondiale utilizzando una *DLT* autorizzata come *Proof of Concept* (Vds. Banca Mondiale, *First World Blockchain Bond Global Price Prices, A\$110 Million*, 2018). Le attività di tokenizzazione riguardano anche la digitalizzazione di titoli finanziari tradizionali (cd. “titoli tokenizzati”) o forme di investimento in cui le emittenti rilasciano *token* digitali come le *Initial Coin Offerings (ICOs)*. Più di recente, il Regolamento 2022/858/UE, relativo al regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito, ha definito tokenizzazione degli strumenti finanziari «la rappresentazione digitale di strumenti finanziari nei registri distribuiti o l'emissione di categorie di attività tradizionali in formato tokenizzato per consentirne l'emissione, la custodia e il trasferimento in un registro distribuito».

¹⁹⁶ Questa definizione adottata dal *MiCA*, come vedremo, è più ampia della definizione del *VASP (Virtual Asset Service Provider)* adottata in ambito GAFI e dalla stessa UE nelle sue direttive *AML*.

¹⁹⁷ Vds. [Banca d'Italia, Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività, 2022.](#)

- avere la capacità di resilienza all'interno del contesto *cyber*, contro attacchi informatici¹⁹⁸;
- essere sostenibile – anche da punto di vista ambientale¹⁹⁹ – rispetto al volume elevato di transazioni;
- avere una *governance* robusta e identificabile.

Il *MiCA*, in ragione di ciò, prevede che gli emittenti di *token* collegati ad *asset* dovrebbero disporre di solidi dispositivi di *governance*, che comprendano una struttura organizzativa trasparente e procedure in grado gestire, monitorare e segnalare i rischi cui potrebbero essere esposti (in tal senso sono chiamati a descriverne il contenuto nelle proprie domande di autorizzazione). In riferimento a quest'ultimo aspetto, può sin d'ora anticiparsi come si assista all'emersione di una sorta di paradosso: la natura eminentemente disintermediata, che qualifica sia la fase di emissione che di negoziazione delle cripto-attività, esclude che possano svolgersi controlli a monte da parte di una qualsivoglia Autorità esterna sulla sottostante infrastruttura *DLT*, caratterizzata da meccanismi di *governance* che appaiono di più difficile inquadramento rispetto alle categorie tradizionali della vigilanza.

La soluzione è quindi quella di adottare un approccio regolatorio non tradizionalmente societario o civilistico, quanto più propriamente di diritto dei mercati finanziari, finalizzato a vigilare “dal di fuori” i processi nel loro complesso, ossia teso a presidiare l'integrità dei mercati, l'ordinata prestazione dei servizi e la tutela degli investitori; in sostanza, un sistema

¹⁹⁸ In tal senso, il *MiCA* va letto a sistema con il Regolamento 2022/2554/UE (*Digital Operational Resilience Act - DORA*) che, dal 17 gennaio 2025, vincolerà gli operatori del settore al rispetto di una serie di requisiti di sicurezza informatica e di resilienza. Normativa che, peraltro, va a collocarsi in un più ampio quadro di produzione normativa del Legislatore europeo, che comprende la Direttiva 2022/2555/UE (*Direttiva NIS 2*) e la Direttiva 2022/2557/UE (*Direttiva CER*).

¹⁹⁹ Nel *Considerando* n. 7 del *MiCA* è esplicitato tale obiettivo. Si afferma, in particolare che «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». In tale contesto, l'*ESMA* e l'*EBA* sono state chiamate ad elaborare progetti di norme tecniche di regolamentazione al fine di specificare «il contenuto, le metodologie e la presentazione delle informazioni in relazione agli indicatori di sostenibilità per quanto riguarda gli impatti negativi sul clima e altri effetti negativi connessi all'ambiente, nonché di delineare i principali indicatori energetici».

simile a quanto avviene oggi per il “sistema dei pagamenti”²⁰⁰. In tale ambito, il controllo a monte non può che esaurirsi sulla verifica dei modelli e sui criteri di *governance* della DLT, che il promotore dell’iniziativa dovrebbe illustrare nel *white paper*; criteri che peraltro dovrebbero seguire degli *standard* in modo da uniformare le linee di azioni conseguenti. Ad esempio, gli stessi potrebbero seguire quelli messi a punto dall’Organizzazione internazionale per la standardizzazione (ISO)²⁰¹ per poi essere integrati adattando le linee guida del Comitato di Basilea in materia di *governance* delle Banche (BCBS 2015)²⁰². Inoltre, l’individuazione dei meccanismi di *governance* presuppone l’esatta definizione del perimetro oggettivo (*i.e.* crypto-attività) e soggettivo (*i.e.* *Crypto-Asset Service Provider*) cui si rivolge la nuova regolamentazione. In tale senso, si può osservare come il MiCA abbia il pregio di fare chiarezza in ordine alla definizione di *crypto-asset* inteso come «una rappresentazione

²⁰⁰ In questi termini, vds. [Carrière P. et al., Tokenizzazione di azioni e azioni tokens, Quaderni giuridici Consob, n. 25, 2023.](#)

²⁰¹ Diversi sono gli interventi avviati da ISO, da parte della Commissione tecnica ISO/TC 307 *Blockchain and distributed ledger technologies*, con la specifica *mission* di predisporre *standard* sul tema. La maggior parte degli *standard* sono in fase di sviluppo (vds. [ISO, Standards by ISO/TC 307. Blockchain and distributed ledger technologies, 2023](#)). Il documento più maturo è il WG1:ISO/DIS 22739 “*Blockchain and distributed ledger technologies – Terminology*”, che ha lo scopo di definire i termini di base che si riferiscono a *blockchain* e DLT, al fine di rendere chiaro il significato dei termini che sono utilizzati nei diversi documenti sul tema e renderli conformi ai criteri ISO. Simili *standard* saranno, infatti, applicabili ad ogni tipologia di organizzazione (commerciale, governativa, non-profit etc.). Risale, invece, al settembre 2019 la pubblicazione del documento [ISO, Overview of an interactions between smart contracts in blockchain and distributed ledger technology systems, ISO/TR 23455:2019](#), in cui sono tra l’altro definiti lo *smart contract* come «programma informatico memorizzato in un sistema di libro mastro distribuito in cui il risultato di ogni esecuzione del programma è registrato sul libro mastro distribuito», ed il *token*, quale «rappresentazione di una raccolta di dati». Altra fondamentale Organizzazione internazionale è l’Unione internazionale delle telecomunicazioni (ITU), che si occupa di definire gli *standard* per le tecnologie di informazione e comunicazione. Nell’ambito dell’ITU è stato istituito sin dal 2017 il *Focus Group on Digital Currency including Digital Fiat Currency*, il cui obiettivo è quello di studiare i vantaggi economici e l’impatto dell’introduzione dei *crypto-asset*, oltre a quello di mappare l’architettura di riferimento e le principali componenti dei processi connessi anche al fine di migliorare l’integrazione con i sistemi di esistenti. Il *Focus Group* ha completato i suoi lavori a giugno 2019, pubblicando la sua relazione [Focus Group on Digital Currency including Digital Fiat Currency, Reference Documentation: Governance Aspects of Digital Fiat Currency, 2019](#). Sempre nel 2017, in ambito ITU, è stato costituito il *Focus Group on Application of Distributed Ledger Technology*, con il compito di identificare ed analizzare applicazioni e servizi basati su DLT, oltre che di elaborare *best practices* e *guidance* per supportare l’implementazione di tali applicazioni e servizi su scala globale e proporre una via da seguire per i relativi lavori di standardizzazione. Una prima sessione del lavoro si è conclusa il 1° agosto 2019 con la presentazione dei seguenti prodotti finali: “*DLT terms and definitions*”, “*DLT overview, concepts, ecosystem*”, “*DLT standardization landscape*”, “*DLT use cases*”, “*DLT reference architecture*”, “*Assessment criteria for DLT platforms*”, “*DLT regulatory framework*”, “*Outlook on DLTs*” (vds. [ITU-T, Focus Group on Application of Distributed Ledger Technology, 2019](#)).

²⁰² Per approfondimenti vds. [Anitec - Assinform, White Paper Attualità e prospettive della Blockchain per la crescita dell’economia italiana, 2021](#); [Gola C. et al., La governance delle blockchain e dei sistemi basati sulla tecnologia dei registri distribuiti, Banca d’Italia, 2023.](#)

digitale di valore o di diritti, che può essere trasferito digitalmente o utilizzato per finalità di pagamento o d'investimento, e che utilizza la crittografia o una tecnologia simile basata o derivata da una Distributed Ledger Technology (DLT)». Come precisato nel considerando n. 2 del Regolamento «le rappresentazioni di valore includono il valore esterno, non intrinseco, attribuito a una cripto-attività dalle parti interessate o dai partecipanti al mercato, vale a dire che il valore è soggettivo e basato solo sull'interesse dell'acquirente della cripto-attività». Una descrizione più approfondita delle caratteristiche di ciascuna specie di *crypto-asset* è contemplata all'art. 3 del Regolamento²⁰³, laddove si riassumono in:

²⁰³ La tassonomia utilizzata è simile a quella proposta sull'*Occasional Paper* di Caponera A. e Gola C., *Aspetti economici e regolamentari delle «cripto-attività»*, in Banca d'Italia, *Questioni di Economia e Finanza*, 2019, ove si prospetta una classificazione che presenta molte affinità, ma anche alcune differenze, con quelle proposte dall'*ESMA* e dall'*EBA*. Molte classificazioni riproposte dalla dottrina rispecchiano, invero, le indicazioni, pubblicate a febbraio del 2018, dall'Autorità di vigilanza dei mercati finanziari svizzera (FINMA) che, a sua volta, non si discosta molto da quella adottata dal *MiCA* (vds. [FINMA, Guida pratica per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle initial coin offerings \(ICOs\)](#), 2018). L'autorità elvetica propone la seguente classificazione:

T1 – criptovalute o *crypto-asset*. Questi gettoni digitali (tipo *bitcoin*) sono privi di diritti incorporati o passività. Sono negoziabili e convertibili in moneta legale di Stato (*fiat money*) o in altri *crypto-asset*, a un prezzo variabile. Se i T1 fossero associati a diritti, andrebbero ricondotti alle categorie T2 o T3, che seguono.

T2 – digital coins o payment token. Si tratta di strumenti che tendono, a differenza dei T1, replicare le funzionalità della moneta mantenendo con essa un valore fisso. Questi gettoni digitali rappresentano un diritto o una passività dell'emittente. Possono essere: privati a valore fisso (*stablecoins*), se sono emessi da una entità giuridica a fronte di una unità di moneta (uno-a-uno con euro, dollaro, ecc.) segregata presso un soggetto regolato. Alcuni progetti cercano di sviluppare *token* privati che hanno un prezzo solo tendenzialmente stabilizzato (*price-peg*) attraverso la costituzione di una riserva di valore basata su un paniere di valute tradizionali, di altri *asset* (come oro, altre valute virtuali, ecc.) o su algoritmi che perseguono il medesimo scopo, ma senza l'uso di un collaterale. Se incorporassero altri diritti, potrebbero ricadere nella categoria T3. In questi casi, si parla di *token* ibridi classificabili cumulativamente come valore mobiliare e mezzo di pagamento; emessi da una Banca Centrale (*Central Bank Digital Currencies - CBDC*), che sono volti a creare, di fatto, una moneta elettronica di una Banca Centrale che usa la *DLT*. Rappresentano, a tutti gli effetti, una passività della Banca Centrale; non convertibili con moneta legale o con altri *crypto-asset*, che danno il diritto a scambiare beni o servizi, ma sono a diffusione e spendibilità limitata.

T3 – security/asset token. Detti anche *investment token* o *asset-backed token*, sono gettoni digitali trasferibili e potenzialmente negoziabili (*capable of being tradable*) su una piattaforma, tipicamente offerti tramite una operazione di *ICO*. Sono simili a titoli smaterializzati, che tuttavia vengono trasferiti tramite la *DLT*. I *security token*, per essere tali, devono essere trasferibili e negoziabili o riconoscere al soggetto che li detiene un diritto di proprietà o di controllo. Ad esempio: diritti di proprietà su quote di capitale, quote di fondi o su materie prime negoziabili (*commodities*); diritti di voto o di partecipazione al progetto, dividendi, diritti su flussi di cassa. Più in generale e secondo la funzione economica, il *token* può rappresentare un'azione, un'obbligazione o uno strumento finanziario derivato e, in tale categoria, possono rientrare anche i *token* che mirano a rendere negoziabili sulla *blockchain* oggetti di valore materiali. Questa tipologia di *token*, quindi, può essere ricondotta nell'alveo dei valori mobiliari ed essere assoggettata alla relativa disciplina finanziaria.

T4 – utility token/consumer token. Sono gettoni digitali non negoziabili (pur essendo talvolta trasferibili) che offrono unicamente diritti amministrativi o licenze d'uso, quali l'accesso a una piattaforma, a una *facility*, a una *network* di persone, a schemi di "fidelizzazione". Se oltre ad essere portatori di un diritto, divenissero anche pienamente trasferibili e negoziabili su un mercato organizzato, perderebbero la caratteristica di *utility token* e diventerebbero un T3.

- **Utility Token**, definito come un tipo di cripto-attività che consentono l'accesso ad una applicazione, servizio o altra tecnologia digitale;
- **Asset-Referenced Token (ART)**, che non è un *token* di moneta elettronica e che mira a mantenere un valore stabile facendo riferimento a un altro valore o diritto o a una combinazione dei due, comprese una o più valute ufficiali²⁰⁴;
- **Electronic Money Token o e-money (EMT)**, cripto-attività il cui valore è riferito a quello di una determinata valuta.

Attraverso tali definizioni il *MiCA* mira a disciplinare il settore delle cripto-attività, che non siano in una qualche misura già regolamentate dalla normativa europea. Di conseguenza, il nuovo *framework* non si applica (per esclusione espressa) alle cripto-attività qualificabili come strumenti finanziari (*security/asset token*) quali definiti dall'art. 4, paragrafo 1, punto 15, della Direttiva 2014/65/UE (c.d. *MiFID II - Markets in Financial Instruments Directive*)²⁰⁵.

²⁰⁴ Cit. [Carrière P. et al., Tokenizzazione di azioni e azioni tokens, Quaderni giuridici Consob, n. 25, 2023](#), i quali evidenziano come «questa definizione accoglie interamente gli emendamenti del Parlamento UE: allarga il perimetro della nozione originaria, prima riferita a «un 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». Si tratta di un ulteriore tentativo di catturare tutti quelle cripto-attività che non sono collegate esclusivamente a monete ufficiali o a merci ma a un valore riferito a qualsiasi attività».

²⁰⁵ In Italia, prima delle modifiche apportate dal “Decreto *FinTech*”, D.L. 25/2023 (su cui torneremo a breve), il Testo Unico della Finanza (TUF) di cui al D. Lgs. 24 febbraio 1998, n. 58 (più volte modificato, in particolare, alla luce della normativa europea, di cui alla Direttiva 2004/39/CE, c.d. *MiFID I*, in parte rifiuta nella Direttiva 2014/65/UE, c.d. *MiFID II*, e in parte sostituita dal Regolamento 600/2014/UE, c.d. *MiFIR*) definiva i prodotti finanziari (art. 1, lett. u) come «strumenti finanziari» (tipici) e «ogni altra forma di investimento di natura finanziaria» (atipici). L'art 1, comma 2, del TUF stabiliva poi che «per strumento finanziario si intende qualsiasi strumento riportato nella Sezione C dell'Allegato I. Gli strumenti di pagamento non sono strumenti finanziari». A sua volta, l'Allegato I, Sezione C, presenta un'elencazione tassativa degli strumenti finanziari, individuando tre gruppi distinti di strumenti: non derivati; derivati; quote di emissione. Alcuni ritenevano che quella indicata fosse un'elencazione con carattere tassativo e chiuso, tanto da non consentire l'inclusione anche dei *crypto-asset*, soprattutto se si considerava la clausola generale dell'art. 1, comma 2, TUF, che esclude gli strumenti di pagamento dalla categoria degli strumenti finanziari, tenuto conto che una delle due funzioni prevalenti delle cripto-attività, oltre a quella che ne denota la vocazione speculativa è individuata proprio in quella di fungere da mezzo di pagamento. Maggiori margini di manovra avrebbe consentito muoversi nell'ambito dei prodotti finanziari atipici. In merito, la dottrina (vds. Comporti V., *La sollecitazione all'investimento*, in Patroni Griffi, Sandulli, Santoro (a cura di), *Intermediari finanziari, mercati di società quotate*, 1999, p. 531) e la giurisprudenza (vds. Cass. Civ. Sez. 2, Sentenza n. 2736 del 05/02/2013), ne ha dato, infatti, una definizione più generale, riconoscendo che gli investimenti di natura finanziaria comprendo ogni forma di conferimento di denaro da parte di un risparmiatore con un'aspettativa di un profitto o di una remunerazione, con un rischio proprio dell'attività prescelta, direttamente correlato all'impiego dei capitali. Sembrava più agevole, in questo caso, anche per la più generica definizione di investimento di natura finanziaria,

Questi ultimi sono, viceversa, oggetto di specifica regolamentazione nell'ambito del *Pilot Regime* di cui al Regolamento 2022/858/UE, la cui *ratio* parte dal presupposto che «la legislazione dell'Unione in materia di servizi finanziari non è stata concepita tenendo conto della tecnologia a registro distribuito e delle cripto-attività, e contiene disposizioni che potenzialmente precludono o limitano l'uso della tecnologia a registro distribuito nell'emissione, nella negoziazione e nel regolamento delle cripto-attività che rientrano nella definizione di strumenti finanziari» (Considerando n. 4). In tal senso vanno lette le modifiche apportate dal Regolamento *Pilot* ai Regolamenti 600/2014/UE (relativo ai mercati degli strumenti finanziari - *MiFIR*) e n. 909/2014/UE (relativo al miglioramento del Regolamento titoli nell'Unione Europea e ai depositari centrali di titoli – *CSDR*) e alla Direttiva 2014/65/UE (relativa anch'essa ai mercati degli strumenti finanziari – *MiFID II*)²⁰⁶.

Al riguardo si evidenzia che in Italia il Regolamento *Pilot* è stato attuato per mezzo del D. L. n. 25 del 17 marzo 2023 (cd. “Decreto *FinTech*”), convertito in Legge, con modificazioni, dall'art. 1, comma 1, L. 10 maggio 2023, n. 52²⁰⁷.

farvi rientrare le operazioni in *crypto-asset* e *token* di investimento, la cui natura finanziaria appare connessa con le aspettative di un rendimento in relazione al capitale investito e con il rischio correlato, causa concreta delle operazioni. Su tale linea di pensiero si è mossa anche la Consob (Vds. [Consob, Le offerte iniziali e gli scambi di cripto-attività, Documento per la Discussione, 2019](#)), che parla più specificamente di *crypto-asset* quali elementi «suscettibili di integrare la nozione domestica di prodotto finanziario, inteso quale investimento di natura finanziaria diverso dagli strumenti». Più specifica è la definizione adottata nel rapporto finale della Consob del 2 gennaio 2020, in cui si identificano «le “cripto-attività” nelle attività diverse dagli strumenti finanziari di cui all'art. 1 comma 2 TUF e da prodotti di investimento di cui al comma 1, lettere w-bis.1, w-bis.2 e w-bis.3, consistenti nella rappresentazione digitale di diritti connessi a investimenti in progetti imprenditoriali, emesse, conservate e trasferite mediante 7 tecnologie basate su registri distribuiti, nonché negoziate o destinate a essere negoziate in uno o più sistemi di scambi» (vds. [Consob, Le offerte iniziali e gli scambi di cripto-attività, Rapporto finale, 2019](#)). Posizione, peraltro, sostenuta anche dall'ESMA, secondo cui «i *crypto-asset* sono un tipo di bene privato che dipende principalmente dalla crittografia e dalla Distributed Ledger Technology (DLT). Esiste un'ampia varietà di *crypto-asset*. Gli esempi di *crypto-asset* vanno dalle cosiddette *criptovalute* o *valute virtuali*, come il Bitcoin, ai cosiddetti *token digitali* emessi attraverso le *Initial Coin Offerings (ICO)*». (Vds. [ESMA, Advice, Initial Coin Offerings and Crypto-Assets, ESMA50-157-1391, 2019](#)).

²⁰⁶ In tal senso, ad esempio, vanno lette le modifiche apportate dall'art. 18 del Regolamento *Pilot*, che ha sostituito l'art 4, par. 1, punto 15 della Direttiva *MIFID II*, modificando la definizione relativa agli strumenti finanziari che considera ora anche quelli «emessi mediante tecnologia a registro distribuito».

²⁰⁷ Il testo, oltre ad introdurre, disposizioni necessarie per dare attuazione al Regolamento 2022/858/UE, introduce misure di semplificazione della sperimentazione relativa alle attività di tecno-finanza (*FinTech*), di cui al decreto-legge 30 aprile 2019, n. 34, con la quale è stato introdotto nell'ordinamento un regime semplificato e transitorio (c.d. *regulatory sandbox*) per la sperimentazione delle attività di innovazione tecnologica digitale nei settori bancario, finanziario e assicurativo, al fine di consentire agli operatori *FinTech* di testare soluzioni innovative dal punto di vista digitale, con un costante dialogo con le autorità di vigilanza. Un *sandbox* (il cui nome richiama il “recinto” riempito di sabbia nel quale i bambini possono giocare e sperimentare in un ambiente controllato) è uno strumento che permette alle imprese *fintech*

È interessante notare quanto precisato dall'*ESMA*²⁰⁸, circa la riconducibilità di alcuni *crypto-asset* sotto l'egida *MiFID*, con riferimento, in particolare, alle principali norme che verrebbero in tal modo ad essere applicate (ad esclusione, come evidenziato in premessa, del *MiCA*), ossia:

- la cd. Direttiva “Prospetto” (Direttiva 2003/71/CE, sostituita dal Regolamento 2017/1129/UE), relativa al prospetto da pubblicare per l'offerta pubblica o l'ammissione alla negoziazione di strumenti finanziari, che si applicherebbe nell'ipotesi di *crypto-asset* offerti al pubblico attraverso *ICO* che superano una determinata soglia;
- la “Direttiva sulla Trasparenza” (Direttiva 2015/50), che imporrebbe agli emittenti di *crypto-asset* di rispettare gli obblighi di informativa periodica e continuativa ivi contemplati;
- il quadro normativo costituito, oltre che dalla Direttiva 2014/65/UE (*MiFID II*), anche dal Regolamento 600/2014/UE (*MiFIR*), da cui deriva la qualificazione delle attività connesse ai *crypto-asset* (es. collocamento, negoziazione, servizi e attività di investimento ecc.);
- il Regolamento sul *Market Abuse (MAR)*, Regolamento 596/2014/UE, da cui deriverebbero una serie di obblighi informativi incombenti principalmente sulle piattaforme di negoziazione finalizzati a prevenire, individuare e segnalare gli abusi di mercato;

di godere di deroghe normative transitorie, sperimentando su scala ridotta e per un periodo limitato tecnologia e servizi. L'utilizzo di tale strumento è in linea con la posizione del Parlamento Europeo (Vds. [Commissione per i problemi economici e monetari, Relazione sulla tecnologia finanziaria: l'influenza della tecnologia sul futuro del settore finanziario, proposta di risoluzione \(relatore: Cora van Nieuwenhuizen\), 2016/2243\(INI\), 2017](#)), il quale «raccomanda che le autorità competenti consentano e incoraggino la sperimentazione controllata con le nuove tecnologie per i nuovi operatori di mercato e per quelli esistenti; osserva che un simile ambiente controllato per le sperimentazioni potrebbe assumere la forma di uno spazio di sperimentazione normativa (“sandbox”) per i servizi fintech che presentano potenziali benefici per la società, che riunisce una vasta gamma di operatori di mercato ed è già stato introdotto con successo in diversi Stati membri». In tale contesto, si segnala il “joint report” pubblicato dalle Autorità di supervisione europee (Vds. [EBA-ESMA-EIOPA, FinTech: Regulatory sandboxes and innovation hubs, 2018](#)) su mandato della Commissione Europea nell'ambito del *Fintech Action Plan*. Su tale impulso molti Stati membri nell'UE (tra cui figura anche l'Italia) hanno costituito i cd. “facilitatori fintech”, che delineano degli spazi di sperimentazione normativa (sotto forma di *innovation hubs* o di *regulatory sandboxes*) che sviluppino ulteriormente l'idea dei poli di innovazione creando un ambiente in cui la vigilanza è adattata alle esigenze delle imprese.

²⁰⁸ [ESMA, Advice, Initial Coin Offerings and Crypto-Assets, ESMA50-157-1391, 2019](#). Per un'analisi approfondita, si veda, [Pantaleo A. e Davico D., ESMA rilascia il proprio parere sui crypto-assets, 2019](#).

- il Regolamento sulle Vendite allo Scoperto (*short selling*), Regolamento 236/2012/UE, il quale risulterebbe applicabile nell'ipotesi in cui una posizione nel mercato dei *crypto-asset* conferisca un vantaggio finanziario in caso di diminuzione del prezzo o del valore di un titolo azionario o di un titolo di debito;
- la Direttiva *SFD* (*Settlement Finality Directive*), Direttiva 2009/44/CE, e il Regolamento *CSDR* (*Central Securities Depository Regulation*), Regolamento 909/2014/UE, con particolare riferimento al sistema di custodia e registrazione dei titoli;
- la Direttiva sui Gestori di Fondi di Investimento Alternativi (*AIFMD*), Direttiva 2011/61/UE, la quale potrebbe essere applicabile a determinati *crypto-asset*, nella misura in cui questi fossero qualificabili come quote di organismi di investimento collettivo;
- la Direttiva sui sistemi di indennizzo degli investitori (Direttiva 97/9/CE), la quale si applica alle imprese *MiFID* in relazione agli strumenti finanziari *MiFID*;
- la V Direttiva antiriciclaggio e sul finanziamento del terrorismo (Direttiva 2018/843/UE).

Come emerge chiaramente al di fuori del perimetro *MiCA*, gli *asset* digitali non regolamentati in tale contesto, pur suscettibili di una loro qualificazione in ambito *MiFID*, appaiono ancora di difficile collocamento e gestione, proprio in quanto indirizzati verso un regime sperimentale e per sua natura transitorio²⁰⁹.

Il *MiCA* non esclude solo gli “strumenti finanziari” dal suo campo di applicazione. L’art. 2, commi 3 e 4, in particolare chiariscono che il Regolamento non si applica alle crypto-attività che sono uniche e non fungibili con altre crypto-attività (es. gli *NFT*), né a quelle che rientrano in una o più delle seguenti definizioni:

- strumenti finanziari (di cui si è già detto);
- depositi, compresi i depositi strutturati;
- fondi, eccetto ove siano qualificabili come *token* di moneta elettronica;
- posizioni inerenti a cartolarizzazione nel contesto di una cartolarizzazione ai sensi dell’articolo 2, punto 1, del Regolamento 2017/2402/UE;

²⁰⁹ Al fine di garantire una chiara distinzione tra, da un lato, le crypto-attività disciplinate dal *MiCA* e, dall’altro, gli strumenti finanziari, l’*ESMA* è stata incaricata di emanare orientamenti sui criteri e sulle condizioni per la qualificazione delle crypto-attività come strumenti finanziari.

- prodotti assicurativi non vita o vita che rientrano nelle classi di assicurazione elencati negli allegati I e II della Direttiva 2009/138/CE del Parlamento Europeo e del Consiglio o contratti di riassicurazione e retrocessione di cui alla stessa Direttiva;
- i prodotti pensionistici che, ai sensi del diritto nazionale, sono riconosciuti come aventi lo scopo principale di offrire all'investitore un reddito durante la pensione e che consentono all'investitore di godere di determinati vantaggi;
- gli schemi pensionistici aziendali o professionali riconosciuti ufficialmente che ricadono nell'ambito di applicazione della Direttiva 2016/2341/UE del Parlamento Europeo e del Consiglio o della Direttiva 2009/138/CE;
- i singoli prodotti pensionistici per i quali il diritto nazionale richiede un contributo finanziario del datore di lavoro e nei quali il lavoratore o il datore di lavoro non può scegliere il fornitore o il prodotto pensionistico;
- un prodotto pensionistico individuale paneuropeo come definito all'articolo 2, punto 2), del Regolamento 2019/1238/UE del Parlamento Europeo e del Consiglio;
- regimi di sicurezza sociale contemplati dal Regolamento 883/2004/CE e 987/2009/CE del Parlamento Europeo e del Consiglio.

Alla luce di quanto sinora evidenziato, possiamo senz'altro osservare come il merito, tutt'altro che scontato, del *MiCA* sia stato quello di fornire un quadro regolamentare unitario, chiaro e coerente per i *crypto-asset* ivi disciplinati, in grado di offrire maggiore certezza giuridica per gli operatori del settore. A questo si devono aggiungere ulteriori aspetti positivi che discendono dagli obiettivi stessi perseguiti con il Regolamento, quali:

- proteggere gli investitori e i consumatori dalla volatilità e dall'insicurezza degli *asset* digitali. Lo scopo è garantire che gli *asset* digitali soddisfino determinati requisiti di trasparenza, informazione e protezione degli investitori, al fine di ridurre al minimo il rischio di truffe o manipolazioni di mercato;
- promuovere l'innovazione e la competitività nel settore degli *asset* digitali, contribuendo così alla crescita e allo sviluppo economico nella UE;

- contribuire a prevenire il riciclaggio di denaro e il finanziamento del terrorismo, con una regolamentazione che si integra con la normativa *AML*;
- garantire la stabilità finanziaria, richiedendo la presenza di requisiti prudenziali per gli operatori del settore, al fine di ridurre il rischio sistemico associato alle crypto-attività.

Il *MiCA*, inoltre, offre chiarimenti definitivi anche in relazione ai servizi di *crypto-asset* e ai loro fornitori. Precisa, in particolare, che per “servizio per le crypto-attività” deve intendersi uno qualsiasi dei seguenti servizi ed attività:

- prestazione di custodia e amministrazione di crypto-attività per conto di clienti;
- gestione di una piattaforma di negoziazione di crypto-attività;
- scambio di crypto-attività con fondi;
- scambio di crypto-attività con altre crypto-attività;
- esecuzione di ordini di crypto-attività per conto di clienti;
- collocamento di crypto-attività;
- ricezione e trasmissione di ordini di crypto-attività per conto di clienti;
- prestazione di consulenza sulle crypto-attività;
- prestazione di gestione di portafoglio sulle crypto-attività;
- prestazione di servizi di trasferimento di crypto-attività per conto dei clienti.

Come già evidenziato, il *MiCA* definisce “*Crypto-Asset Service Provider*” (*CASP*) come «qualsiasi persona la cui occupazione o attività consiste nella fornitura di uno o più servizi di criptovalute a terzi su base professionale». La definizione è più ampia di quella relativa ai “*Virtual Asset Service Provider*” (*VASP*) adottata in ambito GAFI e attualmente vigente nell’ambito delle direttive *AMLD*. In tale contesto, tra i *VASP* sono inclusi i soggetti che svolgono professionalmente una delle attività seguenti: conversione tra *virtual asset* e valute legali; conversione tra *virtual asset*; trasferimento di *virtual asset*; custodia e/o amministrazione di *virtual asset* o di strumenti che ne consentono il controllo; partecipazione e fornitura di servizi finanziari relativi all’offerta e/o alla vendita di *virtual asset* (il riferimento è alle *Initial Coin Offerings – ICO*).

3. La genesi dei CASP: quali profili regolatori oltre i VASP?

3.1. Il quadro normativo italiano in materia di VASP: il nuovo ruolo dell'Organismo Agenti e Mediatori (OAM) dopo il DM 13 gennaio 2022

In sede di commento alla nuova regolazione europea, è apparso fin da subito una certa somiglianza tra la definizione di *Crypto-Asset Service Provider (CASP)* e quella di *Virtual Asset Service Provider (VASP)*. La seconda espressione appena menzionata si rinviene all'articolo 1, comma 2, lettera f) del decreto legislativo 21 novembre 2007, n. 231, concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminosi e di finanziamento del terrorismo, per come modificato successivamente a mezzo del decreto legislativo n. 125 del 2019, attuativo delle Direttive (UE) 2018/843 e 2015/849, su cui avremo modo di soffermarci più diffusamente oltre.

In questa sede, tuttavia, non può non osservarsi come una siffatta analogia non abbia attirato le attenzioni degli addetti ai lavori, suscitando interrogativi in merito alle rispettive delimitazioni definitorie. Conviene dunque indagare gli ambiti di regolazione che per primi hanno fornito una rappresentazione normativa della figura dei VASP. Nello specifico, per *«fornitori di servizi relativi all'utilizzo virtuale»* il succitato decreto legislativo del 2007 ha inteso *«ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, anche online, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute»*.

Nel contesto delle proprie Raccomandazioni (su cui ci soffermeremo più diffusamente oltre), già nel 2018 il GAFI aveva chiarito come le stesse dovessero coinvolgere anche le attività finanziarie in *virtual asset*, al contempo considerando anche la figura dei *«prestatori di servizi in materia di virtual asset»*. Le linee guida del 2019 avevano considerato la questione nel contesto del più ampio ambito del contrasto al finanziamento al terrorismo e della

normativa antiriciclaggio²¹⁰. Più in particolare «le (...) linee guida sottolineano la necessità, per i paesi e i VASP e per altre entità coinvolte in attività concernenti i Virtual Asset, di comprendere i rischi ML/TF associati a dette attività e di adottare appropriate misure correttive per affrontarli. In particolare, le linee guida forniscono esempi di indicatori di rischio che dovrebbero essere considerati nello specifico in un contesto di Virtual Asset, con un'enfasi su fattori che possono offuscare ulteriormente le operazioni o inibire la capacità dei VASP di identificare i clienti»²¹¹.

D'altronde, in quell'occasione il GAFI sceglieva un approccio proattivo alla gestione del fenomeno, consapevole del lavoro sottostante dei governi nazionali indirizzato verso la diramazione di normazioni dirette a regolamentare l'attività di simili prestatori di servizi. Tuttavia, anche nel caso dei VASP è stato messo in luce il rilevante profilo della transnazionalità delle attività in *crypto-asset* che tanto ha ispirato l'intervento del MiCA in materia di CASP²¹².

Come anticipato prima, anche l'Italia ha curato la sistematizzazione del ruolo dei VASP nel contesto del decreto di attuazione della Direttiva 843/2018/UE, descrivendo gli ambiti di operatività di tali prestatori di servizi isolandone le attività di fornitura di servizi:

- a. funzionali allo scambio e alla conservazione di valuta virtuale;

²¹⁰ Cfr. [Gruppo d'Azione Finanziaria Internazionale, Linee guida per un approccio ai virtual asset e ai prestatori di servizi in materia di virtual asset basato sul rischio](#), MEF - Dipartimento del Tesoro, 2019.

²¹¹ Ivi, pag. 6 – Sintesi esecutiva. Si noti, comunque, che «le linee guida descrivono l'applicazione delle raccomandazioni FATF ai paesi e alle autorità competenti, nonché ai VASP e ad altre entità obbligate che svolgono attività concernenti VA, ivi inclusi istituzioni finanziarie quali, tra gli altri, banche e intermediari finanziari gestori di valori mobiliari. Quasi tutte le raccomandazioni FATF sono direttamente formulate per affrontare i rischi ML/TF associati coi VA e i VASP, mentre altre raccomandazioni sono connesse in misura minore, sia ciò direttamente o indirettamente, ai VA e ai VASP - per quanto comunque pertinenti e applicabili. I VASP sono pertanto soggetti allo stesso insieme di obblighi che interessano le istituzioni finanziarie o i DNFBP (...) Infine, le linee guida forniscono esempi di approcci nazionali per disciplinare, vigilare e applicare la normativa alle attività concernenti VA, VASP e alle altre entità obbligate nel contesto AML/CFT».

²¹² Ibidem, pag. 9, ove si afferma che «il rapido sviluppo, la crescente funzionalità, la maggior adozione e la natura globale e transfrontaliera dei VA rendono pertanto una priorità chiave del FATF che i paesi intervengano con urgenza per mitigare i rischi ML/TF posti dalle attività concernenti VA e dai VASP. Se da un lato le presenti linee guida sono pensate per facilitare l'applicazione del summenzionato approccio basato sul rischio per finalità AML/CFT, dall'altro lato il FATF riconosce che altri tipi di considerazioni politiche possano entrare in gioco e che esse possano dare forma alla risposta normativa al settore VASP nelle singole giurisdizioni».

- b. di conversione delle valute virtuali da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali;
- c. di emissione, offerta, trasferimento e compensazione;
- d. ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle valute virtuali.

In punto di controlli, peraltro, in Italia opera l'Organismo Agenti e Mediatori (cd. OAM)²¹³, competente in via esclusiva ed autonoma – come è possibile leggere dalle note legali del portale istituzionale – per la gestione degli elenchi e degli agenti in attività finanziaria e dei mediatori creditizi. L'Organismo svolge una funzione di tutela del consumatore, vigilando sulla professionalità dei soggetti iscritti, sulla compatibilità delle attività realizzate dagli operatori con il quadro normativo, nonché contribuendo alla regolamentazione del mercato di riferimento. Interessante a questo punto pare analizzare le statistiche fornite dall'OAM in relazione all'andamento dei servizi forniti dai *VASP* in Italia. Nel secondo trimestre 2023, in particolare, risulta che il possesso da parte della clientela di criptovalute ammonti ad oltre 1,2 miliardi di euro. Parimenti, sembra crescere anche il numero di *VASP* che hanno comunicato all'Organismo i dati del portafoglio clienti di cui hanno la gestione. *«Rispetto ai dati del I trimestre, rielaborati alla luce delle rettifiche e integrazioni effettuate dagli operatori, risulta in calo sia il controvalore in euro del saldo delle valute virtuali detenuto che il numero di clienti, rispettivamente dell'8% e del 15 per cento. Risultano in aumento invece sia i VASP iscritti al Registro (+9%) sia la percentuale che ha trasmesso i dati (+3%)»*, è quanto fa sapere l'Organismo in parola rispetto ai dati in esame nel periodo considerato.

Al riguardo, occorre precisare che l'istituzione (presso l'OAM) del Registro dedicato ai Prestatori di servizi per l'utilizzo di valuta virtuale e di *wallet* digitali operanti sul territorio italiano è stata introdotta dal decreto ministeriale 13 gennaio 2022. L'iscrizione implica precisi obblighi continuativi di raccolta e trasmissione di informazioni sulle operazioni realizzate, lungi dal potersi limitare ad un generico resoconto compilativo: l'individuazione del cliente, a titolo esemplificativo, deve contenere gli estremi identificativi di ciascuno.

²¹³ L'OAM è stato istituito dal decreto legislativo 13 agosto 2010, n. 141, con personalità giuridica di diritto privato, in forma di fondazione. Dispone, dunque, di autonomia organizzativa, statutaria e finanziaria.

In relazione al dato ricevuto, l'OAM può compiere analisi basate sull'utilizzo delle criptovalute da parte degli investitori, sia in relazione all'operatività dei VASP sia in riferimento alla natura giuridica degli investitori stessi.

Infatti, *«con riferimento alla natura giuridica degli investitori in criptovalute, sia i saldi totali delle valute legali e virtuali che il numero e il controvalore delle operazioni di conversione delle valute legali in valute virtuali e viceversa, assumono percentuali rilevanti soprattutto per i clienti nella forma di persona fisica con età maggiore di 40 anni e per i clienti nella forma di persona giuridica con sede legale all'estero. In merito ai trasferimenti di valuta virtuale sia in uscita che in entrata da/verso il Prestatore di servizi relativi all'utilizzo di valuta virtuale, il maggior numero delle operazioni è stato svolto da clienti persone fisiche con età compresa tra i 18 e i 40 anni (circa il 70%) e da società con sede legale all'estero (oltre il 90%). Tali operazioni hanno riguardato per lo più i VASP di grandi dimensioni»*²¹⁴. Per quanto concerne le variazioni trimestrali dei flussi informativi si legge invece che *«rispetto al primo trimestre 2023, il numero dei VASP iscritti nel Registro tenuto dall'OAM è aumentato del 9%, passando da 105 a 114 operatori al 30 giugno 2023. Il numero dei clienti trasmessi è invece diminuito del 12%. Inoltre, nel secondo trimestre si registrano variazioni percentuali negative sia del numero di investitori che del controvalore in euro del saldo totale delle valute virtuali detenute rispettivamente del 15 e 8 per cento. Con riferimento alle operazioni di conversione da valuta legale a virtuale e viceversa, si evidenzia un calo del numero delle operazioni di oltre 40 punti percentuali e del numero di clienti di oltre 20 punti percentuali»*.

Insomma, l'OAM costituisce certamente un osservatorio privilegiato per quanto concerne l'andamento e la regolamentazione dei cd. VASP sul territorio. D'altra parte, come confermato anche dal Presidente dell'Organismo, si tratta di *«una vigilanza tesa soprattutto a prevenire comportamenti non in linea con la normativa, senza rinunciare ovviamente allo strumento sanzionatorio. Non è casuale che anche nel 2022 si sia fatto ricorso alla moral suasion con 232 raccomandazioni agli iscritti, su aspetti che vanno dalla trasparenza delle condizioni contrattuali e dei rapporti con i clienti, alla non totale adeguatezza dei sistemi di*

²¹⁴ Vds. [OAM, Primo flusso informativo trasmesso all'OAM dai prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale, I° trimestre, 2023](#).

controllo interno rispetto alla struttura societaria del Mediatore creditizio, passando per una gestione della cessione del V non del tutto trasparente, fino a ritardi nel conseguimento dell'aggiornamento professionale e stipula polizza RC»²¹⁵.

È la funzione di vigilanza a costituire un primo baluardo nei confronti degli operatori dei servizi digitali, allo scopo di attuare una concreta opera di sensibilizzazione verso un corretto uso dello strumento virtuale. Comunque, il Comitato di Gestione OAM ha la possibilità di deliberare sanzioni che vanno oltre la mera raccomandazione (utilizzabile laddove si tratti di comportamenti passibili di semplici censure o richiami). Tanto è vero che *«lo scorso anno il Comitato di Gestione ha deliberato, su proposta dell'Ufficio competente, 148 provvedimenti di cui 23 richiami scritti, 84 sanzioni pecuniarie, 9 sospensioni sanzionatorie e 32 archiviazioni. Le violazioni sanzionate dall'Organismo hanno riguardato, per la gran parte dei casi (il 34%), il mancato adempimento all'obbligo di aggiornamento professionale, seguito dal mancato riscontro alle richieste dell'Organismo e dalla mancata o tardiva comunicazione dei dati. Sono stati riscontrati anche casi di elusione della disciplina del mono-mandato, e di cessione o ricezione di segnalazioni di richieste di finanziamento tra soggetti non autorizzati»*.

In tal misura, pare effettivamente tangibile l'intento organizzatorio e, comunque, regolatorio che si pone a fronte della previsione di un organismo qual è l'OAM. Ci si chiede, d'altro canto, in che misura e quale sia la portata legata ad un effetto deterrente allocabile in capo a un'organizzazione con tali fattezze (che opera giuridicamente con lo statuto di Fondazione). Inoltre, come traspare dai lavori preparatori dei progetti di legge della Camera dei Deputati, Consob e Banca d'Italia sono state formalmente individuate *«quali autorità competenti ai sensi dell'articolo 93, paragrafo 1, del regolamento (UE) 2023/1114, anche prevedendo opportune forme di coordinamento per evitare duplicazioni e sovrapposizioni e ridurre al minimo gli oneri gravanti sui soggetti vigilati»*, e di conseguenza anche *«quali punti di contatto, ai sensi dell'articolo 93, paragrafo 2, del regolamento (UE) 2023/1114, per la cooperazione amministrativa transfrontaliera tra le autorità competenti nonché con l'Autorità bancaria europea e l'Autorità europea degli strumenti finanziari e dei mercati,*

²¹⁵ Cfr., [Alfonso F., Intermediari del Credito: dall'Europa la sfida verso il Cambiamento, Intervento del Presidente dell'OAM al Leadership Forum Summer Roma, 2023.](#)

in coerenza con le disposizioni nazionali vigenti che attengono alla cooperazione con le predette autorità europee»²¹⁶. Se suddette Autorità venissero confermate, ci si chiede se (e come) il ruolo dell'OAM (che nel frattempo avrà certamente sviluppato una discreta esperienza nel settore) eventualmente si rinnoverà o verrà invece destituita del tutto dal suo attuale compito. Si tratta di domande e riflessioni inevitabilmente aperte per l'operatore, che non potrà far altro che osservare l'andamento di simili interventi, in una prospettiva che ne assicuri l'utile proiezione a livello di tutela del mercato.

3.2. Da VASP a CASP: una novità formale o sostanziale?

A integrazione di quanto osservato nel paragrafo precedente, nel fornire la definizione di CASP, appare necessario evidenziare come la normativa MiCA si muova entro un perimetro più ampio di quello tracciato dal GAFI con riferimento ai VASP. Pertanto, volendo riassumere le specifiche attività/operazioni che caratterizzano le due categorie soggettive, per come sono state regolamentate nei rispettivi ambiti, valga la seguente ricapitolazione:

CASP	VASP
a. prestazione di custodia e amministrazione di cripto-attività per conto di clienti; b. gestione di una piattaforma di negoziazione di cripto-attività; c. scambio di cripto-attività con fondi; d. scambio di cripto-attività con altre cripto-attività; e. esecuzione di ordine di cripto-attività per conto di clienti; f. collocamento di cripto-attività;	a. cambio tra <i>virtual asset</i> e valute <i>fiat</i>; b. cambio tra una o più forme di <i>virtual asset</i>; c. trasferimento di <i>virtual asset</i>; d. custodia e/o amministrazione di <i>virtual asset</i> o strumenti che consentono controllo di <i>virtual asset</i>; e. partecipazione e prestazione di servizi finanziari correlati all'offerta di un emittente e/o alla vendita di un <i>virtual asset</i>.

²¹⁶ [Camera dei Deputati, Lavori preparatori dei progetti di Legge, Atto Camera: 1342. Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2022-2023" \(1342\), 2023.](#)

g. ricezione e trasmissione di ordini di cripto-attività per conto di clienti; h. ricezione e trasmissione di ordini di cripto-attività per conto di clienti; i. prestazione di gestione di portafoglio sulle cripto-attività; j. prestazione di servizi di trasferimento di cripto-attività per conto dei clienti.	

Pertanto, osservando la differenza di ampiezza dei margini regolatori, si potrebbe asserire come il confine tra le due proiezioni sia questione di sfumature terminologiche. In realtà, proprio la portata più ampia della definizione di *CASP* farà sì che i *VASP* verranno inevitabilmente attratti nel perimetro definitorio allargato adottato nell'ambito del Regolamento *MiCA*. Ciò vale, tuttavia, nell'ambito dell'Unione Europea dove il Legislatore procederà quanto prima ad adeguare le regole definitorie recate nella propria normativa antiriciclaggio, sino ad oggi mutuata dalle linee guida del GAFI, a quelle più allargate introdotte dal *MiCA*. Come vedremo, ciò è già contemplato nella proposta di regolamento relativo alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio e finanziamento del terrorismo (cd. *AMLR VI*); proposta che fa parte di un pacchetto *AML/CFT* composto da quattro proposte legislative considerato come un unico insieme coerente, in attuazione del piano d'azione della Commissione del 7 maggio 2020.

Ciò comporterà che in ambito unionale troverà applicazione ed attuazione (con riferimento al quadro di regole che disciplinano sia i mercati delle cripto-attività sia i connessi presidi antiriciclaggio) la definizione di *CASP*, quale ambito allargato di soggetti che forniscono servizi per le cripto-attività, mentre in ambito sovraunionale continuerà a farsi riferimento al più ristretto nucleo soggettivo tracciato dal GAFI (sempre che quest'ultimo non riveda la proprie raccomandazioni per armonizzarle alla regolamentazione europea).

4. Inquadramento generale dei CASP: la disciplina MiCA

4.1. Premesse: le logiche del bilanciamento tra le istanze regolatorie e le dinamiche di un mercato a-territoriale

Come anticipato in apertura di trattazione, il Regolamento 2023/1114/UE ha delineato per la prima volta il quadro definitorio che ruota attorno ai *Crypto-Asset Service Provider*, fornendone un esaustivo *framework* regolatorio. Anche alla luce degli scarsi contributi dottrinari rinvenibili sul tema nonché in considerazione dell'elevato impatto di tale regolamentazione sul sistema normativo nazionale ed europeo che presiede al corretto andamento dei mercati e alla tutela delle imprese e degli investitori, vale dunque la pena soffermarsi sul testo dell'atto normativo sovranazionale in modo da delinearne i tratti principali e consentire contestualmente la migliore analisi delle problematiche di fondo.

Pare opportuno dare inizio a questa parte del lavoro richiamando la presa d'atto che ha ispirato l'avvio delle discussioni sull'argomento (espressa nel *Considerando* n. 73 del MiCA), ossia che «nella maggior parte degli Stati membri la prestazione di servizi per le crypto-attività non è ancora regolamentata, malgrado i potenziali rischi che essi comportano per la protezione degli investitori, l'integrità del mercato e la stabilità finanziaria. Per far fronte a tali rischi, il presente regolamento prevede requisiti operativi, organizzativi e prudenziali a livello dell'Unione applicabili ai prestatori di servizi per le crypto-attività».

Si è già dato conto, sia pur brevemente, della necessità di intervenire – fornendone una più compiuta sistematizzazione normativa su di un piano quanto più armonizzato possibile – sul mercato dell'intermediazione finanziaria in *crypto-asset*.

D'altro canto, non si può prescindere dall'analisi di un ulteriore profilo critico connesso alle questioni che si vanno ad approfondire. Effettivamente, l'assenza di un vincolo territoriale connesso all'attività di simili prestatori di servizio fa il paio con le criticità marginalmente rilevate da parte della dottrina: come assicurare un efficace controllo della gestione delle attività dei *service provider* ove gli stessi siano in grado di delocalizzare la rispettiva presenza anche in Paesi *extra* europei? Se, da un canto, il Regolamento MiCA ha tenuto ben presente le questioni di giurisdizione che potrebbero venire in rilievo laddove la prestazione di servizi fosse assicurata da soggetti non europei, d'altro canto non si può

manca di evidenziare una tutela sempre “carente” a fronte degli spazi sterminati sui quali si muove il mercato digitale.

D'altronde, il distacco dalla dimensione fisica dell'intermediazione crea inevitabilmente vuoti di de-regolamentazione, con quanto ne consegue in termini di carenze di tutela e rischi per il consumatore. A riguardo, proprio in ragione di tale potenziale *vulnus*, il *MiCA* richiede che i *CASP* siano assoggettati – seppur ai fini della normativa antiriciclaggio - ad obblighi di monitoraggio e di valutazione rafforzati a cui adempiere nel caso in cui le transazioni in cripto-attività riguardino Paesi terzi ad alto rischio²¹⁷.

Va da sé che i prestatori di servizi assoggettati alla disciplina regolamentare in argomento siano quelli la cui sede di direzione effettiva si trovi sul territorio unionale e almeno uno dei soggetti deputati all'amministrazione risieda nell'Unione Europea. Condizione quest'ultima che consente di svolgere una più incisiva “vigilanza prudenziale” sulle attività di intermediazione, oltre alla migliore tutela del mercato e degli stessi investitori (salvaguardandone la stabilità finanziaria).

Inoltre, soprattutto in considerazione delle “dimensioni relativamente ridotte” dei prestatori di servizio in argomento, lo stesso Regolamento tramite l'utilizzo di un'efficace tecnica di rinvio normativo rileva l'opportunità che l'autorizzazione ed il controllo delle attività di simili soggetti sia rimessa alle singole Autorità nazionali competenti (per tali, intendendo quelle dello Stato membro del quale il prestatore mantiene la propria sede legale).

Le autorizzazioni fornite dallo Stato membro di riferimento possono essere modulate in funzione del miglior controllo anche a posteriori dell'attività effettivamente svolta: da qui la necessità che rechino l'esatta indicazione dei servizi per le cripto-attività che il prestatore intende fornire (rimanendo comunque valide su tutto il territorio unionale).

Insomma, inizia a delinearsi il profilo delle tutele e del bilanciamento di valori verso i quali tende la regolamentazione *MiCA* che questa parte della trattazione ha l'onere di esaminare. Per tali motivi, anche la protezione del consumatore, soprattutto in considerazione di

²¹⁷ Più in particolare, come evidenziato nel *Considerando* n. 77 «*al fine di garantire la continua protezione del sistema finanziario dell'Unione dai rischi di riciclaggio e di finanziamento del terrorismo, è necessario garantire che i prestatori di servizi per le cripto-attività effettuino controlli rafforzati sulle operazioni finanziarie che coinvolgono clienti ed enti finanziari di paesi terzi elencati come paesi terzi ad alto rischio poiché hanno giurisdizioni con carenze strategiche nei rispettivi regimi nazionali di lotta al riciclaggio e al finanziamento del terrorismo che pongono minacce significative al sistema finanziario dell'Unione, di cui alla direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio*».

quanto appena osservato in punto di vigilanza che gli Stati membri assicurano, dev'essere esaminata in uno con i rinnovati obblighi imposti ai *provider*. Il diritto del consumo nella nota teorica del “diritto del secondo contratto” non ha mancato di trovare applicazione anche nel contesto delle riflessioni che hanno condotto all'approvazione della normativa in commento.

Al *Considerando* n. 37 è lo stesso Regolamento *MiCA* a richiamare il noto bagaglio giurisprudenziale relativo alla possibilità di recedere dai contratti stipulati per via telematica, in un termine che sia equo (per il consumatore) a rendersi conto della poca convenienza di un affare concluso. Ciò *«al fine di garantire ulteriormente la tutela dei detentori al dettaglio di cripto-attività che acquistano cripto-attività diverse dai token collegati ad attività o dai token di moneta elettronica direttamente dall'offerente o da un prestatore di servizi per le cripto-attività che colloca le cripto-attività per conto dell'offerente dovrebbe essere garantito il diritto di recesso per un periodo di 14 giorni dall'acquisizione. Per assicurare il regolare completamento di un'offerta al pubblico di cripto-attività a tempo limitata, il diritto di recesso non dovrebbe essere esercitato dal detentore al dettaglio dopo la fine del periodo di sottoscrizione. Inoltre, il diritto di recesso non dovrebbe applicarsi nei casi in cui cripto-attività diverse dai token collegati ad attività o dai token di moneta elettronica sono ammesse alla negoziazione prima dell'acquisto da parte del detentore al dettaglio, in quanto in tal caso il prezzo di queste cripto-attività dipende dalle fluttuazioni dei mercati delle cripto-attività»*.

In aggiunta, il *Considerando* n. 79 reca un'ulteriore indicazione di garanzia di tutela per il consumatore (in uno con “l'integrità del mercato” e “la stabilità finanziaria”) asserendo che *«i prestatori di servizi per le cripto-attività dovrebbero sempre agire in modo onesto, corretto e professionale e nel migliore interesse dei loro clienti»*. E ancora, *«i prestatori di servizi per le cripto-attività dovrebbero fornire ai loro clienti informazioni complete, corrette, chiare e non fuorvianti e avvertirli dei rischi connessi alle cripto-attività. I prestatori di servizi per le cripto-attività dovrebbero rendere pubbliche le loro politiche tariffarie, istituire procedure di trattamento dei reclami e adottare una politica solida per individuare, prevenire, gestire e comunicare i conflitti di interesse»*.

In tal misura, si osserva nei *Considerando* al documento, anche i contratti tra prestatori di servizi per le attività crypto e gli stessi consumatori dovrebbero ricadere nell'ambito di applicazione della Direttiva 2002/65/CE (concernente la commercializzazione a distanza dei servizi finanziari ai consumatori), nel caso in cui simili contratti siano oggetto di commercializzazione a distanza. Soffermendosi su quest'ultimo punto, il concetto di "distanza" ha assunto le logiche di un mero parametro classificatorio, per certi versi utile a porre in luce l'obiettivo misura spazio-temporale che si frappone fra il professionista ed il consumatore, che non ha la possibilità di confrontarsi direttamente con il proponente nella fase della negoziazione e della sottoscrizione dello strumento privatistico. Ciò emerge con ancor più chiara evidenza nel contesto della contrattazione virtuale, per il tramite di piattaforme digitali all'uopo strutturate e tali da consentire l'immediata correlazione tra offerta e scambio di prodotti, non sempre favorevole a consentire al consumatore l'acquisizione di una piena consapevolezza in relazione alla bontà e alla convenienza della stipula. Dunque, alla stregua di quanto appena osservato, l'incontrollata diffusione sul *web* di modalità di conclusione di transazioni in crypto-attività ben si presta alla lesione di diritti ormai acquisiti nelle dinamiche consumeristiche.

Chiarito il retroscena che ha plasmato l'intento regolatorio del *MiCA* in questo specifico ambito, lo stesso intento di protezione si rinviene nelle dinamiche connesse all'informativa precontrattuale che i prestatori di servizi in argomento dovrebbero essere chiamati a fornire al cliente.

4.2. Ambito di applicazione del Regolamento MiCA

Nel premettere che il Regolamento entrerà in vigore negli Stati membri a decorrere dal 30 dicembre 2024 (fatta eccezione per il Titolo III e il Titolo IV, che si applicano dal 30 giugno 2024), preme svolgere alcune perimetrazioni relative ai soggetti che ne saranno coinvolti. Tanto, nell'ottica di proseguire nell'inquadramento della figura dei *Crypto-Asset Service Provider*, la cui riconducibilità alle tradizionali classificazioni dottrinali tanto sta facendo discutere gli interpreti.

Com'è possibile derivare dalla lettura dell'articolo 2, già ampiamente citato, l'ambito di applicazione del testo normativo in commento si estende alle «*persone fisiche e giuridiche e*

ad alcune altre imprese coinvolte nell'emissione, nell'offerta al pubblico e nell'ammissione alla negoziazione di crypto-attività o che prestano servizi connessi alle crypto-attività nell'Unione».

D'altronde, interessante è richiamare non solo l'ambito di effettiva perimetrazione soggettiva, ma anche le riserve di esclusione formulate dal Legislatore sovranazionale. Segnatamente, il MiCA, segnatamente *«non si applica:*

- a. alle persone che prestano servizi per le crypto-attività esclusivamente per le loro imprese madri, per le loro filiazioni o per altre filiazioni delle loro imprese madri;*
- b. ai curatori o agli amministratori che agiscono nel corso di una procedura di insolvenza, salvo ai fini dell'articolo 47;*
- c. alla BCE, alle banche centrali degli Stati membri ove agiscano in veste di autorità monetarie o alle altre autorità pubbliche degli Stati membri;*
- d. alla Banca europea per gli investimenti e alle sue controllate;*
- e. al Fondo europeo di stabilità finanziaria e al meccanismo europeo di stabilità;*
- f. alle organizzazioni internazionali pubbliche».*

Non solo, lo stesso Regolamento, come già evidenziato, non si applica alle crypto-attività uniche e non fungibili²¹⁸, né a quelle che rientrano in prodotti già definiti in ambito unionale²¹⁹.

²¹⁸ Cfr. Considerando n. 10: *«Il presente regolamento non dovrebbe applicarsi alle crypto-attività che sono uniche e non fungibili con altre crypto-attività, compresa l'arte digitale e gli oggetti da collezione. Il valore di tali crypto-attività uniche e non fungibili è attribuibile alle caratteristiche uniche di ciascuna crypto-attività e all'utilità che essa offre al possessore del token. Il presente regolamento non dovrebbe applicarsi nemmeno alle crypto-attività che rappresentano servizi o attività materiali che sono unici e non fungibili, come le garanzie dei prodotti o i beni immobili. Sebbene le crypto-attività uniche e non fungibili possano essere negoziate sui mercati ed essere accumulate a fini speculativi, esse non sono facilmente intercambiabili e il valore relativo di una tale crypto-attività rispetto a un'altra, essendo ciascuna unica, non può essere determinato mediante confronto con un'attività di mercato esistente o un'attività equivalente. Tali caratteristiche limitano la misura in cui tali crypto-attività possono avere un uso finanziario, limitando in tal modo i rischi per i possessori e il sistema finanziario e giustificandone l'esclusione dall'ambito di applicazione del presente regolamento».*

²¹⁹ Così si legge all'articolo 2 del Regolamento MiCA *«il presente regolamento non si applica alle crypto-attività che rientrano in una o più delle definizioni seguenti:*

- a) strumenti finanziari;*
- b) depositi, compresi i depositi strutturati;*
- c) fondi, eccetto ove siano qualificabili come token di moneta elettronica;*
- d) posizioni inerenti a cartolarizzazione nel contesto di una cartolarizzazione ai sensi dell'articolo 2, punto 1, del regolamento (UE) 2017/2402;*

Di immediata evidenza è la dinamica residuale e – comunque – unitaria che ha giustificato l'adozione del testo. L'intento del Legislatore sovranazionale è stato quello di sistematizzare il mercato delle crypto-attività, muovendo – per quanto possibile – in direzione di un quadro generale unionale, capace di raccogliere ed aggregare il consenso e la consapevolezza dei cittadini attorno ad una disciplina coordinata e organizzata²²⁰. Si è già dato conto infatti, in apertura, dei requisiti di residualità connessi alla disciplina in esame, dedicata fondamentalmente a tracciare i profili regolatori che la disciplina europea già in vigore nel settore finanziario tralascia di affrontare. In tal misura, è pure evidente come sia lo strumento del controllo e della vigilanza da parte delle competenti autorità ad aver subito il principale rafforzamento, a fronte di una disciplina lungi dal dirsi esaurita nell'adozione del Regolamento in commento²²¹. Secondo un'attenta osservazione dottrinale «*in questa*

e) prodotti assicurativi non vita o vita che rientrano nelle classi di assicurazione elencati negli allegati I e II della direttiva n. 2009/138/CE del Parlamento europeo e del Consiglio o contratti di riassicurazione e retrocessione di cui alla stessa direttiva;

f) i prodotti pensionistici che, ai sensi del diritto nazionale, sono riconosciuti come aventi lo scopo principale di offrire all'investitore un reddito durante la pensione e che consentono all'investitore di godere di determinati vantaggi;

g) gli schemi pensionistici aziendali o professionali riconosciuti ufficialmente che ricadono nell'ambito di applicazione della direttiva (UE) 2016/2341 del Parlamento europeo e del Consiglio o della direttiva 2009/138/CE;

h) i singoli prodotti pensionistici per i quali il diritto nazionale richiede un contributo finanziario del datore di lavoro e nei quali il lavoratore o il datore di lavoro non può scegliere il fornitore o il prodotto pensionistico;

i) un prodotto pensionistico individuale paneuropeo come definito all'articolo 2, punto 2), del Regolamento (UE) 2019/1238 del Parlamento europeo e del Consiglio;

j) regimi di sicurezza sociale contemplati dal Regolamento (CE) 883/2004 (30) e (CE) n. 987/2009 del Parlamento europeo e del Consiglio».

²²⁰ Cfr. Considerando n. 5: «L'assenza di un quadro generale dell'Unione per i mercati delle crypto-attività può portare gli utenti a non avere fiducia in tali attività, il che potrebbe rappresentare un notevole ostacolo allo sviluppo di un mercato delle crypto-attività e condurre alla perdita di opportunità in termini di servizi digitali innovativi, strumenti di pagamento alternativi o nuove fonti di finanziamento per le imprese dell'Unione. Inoltre, per le imprese che utilizzano crypto-attività non vi sarebbe alcuna certezza del diritto sul modo in cui le crypto-attività in loro possesso sarebbero trattate nei diversi Stati membri, il che ne pregiudicherebbe gli sforzi tesi a utilizzare le crypto-attività per l'innovazione digitale. L'assenza di un quadro generale dell'Unione in materia di crypto-attività potrebbe anche portare a una frammentazione normativa che falserebbe la concorrenza nel mercato unico, renderebbe più difficile per i prestatori di servizi per le crypto-attività espandere le loro attività su base transfrontaliera e determinerebbe un arbitraggio normativo. I mercati delle crypto-attività sono ancora di dimensioni modeste e ad oggi non costituiscono una minaccia per la stabilità finanziaria. È tuttavia possibile che in futuro i detentori al dettaglio adottino in larga misura tipi di crypto-attività che mirano a stabilizzare il loro prezzo in relazione a una specifica attività o a un paniere di attività, e tale sviluppo potrebbe comportare ulteriori sfide in termini di stabilità finanziaria, regolare funzionamento dei sistemi di pagamento, trasmissione della politica monetaria o sovranità monetaria».

²²¹ V. Paracampo M.T., *I prestatori di servizi per le crypto-attività: tra mifidizzazione della MiCA e tokenizzazione della MiFID*, Giappichelli, 2023, p. 5: «Le finalità indicate, all'origine della regolamentazione di detti mercati in funzione di un efficiente funzionamento, unitamente alla supervisione delle Autorità, coinvolgono tutta la filiera, che parte dall'emissione delle crypto-attività e si conclude con la successiva

direzione MiCA diviene la strada normativa per tracciare il primo framework, teso a favorire la creazione e lo sviluppo di mercati – primari e secondari – di cripto-attività non regolamentate dalle vigenti legislazioni settoriali in materia finanziaria e basati inter alia su taluni presupposti fondanti, quali: 1) il riconoscimento di un passaporto europeo per gli emittenti di cripto-attività e per i prestatori di servizi per le cripto-attività; 2) la prestazione cross border dei servizi per le cripto-attività sulla base di regole europee; 3) il rispetto del level playing field per i prestatori di servizi per le cripto-attività, unitamente ad una maggiore chiarezza del relativo trattamento normativo; 4) il superamento della frammentazione del mercato unico e di fenomeni di arbitraggio regolamentare, causati da isolati interventi nazionali in materia; 5) il buon funzionamento del mercato unico delle cripto-attività»²²².

Infine, vale notare che l’elaborazione degli orientamenti utili a stabilire le condizioni e i criteri per la qualificazione delle cripto-attività come strumenti finanziari è rimessa ad una successiva determinazione dell’ESMA (l’Autorità europea degli strumenti finanziari e dei mercati), da adottare entro il 30 dicembre 2024. Ciò, nell’evidente considerazione per cui fornire una classificazione degli *asset* come “strumenti finanziari” o come “cripto-attività”, appare un compito arduo in questa fase del processo²²³. A tal proposito, l’ESMA (la cui timeline è riportata in Figura 7) ha già avviato la fase di implementazione del MiCA ponendo in consultazione tre pacchetti di misure²²⁴ la cui applicazione è subordinata alla loro adozione da parte della Commissione Europea e all’approvazione del Parlamento Europeo e del Consiglio dell’UE.

distribuzione sul mercato, sebbene nel prosieguo l’attenzione sarà dedicata sul secondo momento, quello della circolazione delle cripto-attività sul mercato e, in particolare, sui players ivi coinvolti».

²²² Paracampo M.T., *I prestatori di servizi per le cripto-attività: tra mifidizzazione della MiCA e tokenizzazione della MiFID*, Giappichelli, 2023, pp. 5-6.

²²³ Ivi, cfr. pag. 10.

²²⁴ Il terzo pacchetto, in particolare, copre i seguenti mandati:

- qualificazione delle cripto-attività come strumenti finanziari;
- monitoraggio, rilevamento e notifica degli abusi di mercato;
- tutela degli investitori:
 - sollecitazione inversa;
 - adeguatezza dei servizi di consulenza e di gestione del portafoglio al cliente;
 - politiche e procedure per i servizi di trasferimento di *crypto-asset*, compresi i diritti dei clienti;
- resilienza del sistema e protocolli di accesso di sicurezza.

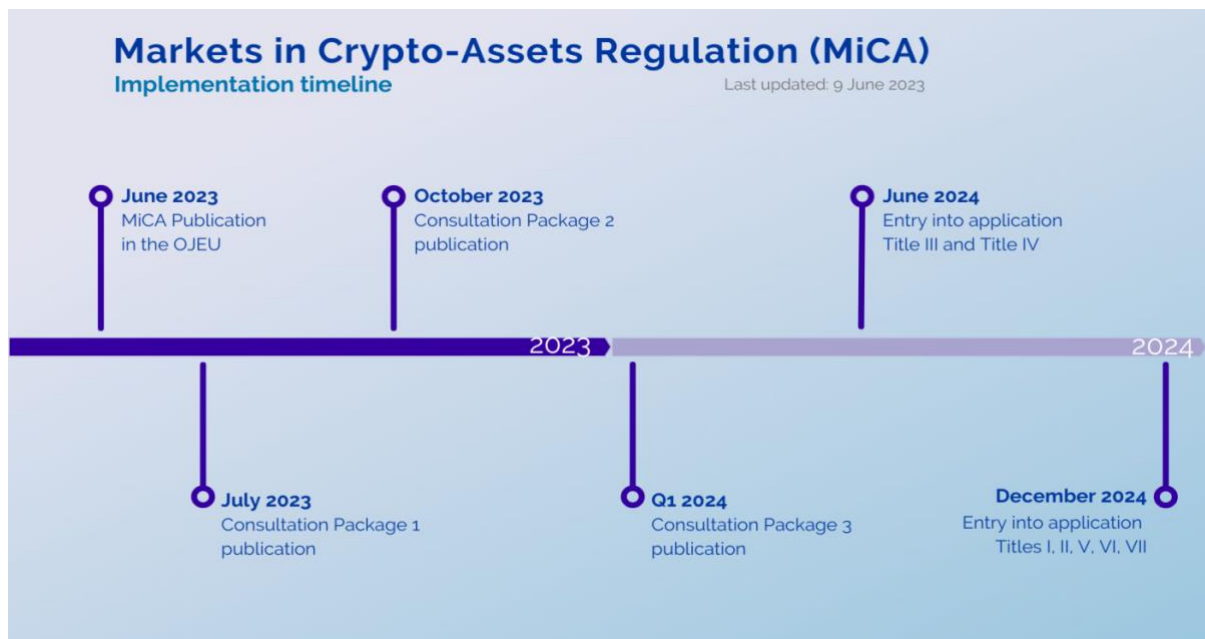


Figura 7 – Fonte: [ESMA, Markets in Crypto-Assets Regulation \(MiCA\), 2023.](#)

4.3. La definizione normativa di “CASP”

Svolta la doverosa premessa di cui sopra, preme subito delineare i profili dei CASP da un punto di vista prevalentemente soggettivo, richiamandosi alla prima definizione che ne fornisce il Legislatore unionale, all’articolo 3, par. 1, punto 15) del Regolamento.

Il CASP è «una persona giuridica o altra impresa la cui occupazione o attività consiste nella prestazione di uno o più servizi per le crypto-attività ai clienti su base professionale e che è autorizzata a prestare servizi per le crypto-attività conformemente all’articolo 59».

Ribadendolo per facilità di lettura, per “servizio per le crypto-attività” si intende «qualsiasi servizio e attività elencati di seguito in relazione a qualsiasi crypto-attività:

- a. prestazione di custodia e amministrazione di crypto-attività per conto di clienti;
- b. gestione di una piattaforma di negoziazione di crypto-attività;
- c. scambio di crypto-attività con fondi;
- d. scambio di crypto-attività con altre crypto-attività;
- e. esecuzione di ordine di crypto-attività per conto di clienti;
- f. collocamento di crypto-attività;
- g. ricezione e trasmissione di ordini di crypto-attività per conto di clienti;

- h. ricezione e trasmissione di ordini di cripto-attività per conto di clienti;
- i. prestazione di gestione di portafoglio sulle cripto-attività;
- j. prestazione di servizi di trasferimento di cripto-attività per conto dei clienti»²²⁵.

All'interno di tale inquadramento i *CASP* si mostrano come soggetti dalla natura giuridica alquanto variegata: il Regolamento non fa riferimento ad una precisa condizione, ma accomuna simili prestatori sulla scorta del servizio prestato e delle autorizzazioni acquisite. La dottrina²²⁶, invero, ha ampiamente argomentato in ordine a simile criterio classificatorio, ipotizzando una partizione tipologica fondata su tre categorie di *CASP*:

- a. i prestatori su richiesta: rappresentano in buona sostanza la tipologia soggettiva “ordinaria”, per i quali il *MiCA* introduce un'apposita procedura autorizzativa;
- b. i prestatori di diritto europeo: si tratta di una serie di soggetti, individuati dall'art. 60 del *MiCA*, già dotati di un “passaporto europeo”, ossia già autorizzati sulla base della normativa europea vigente (vds., ad esempio, i prestatori di servizi di investimento su strumenti finanziari autorizzati ai sensi della regolamentazione *MiFID II*); tali soggetti beneficiano di specifiche esenzioni procedurali ove intendano fornire servizi su cripto-attività;
- c. i prestatori di diritto nazionale: ossia quei soggetti già autorizzati a prestare servizi per le cripto-attività a norma del diritto nazionale, per i quali l'art. 140 del *MiCA* detta un regime transitorio di esenzione procedurale temporanea.

4.4. Autorizzazioni e condizioni di esercizio per i prestatori di servizi per le cripto-attività

Il *MiCA*, come abbiamo osservato, prevede una serie di requisiti e obblighi per gli emittenti e i fornitori di servizi relativi alle criptovalute, al fine di assicurare la trasparenza delle informazioni e la valutazione dei rischi per gli investitori.

²²⁵ *MiCA* – art. 3 “Definizioni”, par. 1, n. 16).

²²⁶ Cfr. Paracampo M.T., *I prestatori di servizi per le cripto-attività. Tra mifidizzazione della MiCA e tokenizzazione della Mifid*, Giappichelli, 2023, p.19 e ss.

In particolare, il Titolo II reca disposizioni tese a garantire che tutte le offerte al pubblico nell'Unione di crypto-attività diverse dai *token* collegati ad attività o dai *token* di moneta elettronica e che tutte le ammissioni di crypto-attività alla negoziazione su una piattaforma di negoziazione (“ammissione alla negoziazione”) nell'Unione siano adeguatamente monitorate e controllate dalle autorità competenti²²⁷.

Al tal fine, i potenziali detentori al dettaglio di crypto-attività devono essere informati in merito alle caratteristiche e ai rischi delle crypto-attività che intendono acquistare. Di conseguenza gli offerenti o le persone che chiedono l'ammissione alla negoziazione sono chiamati a redigere, notificare alla rispettiva autorità competente e pubblicare un documento informativo contenente elementi obbligatori, il cd. “*White Paper* sulle crypto-attività”, che deve recare informazioni di carattere generale sull'emittente, sull'offerente o sulla persona che chiede l'ammissione alla negoziazione, sul progetto da realizzare con i capitali raccolti, sull'offerta al pubblico di crypto-attività o sulla loro ammissione alla negoziazione, sui diritti e sugli obblighi connessi alle crypto-attività, sulla tecnologia sottostante utilizzata per tali crypto-attività, sui relativi rischi e sui principali impatti negativi sul clima e su altri effetti negativi legati all'ambiente del meccanismo di consenso utilizzato per emettere le crypto-attività.

Al fine di garantire un approccio proporzionato, i requisiti di redazione di un *White Paper* sulle crypto-attività previsti dal Regolamento non si applicano alle offerte di crypto-attività diverse dai *token* collegati ad attività o dai *token* di moneta elettronica che sono rivolte a meno di 150 persone per ogni Stato membro o che sono rivolte esclusivamente agli investitori qualificati laddove le crypto-attività possono essere detenute esclusivamente da tali investitori qualificati. Ulteriore esclusione riguarda le piccole e medie imprese e le *start-up* che sono esentate da oneri amministrativi ritenuti eccessivi e sproporzionati. Pertanto, le offerte al pubblico di crypto-attività diverse dai *token* collegati ad attività o dai *token* di moneta elettronica il cui corrispettivo totale non supera la somma di 1.000.000 € su un periodo di 12

²²⁷ In tale contesto si rinviengono talune esclusioni di natura soggettiva, quali: quei soggetti che prestano servizi di crypto-attività all'interno di un gruppo societario, senza rivolgersi al mercato; i curatori o amministratori che agiscano nel corso di una procedura di insolvenza; la BCE e le Banche Centrali degli Stati membri o le altre autorità pubbliche degli Stati membri; la Banca europea per gli investimenti e le sue controllate; il fondo europeo di stabilità finanziaria; le organizzazioni internazionali pubbliche.

mesi sono escluse dall'obbligo di redigere il *White Paper* (non si esclude la possibilità che sia redatto e pubblicato in forma volontaria).

È poi previsto che, prima di presentare qualsiasi offerta al pubblico di cripto-attività nell'Unione o prima che tali cripto-attività siano ammesse alla negoziazione, gli offerenti e le persone che chiedono l'ammissione alla negoziazione notifichino il *White Paper* all'Autorità competente dello Stato membro in cui hanno la sede legale. Autorità che ha il potere di chiedere modifiche o integrazioni al *White Paper* ed eventualmente sospendere o vietare l'offerta al pubblico o l'ammissione alla negoziazione qualora queste non siano conformi ai requisiti previsti dal Regolamento, compresi i casi in cui il *White Paper* non siano corretti, siano poco chiari o forniscano informazioni fuorvianti, con la possibilità di pubblicare avvertenze relative alla denegata autorizzazione. Procedure particolari sono poi previste per gli enti creditizi, per i quali non è prevista la procedura autorizzatoria, pur permanendo l'obbligo di predisporre un *White Paper* da notificare all'Autorità di controllo competente almeno 90 giorni prima dell'emissione del *token*.

Per coerenza argomentativa, va detto che il parametro rimane quello del “*best interest of the client*”, cioè del miglior interesse del cliente, intendendosi per tale non solo il cliente effettivo, ma anche quello solo potenziale, abbracciando una chiara visione prospettica delle possibilità di sviluppo del raggio d'azione dell'intermediazione finanziaria, se così può essere definita.

Come anticipato, i prestatori di servizi vengono inseriti nel più ampio contesto dei lunghi ragionamenti che il diritto unionale ha speso attorno alla tutela dell'informazione negoziale, e dunque alla possibilità che il contraente possa effettivamente godere dell'assetto di informazioni più completo nell'atto dell'adozione della propria intima deliberazione circa la convenienza dell'affare. In quest'ottica, il Regolamento *MiCA* prevede che prestatori di servizi per le cripto-attività forniscano ai loro clienti informazioni corrette, chiare e non fuorvianti, anche nelle comunicazioni di *marketing* che devono essere coerenti con le informazioni contenute nel *White Paper* sulle cripto-attività.

Gli offerenti devono poi garantire l'adozione di misure adeguate volte a monitorare e tutelare i fondi o le altre cripto-attività raccolti durante la loro offerta al pubblico. A tutela degli investitori sono previste diverse forme di garanzia: gli emittenti devono essere persone

giuridiche stabilite in Unione Europea; il possesso, da parte dei prestatori, dei requisiti di onorabilità e professionalità – ad es. non devono essere stati condannati per alcun reato nell’ambito del riciclaggio o del finanziamento del terrorismo -; la restituzione dei fondi in caso di annullamento, per qualsiasi motivo, di un’offerta al pubblico; la tutela offerta da terze parti; il diritto di recesso per un periodo di 14 giorni dall’acquisizione; forme di responsabilità civile a carico dell’offerente.

La normativa europea ha, dunque, modulato attorno alla figura dei *Crypto-Asset Service Provider* una serie di requisiti utili a valutarne l’onestà, la correttezza e la professionalità d’azione *«per garantire la tutela dei detentori al dettaglio, gli emittenti di token collegati ad attività dovrebbero sempre agire in modo onesto, corretto e professionale e nell’interesse dei possessori di token collegati ad attività. Gli emittenti di token collegati ad attività dovrebbero inoltre adottare una procedura chiara per il trattamento dei reclami ricevuti dai possessori di token collegati ad attività»*²²⁸. È lo stesso Regolamento ad evidenziare la necessità che le modalità d’azione del prestatore di servizi si conformi a quelle regole di prudenza che assicurano il corretto funzionamento del sistema economico nel complesso. La volontà di rendere effettivo il rispetto di simili *standard* a mezzo della previsione di modalità

²²⁸ Cfr. Considerando n. 49 al MiCA. E, ancora, al Considerando n. 50: «Gli emittenti di token collegati ad attività dovrebbero mettere in atto una politica volta a individuare, prevenire, gestire e comunicare i conflitti di interesse che possono scaturire dai rapporti che intrattengono con i loro azionisti o soci, o con qualsiasi azionista o socio, siano essi diretti o indiretti, che detenga una partecipazione qualificata negli emittenti, o con i membri dell’organo di amministrazione, i loro dipendenti, i possessori di token collegati ad attività o fornitori terzi di servizi».

Al Considerando n. 51: «Gli emittenti di token collegati ad attività dovrebbero disporre di solidi dispositivi di governance, compresa una chiara struttura organizzativa con linee di responsabilità ben definite, trasparenti e coerenti e procedure efficaci per individuare, gestire, monitorare e segnalare i rischi ai quali sono o potrebbero essere esposti. I membri dell’organo di amministrazione di tali emittenti dovrebbero soddisfare i requisiti di competenza e onorabilità e, in particolare, non dovrebbero essere stati condannati per alcun reato nell’ambito del riciclaggio o del finanziamento del terrorismo o per qualsiasi altro reato che possa incidere sulla loro onorabilità. Gli azionisti o i soci, siano essi diretti o indiretti, persone fisiche o giuridiche, che detengono partecipazioni qualificate in tali emittenti dovrebbero possedere sufficienti requisiti di onorabilità e, in particolare, non dovrebbero essere stati condannati per reati nell’ambito del riciclaggio o del finanziamento del terrorismo o per qualsiasi altro reato che possa incidere sulla loro onorabilità. Gli emittenti di token collegati ad attività dovrebbero inoltre utilizzare risorse proporzionate alla portata delle loro attività e dovrebbero sempre garantire la continuità e la regolarità nello svolgimento delle loro attività. A tal fine, gli emittenti di token collegati ad attività dovrebbero stabilire una politica di continuità operativa che mira a garantire lo svolgimento delle loro attività di base relative ai token collegati ad attività in caso di interruzione dei loro sistemi e delle loro procedure. Gli emittenti di token collegati ad attività dovrebbero inoltre disporre di un solido meccanismo di controllo interno e di procedure efficaci per la gestione del rischio, nonché di un sistema che garantisca l’integrità e la riservatezza delle informazioni ricevute. Tali obblighi mirano a garantire la protezione dei possessori di token collegati ad attività, in particolare dei detentori al dettaglio, senza creare inutili ostacoli».

di reclamo di cui il consumatore/fruttore del servizio possa avvalersi per tutelare al meglio le proprie ragioni. Il Regolamento, inoltre, prevede che gli emittenti di *token* collegati ad attività dovrebbero disporre di solidi dispositivi di *governance*, compresa una chiara struttura organizzativa con linee di responsabilità ben definite. Dovrebbero anche disporre di un solido meccanismo di controllo interno e di procedure efficaci per la gestione del rischio, nonché di un sistema che garantisca l'integrità e la riservatezza delle informazioni ricevute. In particolare, il Titolo III reca disposizioni analoghe ma ben più restrittive con riferimento alle offerte al pubblico e all'ammissione alla negoziazione *token* collegati ad attività (*Asset-referenced token - ART*). Per avviare simili iniziative è necessaria un'apposita autorizzazione da parte dell'Autorità di controllo, salvo che non si rientri in un'ipotesi di esenzione (valore medio dei *token* nei 12 mesi non supera i 5.000.000 € oppure offerta rivolta solamente ad investitori qualificati). Anche in questo caso gli emittenti devono essere persone giuridiche stabilite nella UE e rispettare una serie di requisiti organizzativi, di *governance* e di condotta. Analogamente a quanto già osservato, anche per tali strumenti, le banche non sono soggette ad una particolare procedura autorizzatoria, mentre è necessario che predispongano un *White Paper* da notificare all'Autorità di controllo competente almeno 90 giorni prima dell'emissione del *token*.

Dal momento che gli *ART* sono *token* il cui valore è collegato ad un sottostante (valute, altre crypto-attività, strumenti finanziari ecc.) è previsto l'obbligo per gli emittenti di costituire delle riserve volte a garantire il valore degli *ART* stessi. Riserve che, a seconda della tipologia, devono essere custodite da appositi soggetti, diversi a seconda della tipologia di *asset* a cui si riferiscono. I possessori di *ART* devono avere un diritto di rimborso permanente in modo che l'emittente sia tenuto a rimborsare i *token* in qualsiasi momento. L'emittente di *token* deve rimborsare pagando un importo in fondi diversi dalla moneta elettronica equivalente al valore di mercato delle attività cui si riferiscono gli *ART*, o consegnando le attività cui sono collegati i *token*, o garante la possibilità di riscattare gli *ART* in fondi diversi dalla moneta elettronica denominati nella stessa valuta ufficiale accettata dall'emittente al momento della vendita dei *token*.

Infine, gli emittenti sono chiamati ad effettuare delle comunicazioni trimestrali verso l'Autorità di controllo inerenti ad alcuni elementi rilevanti, in quanto in caso di superamento

di determinati limiti (1 milione di transazioni e €200 milioni all'interno di un'area valutaria unica) è previsto l'obbligo di interrompere l'emissione del *token* e l'indicazione di un piano per la riduzione dei volumi, che deve essere approvato dall'Autorità competente.

Per quanto riguarda i *token* di moneta elettronica (*e-money tokens - EMT*), cui è dedicato il Titolo III, il Regolamento reca delle limitazioni prevedendo in particolare che l'offerta al pubblico o l'ammissione alla negoziazione del *token* siano attivate da un ente creditizio o da un istituto di moneta elettronica. Per tale attività è prevista la redazione di un *White Paper* con contenuti analoghi a quelli previsti per le altre tipologie di *token* già analizzati. I fondi ricevuti in cambio dei *token* devono essere tutelati secondo i requisiti specifici di vigilanza prudenziale, ed almeno il 30% degli stessi deve essere depositato in conti separati mentre la parte rimanente può essere investita in strumenti a basso rischio ed altamente liquidi che sono qualificabili come strumenti finanziari altamente liquidi (denominati nella valuta ufficiale di riferimento del *token* di moneta elettronica). Anche per questa tipologia di *token* è previsto un diritto di riscatto da parte dei possessori, che può essere esercitato in ogni momento con obbligo dell'emittente di liquidare il controvalore nella valuta corrispondente.

A fattor comune, i prestatori di servizi per le cripto-attività sono chiamati ad adottare ed attuare norme operative tese a stabilire i processi di approvazione, inclusi obblighi di adeguata verifica della clientela commisurati al rischio di riciclaggio di denaro o finanziamento del terrorismo che il richiedente presenta in conformità della Direttiva 2015/849/UE. Infine, si evidenzia che l'EBA è stata dotata di speciali poteri di vigilanza, tesi a scongiurare minacce alla stabilità finanziaria o monetaria, prevedendo la possibilità di condurre *stress test* tesi a valutare eventuali pericoli in termini di liquidità e di disponibilità da parte degli emittenti dei fondi corrispondenti.

Il Titolo V del Regolamento è dedicato all'analisi delle autorizzazioni e condizioni di esercizio per i prestatori di servizi per le cripto-attività, cui questo lavoro ritiene di dedicare uno specifico approfondimento, soprattutto in ragione dell'evidenza strategica che simile profilo riveste nell'economia della complessiva trattazione. Nello specifico, la prestazione di servizi per le cripto-attività all'interno degli Stati membri è espressamente riservata, ai sensi dell'art. 59 del *MiCA*, a:

- a. persone giuridiche o altre imprese autorizzate come prestatori di servizi per le cripto-attività²²⁹;
- b. gli enti creditizi o depositari centrali di titoli, imprese di investimento, gestori del mercato, istituti di moneta elettronica, società di gestione di OICVM o gestori di fondi di investimento alternativi autorizzati a prestare servizi per le cripto-attività.

Comunque, quanto appena osservato è da coordinare con le successive previsioni dettate dall'articolo 60 del Regolamento, relativamente alle condizioni alle quali «*talune entità finanziarie*» sono abilitate a prestare servizi per le cripto-attività (il riferimento è, tra gli altri, a: enti creditizi, depositari centrali di titoli autorizzati, imprese di investimento, istituti di moneta elettronica, società di gestione). In ossequio ai principi di libertà di stabilimento, fondanti le dinamiche di integrazione unionale, simili prestatori di servizi sono comunque autorizzati ad operare su tutto il territorio dell'UE, anche fondandovi succursali o prestandovi liberamente la propria attività. La disciplina prevede quale elemento di più rilevante demarcazione la richiesta di un'autorizzazione alle autorità competenti, utile a legittimare la prestazione dei servizi erogati. Per precisione descrittiva, tale richiesta andrà formalizzata presso lo Stato membro d'origine della persona giuridica o dell'impresa interessata dall'ambito di applicazione del Titolo in commento²³⁰. All'esito della presentazione della

²²⁹ Art. 59, par. 3: «*Ai fini del paragrafo 1, lettera a), altre imprese che non sono persone giuridiche prestano servizi per le cripto-attività se la loro forma giuridica garantisce un livello di tutela degli interessi dei terzi equivalente a quello offerto dalle persone giuridiche nonché se sono soggette a una vigilanza prudenziale equivalente adeguata alla loro forma giuridica*».

²³⁰ Si invita a consultare, all'art. 3, comma 1, n. 33) la definizione di Stato membro d'origine, così individuato: «*Stato membro d'origine:*

a) se l'offerente o la persona che chiede l'ammissione alla negoziazione di cripto-attività diverse dai token collegati ad attività o dai token di moneta elettronica ha la propria sede legale nell'Unione, lo Stato membro in cui l'offerente o la persona ha la propria sede legale;

b) se l'offerente o la persona che chiede l'ammissione alla negoziazione di cripto-attività diverse dai token collegati ad attività o dai token di moneta elettronica non ha sede legale nell'Unione ma ha una o più succursali nell'Unione, lo Stato membro scelto dall'offerente o dalla persona tra gli Stati membri in cui l'emittente ha succursali;

c) se l'offerente o la persona che chiede l'ammissione alla negoziazione di cripto-attività diverse dai token collegati ad attività o dai token di moneta elettronica è stabilito in un paese terzo e non ha alcuna succursale nell'Unione, il primo Stato membro in cui intende offrire le cripto-attività al pubblico o, a scelta dell'offerente o della persona che chiede l'ammissione alla negoziazione, il primo Stato membro in cui presenta la domanda di ammissione alla negoziazione di tali cripto-attività;

d) per gli emittenti di token collegati ad attività, lo Stato membro in cui l'emittente di tali token ha la propria sede legale;

richiesta, spetterà alle Autorità competenti fornire (nel termine di cinque giorni lavorativi decorrenti dal ricevimento della domanda) al prestatore di servizi un riscontro nei termini di cui all'articolo 63 del *MiCA*, e dunque in relazione all'effettiva ricezione della domanda stessa. In ossequio ai principi generali già definiti nel diritto europeo, sono concesse forme di interlocuzione con le Autorità deputate alla concessione dell'autorizzazione. In tal misura, il prestatore di servizi sarà abilitato all'integrazione della domanda, nel caso in cui la stessa risulti in qualche misura carente rispetto alle indicazioni di corredo contenute nella normazione sovranazionale²³¹.

e) per gli emittenti di token di moneta elettronica, lo Stato membro in cui l'emittente di tali token è autorizzato come ente creditizio ai sensi della direttiva 2013/36/UE o come istituto di moneta elettronica ai sensi della direttiva 2009/110/CE;

f) per i prestatori di servizi per le crypto-attività, lo Stato membro in cui il prestatore di servizi per le crypto-attività ha la propria sede legale».

²³¹ Il riferimento, com'è di pronta evidenza, è alle condizioni enunciate all'articolo 62 del *MiCA*, previsione che si richiama per comodità di consultazione: «La domanda di cui al paragrafo 1 contiene tutte le informazioni seguenti:

a) il nome, compresa la denominazione legale e qualsiasi altra denominazione commerciale utilizzata, l'identificativo della persona giuridica del prestatore di servizi per le crypto-attività richiedente, il sito web gestito da tale prestatore, un indirizzo di posta elettronica di contatto, un numero di telefono di contatto e il suo indirizzo fisico;

b) la forma giuridica del prestatore di servizi per le crypto-attività richiedente;

c) lo statuto del prestatore di servizi per le crypto-attività richiedente, ove applicabile;

d) un programma operativo che indichi i tipi di servizi per le crypto-attività che il prestatore di servizi per le crypto-attività richiedente intende prestare, compresi i luoghi e le modalità di commercializzazione di tali servizi;

e) la prova che il prestatore di servizi per le crypto-attività richiedente soddisfa i requisiti per le tutele prudenziali di cui all'articolo 67;

f) una descrizione dei dispositivi di governance del prestatore di servizi per le crypto-attività richiedente;

g) la prova che i membri dell'organo di amministrazione del prestatore di servizi per le crypto-attività richiedente possiedono sufficienti requisiti di onorabilità e le conoscenze, le competenze e l'esperienza adeguate per amministrare detto prestatore;

h) l'identità di qualsiasi azionista e socio, siano essi diretti o indiretti, che detiene partecipazioni qualificate nel prestatore di servizi per le crypto-attività richiedente e gli importi di tali partecipazioni, nonché la prova che tali persone possiedono sufficienti requisiti di onorabilità;

i) una descrizione dei meccanismi di controllo interno, delle politiche e delle procedure per individuare, valutare e gestire i rischi, inclusi i rischi di riciclaggio di denaro e finanziamento del terrorismo, e del piano di continuità operativa del prestatore di servizi per le crypto-attività richiedente;

j) la documentazione tecnica dei sistemi TIC e dei dispositivi di sicurezza e una descrizione della stessa in linguaggio non tecnico;

k) una descrizione della procedura per la separazione delle crypto-attività e dei fondi del cliente;

l) una descrizione delle procedure del prestatore di servizi per le crypto-attività richiedente per il trattamento dei reclami;

m) se il prestatore di servizi per le crypto-attività richiedente intende prestare il servizio di custodia e amministrazione delle crypto-attività per conto di clienti, una descrizione della politica di custodia e amministrazione;

Di contro, il rifiuto reso all'esito dell'esame della richiesta di autorizzazione è associato alla sussistenza di motivi oggettivi, adeguatamente dimostrabili, che mirano in direzione di una situazione tale per cui:

- a. *«l'organo di amministrazione del prestatore di servizi per le crypto-attività richiedente possa mettere a repentaglio la gestione efficace, sana e prudente e la continuità operativa del prestatore, nonché l'adeguata considerazione degli interessi dei suoi clienti e l'integrità del mercato, o possa esporre il prestatore di servizi per le crypto-attività richiedente a un grave rischio di riciclaggio di denaro o finanziamento del terrorismo;*
- b. *i membri dell'organo di amministrazione del prestatore di servizi per le crypto-attività richiedente non soddisfino i criteri di cui all'articolo 68, paragrafo 1;*
- c. *gli azionisti o i soci, siano essi diretti o indiretti, che detengono partecipazioni qualificate nel prestatore di servizi per le crypto-attività richiedente non soddisfino i criteri di sufficiente onorabilità di cui all'articolo 68, paragrafo 2;*
- d. *il prestatore di servizi per le crypto-attività richiedente non soddisfi o rischi di non soddisfare uno qualsiasi dei requisiti del presente titolo»²³².*

Per vero, l'autorizzazione concessa è suscettibile di revoca nel caso in cui il prestatore di servizi non abbia osservato le prescrizioni imposte e sia ricaduto in una delle circostanze descritte dall'articolo 64 del Regolamento.

n) se il prestatore di servizi per le crypto-attività richiedente intende gestire una piattaforma di negoziazione di crypto-attività, una descrizione delle norme operative della piattaforma di negoziazione e della procedura e del sistema per individuare gli abusi di mercato;

o) se il prestatore di servizi per le crypto-attività richiedente intende scambiare crypto-attività con fondi o altre crypto-attività, una descrizione della politica commerciale non discriminatoria che disciplina il rapporto con i clienti nonché una descrizione della metodologia per determinare il prezzo delle crypto-attività che il prestatore di servizi per le crypto-attività richiedente propone di scambiare con fondi o con altre crypto-attività;

p) se il prestatore di servizi per le crypto-attività richiedente intende eseguire ordini di crypto-attività per conto di clienti, una descrizione della politica di esecuzione;

q) se il prestatore di servizi per le crypto-attività richiedente intende prestare consulenza sulle crypto-attività o prestare servizi di gestione del portafoglio di crypto-attività, una prova che le persone fisiche che prestano consulenza per conto del prestatore di servizi per le crypto-attività richiedente o che gestiscono portafogli per suo conto dispongono delle conoscenze e delle competenze necessarie per adempiere i loro obblighi;

r) se il prestatore di servizi per le crypto-attività richiedente intende prestare servizi di trasferimento di crypto-attività per conto di clienti, informazioni sulle modalità con cui saranno prestati tali servizi di trasferimento;

s) il tipo di crypto-attività cui fa riferimento il servizio per le crypto-attività».

²³² Art. 63, par. 10 MiCA.

Detto articolo, infatti, è strutturato secondo prassi già sperimentate nel contesto del diritto unionale: prevede alcune ipotesi (enunciate al par. 1) al verificarsi delle quali le Autorità competenti sono obbligate a disporre la revoca dell'autorizzazione stessa²³³; v'è, poi, una ulteriore serie di casi in cui le predette Autorità hanno solo la facoltà di disporre la revoca ("possono revocare"), dopo aver compiuto una valutazione discrezionale di opportunità in merito alla condotta tenuta dal prestatore di servizi, sul parametro dell'idoneità di quest'ultimo a conservare la posizione rivestita nell'ambito della autorizzazione già concessa²³⁴.

5. Analisi empirica: scenari attuali e sviluppi futuri sul panorama dei CASP

Si propongono adesso una serie di analisi (anche su supporto grafico) al fine di offrire una panoramica chiara ed immediata dello stato di normazione nei diversi contesti continentali in ordine alle attività/operazioni condotte dai fornitori/prestatori di cripto-attività. Al riguardo, si è proceduto innanzitutto a individuare un totale di 213 Paesi e/o giurisdizioni, classificate per area geografica e misurate in termini percentuali (Figura 8).

²³³ Si tratta, nello specifico, dei casi in cui il prestatore di servizi:

«a) non si è avvalso dell'autorizzazione entro 12 mesi dalla data della stessa;

b) ha espressamente rinunciato alla sua autorizzazione;

c) non ha prestato servizi per le cripto-attività per nove mesi consecutivi;

d) ha ottenuto l'autorizzazione in modo irregolare, ad esempio presentando dichiarazioni false nella domanda di autorizzazione;

e) non soddisfa più le condizioni di concessione dell'autorizzazione e non ha adottato le azioni correttive richieste dall'autorità competente entro il termine fissato;

f) non dispone di sistemi, procedure e dispositivi efficaci per individuare e prevenire il riciclaggio di denaro e il finanziamento del terrorismo a norma della direttiva (UE) 2015/849;

g) ha violato gravemente il presente regolamento, incluse le disposizioni relative alla tutela dei possessori di cripto-attività o dei clienti di prestatori di servizi per le cripto-attività, o dell'integrità del mercato».

²³⁴ Art. 64, par. 2: «Le autorità competenti possono revocare l'autorizzazione come prestatore di servizi per le cripto-attività nei casi seguenti:

a) il prestatore di servizi per le cripto-attività ha violato le disposizioni di diritto nazionale che recepiscono la direttiva (UE) 2015/849;

b) il prestatore di servizi per le cripto-attività ha perso l'autorizzazione come istituto di pagamento o l'autorizzazione come istituto di moneta elettronica e lo stesso prestatore di servizi per le cripto-attività non ha posto rimedio alla situazione entro 40 giorni di calendario».

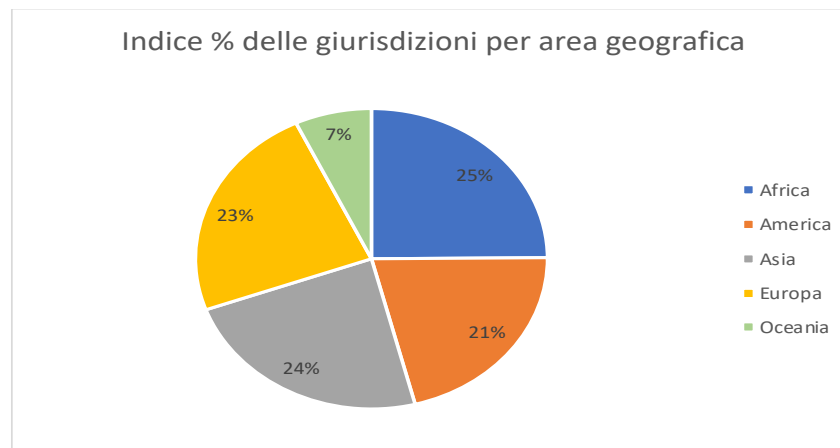


Figura 8 – Continente (n° nazioni): Africa (53), America (45), Asia (50), Europa (50) e Oceania (15)

Per ciascuna giurisdizione si è cercato dapprima di rispondere ai seguenti quesiti: **“è presente una regolamentazione VASP/CASP? O quanto meno si è riusciti a ricomprendere tali soggetti in normative preesistenti? (Sì, no, in corso/c’è intenzione)”**. Nel tentativo di ritrarre in maniera netta l’atteggiamento che ciascuna giurisdizione ha assunto rispetto alla regolazione di tali soggetti, la Figura 9 mostra un’evidente spaccatura a livello globale.

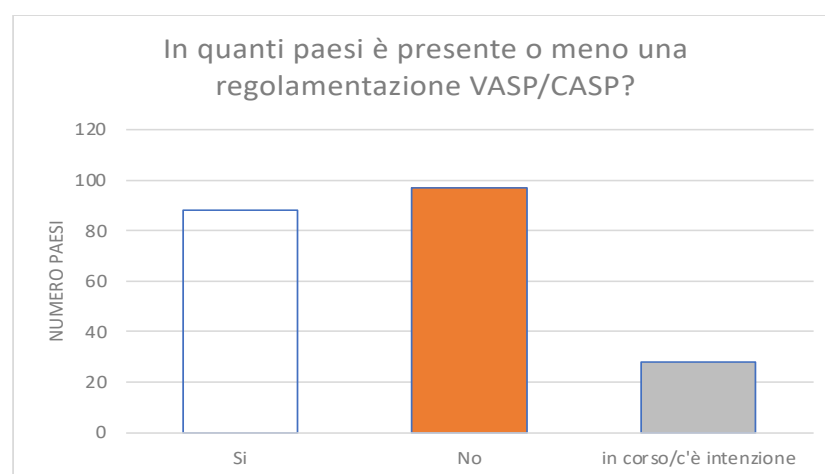


Figura 9 – Sì (88), No (97), in corso/c’è intenzione (28)

Sebbene ci sia una sostanziale parità tra Paesi che si sono occupati di normare il fenomeno e Paesi che non hanno compiuto questo passo, quest’ultima categoria spicca, seppur lievemente. Da queste prime immagini non si può non constatare come il tema dei *Crypto-Asset Service Provider* (o *Virtual Asset Service Provider*) abbia solo recentemente stimolato

gli organi legislativi nazionali ad agire. La strada da percorrere sembra ancora in salita. Tuttavia, i 28 Paesi²³⁵ intenzionati a incamerare nel proprio ordinamento tali operatori trasmettono la sensazione che si è prossimi ad un giro di boa²³⁶.

In risposta alla prima sotto-domanda “*Se no, perché?*”, le ragioni emerse al riguardo sono molteplici, ma sono state racchiuse nelle seguenti categorie:

- **Crypto ban espliciti.** Divieto assoluto di circolazione di prodotti crittografici con annesse ripercussioni sulla sfera giuridica di chi viene colto nel loro utilizzo. Pertanto, i prestatori di questo genere di servizi sono impossibilitati a operare²³⁷;
- **Crypto ban impliciti.** Le cripto-attività non sono formalmente vietate ma alcuni Paesi hanno spinto maggiormente sulla deterrenza e sul rigore, minacciando l'applicazione di norme penalmente rilevanti (con sanzioni assai severe) o multe piuttosto esose. In altre situazioni, l'organo governativo vieta direttamente agli istituti finanziari e di credito di utilizzare o facilitare transazioni per mezzo di *digital asset*²³⁸;
- **Non sono stati individuati evidenti segni d'interesse sul piano legislativo.** I Paesi appartenenti a questo gruppo danno segno di tollerare la compresenza di *asset* digitali con le valute nazionali o, quanto meno, non sembrano manifestare una particolare avversione verso i prodotti crittografici, ricordando ai consumatori di utilizzarli con cautela data la loro volatilità e quindi instabilità sul mercato;
- **Non sono state trovate informazioni al riguardo.** Nel tentativo di reperire dati utili per la ricerca, non sono mancate difficoltà dovute a barriere linguistiche o all'inaccessibilità

²³⁵ Es. Arabia Saudita, Argentina, Nuova Zelanda e Turchia.

²³⁶ Chi si trova in questa sorta di limbo (o fase di transizione) o è in procinto di effettuare un *risk assessment* (valutazione del rischio) in merito alla convenienza o meno di attivare un *iter* legislativo volto a regolamentare i *CASP/VASP* oppure – laddove questo passaggio fosse già avvenuto – sta sottoponendo il disegno di legge a emendamenti nelle opportune sedi istituzionali in attesa di essere approvata o rigettata. Caso eccezionale è quello panamense. Nel gennaio 2021 il parlamentare Rolando Rodriguez ha presentato un disegno di legge al “*Commerce Commission of Panama's National Assembly*”. Se approvato, il testo avrebbe introdotto il primo perimetro normativo per le società panamensi che vogliono attuare attività per mezzo dei *digital asset*, nonché ambirebbe a portare “libertà finanziaria” a tutti i cittadini che non hanno accesso al sistema bancario tradizionale. Tuttavia, la Suprema Corte di Panama ha rigettato la normativa *crypto* nel 2023.

²³⁷ Nel primo gruppo, a titolo meramente esemplificativo, si registrano Paesi come Afghanistan, Algeria, Bangladesh, Cina, Egitto e Libia. Generalmente questo fenomeno riguarda i Paesi dell'Africa e dell'Asia, ma tra questi vi è anche la Macedonia del Nord, unico Paese europeo ad avere emesso un *ban* ufficiale sulle cripto-attività.

²³⁸ Nel secondo caso, sempre senza pretesa di esaustività, si annoverano Paesi come Birmania, Colombia, Ghana, Giordania.

dei siti *web* istituzionali²³⁹. Financo generici siti d'informazione o quotidiani *online* non hanno lasciato tracce concrete cui poter attingere. Quanto detto è valso soprattutto per alcune giurisdizioni asiatiche ed africane.

Cambiando il raggio d'azione, le Figure 10 e 11 riportano specularmente e con maggiore precisione la concentrazione dei Paesi in cui è presente (o assente) una regolamentazione *VASP/CASP*. La lettura combinata di entrambi i grafici lascia poco spazio alle interpretazioni. Senza rischio di smentita, i Paesi europei mostrano una significativa compattezza nella disciplina degli operatori *crypto*.

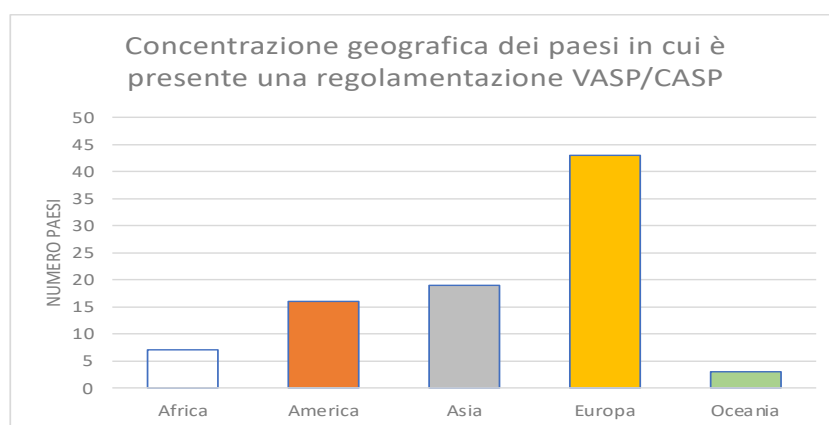


Figura 10 – Africa (7), America (16), Asia (19), Europa (43) e Oceania (3)

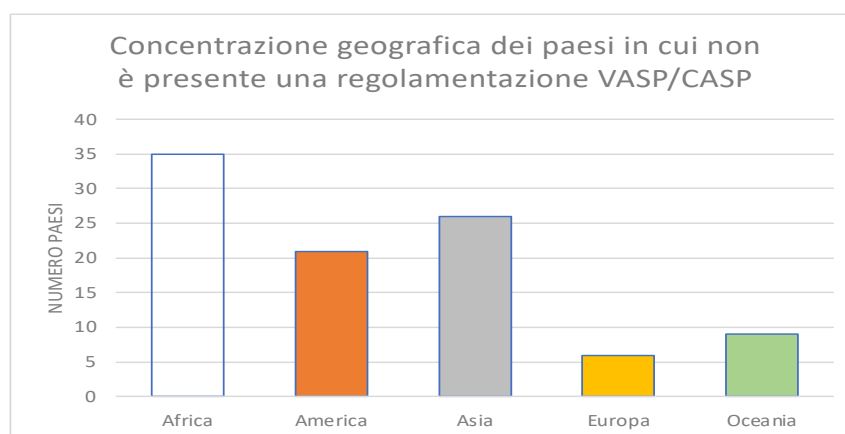


Figura 11 – Africa (35), America (21), Asia (26), Europa (6) e Oceania (9)

²³⁹ Essenzialmente Banche Centrali e autorità nazionali di vigilanza finanziaria.

Oltre a una connaturata propensione storica alla regolamentazione nonché ai primi impulsi dettati dal *Digital Finance Package*²⁴⁰ nel 2020, l'allineamento europeo va con molta probabilità ricollegato al tempestivo recepimento delle recenti Raccomandazioni GAFI che, in ottica di prevenzione antiriciclaggio (*AML*) e contrasto al finanziamento terroristico (*CFT*), hanno catalizzato l'innesto degli intermediari crittografici nel tessuto normativo dei rispettivi Stati membri (Italia compresa) che di quelli afferenti all'intero circuito internazionale GAFI²⁴¹. Ad ogni modo, non si può fare a meno di notare che America (facendo particolare riferimento all'area centrale), Asia (Sud-est asiatico soprattutto) ed Europa (intendendo l'Eurozona) sono al momento i principali *hub* in cui si stanno trattando simultaneamente due tendenze dal punto di vista tecnico e normativo: prodotti crittografici e monete digitali di Stato²⁴².

Vere e proprie sorprese emergono se si tenta di rispondere alla seconda sotto-domanda che ci eravamo posti: “*Se sì, come vengono denominati tali soggetti?*”. Dagli approfondimenti condotti è emersa una sconfinata varietà di espressioni, sebbene quella di “*Virtual Asset Service Provider (VASP)*” appare la più in voga. Trattandosi di una formulazione promossa dal GAFI, non stupisce la sua netta prevalenza in quasi la metà degli ordinamenti nazionali.

²⁴⁰ Le potenziali criticità connesse alla finanza decentralizzata ed al mondo *crypto* hanno recentemente sollecitato l'attenzione dei regolatori interessati alla costruzione di un quadro normativo che tenga conto dell'innovazione tecnologica. In ambito europeo, il Legislatore è intervenuto con un ampio pacchetto dedicato alla finanza digitale (c.d. *Digital Finance Package*) su cui ci siamo ampiamente soffermati nei paragrafi precedenti. Per maggiori approfondimenti vds. [Pezzuto A., *Negoiazione e regolamento di valute virtuali qualificabili come strumenti finanziari ai fini della MiFID II – Il regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito \(DLT\)*, Magistra Banca e Finanza, 2022.](#)

²⁴¹ In attesa di poter applicare il Regolamento *MiCA*, al momento nel contesto normativo italiano si discorre solo di *VASP* ai sensi del «decreto del Ministero delle Finanze del 13 gennaio 2022, prevedendo che gli operatori di valuta virtuale debbano iscriversi obbligatoriamente all'interno di una sezione speciale tenuta dall'Organismo degli Agenti e dei Mediatori (OAM)». Per maggiori approfondimenti si rimanda al webinar [Daga M.C. e Buscema S., *La disciplina dei CASP nel contesto nazionale ed europeo*, Osservatori.net digital innovation, 2023.](#)

²⁴² L'affermazione vuole segnalare come scenario monetario digitale stia assumendo contorni sempre meno indefiniti, e non costituisce più di un orizzonte lontano. Inoltre, non si vuole sottintendere che i due *trend* siano strettamente correlati. Anzi, facendo l'esempio della Cina, mentre la circolazione di qualsiasi cripto-attività è assolutamente vietata, la predilezione per le valute digitali di Stato è invece giustificata dalla possibilità di ottenere maggiore controllo sulla propria politica economica nonché sulle transazioni effettuate dai cittadini-utilizzatori. Nonostante ciò, per quanto vada riconosciuto come il mercato criptovalutario rappresenti sotto determinati aspetti una minaccia al potere monetario di esclusiva pertinenza degli Stati, *crypto-asset* e *CBDC* sembrano poter teoricamente coesistere e una loro eventuale convivenza non dovrebbe pregiudicare in nessun modo la discrezionalità dell'utente finale, il quale può scegliere se e quale *digital asset* adottare. Tuttavia, queste sono solo riflessioni che debbono trovare riscontro nella realtà, specie quando il cd. *Digital Euro* avrà preso piede nella quotidianità dei cittadini e consumatori digitali europei.

È pur vero che buona parte di questi Paesi sono europei e che in futuro convergeranno, come si è avuto modo di evidenziare, sulla più ampia nozione giuridico-soggettiva di *Crypto-Asset Service Provider (CASP)*, definizione che, peraltro, risulta apprezzata anche sul piano accademico dal momento che i *crypto-asset* consentono una maggiore estensione interpretativa rispetto ai *virtual asset*²⁴³. In ambito europeo, ad esempio, assonanze simili si registrano invece in Francia dove vigono i cd. *Digital Asset Service Provider (DASP)*.

Nel mercato dei prodotti digitali la mancanza di un coordinamento a livello internazionale che converga su un unico termine o che stabilisca un regime tassonomico preciso si sta, comunque, facendo avvertire. Stando così le cose, la discrezionalità di determinate giurisdizioni si è imposta comprensibilmente in merito a come definire i prodotti crittografici, che sono stati poi automaticamente traslati nei nomi dei soggetti che forniscono queste cripto-attività²⁴⁴. Ne sono un esempio i *Virtual Currencies Services Provider* (Austria, Polonia, Slovenia, Finlandia, Norvegia); i *Virtual Digital Asset Service Provider* (India); i *Digital Currency Service Provider* (Kazakhstan); i *Bitcoin Service Provider* (El Salvador)²⁴⁵; i *Digital Payment Token (DPT) Provider* (Singapore).

Inoltre, per quanto il termine “*provider*” sia largamente adottato, trovano spazio anche qualificazioni come “*operator*” o altri sinonimi. Il riferimento riguarda i *Digital Token Agent* (Albania); i *Virtual Currency Dealer* (Canada); le *Crypto Company* (Comore); i *Digital Asset Business Operator* (Thailandia); i *Crypto Operator* (Uzbekistan).

In alcuni casi, vengono inserite direttamente nel nome le attività specificatamente ammesse nelle proprie giurisdizioni: *Utility Token Administrator/Issuer* (Anguilla); *Digital Currency*

²⁴³ AA.VV., *Is a VASP a CASP?*, 21Analytics, 2022. «Quando si parla casualmente di VASP e CASP, è perfettamente accettabile usare questi termini in modo intercambiabile. Tuttavia, se si discute in un contesto più formale, è importante tenere presente che la definizione del MiCA è più ampia di quella del GAFI e include elementi aggiuntivi che non sono coperti dalla definizione del GAFI. Inoltre, se la vostra azienda ha sede nell'UE e svolge una qualsiasi delle attività definite come servizio di criptovaluta dal MiCA, allora è considerata una CASP. Nel caso in cui la vostra azienda abbia sede al di fuori dell'UE, molto probabilmente conoscerete la definizione di VASP data dal GAFI o, in alcuni casi, la definizione di attività VASP data dalla vostra giurisdizione. Se non offrite servizi all'interno dell'UE, l'utilizzo della definizione di VASP del GAFI per riferirsi alla vostra attività è accettabile, anche se la vostra attività offre i servizi definiti dal MiCA».

²⁴⁴ Questa constatazione è emersa soprattutto confrontando le risposte tra la seconda sotto-domanda succitata e la domanda “*Laddove possibile, qual è la terminologia utilizzata per definire le cripto-attività?*”. Pertanto, in ragione di quanto suesposto, le risposte a questi due quesiti si sono rivelate pressoché identiche con la semplice differenza che nel primo quesito si parla di soggetti nel secondo caso si parla di oggetti.

²⁴⁵ Unico Paese al mondo, unitamente alla Repubblica Centrafricana, ad adottare il *bitcoin* come valuta a corso legale.

Exchange Provider (Australia); *Wallet Provider* (Bulgaria); *Virtual Asset Trading Platform (VATP) Operator* (Hong Kong); *Crypto Exchange Provider* (Indonesia); *Provider of exchange service* (Islanda); *Convertible virtual currency activity* (Isola di Man); *Virtual Currency Exchange Operator/Custodian* (Lituania); *Digital Asset Exchange (DAX)/Digital Asset Custodian (DAC)* (Malesia); *Digital Asset Exchange (DAX)* (Nigeria).

In diverse circostanze ci si è imbattuti invece in nomenclature che mettono in risalto la natura tecnologica o decentralizzata di questi intermediari. Degni d'interesse in tal senso sono i *Digital signs (token) Operator* (Bielorussia); *DLT Provider* (Gibuti); *Trustworthy Technology Service Provider* (Liechtenstein); *DLT commercial entity* (San Marino); *Enterprise handling Virtual Currency platform* (Taiwan).

Altri Paesi – specie nel contesto caraibico e più in generale dove l'inglese risulta lingua ufficiale – non sembrano preoccuparsi tanto delle sfumature intercorrenti tra “*digital*” e “*virtual*” o tra “*asset*”, “*currency*” e “*token*”, ma preferiscono rimarcare i prestatori di cripto-attività come “*Business*”, esaltando implicitamente il carattere imprenditoriale di tali figure. “*Digital Asset Business*” nel caso di Antigua e Barbuda e Bahamas; “*Virtual Asset Business*” nel caso di Dominica e Grenada. Quest'ultima espressione è riscontrabile anche in Botswana (Africa). Nel Regno Unito (Europa) invece si parla di “*Crypto-Asset Business*”.

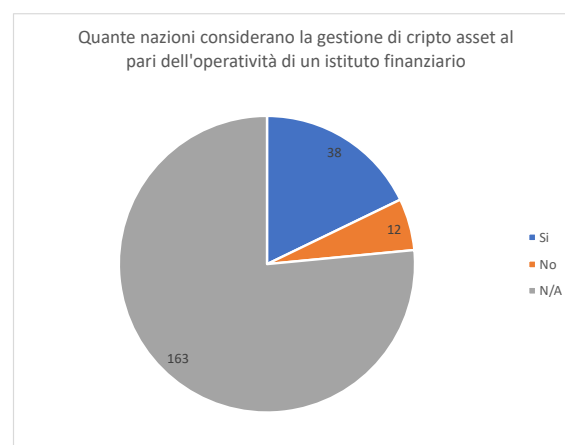


Figura 12 – Sì (38), No (12), Non classificabili (163)

Volendo scandagliare più a fondo, la figura 12 dà un'idea perlomeno approssimativa del numero di giurisdizioni – almeno tra quelle individuate – che ricomprendono i prestatori di

servizi per le cripto-attività nella grande famiglia degli intermediari finanziari (in casi peculiari addirittura tra quelli bancari)²⁴⁶.

Da un lato, questo aspetto lo si può facilmente dedurre dai loro nomi, come i “*Services related to a financial asset*” (Israele) o i “*Digital Financial Asset Operator*” (Russia). Per la restante parte, si è fatto ricorso ai dati contenuti nella sezione “Altro (curiosità/peculiarità da segnalare)”. Sulla base di quanto raccolto, sono emerse varie motivazioni per le quali una singola giurisdizione considera i fornitori di cripto-attività alla stregua di intermediari finanziari. Volendo opportunamente fare una sintesi, il quadro che emerge è il seguente:

- **Applicazione di regimi normativi preesistenti.** Anche in assenza di una normativa *ad hoc* sui VASP/CASP, alcuni Paesi li ricomprendono in normative finanziarie già vigenti, imponendo loro gli stessi obblighi di qualsiasi altro istituto finanziario (Austria, Nuova Zelanda²⁴⁷, USA²⁴⁸);
- **Obbligo di registrazione/licenza.** In determinati Paesi non sono contemplate procedure speciali, o comunque appositamente modellate per i fornitori di cripto-attività al fine di poter operare, mentre è sufficiente registrarsi (Germania²⁴⁹, Guatemala²⁵⁰ e Norvegia²⁵¹) o ottenere il rilascio di una licenza (Repubblica Ceca²⁵²) come un qualsiasi intermediario finanziario. Ragionamento inverso vale per Aruba, che obbliga i VASP/CASP a registrarsi

²⁴⁶ La Banca Internazionale delle Comore ha introdotto una licenza bancaria che include il *trading in "crypto digital currency"*. Tale licenza è necessaria per imprese come *startup* nel settore *blockchain, exchange crypto*, piattaforme di *trading* e progetti *blockchain*. Altro caso sono le Isole Marshall, in cui i VASP devono ottenere l'autorizzazione dalla “*Banking Commission*”, la quale è responsabile per il rilascio delle licenze, regolamentazione e supervisione di banche ed istituti finanziari.

²⁴⁷ Secondo l'Autorità neozelandese DIA, l'attuale definizione di “*financial service provider*” è sufficientemente ampia da ricomprendere tutti quei prestatori di servizi per le cripto-attività che sono stati individuati dal GAFI.

²⁴⁸ I VASP/CASP sono soggetti alla legislazione che è esistita per anni per i “*financial services provider*”. Perciò, gli USA considerano i VASP/CASP come intermediari finanziari nel contesto normativo AML/CFT e l'approccio regolatorio statunitense non considera i VASP/CASP come una categoria separata a sé, ma piuttosto li regola a seconda del tipo di attività/servizio che erogano: Broker-dealers sono sotto la giurisdizione della “*Securities Exchange Commission*” (SEC), *futures commission merchants* e *introducing brokers* sono sotto la giurisdizione della “*Commodity Futures Trading Commission*” (CFTC); i *money transmitters*, che sono un tipo di attività di servizi monetari regolamentati esclusivamente dal FinCEN a livello federale.

²⁴⁹ Dal momento che i VASP/CASP sono ricompresi sotto il termine di “*financial services provider*”, non esiste nel contesto normativo tedesco un registro esclusivamente dedicato ai VASP/CASP.

²⁵⁰ VASP/CASP possono registrarsi come un qualsiasi “*commercial service provider*”.

²⁵¹ In Norvegia i *Virtual Currencies Services Provider* debbono registrarsi come “*Business Enterprises*”.

²⁵² Anche se non ci sono normative regolanti i VASP, fornire servizi in modo continuativo a scopo di lucro nel territorio nazionale ceco richiede una licenza commerciale generale emessa dalla “*Czech Trade Authority*”.

in un elenco afferente alla categoria “*designated non-financial business and professions*” (si presume quindi che i *VASP* non siano soggetti finanziari in quest’ultima giurisdizione)²⁵³;

- **Conformità con leggi antiriciclaggio.** In altri Paesi ancora (Andorra, Azerbaijan, Estonia²⁵⁴, Slovenia) i fornitori di crypto-attività, rientranti nel novero dei “*Financial reporting entity*” o “*Reporting person*”, sono considerati istituzioni finanziarie per motivi di conformità con la legge antiriciclaggio.

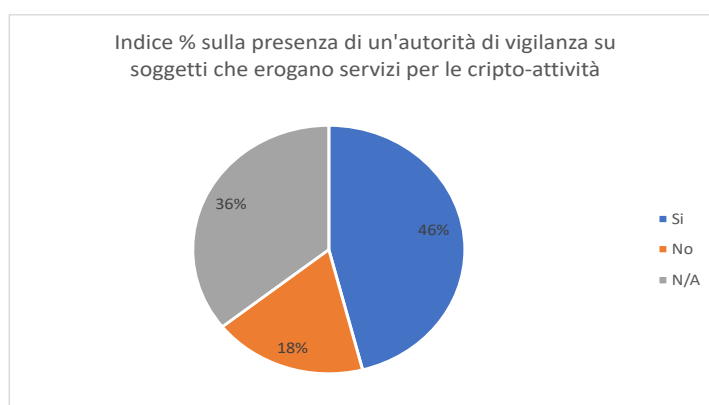


Figura 13 – Si (98), No (39), N/A 76

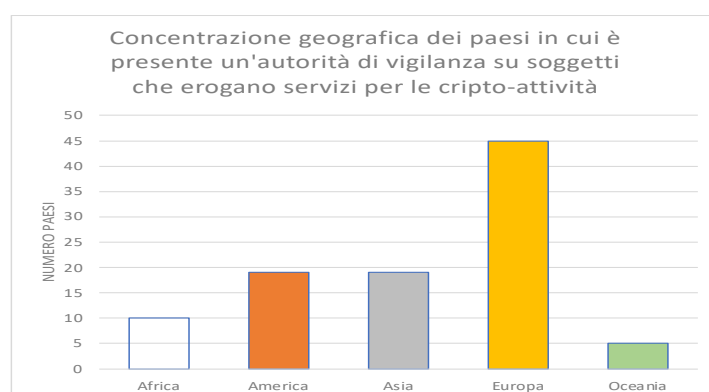


Figura 14 – Africa (10), America (19), Asia (19), Europa (45) e Oceania (5)

Infine, la ricerca si è spinta a catturare un’ultima sfumatura. Replicando alla domanda “***A prescindere dalla presenza di una normativa ad hoc, è comunque prevista un’autorità di***

²⁵³ Ciò teoricamente sembrerebbe valere anche per l’Italia dal momento che i *VASP* debbono iscriversi per mezzo dell’OAM in registri dedicati.

²⁵⁴ In Estonia, i *VASP* sono considerati al pari delle istituzioni finanziarie, regolandole allo stesso modo.

vigilanza su soggetti che erogano servizi per le cripto-attività?”, le Figure 13 e 14, seppur in modo diverso, ribadiscono quanto già detto prima. La supervisione dei *VASP/CASP* risulta in larga misura scoperta a livello globale. In merito al 64% delle giurisdizioni che non presentano una supervisione dei fornitori di cripto-attività, il 18% include quelli che principalmente hanno stabilito un *ban*, mentre nel restante 46% l'ordine dei motivi è ampio (es. assenza di una regolamentazione, assenza di un interesse legislativo, *iter* legislativo in corso o dati non sufficienti). Del 36% del campione dei Paesi che prevedono un'Autorità di vigilanza, più della metà sono europei, confermando come l'attenzione su questo tema sia particolarmente percepito e recepito nel Vecchio Continente. Interessante è parso osservare, in ultima istanza, le diverse tipologie di soggetti cui viene affidata la supervisione dei *CASP*, che possono riassumersi in tre macrocategorie: Banche Centrali, Autorità di Vigilanza Finanziaria ed entità in seno a una delle precedenti categorie oppure in altre Amministrazioni. Dai dati riportati emerge come il tema della vigilanza dei *CASP* risulti di difficile trattazione poiché necessita di un quadro regolamentare che possa garantire, da un lato, l'integrità del sistema e della stabilità finanziaria e, dall'altro, la crescita e lo sviluppo attraverso l'innovazione tecnologica.

È innegabile che di fronte alle sfide poste complessivamente dai nuovi fenomeni, caratterizzati anche dalla difficoltà di collocarli in un preciso punto “geografico” e perciò, per loro natura a-territoriali (*cyber-space*), i singoli Stati si trovano nell'impossibilità, da un lato, di disciplinare attività che si svolgono fuori dai propri confini territoriali o, peggio, sulla “rete” e, dall'altro lato, colpire quelle attività illecite che una globalizzazione senza norme favorisce e alimenta. In ragione di ciò, è facile cogliere la non semplice missione cui sono demandate le Autorità di vigilanza e *regulators*, chiamati a confrontarsi con fenomeni che mutano in modo repentino e che traggono la propria forza proprio dalle lacune regolamentari. In conclusione, al di là delle considerazioni che si possono trarre su di un piano comparatistico, dalla vasta casistica di denominazioni e grafici sopra riportati emergono alcune importanti evidenze:

- la regolamentazione dei *CASP* presenta una diffusione a macchia di leopardo, in cui sveltano gli Stati dell'area geografica europea;

- l'assenza di univocità terminologica se da un lato è sintomo di una forte discrezionalità all'interno di ogni giurisdizione, dall'altro inficia negativamente sulla possibilità di costruire una tassonomia concordata a livello internazionale;
- nella stragrande maggioranza dei Paesi non si riesce a cogliere con chiarezza se i *CASP* siano degli intermediari finanziari o una categoria a sé, dal momento che si rinvencono esempi nell'uno e nell'altro senso;
- la supervisione di questi soggetti appare largamente scoperta a livello globale;
- l'Europa, sia intesa nella sua accezione geografica che in riferimento al contesto UE, sembra procedere speditamente rispetto agli altri continenti e l'approvazione del *MiCA* sembra consolidare questo primato.

6. Verso una conclusione: *CASP* come nuovi operatori finanziari?

L'istituzione di un quadro normativo generale per le attività cripto rappresenta un importante passo verso la giusta direzione, in ragione della rapida crescita del mercato dei *crypto-asset* e dei rischi ad essi associati, che richiedono l'adozione di misure adeguate a proteggere i consumatori e gli investitori e per prevenire azioni fraudolente e dannose, oltre che attività di riciclaggio o reimpiego di proventi di provenienza illecita.

Ritornando alle considerazioni svolte in esordio di questa sezione, è possibile affermare che il metodo seguito in Europa risponda al modello dello “*status quo approach*”, improntato sulla possibilità di regolare la maggior parte delle innovazioni sviluppatesi in ambito *DeFi* attingendo ad istituti tipici del *TradFi*, così da mitigare i rischi di una disintermediazione troppo spinta.

D'altronde, è noto che i modelli finanziari tradizionali si fondano essenzialmente sul ruolo degli intermediari, ossia di entità i cui esponenti devono rispondere a requisiti di onorabilità, professionalità e indipendenza e la cui attività si dipana seguendo in modo scrupoloso paradigmi conformi alla normativa di settore, entro pervasivi presidi di controllo. Mentre i nuovi fenomeni, come quelli legati allo sviluppo delle *DLT* e, in particolar modo ai servizi per le cripto-attività, tendono per la loro stessa natura a sfuggire ad ogni forma di intermediazione istituzionale prefigurando dei modelli autoprodotti di intermediazione “deregolata”, caratterizzata da dispositivi di governance che prefigurano delle modalità di

controllo tecnologico, piuttosto che giuridico, prive di restrizioni eccessive in punto di fruizione dei servizi da parte dell'utente finale.

Lo sforzo del Regolatore unionale è stato dunque quello di tornare sulle categorie tradizionali del diritto per adattarvi le novità tecnologiche che impattano sui mercati e sugli asset digitali ivi negoziati, nella consapevolezza che l'approccio neutrale sinora seguito ha consentito a nuovi attori *crypto* (*VASP* o *CASP* che dir si voglia) di agire al di fuori di quelle regole - ad esempio di vigilanza prudenziale - che sono invece applicabili agli intermediari tradizionali. Ulteriore scopo in tal senso perseguito dal Legislatore europeo è stato quello di superare la frammentazione normativa (di cui si è dato conto nei precedenti paragrafi) che, da un lato, ostacola quei prestatori di servizi per le cripto-attività che intendano espandere legittimamente le loro attività su base transfrontaliera e, dall'altro, favoriscono forme di arbitraggio normativo da parte delle singole giurisdizioni, che possono comportare potenziali rischi per l'integrità del sistema, anche in termini di abuso di mercato e di criminalità finanziaria.

Il quadro regolamentare dell'Unione di recente emanazione, lungi dall'imporre un onere normativo superfluo e sproporzionato sull'uso della tecnologia sottostante, ha il pregio di delineare un nuovo mercato regolamentato (per le cripto-attività), riconducendo in un perimetro di regole certe l'accesso degli investitori per il tramite dei nuovi attori *crypto*, che saranno assoggettati ad un regime di vigilanza prudenziale equivalente a quello cui sono sottoposti gli intermediari finanziari tradizionali. In tal senso, deve leggersi ad esempio l'art. 93 del *MiCA*, che prevede che gli Stati membri designino le autorità competenti con poteri di vigilanza e di indagine, e l'art. 111 che affida alle medesime autorità il potere di adottare sanzioni.

In Italia il disegno di legge di delegazione 2022-2023 chiamato a dare attuazione anche al Regolamento 2023/1114/UE ha individuato la Banca d'Italia e la Consob, secondo le relative attribuzioni e finalità, quali autorità competenti, attribuendo alle stesse poteri di vigilanza e di indagine, quelli di adozione di provvedimenti cautelari e di intervento sul prodotto e quelli di trattamento dei reclami, nonché quelli di irrogare sanzioni e di imporre le altre misure amministrative, anche interdittive.

A questo punto, volendoci spingere ancora oltre, dovremmo domandarci se i *CASP* siano una

categoria soggettiva a sé stante o, viceversa, se è ipotizzabile un loro collocamento tra gli intermediari finanziari. È del tutto evidente che la risposta ad una simile domanda implica necessariamente la riferibilità della specifica nozione di *crypto-asset service provider* a quella elaborata con riferimento agli “intermediari finanziari”. In economia questi ultimi vengono definiti come istituzioni preposte al collegamento tra settori *in surplus* e settori *in deficit* finanziario, che raccolgono capitale per impiegarlo a copertura dei fabbisogni finanziari. A tal fine, gli intermediari finanziari svolgono una pluralità di attività e servizi finanziari che sulla scorta di una logica funzionale vengono così riassunti:

- operazioni di pagamento/incasso di denaro;
- gestione di carte di credito/debito;
- varie forme di prestiti monetari;
- rilascio di garanzie e di impegni di firma;
- intermediazione non discrezionale (senza delega) di strumenti finanziari per l'investimento del risparmio privato (raccolta e trasmissione, negoziazione c/terzi di ordini di compravendita di strumenti finanziari in mercati organizzati e distribuzione di prodotti finanziari);
- consulenza in materia di investimenti in prodotti finanziari;
- intermediazione discrezionale (su delega-mandato) del risparmio finanziario privato con diversificazione dei rischi di portafoglio (attività di gestione di patrimoni collettivi e individuali);
- organizzazione di (o partecipazione a) sindacati di collocamento – al pubblico e/o riservato (c.d. *private placement*) – di strumenti finanziari (azioni, obbligazioni o ibridi) per conto di società-emittenti, con o senza assunzione di garanzia o preventiva sottoscrizione a fermo;
- investimenti diretti di risorse finanziarie.

Da una sommaria ricognizione normativa, invece, si rileva che quello degli intermediari finanziari è un concetto a geometria variabile, la cui esatta definizione sembra dipendere dal contesto normativo di riferimento, tant'è che sembra possibile individuare almeno 3 categorie di intermediari finanziari:

- intermediari che operano nel mercato mobiliare, disciplinati dal Testo unico delle disposizioni in materia di intermediazione finanziaria – TUB (D. Lgs. 24 febbraio 1998, n. 58). Sono costituiti dalle imprese che svolgono l'esercizio professionale di servizi di investimento nei confronti del pubblico. A questa categoria appartengono le banche, le società fiduciarie, gli agenti di cambio, le società di intermediazione mobiliare (SIM), le società di gestione del risparmio (SGR) e le società di investimento a capitale variabile (SICAV);
- intermediari finanziari²⁵⁵ di cui all'art. 106 del Testo Unico delle leggi in materia bancaria e creditizia – TUF (D. Lgs. 1° settembre 1993, n. 385). Trattasi di soggetti, diversi dalle banche, ai quali l'ordinamento nazionale consente di concedere finanziamenti sotto qualsiasi forma – ivi incluso il rilascio di garanzie – in via professionale nei confronti del pubblico nel territorio nazionale. Si tratta di soggetti la cui disciplina non è armonizzata a livello europeo, per cui non è consentito il mutuo riconoscimento in ambito UE;
- intermediari disciplinati dal Codice delle assicurazioni private (D. Lgs. n. 209/2005), cui è demandato l'esercizio dell'attività di distribuzione assicurativa e dell'attività di distribuzione riassicurativa.

Dopo questa attenta disamina, bisogna trarre delle conclusioni. In ragione della peculiarità dei servizi offerti, dall'elevato profilo tecnologico e da una spiccata tendenza all'innovazione continua, i *CASP* danno l'impressione di possedere caratteristiche talmente peculiari da potersi teoricamente distaccare dai soggetti bancari e finanziari e costituire una nuova *species* nel panorama finanziario. Difatti, tali *provider* non sembrano essere perfettamente sovrapponibili agli intermediari finanziari, quanto meno rispetto a determinati servizi, come, per esempio, la custodia o il controllo, per conto di clienti, delle cripto-attività o dei mezzi di

²⁵⁵ Oltre all'erogazione del credito, gli intermediari finanziari possono:

- a) emettere moneta elettronica e prestare servizi di pagamento;
- b) prestare servizi di investimento;
- c) esercitare le altre attività a loro eventualmente consentite dalla legge nonché attività connesse o strumentali, come per esempio:
 - la promozione e conclusione di contratti relativi alla concessione di finanziamenti sotto qualsiasi forma e alla prestazione di servizi di pagamento;
 - l'erogazione di finanziamenti agevolati e la gestione di fondi pubblici.

accesso a tali cripto-attività (chiavi crittografiche private). Del resto, si tratta invero di una problematica che viene rimarcata anche da Troiano, asserendo che *«in dottrina, si rilevava come risultasse difficoltoso identificare un concetto unitario di attività finanziaria nel quale ricondurre ipotetici tratti comuni delle singole attività riservate agli intermediari in parola, trattandosi di attività tra loro diverse nei presupposti finanziari, nella causa e nelle modalità di svolgimento; l'unico elemento comune veniva rinvenuto nella finalità di economicità»*²⁵⁶. Andando oltre queste argomentazioni e analizzando oggettivamente il fenomeno, la categoria dei *CASP* va considerata a tutti gli effetti una “*financial entity*”, ai sensi dell’art. 1 del Regolamento *DORA*. Tuttavia, a parere di chi scrive, questa constatazione può risultare agevole solo attraverso una lettura combinata delle varie normative europee ricomprese sotto un’unica prospettiva. Qualora invece tale ragionamento si basasse esclusivamente sulla lettura del *MiCA*, va allora ammesso come vi siano non poche difficoltà nel giungere alla medesima conclusione.

²⁵⁶ Troiano, V., *I soggetti operanti nel settore finanziario*, Capriglione F. (a cura di), *Manuale di diritto bancario e finanziario*. Seconda edizione, 2019.

III. L'IMPATTO DELLE CRIPTO-ATTIVITÀ E DEI *CASP*: SPECIFICI AMBITI DI ATTENZIONE PERIMETRATI DAL *MICA* E ALTRE NORMATIVE EUROPEE

Facendo un rapido riepilogo, il primo capitolo è stato speso per dare un'illustrazione – il più esaustiva e lineare possibile – dei fattori che hanno portato allo sdoppiamento della *TradFi* in “*crypto financial system*” (perimetro comprendente al suo interno *CeFi* e *DeFi*) nonché individuare i punti di interazione che intercorrono tra questi due paradigmi. Col secondo capitolo invece ci siamo propriamente addentrati nell'ecosistema crittografico, osservando i prodotti circolanti (*digital asset*) e soprattutto i soggetti che vi abitano (*CASP*). Segnatamente, alla luce del Regolamento *MiCA*, si è operata un'approfondita analisi giuridica dei *Crypto-Asset Service Provider*. Nonostante l'adozione di una (previamente dichiarata) prospettiva prevalentemente europea, non si è mancato di registrare (e di confrontare) i risultati raggiunti da altre parti del mondo attraverso una ricerca empirica personalmente svolta.

Muovendo da questi presupposti, ora il terzo capitolo si prefigge l'obiettivo di restringere ulteriormente il campo scandagliando diversi ambiti in cui si ritiene che l'operato dei *CASP* possa maggiormente svilupparsi e/o incidere sollevando potenziali criticità. Difatti, per quanto notevoli, gli sforzi realizzati dalle istituzioni sovranazionali volti a garantire la certezza del diritto nell'ambito delle cripto-attività o una migliore tutela di consumatori ed investitori in questo settore potrebbero non bastare. È pertanto d'uopo chiedersi se il complesso delle norme domestiche ed europee (*MiCA in primis*, unitamente ad altre normative di rango unionale e/o nazionale) circoscriventi l'*habitat* dei *CASP* sia riuscito a regolamentare esaurientemente tutti i possibili profili di criticità. E nell'eventualità che qualcosa sia sfuggito, si tenterà di convertire il potenziale *vulnus* individuato in spunti di riflessione o suggerimenti condivisibili sul piano legislativo. Gli ambiti di attenzione individuati sono:

- Riciclaggio e contrasto al finanziamento terroristico;
- Tassazione;

- Ambiente/energia;
- *Privacy*, unita a profili di cybersicurezza.

Queste specifiche aree d'osservazione non sono casuali, ma sono piuttosto accomunate dal fatto di essere tutte segnalate (certe con maggiore evidenza, altre meno ma comunque intravedibili) dalla normativa *MiCA*. E in ciascuno di questi ambiti tematici, gli operatori devono necessariamente soddisfare requisiti o adempiere obblighi, sia direttamente che indirettamente. Pertanto, l'analisi giuridica verterà inizialmente sulle dimensioni in cui la normazione appare più fitta (antiriciclaggio), esplorando successivamente gli ambiti meno legislativamente meno battuti ma degni di essere approfonditi (tassazione ed ambiente). Allargando il contesto normativo europeo (*DORA* e *GDPR in primis*), può includersi anche la *privacy* come ulteriore campo di analisi. Difatti, è ormai indiscutibile la particolare rilevanza che la protezione dei dati personali ha assunto nella società odierna. Nonostante questi soggetti non siano generalmente obbligati a trattare le informazioni dei clienti relative al trasferimento di *crypto-asset* come dati personali ai sensi delle leggi sulla protezione dei dati applicabili (es. *GDPR*), è ragionevole ritenere che in futuro i numerosi oneri già dettati dal *MiCA* si allarghino anche su questo fronte.

SEZIONE 1. ANTIRICICLAGGIO E LOTTA AL FINANZIAMENTO AL TERRORISMO: LA DIMENSIONE NATIVA DEI *CASP*

1. Analisi del fenomeno: i rischi del riciclaggio nella *DeFi*

Come sinora osservato, la portata rivoluzionaria della *DeFi* ha spinto le stesse istituzioni nazionali e sovranazionali a considerare la tecnologia *DLT* e la sua derivata più nota, ossia la *blockchain*, come un indispensabile motore di sviluppo capace di offrire nuove opportunità di crescita per le imprese e gli investitori, ma anche come un possibile incubatore di rischi per la stabilità del sistema con impatti diretti in molteplici settori del *TradFi*. Abbiamo anche evidenziato come sullo scenario della nuova finanza si siano affacciati nuovi operatori come i *Crypto-Asset Service Provider (CASP)*, soggetti che sono sorti con la finanza cd. decentralizzata e progressivamente ricondotti dal Legislatore entro il perimetro delle regole *TradFi*, senza riconoscere alla peculiarità dei servizi offerti alcuna portata derogatoria rispetto al sistema delle norme che regolano le attività finanziarie e il mercato. Difatti, seppur tecnicamente qualificabili come intermediari bancari e finanziari, questi *crypto player* forniscono servizi di intermediazione nell'acquisto e vendita di cripto-attività e sono destinatari di regole simili (ma apparentemente più severe) in tema di abilitazione ad operare, di monitoraggio delle transazioni ai fini dell'antiriciclaggio e di obblighi tipici dei sostituti di imposta.

In questa prima parte del capitolo, ci soffermeremo sulle più significative derive patologiche proveniente dal mercato dei *crypto-asset*, palesanti degli scenari assai critici e non facilmente decifrabili e che potrebbero impattare direttamente sui comportamenti dei cittadini e delle aziende, sui sistemi di comunicazione e sugli assetti economico-finanziari degli Stati. Ciò è reso possibile grazie alla facilità con cui possono interagire con il tessuto illegale dell'economia sommersa facendo leva sull'anonimato e la crittografia dei processi di trasferimento degli *asset* digitali. D'altronde, nell'approcciarsi a tale fenomeno per comprendere in che modo regolamentarli, gran parte delle istituzioni governative, delle Autorità di vigilanza e delle Banche Centrali²⁵⁷ ne hanno segnalato l'insidiosa pericolosità

²⁵⁷ Il fenomeno è stato analizzato da diverse Banche Centrali. A mero titolo esemplificativo vds. *ex plurimis* [Deutsche Bundesbank, Crypto tokens and decentralised financial applications, 2021](#); [Deutsche Bundesbank, Distributed ledger technologies in payments and securities settlement: potential and risks, 2017](#); [Banca](#)

sul piano dell'utilizzo, diretto o indiretto, per scopi illegali. A più riprese, la stessa Banca d'Italia ha condotto approfondimenti sul tema, partecipando da tempo ai lavori in materia di *crypto-asset* in diversi consessi internazionali ed europei. Inoltre, spesso d'intesa con la Consob e l'Unità di Informazione Finanziaria per l'Italia (UIF), ha pubblicato avvertenze per gli intermediari vigilati e per gli utenti, mettendo in luce i rischi collegati all'acquisto e alla custodia di *crypto-asset* specie in tema di antiriciclaggio, alla varietà e complessità delle tecnologie sottostanti, alla carenza di tutele legali, oltre che contrattuali e, in ultima istanza, alla possibilità di essere frodati o di perdere i propri investimenti²⁵⁸.

Diverse sono le considerazioni che militano a favore di tali preoccupazioni. Infatti, i *crypto-asset* hanno stravolto il concetto stesso di globalizzazione e con esso il significato di ricchezza. Non si tratta più solo di definire le problematiche allocative e di dislocazione geografica dei capitali, ma di comprenderne le modalità di generazione che possono trarre origine anche da fonti virtuali ed anonime, capaci di autorappresentare un valore che si autoimpone come riserva e come mezzo di scambio, ancorché altamente inaffidabile. Il tutto per il tramite di protocolli di comunicazione crittografati²⁵⁹. Moltissimo si è fatto con riferimento al primo aspetto, legato alla geolocalizzazione dei flussi finanziari tradizionali, implementando gli *standard* di trasparenza globali ed automatizzando la cooperazione tra

[d'Inghilterra, *Financial Stability in Focus: Cryptoassets and decentralised finance*, 2022;](#) [Federal Reserve, *Distributed ledger technology in payments, clearing, and settlement*, 2016.](#)

²⁵⁸ La Banca d'Italia, in linea con i comunicati adottati dagli organismi internazionali (*Financial Stability Board – FSB; Financial Action Task Force – FATF/GAFI; Basel Committee on Banking Supervision – BCBS; International Organization of Securities Commissions – IOSCO; Committee on Payment and Market Infrastructures – CPMI*) e dalle tre autorità di supervisione europee (*European Securities and Markets Authority – ESMA; European Banking Authority – EBA; European Insurance and Occupational Pensions Authority – EIOPA*) ha pubblicato, a partire dal 2015, diverse avvertenze all'indirizzo degli intermediari vigilati e degli utenti relativi ai *crypto-asset*. Vds. in particolare, [Banca d'Italia, *Avvertenza sull'utilizzo delle cosiddette "valute virtuali"*, 2015;](#) [Banca d'Italia, *Avvertenza per i consumatori sui rischi delle valute virtuali da parte delle Autorità europee*, 2018;](#) [Banca d'Italia, *Consob e Banca d'Italia mettono in guardia contro i rischi insiti nelle crypto-attività*, 2021.](#) Vds. tra gli approfondimenti, [Banca d'Italia, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e crypto-attività*, 2022.](#)

²⁵⁹ Sulle enormi implicazioni dell'utilizzo delle DLT, vds. il documento [Scheda C. et al., *Lo sviluppo del Fintech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, Quaderni FinTech Consob, 2018.](#) Vds. Anche [Carrière P. et al., *Tokenizzazione di azioni e azioni tokens*, Quaderni giuridici Consob, n. 25, 2023,](#) in cui si mette in guardia dal fatto che «ai vantaggi sono correlati altrettanti rischi che alimentano l'esigenza di una immediata e ampia regolamentazione delle attività emesse e negoziate nell'ambito del circuito delle DLT. In primo luogo, i titolari delle attività di negoziazione e circolazione della ricchezza sono coperti da pseudonimi e possono strumentalmente utilizzare le tecnologie DLT per realizzare fattispecie criminose, in particolare di riciclaggio di denaro o, comunque, di ricchezza *latu sensu* intesa, con la conseguente impossibilità da parte delle autorità di identificarli, incriminarli e recuperare i capitali investiti».

Autorità finanziarie; poco è stato fatto, invece, sul versante della *crypto-economy* e *DeFi*²⁶⁰. Da questo dato si ritiene possibile desumere un primo elemento incontrovertibile: la stretta regolatoria a livello globale sulla movimentazione dei capitali (sul versante del *TradFi*), non può che alimentare la domanda di altri mezzi illeciti per immagazzinare e spostare denaro, specie se caratterizzati da zone d'ombra e da sistemi opachi di difficile regolamentazione. Se a tutto ciò si aggiungono gli ulteriori fattori di attrattività per l'economia illegale, rappresentati dalla sconfinata dimensione del *deep web*, dall'anonimato della transazioni, dalla decentralizzazione dei processi, dalla ibridazione continua dei modelli esistenti (dei *virtual asset*, degli *smart contract* e delle piattaforme) e dalla carenza di legislazioni internazionali e domestiche in grado di regolare tali fenomeni e dalla scarsa sensibilità in termini di *law enforcement*, si comprende come il pericolo di penetrazione criminale sia effettivamente reale. In buona sostanza, esistono diversi aspetti connessi a tale fenomenologia che facilitano l'occultamento, l'accumulazione, il lavaggio e il reimpiego dei proventi illeciti. In realtà, non mancano elementi che farebbero giungere a conclusioni di segno opposto. Studi sull'analisi economica del riciclaggio dimostrano che la remunerazione del rischio (inteso come percentuale dei flussi riciclati) e dunque il costo del riciclaggio aumentano al crescere dell'efficacia della regolamentazione²⁶¹. Tuttavia, nel caso di specie, appare insensato immaginare che un riciclatore utilizzi un sistema che, per le note problematiche di volatilità, aggiunge un ulteriore fattore di rischio suscettibile di distruggere il valore accumulato. Quindi, la regolamentazione dei mercati che scambiano *crypto-asset* da parte dei regolatori europei ed internazionali, tesa a rendere maggiormente stabile l'intero sistema contro possibili bolle speculative, potrebbe avere l'effetto contrario rispetto a quello cui ordinariamente si perviene attraverso lo strumento della regolamentazione, ossia quello di attrarre maggiormente il crimine finanziario.

²⁶⁰ Ci soffermeremo sulle iniziative dell'OCSE verso questa direzione e, in particolare, sul [OCSE, *Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard*, 2022](#), documento contenente una proposta di regolamentazione volta a implementare lo scambio di informazioni tra gli intermediari coinvolti nella circolazione di cripto-attività e le amministrazioni finanziarie nazionali, fornendo al contempo uno *standard* internazionale per la raccolta e lo scambio automatico dei dati.

²⁶¹ Cfr. [Masciandaro D., *Il riciclaggio dei capitali illeciti profili di analisi economica*, GNOSIS n. 3, 2007](#), il quale evidenzia che «il costo del riciclaggio dipende dall'efficacia appunto della regolamentazione. Al crescere dell'efficacia della regolamentazione, aumentano le probabilità di essere scoperti per gli operatori attivi nel riciclaggio, ne deriva un aumento della remunerazione del rischio; il costo aggregato del riciclaggio sale, il moltiplicatore scende».

Se è vero che giornalmente si rincorrono notizie su singoli episodi illeciti che coinvolgono il mondo di *crypto-asset*, è altrettanto vero che mancano studi o comunque evidenze in grado di delineare un *trend* circa lo spostamento di grandi masse di capitali illeciti verso questi sistemi (o viceversa), la cui fragilità rappresenta al momento un freno per gli stessi riciclatori. Dal momento che la materia è divenuta vasta ed articolata nelle sue potenziali declinazioni a causa della proliferazione di *crypto-asset* e delle tecnologie ad esse associate, in *primis* la *blockchain*, l'argomento è piuttosto complesso e necessita di ulteriori approfondimenti su cui si confrontano sensibilità anche contrapposte da parte da parte dei legislatori.

Tali problematiche non appaiono scontate se si considera che le attività condotte nel cyberspazio vengono realizzate senza alcun diaframma centralizzato e sono spesso nascoste dietro la “pseudonimia” e sviluppate secondo modalità idonee a schermare o, comunque, a rendere difficilmente riscontrabili le interrelazioni tra i vari *player* e ad oscurare l'origine dei flussi economico-finanziari impiegati nelle transazioni. La “pseudonimia”, in particolare, garantisce un certo grado di sicurezza a tutti coloro che fanno parte del *network* e negli anni ha attirato una parte di utenza che, proprio grazie all'opacità di questo espediente, trae vantaggio nell'utilizzare *crypto-asset* e *blockchain* per mascherare compravendite di beni/servizi illegali o di svolgere attività di riciclaggio o reimpiego di proventi di provenienza illecita²⁶². In Europa, l'attenzione verso tali fenomeni è particolarmente alta, tanto da rappresentare un vero e proprio pilastro nell'ambito dell'*Action Plan* definita dalla Commissione Europea nel 2020. Su tali premesse, è stato pubblicato il 20 luglio 2021 l'*AML Package*, teso ad introdurre una riforma complessiva che mira ad armonizzare le regole per l'emissione e l'offerta al pubblico di cripto-attività, nonché a rafforzare i presidi di contrasto del riciclaggio e del finanziamento del terrorismo. Il pacchetto normativo al momento

²⁶² Ad ogni modo, è doveroso sul punto sottolineare un aspetto. Il cd. “sistema *Bitcoin*” può essere considerato pseudo-anonimo (o se si preferisce di quasi-anonimo da non confondere con il concetto di “pseudonimo”, sopra citato) e, anche se nel tempo è stato utilizzato per scopi illegali, questo aspetto ha portato l'utenza ad uno “spostamento” verso altre *crypto-asset* e strumenti digitali in grado di garantire ancora maggiore *privacy*. Infatti, almeno tecnicamente, si deve considerare che il sistema rimane trasparente poiché i dati contenuti all'interno di una *blockchain* risiedono all'interno della catena per sempre, replicati tante volte quanti sono i nodi all'interno della rete. Inoltre, la *blockchain* non solo contiene l'ultimo stato dei dati, ma anche l'intera storia degli stati precedenti, in modo che ciascun nodo possa verificare la correttezza e l'integrità dello stato finale. Strumenti di *blockchain analysis* sono nati proprio in virtù di queste peculiarità, traendo spunto dalle tecniche più sofisticate di informatica forense.

comprende:

- una proposta di regolamento tesa ad istituire una nuova Autorità antiriciclaggio dell'UE (*Anti-Money Laundering Authority, AMLA*), con poteri di imporre sanzioni;
- una proposta di regolamento di refusione del Regolamento sui trasferimenti di fondi, inteso a rendere i trasferimenti di cripto-attività più trasparenti e pienamente tracciabili;
- una proposta di regolamento sugli obblighi in materia di lotta al riciclaggio applicabili al settore privato;
- una proposta di direttiva relativa ai meccanismi antiriciclaggio²⁶³.

Pertanto, il pacchetto normativo si propone di ridisegnare il quadro regolamentare in materia *AML* e *CFT*, allineandolo alla regolamentazione introdotta per i *CASP* dal *MiCA*, per i quali attualmente le norme antiriciclaggio trovano applicazione non per tutte le cripto-attività ma limitatamente alle “valute virtuali” e ai *VASP*, ossia ai prestatori di servizi relativi all'utilizzo di valuta virtuale.

2. Focus sulle metodiche tradizionali dell'attività di riciclaggio

Prima di domandarci come il “sistema dei *crypto-asset*” possa essere sfruttato a fini di riciclaggio, l'analisi del fenomeno richiede di soffermarsi sui tradizionali schemi definitivi riferiti all'attività di riciclaggio. La condotta criminale complessiva comprende la realizzazione di illeciti a monte suscettibili di generare profitti, l'acquisizione delle relative disponibilità economiche, il compimento su di esse di una ampia gamma di atti di dissimulazione, trasferimento e trasformazione con il fine ultimo di immetterli nel circuito dell'economia legale. Si tratta di un'attività complessa che muove da una serie estesa di reati presupposto e si riverbera, a valle, in molteplici operazioni di “ripulitura” attraverso diversi passaggi nei luoghi fisici e/o virtuali, volti a mascherare o modificare la titolarità giuridica e ad incidere sulla natura stessa degli *asset* impiegati.

²⁶³ Vds. [Consiglio dell'UE, Anti-money laundering: Council agrees its position on a strengthened rulebook, Comunicato stampa, 2022.](#)

I sodalizi criminali traggono vantaggio dalla diversità dei presidi nazionali posti a contrasto del riciclaggio dei proventi illeciti e dal diverso grado di incisività dei controlli, al punto che si è spesso assistito ad una frammentazione delle fasi “produttive” (illeciti generatori di proventi), delle operazioni di collocamento e trasformazione, dell’imputazione e dell’intestazione dei beni in diversi luoghi, scegliendo di volta in volta le giurisdizioni nazionali più “ospitali”.

La portata transnazionale del riciclaggio si presta dunque a forme di arbitraggio da parte della criminalità, ma anche degli stessi ordinamenti nazionali, coinvolti in meccanismi nocivi di concorrenza per mantenere il massimo grado di attrattività di capitali (non importa se leciti o illeciti), collocando al minimo la soglia dei controlli preventivi e dell’*enforcement*. Nonostante l’eterogeneità dei comportamenti messi in atto, gli organi investigativi di tutti i Paesi più industrializzati hanno elaborato un “modello a fasi”²⁶⁴, secondo uno schema delineato nei suoi termini essenziali dal GAFI sin dal 1990 nelle proprie raccomandazioni, che si articola in tre differenti momenti del processo:

1. **Placement.** Questa prima fase corrisponde al “collocamento” materiale dei proventi da reato, che abitualmente avviene mediante una serie anche ripetuta e di operazioni (deposito, cambio, trasferimento, acquisto, ecc.), tese a trasformare i proventi illeciti in “moneta scritturale”, normalmente allocata in depositi bancari. La fase del “collocamento” consente di elidere l’origine illecita dei proventi, dissociandoli dal luogo o dal momento della loro genesi. Tali attività possono essere svolte anche con l’acquisizione di prodotti e/o servizi sul mercato, ovvero attraverso l’esportazione dei

²⁶⁴ In origine veniva considerato un modello che si articolava in due fasi: il “lavaggio” (*money laundering*), individuato nelle operazioni a breve termine volte a camuffare l’origine illecita del denaro o di altri beni; e “l’impiego” (*recycling*), coinvolgente operazioni di medio o lungo termine volte a reimmettere i capitali lavati nel ciclo dell’economia legale. Questa suddivisione, peraltro, è all’origine della disciplina penale italiana, che prevede una fattispecie di riciclaggio (art. 648 *bis* c.p.) ed una di impiego di denaro, beni o utilità di provenienza illecita (art. 648 *ter* c.p.). Vds. Capolupo S., Carbone M. e Sturzo G., *Antiriciclaggio: gli obblighi dei professionisti*, IPSOA, 2007, p. 4; Magri P., *Delitti contro il patrimonio mediante frode, usura, appropriazione indebita, ricettazione riciclaggio*, Cedam, 2007, p. 443 e ss.; Pecorella G., *Denaro (sostituzione di)*, in *Dig. disc. pen.*, III, UTET, 1989, p. 369; Pollari N. e Dal Cioppo A., *Tecnica delle inchieste patrimoniali per la lotta alla criminalità organizzata*, Laurus Robuffo, 2006; Valente P. et al., *Riciclaggio e criminalità. Idra per gli Stati, Sisifo per la Società, Nesso per gli Organismi Sovranazionali*, Eurilink, Roma, 2017, p. 32, nonché a Thione M. e Silvani M., *Le nuove frontiere del riciclaggio: analisi del fenomeno, linee evolutive ed elaborazioni statistiche di settore*, Il fisco, n. 23/2006, p. 3529.

proventi verso Paesi poco collaborativi, attraverso operazioni che vengono spesso poste in essere tramite un “frazionamento artificioso” (*splitting*) delle movimentazioni, così da eludere gli obblighi di identificazione e segnalazione previsti dalla normativa antiriciclaggio.

2. **Layering.** La seconda fase, detta della stratificazione, implica il compimento di ulteriori attività tese al “lavaggio”²⁶⁵ vero e proprio del denaro sporco, tramite l’effettuazione di una serie di operazioni finanziarie dirette ad ostacolare la ricostruzione investigativa dei flussi finanziari e della loro provenienza illecita, ricorrendo a trasferimenti elettronici oppure alla riconversione in denaro contante rendendo quanto più possibile anonima la ricchezza e creando una copertura apparentemente legittima²⁶⁶. In questo momento viene eliminato ogni collegamento tra i fondi riciclati e l’attività criminale.
3. **Integration.** Questa fase consiste nel reimpiego dei capitali nel circuito dell’economia legale²⁶⁷, attraverso il ricorso a specialisti, a istituti bancari e/o ad altri tipi di intermediari finanziari, situati anche in Paesi aventi una legislazione poco attenta alla tutela del segreto bancario (cc.dd. paradisi bancari)²⁶⁸. Il completamento del ciclo con l’“integrazione” del denaro sporco nel sistema legale fa sì che lo stesso acquisti una facciata di legittimità.

²⁶⁵ Da qui l’espressione *money laundering* che definisce per l’appunto il fenomeno del riciclaggio riferendosi all’abitudine delle organizzazioni criminali, al tempo del proibizionismo, di reinvestire i guadagni ottenuti dal contrabbando di alcolici nell’apertura di esercizi commerciali “di facciata”, solitamente lavanderie.

²⁶⁶ Le operazioni di *layering* sono complesse in quanto implicano molto spesso trasferimenti internazionali di fondi e/o operazioni societarie in Paesi *off-shore*, attraverso instaurazione di rapporti negoziali di natura simulata. Tutte queste operazioni sono volte a depistare qualsiasi indagine, in modo tale da far perdere le tracce documentali che possono ricondurre all’origine illecita dei fondi (Cfr. Travaglino G., *Riciclaggio: storia, comparazione, struttura, Dir. pen. proc.*, 1996, p. 233; Stile A., *Riciclaggio e reimpiego di proventi illeciti*, Enciclopedia giuridica Treccani, 2009, p.6).

²⁶⁷ Vds. [Brizzi F. et al., La reimmissione della liquidità illecita nel circuito economico ed il delitto di reimpiego tra prevenzione patrimoniale e giustizia penale: prospettive di future armonizzazioni, Archivio Penale, n. 2, 2014, p.3.](#)

²⁶⁸ Queste giurisdizioni costituiscono delle asimmetrie distorsive poiché influenzano l’allocazione delle risorse e degli investimenti, erodono le basi imponibili degli altri paesi e incidono negativamente su equità e neutralità. In termini concreti, esse esprimono una nocività ancor maggiore per il fatto che possono evolversi in centri *off-shore*, ossia mete privilegiate dei movimenti internazionali di capitale grazie, agli alti livelli di remunerazione netta offerti (cc.dd. “paradisi finanziari”), ovvero in virtù di una tutela assoluta dell’anonimato (cc.dd. “paradisi bancari”), tanto da offrire rifugi opachi ai proventi di illecita provenienza, anche di matrice terroristica (cfr. Pollari N. e Nota S., *Percorsi di fiscalità internazionale*, Aracne, 2019; vds. Anche Pollari N., *Il controllo internazionale sui paradisi finanziari*, Riv. G.d.F., n. 5, 1997, p. 1888; id., *La globalizzazione dell’economia e dei presupposti impositivi*, in Riv. G.d.F., n. 1, 2001, p. 103; Valente P., *Concorrenza fiscale dannosa e paradisi fiscali - Nuovi scenari e tendenze in atto*, Rass. fis. int., n. 3, 1999, p. 149 e ss., allegato a *Il fisco*, n. 26, 1999; Cucuzza O., *Economia internazionale e criminalità organizzata*, Riv. G.d.F., n. 6, 1996, p. 2091).

3. Variabili evolutive del riciclaggio: dal *cyber-laundering* al *crypto-laundering*

Nel tempo, il fenomeno “riciclaggio” si è arricchito di due ulteriori variabili di complessità: una connessa con la dimensione transnazionale dell’economia, l’altra dalla diversificazione dei processi favorita dalle innovazioni tecnologiche che oggi garantiscono tecniche di *money laundering* sempre più sofisticate.

Sotto il primo profilo, l’internazionalizzazione e poi la globalizzazione dell’economia e dei mercati hanno comportato una maggior libertà operativa non soltanto per i traffici commerciali leciti, ma anche per l’economia criminale. A livello europeo, questo processo è stato accompagnato, e per certi versi favorito, dalla libertà di circolazione delle merci e dei capitali²⁶⁹, mentre a livello globale, grazie all’opera del *WTO*, dalla riduzione delle barriere tariffarie al commercio internazionale.

Come abbiamo già osservato, il riciclaggio è intimamente connesso con una serie di attività criminose a monte che di per sé sono contraddistinte dalla dimensione transnazionale²⁷⁰. Non a caso la repressione del fenomeno ha tratto origine dalla necessità di contrastare il profitto economico derivante dal traffico internazionale di sostanze stupefacenti (*drug money laundering*)²⁷¹.

²⁶⁹ Cfr. Lembo M. e Scialoja A., *Antiriciclaggio*, Apogeo Education, 2012, p. 27, secondo il quale «la deregulation, cioè l’eliminazione di regole rigide in campo commerciale e finanziario e la globalizzazione sono principi assimilabili con estrema facilità anche dalla criminalità organizzata, in virtù delle proprie caratteristiche di estrema duttilità».

²⁷⁰ Per la definizione di “reato transnazionale” si può fare riferimento alla [Legge 16 marzo 2006, n. 146 di ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall’Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001](#). L’art. 3 così recita: «1. Ai fini della presente legge si considera reato transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:

a) sia commesso in più di uno Stato;
b) ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
c) ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
d) ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato».

Per quanto, invece, attiene alla nozione di gruppo criminale organizzato, si ritiene che essa coincida con una aggregazione dotata di una certa stabilità di rapporti fra i partecipi, un *minimum* di organizzazione non necessariamente comportante una previa definizione di ruoli tra essi, la non occasionalità o estemporaneità della stessa, la costituzione in vista anche di un solo reato e per il conseguimento di un vantaggio finanziario o di altro vantaggio materiale: qualcosa, insomma, che sta a metà tra il concorso di persone nel reato e l’associazione per delinquere (cfr. [Cass., Sez. un. pen., 31 gennaio 2013, n. 18374](#)).

Cfr. Manes V., *Il riciclaggio dei proventi illeciti: teoria e prassi dell’intervento penale*, Riv. trim. dir. pen. econ., 2004, p. 38.

Altra fondamentale e non scontata connotazione del riciclaggio è che quest'ultimo si atteggia, sin dalle originarie elaborazioni, come fenomeno di portata esclusivamente economico-finanziaria²⁷². Ciò non tanto perché esso ha ad oggetto beni o altre utilità economiche, ma perché l'utilizzo di detti beni o utilità economiche, per le caratteristiche dimensionali e transnazionali dei fenomeni delittuosi più significativi cui si ricollegano, è idoneo ad alterare l'ordinato assetto economico-finanziario e monetario di un Paese e, talvolta, di intere aree regionali. Il crimine organizzato presta particolare attenzione all'efficienza dei processi produttivi e alla massimizzazione del profitto del riciclaggio, tanto che le scelte divengono sempre più spesso di tipo imprenditoriale e fondate su principi aziendalistici. In questo senso, le "imprese criminali" delocalizzano le attività in Paesi in cui il "costo riciclaggio" è più basso, ne frazionano le tra diversi ordinamenti per renderne più difficile la ricostruibilità ed investono dove il rendimento è più elevato²⁷³. In sostanza, sfruttano i vantaggi della globalizzazione, che offre un orizzonte di operatività più vasto, di possibilità di arbitraggi regolamentari tra le diverse giurisdizioni, di rapporti preferenziali con ordinamenti non cooperativi o con Stati bisognosi di risorse, con i quali instaurare direttamente dei canali preferenziali. Ora, se è vero che il ridimensionamento del ruolo dell'intermediazione bancaria (e connessa deregolamentazione dei movimenti di capitali), l'abbattimento delle frontiere e l'integrazione dei mercati, hanno congiuntamente contribuito ad accelerare il processo di

²⁷² La Comunità internazionale si è mossa dapprima sul piano della prevenzione e solo successivamente sul piano della repressione. Ed infatti, i primi strumenti di (auto)regolamentazione in materia di riciclaggio, non facevano alcuna menzione dei profili penali del fenomeno, essendo essi finalizzati a scongiurare infiltrazioni della criminalità economica nella finanza; tale è il caso della prima Risoluzione del Comitato dei Ministri del Consiglio d'Europa del 1980 (*Recomandation R(80)10*) e della Dichiarazione di principi per la prevenzione dell'utilizzo del sistema bancario per il riciclaggio di fondi di origine illecita, adottata dal Comitato di Basilea il 12 dicembre 1988. Per contro, è del 19 dicembre 1988 la Convenzione di Vienna, finalizzata alla criminalizzazione del riciclaggio, con la quale si dispone che ciascuna parte deve adottare i provvedimenti necessari per "attribuire il carattere di reato" ad una serie di condotte, tra le quali figurano la conversione, il trasferimento, la dissimulazione o la contraffazione dell'origine (o delle altre circostanze) di beni che si conosce essere proventi di reati relativi al traffico di stupefacenti e di sostanze psicotrope.

²⁷³ Vds. Pollari N., *L'impresa criminale ed i suoi effetti sui mercati e sugli aggregati macroeconomici*, *Rivista GdF.*, 3/1999, p. 1037, il quale afferma: «allorché si parla di crimine organizzato si deve fare riferimento ad entità simili ad un'impresa, potendosene ravvisare non poche analogie, specie per quel che attiene alla caratterizzazione economico-aziendalistica dei sodalizi delinquenziali. Tali soggetti, al pari di qualsiasi operatore economico, perseguono un obiettivo di efficienza allocativa delle risorse, nell'intento di massimizzare l'utilità delle scelte di investimento compiute e di cogliere nuove opportunità di affermazione e crescita, anche su scala transnazionale». Cfr. anche Arlacchi P., *La mafia imprenditrice. L'etica mafiosa e lo spirito del capitalismo*, Il Mulino, 1983, p. 84; di Nuzzo U. e Morgante A., *La rilevanza fiscale dell'impresa illecita*, *Finanza e Fisco*, n. 10, 1998, p. 1187.

sviluppo dell'economia, è altrettanto vero che ciò ha offerto i medesimi vantaggi agli operatori dell'economia "illegale", favorendo anche per le imprese criminali il ricorso alle "economie di scala" grazie alla disponibilità di una sempre più vasta gamma di strumenti di occultamento e investimento²⁷⁴. Infatti, si deve tener conto che l'incremento esponenziale dei flussi di capitale da riciclare e la necessità di reperire sempre maggiori provviste finanziarie da destinare al finanziamento del crimine transnazionale, uniti al crescente perfezionamento delle metodologie di controllo, hanno indotto tali organizzazioni a ricorrere anche ad altri meccanismi, quali società schermo possibilmente anonime e istituti finanziari anche non bancari²⁷⁵, uffici di cambio, assicurazioni, *brokers*, uffici *import-export*, commercianti in oro e altri metalli preziosi, casinò, servizi di posta celere e altre attività più o meno sofisticate di trasferimento del denaro.

Infine, la portata transnazionale del fenomeno presenta l'effetto di amplificarne la portata dissimulatoria anche a causa dei cd. "disallineamenti da ibridi" (*hybrid mismatch arrangements*), ossia strumenti pianificatori in grado sfruttare le differenze nella qualificazione giuridica di un rapporto finanziario o di un'entità (società anonima, fondazione, *trust*, fiduciaria ecc.) nelle diverse giurisdizioni con cui interagiscono.

L'altra variabile, che si pone come fattore di accelerazione ed agevolazione del riciclaggio, è rappresentata dallo sviluppo dei sistemi informatici e digitali²⁷⁶: l'uso della rete appare essere il più semplice ed immediatamente fruibile "strumento di lavoro" utilizzato correntemente dalla criminalità transnazionale, che è in grado di avvalersi di moderne tecnologie informatiche e degli strumenti finanziari innovativi più innovativi²⁷⁷. In un primo momento utilizzata per facilitare il trasferimento e la gestione delle risorse finanziarie di natura illecita di natura tradizionale, oggi è in grado di offrire prodotti e servizi digitali nativi, ossia originati nella stessa dimensione virtuale. Alla luce di ciò, appare evidente come i principali luoghi della *TradFi* (banche ed intermediari finanziari tradizionali) non sembrano più rappresentare dei passaggi obbligati per le attività di riciclaggio (se si escludono quelle

²⁷⁴ Cfr. Licini C., *Normativa antiriciclaggio e antiterrorismo per i professionisti*, Ipsoa, 2009, p. 9.

²⁷⁵ Tra l'altro, è stata osservata la tendenza delle evolute organizzazioni criminali a rivolgersi sempre meno alle grandi banche commerciali e sempre più spesso a quelle di più modeste dimensioni, denominate "*second line banks*" ed allocate in centri *off-shore*.

²⁷⁶ Cfr. Carta L. e Altiero N., *L'utilizzo di sistemi telematici a scopo di riciclaggio*, Riv. G.d.F., n. 3, 1999, p. 949 e ss.

²⁷⁷ Vds. Lembo M. e Scialoja A., *Antiriciclaggio*, cit., p. 28.

ricondotte ad organizzazioni criminali particolarmente legate ad un determinato territorio e alla dimensione locali dei propri traffici)²⁷⁸.

Diversamente, hanno assunto un ruolo centrale altri attori che svolgono attività (peraltro, non *stricto sensu* finanziarie) sulle quali ha esercitato un forte influsso la *net-economy*²⁷⁹, che si alimenta e si propaga grazie al *network* senza alcun diaframma centralizzato di tipo bancario o governativo, attraverso strumenti tecnologici flessibili, interoperabili e con elevati livelli di resilienza (*id est* la *Distributed Ledger Technology DLT* o il *blockchain management system BMS*). La dottrina parla di *cyber-laundering*²⁸⁰, chiarendo come questa nuova frontiera del riciclaggio non realizzi nuovi schemi, ma più semplicemente associ alle tradizionali e note fasi delle attività di lavaggio dei proventi illeciti veicoli e strumenti tecnologici ed altamente innovativi. In questa sede, tuttavia, non si ritiene che tale espediente definitorio colga appieno la portata rivoluzionaria dei *crypto-asset* e, più in generale, della *DeFi*, che ha conferito al fenomeno indagato caratteristiche sinora inedite e che involge un ventaglio di soluzioni veramente ampio unitamente a spazi di manovra pressoché illimitati. Queste considerazioni inducono chi scrive²⁸¹ ad operare un'ulteriore classificazione di tale fenomeno adoperando un'espressione che riassume le peculiari connotazioni del riciclaggio riferito agli *asset* digitali, ovvero il "*crypto-laundering*"²⁸². Tale definizione impone di considerare nelle fasi del riciclaggio un'ulteriore variabile, quella del cripto-anonimato.

Da questa angolazione prospettica, è possibile comprendere i motivi per i quali le Istituzioni finanziarie, le Autorità di vigilanza ed i Governi mondiali stiano pian piano assumendo più chiare posizioni sulle derive patologiche dell'uso dei *crypto-asset*, soprattutto con riferimento

²⁷⁸ Cfr. Manes V., *Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale*, Riv. trim. dir. pen. econ., 2004, p. 39.

²⁷⁹ Vds. Flick G. M., *Antiriciclaggio, corruzione e ruolo degli intermediari: un'agenda comune*, in Masciandaro D. (a cura di), *La legalità come valore di mercato*, Bancaria Editrice, 2000, p. 63 e ss..

²⁸⁰ Vds. Simoncini E., *Il cyberlaundering: la nuova frontiera del riciclaggio*, Riv. trim. dir. pen. econ., n. 4, 2015, p. 901; Picotti L., *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, Riv. trim. dir. pen. econ., n. 3-4, 2018, p. 591. Quest'ultimo definisce il *cyber-laundering* come il complesso «di tutte le attività illecite finalizzate a "ripulire" (letteralmente: "lavare") non solo il denaro (*money laundering*), ma più in generale i capitali, i beni, i valori o le altre "utilità" di provenienza delittuosa, ricorrendo a sistemi o mezzi elettronici o, meglio, "cibernetici", resi disponibili dalle tecnologie dell'informazione e della comunicazione (TIC), che coinvolgono oggi soprattutto la rete».

²⁸¹ Vds. gli approfondimenti già condotti in Tedeschi E., *Le criptovalute e i rischi di riciclaggio: lo stato dell'arte a contrasto del fenomeno*, La piazza d'Italia, 2022, cit.

²⁸² Questa dizione ha trovato ingresso anche in alcuni consessi internazionali: vds. Ilbiz E. e Kaunert C., *Sharing Economy for Tackling Crypto-Laundering: The Europol Associated "Global Conference on Criminal Finances and Cryptocurrencies"*, Sustainability, 2022.

alla commissione di illeciti, quali il riciclaggio di denaro, il finanziamento al terrorismo internazionale, la manipolazione dei mercati, l'evasione fiscale ed i reati finanziari, e stiano cercando di individuare dei *framework* regolamentari, contemperando il non semplice obiettivo di non disincentivarne eccessivamente l'utilizzo e le attività di ricerca e sviluppo dell'innovazione tecnologica a cui sono collegate.

Mentre fervono già da tempo iniziative proprio in tale ultima direzione, tanto da cominciare a parlare di una vera e propria *lex cryptographica*²⁸³, che trasversalmente mutua istituti giuridici comuni a diversi rami dell'ordinamento con aspetti molto specialistici della fiscalità finanziaria e d'impresa e della disciplina valutaria e finanziaria, solo di recente hanno cominciato a trovare ingresso proposte dirette ad integrare le modifiche alla normativa sostanziale con disposizioni che potenziano, in termini di *enforcement*, le *policy* di sicurezza e le procedure di controllo e di cooperazione internazionale tra Autorità competenti. Si è avvertita, in altri termini, la necessità che lo sviluppo di questi nuovi paradigmi tecnologici sia accompagnato da una più puntuale regolamentazione della materia, che garantisca efficaci misure di sicurezza e di tutela e che contempli, ad esempio, norme di diritto contrattuale in grado di arginare i fallimenti del mercato, meccanismi di protezione rivolti alla tutela della concorrenza sul mercato e della *privacy* a favore degli investitori e dei consumatori, misure atte a far sì che determinate attività rimangano circoscritte entro i limiti consentiti dall'ordinamento (a contrasto del finanziamento del terrorismo o del riciclaggio di denaro e di altre forme di criminalità economica) e via discorrendo in tal senso.

4. Cripto-attività e rischio di riciclaggio

Passando a un piano più squisitamente fattuale, è necessario soffermarsi su tutti quegli elementi connessi a tali fenomenologie che si ritiene facilitino l'occultamento, l'accumulazione e il reimpiego dei proventi illeciti e che delineano un vero e proprio canale

²⁸³ A tale definizione si riferisce l'odierna dottrina (Vds. [Wright A. e De Filippi P., *Decentralized Blockchain Technology and The Rise of Lex Cryptographia*, Social Science Research Network, 2015](#), secondo cui attraverso la "*Lex Cryptographia*" gli individui possono strutturarsi in autonome organizzazioni decentralizzate (*DAO*, "*decentralized autonomous organization*") e le transazioni e le relazioni vengono sviluppate mediante l'autoesecuzione di *smart contract*. Dottrina che, tuttavia, non manca di evidenziare le diverse criticità che permangono allo stato della tecnologia: sembra, infatti, difficile ipotizzare degli algoritmi in grado di emulare la *lex*/dottrina contrattuale in tema di errore, frode, coercizione, necessità o capacità.

parallelo e alternativo per il riciclaggio attraverso cui poter svolgere transazioni finanziarie non tracciabili al riparo da possibili controlli della Autorità di vigilanza. Sul punto, il mondo degli *asset* virtuali è fonte di minacce integrate di natura sia cibernetica sia economico-finanziaria: mentre le prime offrono il veicolo di trasmissione dei fenomeni criminogeni, le seconde designano l'ambito di proiezione e di penetrazione finale. Parliamo di fattori che appaiono correlati e caratterizzati da estrema liquidità e da relazioni totalmente immateriali, scollegate dai vetusti concetti del geograficamente delimitato e della dimensione fisica dei fenomeni cui sono normalmente connesse le norme giuridiche poste a presidio²⁸⁴. Dunque, non è semplice associare a questo mondo i concetti di riciclaggio o di reimpiego di capitali illeciti, le cui modalità attuative continuano ancora ad essere associate agli schemi classici che abbiamo analizzato nei precedenti paragrafi, ancorché facilitate attraverso le innovazioni apportate dalla *DeFi*. In tal senso, anche se da un punto di vista meramente terminologico, si coglie anche il tentativo di proporre in questa sede il concetto di *crypto-laundering*. In molti, infatti, ritengono che la concreta sussumibilità del riciclaggio "via cripto" nelle fattispecie codicistiche (articoli 648-bis, 648-ter e 648-ter.1 c.p. – riciclaggio, impiego di proventi illeciti, autoriciclaggio) sia possibile allorquando, ad un certo punto della progressione criminosa, i flussi finanziari virtuali di origine delittuosa assumano una più stretta connessione con il mondo reale attraverso la reimmissione di denaro nel circuito dell'economia legale (ad esempio, nel momento in cui interviene un *exchange* per la conversione in monete *fiat*)²⁸⁵. Come è stato infatti notato, gli scambi di cripto-attività forniscono liquidità ai relativi mercati, fungendo da *gateway* vitali tra ecosistemi *fiat* e *crypto*, motivo per il quale rappresentano un importante canale per le attività di riciclaggio, con rischi ancor più elevati laddove i criminali riescono a sfruttare le lacune normative di alcuni Stati, spostando i loro fondi illeciti verso *VASP* domiciliati in giurisdizioni con normative *AML/CFT* inesistenti o minime²⁸⁶.

Tuttavia, le analisi sino ad oggi condotte appaiono ancora incomplete, in quanto non sono

²⁸⁴ Cfr. Valente P. et al., *Riciclaggio e criminalità. Idra per gli Stati, Sisifo per la Società, Nesso per gli Organismi Sovranazionali*, Eurilink, Roma, 2017.

²⁸⁵ In questi, sul piano della condotta, più che di un'attività diretta alla "ripulitura", appare configurarsi come una sostituzione di "beni, denaro o altre utilità" provenienti da delitto non colposo. Vds. sull'argomento Sicignano G. J., *Bitcoin e riciclaggio*, Giappichelli, 2019, p. 122.

²⁸⁶ Vds. [Elliptic, Preventing Financial Crime in Crypto-assets, Elliptic typologies report 2022 edition, 2022.](#)

comprehensive di tutte le casistiche prospettabili²⁸⁷. Attraverso i *crypto-asset* sarebbe possibile commettere diversi atti criminosi (dalla vendita di beni/materiali illeciti, alle frodi contro i consumatori/investitori, alla richiesta di riscatti attraverso dei *virus ransomware*) e reinvestire in forme legali i proventi nei mercati dedicati alle cripto-attività o nelle molteplici aziende e *start-up* accettanti fondi in *crypto-asset*, oppure ridestinarli in altre attività criminali sempre attraverso il *deep web*. Il tutto senza mai abbandonare il perimetro virtuale della *blockchain* e senza integrarsi con i canali dell'economia reale, non consentendo di registrare anomalie sintomatiche del transito di fondi di derivazione criminosa²⁸⁸.

Muovendo da tali considerazioni, possiamo almeno osservare come la prima fase del riciclaggio (c.d. *placement*) possa svolgersi proprio entro il perimetro dei *crypto-asset* e come l'ultima fase l'*integration* non necessariamente richieda la preliminare conversione in denaro *fiat* degli *asset* virtuali. Non possiamo tantomeno escludere che l'attività di ripulitura si realizzi attraverso schemi inversi di quelli che abbiamo considerato in premessa, ossia che capitali illeciti espressi in moneta tradizionale trovino ingresso nel mercato dei *crypto-asset* e vengano riciclati attraverso scambi legittimi nei mercati di riferimento²⁸⁹.

I fattori sin qui elencati forniscono una sintetica panoramica della complessità e delle principali criticità insite nel settore finanziario, che appaiono amplificarsi se ci poniamo in relazione al funzionamento delle cripto-attività e alla loro naturale propensione ad essere impiegate per finalità di riciclaggio. In merito a ciò, a parere di chi scrive, i *crypto-asset* sono stati accompagnati sin dalla loro nascita da misure di autoregolamentazione, disciplinate autonomamente ed accettate dalla stessa comunità di utenti, interessati a trovare senza alcuna mediazione gli anticorpi per rendersi immuni da possibili deviazioni patologiche. Non si può non osservare come tali tentativi rimangano relegati nel campo delle buone intenzioni. In altri termini, queste misure non appaiono né vincolanti, né strutturate con adeguate limitazioni

²⁸⁷ Vds. [Fanusie Y.J. e Robinson T., Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services, Center on Sanctions & Illicit Finance, 2018.](#)

²⁸⁸ Volendo rifarsi alla terminologia utilizzata in ambito GAFI, il processo descritto può svilupparsi attraverso operazioni “*virtual-to-virtual*”, “*virtual to-fiat*” e “*fiat-to-virtual*”, in quanto possono coinvolgere attività che forniscono punti di accesso da e verso il sistema finanziario tradizionale regolarmente disciplinato (ossia i canali in entrata e in uscita). Vds. in merito [Gruppo d'Azione Finanziaria Internazionale, Linee guida per un approccio ai virtual asset e ai prestatori di servizi in materia di virtual asset basato sul rischio, MEF - Dipartimento del Tesoro, 2019.](#)

²⁸⁹ Vds. [Cancelli L., The Growing Crypto-assets Threat to Anti-money Laundering: How Institutions Are Coping with This Phenomenon, Università Ca'Foscari Venezia, 2020.](#)

tecniche, né ancora in grado contrastare le continue ibridazioni dei modelli originari in forme sempre più aggressive. Di qui, la necessità che gli Stati orientino la propria azione di contrasto al riciclaggio in tali settori attraverso la propria attività regolatoria.

Non si tratta certamente di un'opera semplice, considerando che le tecnologie alla base degli scambi di *crypto-asset* si sono evolute anche in reazione alle prese di posizione dei regolatori pubblici e alle opposte istanze di quanti domandano sicurezza e anonimato. Recenti studi²⁹⁰ evidenziano come le iniziative avviate dal GAFI, volte a far sì che gli Stati introducano sempre più restringenti misure di *enforcement*, rischiano di incoraggiare contromisure da parte degli sviluppatori che potrebbero ridurne l'efficacia. Ad esempio, l'avvento di strumenti di identificazione degli utenti ha incoraggiato in parallelo lo sviluppo di tecniche di anonimizzazione sempre più sofisticate (es. *mixer* o *tumbler*).

A questo punto bisogna domandarci come l'ecosistema dei *virtual asset* possa essere sfruttato a fini di riciclaggio, ossia in operazioni di ripulitura di fondi di origine illecita e di eventuale collocazione del controvalore nel circuito dell'economia reale²⁹¹. Al riguardo, mentre inizialmente la *FinTech* operava come mero strumento-veicolo per la prima immissione dei proventi di reato (*placement*), oggi si presta per la creazione di stratagemmi che possono facilitare anche le ulteriori fasi del *layering* ed *integration* attraverso sofisticate operazioni finanziarie che sfruttano proprio il sistema *DeFi*.

Nel mondo dei *crypto-asset*, l'assenza di intermediari, la possibile gestione *off-line* dei *wallet*, l'utilizzo della crittografia avanza, uniti alla possibilità di avvalersi di sviluppi applicativi che rendono sempre meno trasparente l'utilizzo della *blockchain*, sono tutti elementi che appaiono favorire operazioni di riciclaggio²⁹². Oltre alla crittografia, è soprattutto lo pseudo-anonimato a rappresentare l'elemento di maggiore criticità per i moderni sistemi di contrasto al riciclaggio, poiché ne vanifica ogni sforzo di contrasto (si pensi solo alla difficile applicazione del principio dell'adeguata verifica della clientela). In tale contesto, pertanto, si ritiene essenziale procedere ad un breve cenno su tali elementi prima di ritornare ad

²⁹⁰ [Campbell-Verduyn M., Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance, Crime, Law and Social Change, 2017.](#)

²⁹¹ Vds. Caramignoli G. e Di Pietro I., *Il fenomeno Bitcoin: moneta "virtuale" con effetti "reali" sull'economia*, Riv. G.d.F., n. 6, 2013, p. 1731 e ss.

²⁹² Cfr. La Rocca L., *La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*, Analisi Giuridica dell'economia, 2015, pp. 201 -222.

analizzare, ancora su di un piano fattuale, come il tradizionale processo del riciclaggio sia evoluto proprio attraverso tali espedienti tecnologici.

5. Il ruolo dello pseudo-anonimato

Come abbiamo già ampiamente illustrato, la *blockchain* è un database decentralizzato strutturato in blocchi, ciascuno dei quali contenente un determinato numero di informazioni, distribuiti in una struttura a catena all'interno di un *network*. Si tratta di una modalità di conservazione digitale di dati semi-pubblica, in quanto ciascun nodo, all'interno di una infrastruttura *blockchain*, è in grado di verificare se un altro utente detiene un'informazione, ma solo quello specifico utente può sbloccare il contenuto dell'informazione, poiché è l'unico che possiede le credenziali ovvero le chiavi per accedere al dato. La trasparenza, in questo caso, riguarda solo le informazioni registrate nei blocchi relative alle transazioni.

Diversamente, queste informazioni non riguardano i profili degli utenti che operano all'interno della *blockchain*, che non sono direttamente rintracciabili con la propria identità fisica, quanto invece con quella digitale attraverso la quale sono entrati a far parte della rete. Si tratta di una fattispecie definibile di “pseudonimia”²⁹³, caratteristica che certamente garantisce, di per sé, un elevato grado di opacità a tutti coloro che fanno parte del *network* e che negli anni ha attirato una parte di utenza che, proprio grazie a questo espediente, ha tratto vantaggio nell'utilizzare *crypto-asset* e *blockchain*, potendo così mascherare compravendite di beni/servizi illegali o svolgere attività di riciclaggio o reimpiego di proventi di provenienza illecita²⁹⁴. Al riguardo, occorre sottolineare un aspetto: il “sistema *Bitcoin*” viene considerato pseudo-anonimo (o forse sarebbe meglio discorrere di “quasi-anonimo” da non confondere

²⁹³ Il *GDPR* (Regolamento 2016/679/UE del parlamento europeo e del consiglio del 27 aprile 2016), all'art. 5 definisce la “pseudonimizzazione” come «il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile».

²⁹⁴ Vds. [Rinaldi G., *Approcci normativi e qualificazione giuridica delle criptomonete*, in *Contratto e impresa*, n. 1, 2019, p. 265](#) il quale afferma che «le transazioni bitcoin non sono anonime, bensì pseudo-anonime. Tutte le operazioni effettuate all'interno del sistema sono registrate e archiviate nella blockchain (ciascuna con una propria marcatura temporale), e restano liberamente consultabili, per un periodo di tempo illimitato, da qualunque soggetto, anche se questi non partecipa alla rete».

con il concetto di “pseudonimo”²⁹⁵) aspetto non trascurabile se si considera come l’utenza si sia spostata nel tempo verso altri *crypto-asset* e strumenti digitali in grado di garantire ancora maggiore *privacy* ed opacità²⁹⁶. Almeno tecnicamente, si deve considerare che il “sistema *Bitcoin*” rimane trasparente poiché i dati contenuti all’interno di una *blockchain* risiedono all’interno della catena per sempre, replicati tante volte quanti sono i nodi all’interno della rete. Inoltre, la *blockchain* non solo contiene l’ultimo stato dei dati, ma anche l’intera storia di quelli precedenti, in modo che ciascun nodo sia in grado di verificare la correttezza e l’integrità dello stato finale. Esistono strumenti di *blockchain analysis* che sono stati sviluppati proprio in virtù di queste peculiarità, traendo spunto dalle tecniche più sofisticate di informatica forense. La *blockchain analysis* consiste nell’ispezione, identificazione, *clustering*²⁹⁷, modellazione e rappresentazione visiva dei dati contenuti all’interno della “catena dei blocchi”. Poiché i *crypto-asset* sono utilizzati anche nel commercio di beni illegali e le relative transazioni risiedono all’interno della *blockchain*, attraverso la *blockchain analysis* è possibile ricavare informazioni utili circa i diversi utenti che eseguono le operazioni e che, a prescindere dall’utilizzo di *nickname*, possono essere più facilmente identificati con le tecniche di analisi descritte²⁹⁸.

²⁹⁵ Ciò non esclude che vengano anche utilizzati “pseudonimi”, sulla cui pericolosità si è espressa anche la Consob. Sull’argomento, vds. [Carrière P. et al., Tokenizzazione di azioni e azioni tokens, Quaderni giuridici Consob, n. 25, 2023](#).

²⁹⁶ Le caratteristiche di “pseudo-anonimato” dei *bitcoin* e il loro registro trasparente hanno favorito lo sviluppo di ulteriori *crypto-asset* (cd. *altcoin*) in grado di garantire superiori *standard* di sicurezza. Tali *virtual asset*, definite dalla letteratura come “più opache” rispetto a *bitcoin*, appaiono perfettamente congeniali per le finalità criminali di cui si è detto (Vds. [Foley S., et al., Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Crypto-currencies?, Review of Financial Studies, Forthcoming, 2018](#)). Non è un caso che il loro sviluppo coincida temporalmente con una riduzione, in termini proporzionali, delle attività illecite condotte attraverso l’utilizzo dei *bitcoin*. Questi aspetti sono stati richiamati anche dalla rivista britannica “*Independent*”, [Bitcoin price is so high because criminals are using it for illegal trades, research suggests, 2018](#), articolo in cui vengono presentati i risultati della ricerca della University of Sidney e della University of Technology of Sidney.

²⁹⁷ L’attività di *clustering* si preoccupa con delle euristiche di estendere l’etichetta a tutti gli indirizzi considerati dello stesso proprietario. Infatti, il protocollo *Bitcoin* suggerisce, anche se non impone, l’uso di un nuovo indirizzo ogni volta che un utente effettua una transazione. Questo significa che un utente diligente possiede decina, centinaia o anche migliaia di indirizzi, raccolti in uno o più wallet. Vds. [Bistarelli S., Bitcoin forensics: le tecniche labeling, clustering e mixnet recognition, 2018](#). L’articolo si sofferma sugli sviluppi dell’attività di ricerca condotti in questo specifico campo dall’Università degli Studi di Perugia e, in particolare dal Nodo perugino del *Cyber Security National Lab* del CINI (Consorzio Interuniversitario Nazionale per l’Informatica).

²⁹⁸ Uno dei metodi più utilizzati nell’analisi forense è lo *scraping*, che si occupa di trovare indirizzi *Bitcoin* utilizzati per scopi illeciti grazie all’analisi di pagine *web*. Lo *scraping* implementa anche una parte di *clustering* che utilizza degli *script* per il recupero di informazioni da *social-forum* o gruppi di discussione comunque denominati.

Anche alla luce delle considerazioni sin qui svolte, possiamo affermare come l'intero sistema delle cripto-attività inverta il tradizionale rapporto – verso cui tendono i presidi normativi in materia di antiriciclaggio – secondo cui “a transazione sconosciuta corrispondono delle parti conosciute”, in quanto ad essere anonime, in questo caso, possono essere proprio le parti e ciò rende molto più complicato contrastare tale fenomeno. Il sistema, dunque, rappresenta di fatto un vero “paradiso virtuale”, in cui restare impuniti grazie al completo anonimato è garantito grazie alla vasta sequela di atti che compongono le tre fasi in cui si articola il riciclaggio²⁹⁹.

Nella fase del collocamento (*placement*) lo pseudo-anonimato è una caratteristica che, senza dubbio, è in grado di attirare chiunque intenda trasferire illecitamente dei fondi, mentre la velocità delle transazioni consente di convertire le *altcoin* tra loro con livelli di anonimato ancora più elevati o in valute *fiat* in Stati con un basso livello di contrasto al fenomeno del riciclaggio. Nella fase della stratificazione (*layering*), i *cyber* criminali possono fare affidamento sull'impossibilità di tracciare e bloccare le transazioni una volta eseguite e sulla disponibilità di conti correnti intestati a soggetti “presta conto” (i cosiddetti “*money mule*”) che, una volta ricevuto l'accredito delle somme, procedono al loro incasso ed al successivo trasferimento al reale destinatario, ovvero possono svolgere tutta l'intera filiera di attività illecite (commissione del crimine, ottenimento del profitto, riciclaggio e utilizzo dei fondi ripuliti) senza mai uscire dall'area degli *asset* virtuali³⁰⁰. Sempre nella fase della “stratificazione”, i soggetti possono distribuire i fondi illeciti su più *dark wallet* (utilizzando

²⁹⁹ In merito, corre l'obbligo di evidenziare come autorevole dottrina abbia inteso focalizzare l'attenzione proprio su alcune caratteristiche ordinarie di alcuni Paesi che, in passato, avevano semplicemente schermato “amministrativamente” le proprie giurisdizioni da indagini conoscitive finalizzate al contrasto dell'evasione fiscale, fornendo una definizione degli stessi più al passo con i tempi e in grado di coglierne intuitivamente le nuove connotazioni, ovvero quella di “*paradisi fisco-informatici*”. Vds. Valente P. *et al.*, *Riciclaggio e criminalità. Idra per gli Stati, Sisifo per la Società, Nesso per gli Organismi Sovranazionali*, Eurilink, Roma, 2017 cit., p. 548; [Tedeschi E., Le criptovalute e i rischi di riciclaggio: lo stato dell'arte a contrasto del fenomeno, La piazza d'Italia, 2022](#), cit.

³⁰⁰ Per approfondimenti vds. l'[APG, Typologies Report, 2022](#), organismo regionale che opera come il GAFI. Nel rapporto si evidenzia come un punto in comune che riguarda molti dei casi di studio è rappresentato dall'uso di *money mule* per offuscare le attività di stratificazione nelle transazioni tra fiat e crittografiche. In Australia, ad esempio, un'organizzazione coinvolta nel riciclaggio di denaro ha aiutato dei criminali a riciclare grandi quantità di denaro utilizzando appunto *money mule*, depositando il denaro nei loro conti bancari prima di convertirlo in *bitcoin* e quindi trasferire nuovamente *bitcoin* ai “clienti” criminali. Un *modus operandi* simile è stato utilizzato da un sodalizio criminale dedito a truffe transfrontaliere, che ha utilizzato 15 *money mule* per aprire oltre 80 conti bancari a Hong Kong per riciclare i proventi criminali, parte dei quali sono stati utilizzati per acquistare *bitcoin* e *ether*.

diverse *altcoin*) o *cold wallet* (come un *hard disk*), che assicurano servizi di conservazione *off-line* dei portafogli digitali³⁰¹. Nella fase dell'integrazione (*integration*), l'anonimato consente di incassare il controvalore dei proventi illeciti e di inviarlo successivamente a soggetti terzi, anche estranei alla rete criminale ed anche se localizzati in Stati diversi³⁰².

Ulteriori elementi critici, che si traducono ovviamente in una maggiore appetibilità dei *crypto-asset* per riciclatori, sono dovuti al fatto che le cripto-attività possono essere acquistate o convertite in moneta *fiat*, non solo attraverso un *exchange*, ma anche avvalendosi di uno dei numerosi *ATM* presenti nel mondo (tali casse automatiche sono installate soprattutto presso i locali di società italiane che operano come concessionarie di fornitori esteri di servizi di *asset* virtuali³⁰³) dal quale è possibile caricare sul proprio *digital wallet crypto-asset* ovvero convertirli e prelevare moneta *fiat*.

Peraltro, uno dei metodi più diffusi di scambio/cambio di *crypto-asset*, segue gli schemi tradizionali dell'uso contante. Parliamo del cosiddetto "scambio faccia a faccia" (o *face to face*), ove i *crypto-asset* (principalmente *bitcoin*) sono acquistati in contanti, in occasione di incontri fisici tra il cedente e l'acquirente (durante raduni o riunioni *organizzate proprio* per tali finalità). Gli incontri generalmente seguono un accordo sul prezzo di vendita avvenuto su siti specializzati, di cui il più noto era *Localbitcoin* (operativo anche in Italia)³⁰⁴, che permetteva ad individui geograficamente vicini ed intenzionati all'acquisto o alla cessione di *Localbitcoin* di accordarsi sul prezzo e regolare di persona la compravendita in contanti (ferma la possibilità, comunque di finalizzare l'accordo in modo trasparente attraverso bonifico bancario). Tale metodologia può prevedere anche la presenza di un terzo soggetto, che funge da *trader* occupandosi materialmente di cedere dietro corrispettivo, sempre in contanti, i *crypto-asset*³⁰⁵. A differenza di un *exchange*, ovviamente, il *trader* richiede

³⁰¹ Vds. gli approfondimenti già condotti in [Tedeschi E., *Le criptovalute e i rischi di riciclaggio: lo stato dell'arte a contrasto del fenomeno*, La piazza d'Italia, 2022](#), cit.

³⁰² Vds. Choo K. R., *Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks?*, in Chuen D. L. K., *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, Academic Press, Londra, 2015.

³⁰³ Cfr. [Borgobello M., *Riciclaggio con criptovalute, gli sportelli ATM ultima frontiera: vulnerabilità e tutele*, Agenda Digitale, 2021](#).

³⁰⁴ *LocalBitcoins* è uno storico *marketplace* di *Bitcoin* con sede in Finlandia che agli inizi del 2023 ha, tuttavia, deciso di sospendere i propri servizi.

³⁰⁵ Un indubbio aspetto problematico delle attività dei *trader* riguarda il quantitativo di contante oggetto di scambio, che può superare il limite di utilizzo fissato per legge.

commissioni più elevate, oscillanti fra il 7 ed il 15% del valore totale della transazione³⁰⁶. Il *trader* può accordarsi (attraverso mezzi di comunicazione e servizi di messaggistica istantanea come *Telegram* o *Whatsapp*³⁰⁷) con gli acquirenti su siti presenti sia sul *surface web* che sul *dark web*. Negli accordi, il venditore specifica il tasso di cambio e la soglia minima e massima di contante da versare per completare l'operazione.

Come già evidenziato, il sistema di scambio può essere reso ulteriormente opaco attraverso sistemi capaci di offuscare la relazione tra venditori ed acquirenti e di oscurare del tutto l'origine di qualsiasi transazione. Oltre alla possibilità di modificare o occultare l'indirizzo *IP* dell'utente collegato alla rete (specie su *TOR*), ulteriori possibilità sono date dall'utilizzo di un *mixer*, anche definito come *laundry service mixer* o *tumbler*³⁰⁸. Tali strumenti si fondano su algoritmi in grado di "mixare" i *bitcoin*, attraverso pratiche di *tumbling*, condotte prevalentemente sul *dark web*, che consentono di spaccettare un consistente ammontare di *crypto-asset* in una moltitudine di frammenti, così da ottenere effetti di "diversificazione" e "confusione". Un *mixer* può essere "centralizzato" o "*peer to peer*". Il primo, oramai tecnologicamente superato, opera attraverso un servizio di *mixing* centralizzato che riceve *bitcoin* dagli utenti e provvede a riconsegnare altri *bitcoin* provenienti da altre transazioni, così da nascondere la reale provenienza, in pratica, mescolando le operazioni con quelle svolte da altri utenti su portafogli collegati al medesimo *mixer* che, in questo modo, viene ad interpersi nella fase di mixaggio tra l'utente che intende nascondere i propri *bitcoin* e chi riceve *crypto-asset* "ripuliti". Trattandosi di una tecnologia centralizzata il sistema presenta i rischi di furto o frode da parte dei gestori dei servizi. Il *mixer peer to peer*, invece, è basato sullo sfruttamento di tecnologie decentralizzate e sull'operatività di una comunità di utenti, tutti contestualmente interessati a celare le disponibilità digitali. Tale metodo non consente di individuare da quale *wallet* provengono i *crypto-asset*, specie se utilizzato in combinazione con i nuovi protocolli di crittografia, definiti "*blind mixing*", come *crypto-blinding*, *zero knowledge proofs* (ZKP) e *Succinct Non-interactive Arguments of Knowledge* (SNARK), che

³⁰⁶ Cfr. [Anti Money Laundering Centre, The Bitcoin trader: a facilitating role in the cash out of criminal proceeds, De Bilt, 2017.](#)

³⁰⁷ Su *Telegram* operano numerosissimi gruppi e canali che riuniscono le community dedicate al *crypto-trading*. Ciò ha spinto *Telegram* a creare un proprio *crypto wallet* nativo nella sua *app*, che permette di detenere alcune cripto-attività ed inviarle ad altri utenti *Telegram* in modo istantaneo e a costo zero.

³⁰⁸ Cfr. La Rocca. L., *La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*, Analisi giuridica dell'Economia, 2015, pp. 201-220.

sembra riescano ad impedire allo stesso server di conoscere gli indirizzi di partenza e di arrivo³⁰⁹. Alcuni siti specializzati pubblicizzano in rete questi servizi per garantire una maggior grado di sicurezza contro attacchi esterni. Appare di tutta evidenza, che questi sistemi appaiono assicurare ripari non solo da malevole penetrazioni *hacker* ma anche da possibili verifiche delle Autorità di controllo.

In ultima analisi, va segnalata l'esistenza di *altcoin* che utilizzano protocolli particolarmente impermeabili alla verifica delle identità degli utenti con sistemi automatici di *mixing* o con sistemi che creano *crypto-asset* separati, anonimi e simulati, che esiste a fianco di uno (non-anonimo) denominato *basecoin* e che può essere convertito in qualsiasi altra *altcoin*³¹⁰.

Volendo a questo punto tirare le fila, possiamo senz'altro concludere che il sistema descritto appare perfettamente congeniale per le organizzazioni criminali intente a riciclare il frutto delle proprie attività illecite, ciò in quando il mondo dei *crypto-asset* sembra segnare il passo al passaggio dallo *Shadow Banking System*³¹¹, complesso di mercati, istituzioni e intermediari che erogano servizi finanziari senza essere soggetti alla relativa regolamentazione, ad un sistema definibile, ad avviso di chi scrive, come una sorta di *Stealth Banking System*, ossia un complesso di strumenti che, oltre all'assenza di regolamentazione,

³⁰⁹ Vds. [Sat D. M. et al., Investigation of money laundering methods through crypto-currencies, in Journal of Theoretical and Applied Information Technology, Vol. 83, n. 2, 2016.](#)

³¹⁰ Parliamo, principalmente, di *ZeroCoin* e *Monero*, dove la prima, utilizza il protocollo *ZeroCash*, che assicura anche l'anonimato sull'origine dei pagamenti e sugli importi scambiati sulla *blockchain*, mentre la seconda, sfrutta il *deep web* e la tecnologia del *node to node* per creare una rete di copertura anonima ed incrementare la *privacy* delle transazioni. Per approfondimenti si rimanda a [Tedeschi E., Le criptovalute e i rischi di riciclaggio: lo stato dell'arte a contrasto del fenomeno, La piazza d'Italia, 2022.](#) cit.

³¹¹ L'espressione *shadow banking system* è stata introdotta nell'agosto del 2007 quando, durante un intervento presso il simposio annuale della *Federal Reserve* un esponente di mercato (McCulley P., *Teton Reflections*, Global Central Bank Focus, Federal Reserve of Kansas City, Jackson Hole Economic Symposium, 2007) sottolineò che in quegli anni si era andata sviluppando una forma di intermediazione basata su una varietà di veicoli di investimento con elevata leva finanziaria, di *conduits* e di altre strutture al di fuori del sistema bancario. Veniva sottolineato che, a differenza delle banche tradizionali che si finanziano prevalentemente attraverso i depositi e hanno accesso, se necessario, alla liquidità della Banca Centrale, queste "banche ombra non regolamentate" raccoglievano attraverso il mercato, esponendosi a una potenziale carenza di liquidità. In seguito, si sviluppò un ampio dibattito, sia in ambito accademico, sia presso le istituzioni internazionali e i regolatori. Alcuni autori associarono questa terminologia alla generazione di rischi di natura bancaria al di fuori del sistema bancario tradizionale; altri posero l'accento sulla disarticolazione del processo di intermediazione creditizia attraverso tecniche di trasferimento del rischio di credito, l'uso dei mercati *repo* e del prestito titoli, nonché l'utilizzo di collaterale poco liquido per costruire posizioni con leva elevata; altri ancora considerarono più semplicemente *shadow banking* ogni forma di intermediazione creditizia non regolamentata o, infine, ogni forma di intermediazione non bancaria. Fu, così, istituita, nel dicembre 2010, una *task force* dall'*FSB* nelle cui conclusioni venivano definite *shadow banking* «ogni forma di intermediazione creditizia che coinvolge entità o attività in parte o completamente al di fuori del sistema bancario tradizionale».

rende totalmente invisibile la quantità di *crypto-asset* transati, il numero delle transazioni e l'identità degli soggetti intervenuti nelle operazioni. Sistemi di questa tipologia appaiono preconizzare quanto affermato dal Comitato di Basilea, dove veniva sottolineato come le banche tenderanno a trasformarsi in *disintermediated bank*, perdendo il loro ruolo di intermediari a favore di piattaforme basate su tecnologie *peer-to-peer*, caratterizzate dall'incontro diretto tra domanda ed offerta di servizi bancari e finanziari di qualsiasi tipo senza alcun diaframma centralizzato³¹².

6. La *blockchain* ed il finanziamento al terrorismo

Nell'ottobre 2018 il *web magazine al-Haqiqa*, curato dalla coalizione di *al-Qaeda* in Siria, ha pubblicato un *post* che invita i lettori a usare i *bitcoin* per finanziare l'organizzazione terroristica. Si tratta di un episodio che ha avuto ampia risonanza mediatica dal momento che per la prima volta un ramo centrale di *al-Qaeda* ha promosso l'uso delle monete virtuali per finanziare la *jihad*³¹³. Le transazioni effettuate tramite *crypto-asset* da organizzazioni terroristiche islamiche non supererebbero mediamente l'equivalente di \$1 milione³¹⁴. Cifra marginale rispetto al totale finanziato al terrorismo internazionale che, tuttavia, si ritiene

³¹² Vds. [Comitato di Basilea, Implications of Fintech Developments for Banks and Bank Supervisors, Sound Practices, 2018](#), ove si afferma che, sotto la spinta del *Fintech*, nei prossimi anni - secondo la previsione in un certo senso "provocatoria" del Comitato - avremo:

- *The better bank*: ovvero banche che hanno sposato l'innovazione con evidenti benefici a livello di processi interni e di relazione con il cliente;
- *The new bank*: nuove banche, nate già con un forte DNA digitale, rimpiazzeranno le banche che non avranno saputo accogliere e implementare la sfida e quindi sono destinate a un mesto tramonto;
- *The distributed bank*: pensare alla "banca distribuita" significa immaginare un prossimo futuro nel quale le funzioni e i servizi finanziari oggi in capo a una singola istituzione vengano spezzettati tra più soggetti; in parte rimarranno alle banche tradizionali, in buona parte verranno gestiti da *fintech* specializzate;
- *The relegated bank*: in questo scenario, considerato improbabile in una prima fase, le banche tradizionali diventeranno *provider* di servizi-*commodity* (ovvero non più percepiti dal cliente come servizi a valore aggiunto), mentre i servizi a valore aggiunto e la relazione con il cliente saranno gestiti dai nuovi intermediari tecnologici, *fintech* o *bigtech*, che avranno in questo scenario il controllo predominante di dati della clientela, che sono il bene più prezioso.
- *The disintermediated bank*: è lo scenario considerato più estremo e remoto: le banche saranno ormai diventate irrilevanti e i clienti interagiranno ormai direttamente con le realtà *fintech* senza l'intermediazione o il collegamento con la banca tradizionale.

³¹³ Vds. Barone D. B., *Il terrorismo islamico si finanzia con i Bitcoin. Ecco perché è allarmante più per la propaganda che per l'economia*, 2018.

³¹⁴ Cfr. [Barone D.B., Criptovalute e Jihad: Propaganda, ideologia e comunicazione, difesa.it, 2019.](#)

possa essere lievitata in tempi più recenti considerando che la sola *Hamas* ha raccolto \$41 milioni in *crypto-asset*³¹⁵.

Sebbene i requisiti delle operazioni di finanziamento del terrorismo varino a seconda del tipo di organizzazione e della matrice endogena o esogena degli eventi terroristici, generalmente facciamo riferimento al reperimento di risorse necessarie ad operazioni specifiche, a mantenere in vita e gestire l'organizzazione terroristica, a reclutare nuovi adepti e a promuoverne l'ideologia e gli obiettivi. Le più grandi organizzazioni richiedono, ovviamente, finanziamenti significativi: il *budget* annuale di *al-Qaeda* precedente all'11 settembre era stimato intorno ai \$30 milioni; invece nel 2015, l'*ISIS* ha potuto contare su di un *budget* di \$2 miliardi.

Le tecniche comunemente associate al finanziamento del terrorismo si articolano in tre momenti, speculari alle tre fasi del riciclaggio: la raccolta (*collection*) dei fondi, non importa se di origine lecita o illecita, che sono inviati ad un collettore principale; il trasferimento o l'occultamento (*transmission or dissimulation*), attraverso cui sono oscurate le finalità ultime dei movimenti dei fondi; l'impiego (*use*) dei fondi per complete atti di terrorismo. Diversamente dal riciclaggio, appare di tutta evidenza che il finanziamento del terrorismo si prefigge l'obiettivo di occultare la destinazione dei capitali, più che la loro origine, che può essere sia lecita che illecita. Ciò non toglie che anche nelle attività di finanziamento al terrorismo si registrano metodiche tese a dissimularne anche la provenienza. In tale ambito, assumono particolare rilevanza i circuiti bancari informali, definiti dal Dipartimento di Stato americano *Informal Value Transfer Systems (IVTS)*³¹⁶, che operano al di fuori del settore finanziario regolamentato. Questi sistemi informali di pagamento, particolarmente diffusi nel Continente asiatico, si sono gradualmente affermati in tutto il mondo e sono conosciuti con diversi nomi. I più noti sono l'*hawala* di origine indiana, l'*hundi* di origine pakistana, il *fei ch'ien*, l'*hui k'uan*, il *ch'iao hui* e il *nging sing kek* di origine cinese e il *phoe kuan* thailandese. Il sistema informale di pagamento più importante è, senza dubbio, l'*hawala*, che opera in moltissimi Paesi parallelamente a quello bancario. Il significato del

³¹⁵ Cfr. [Berwick A. e Talley I., Hamas Militants Behind Israel Attack Raised Millions in Crypto, in Wall Street Journal, 2023.](#)

³¹⁶ Cfr. Durrieu R., *Rethinking money laundering and financing of terrorism in international law*, 2013; Fiocca M. e Cosci S, *La Dimensione Finanziaria del Terrorismo e del Contro-Terrorismo Transnazionale*, Rubbettino, 2004, p.49.

termine *hawala* (che in *hindi* significa “in fede”) esprime la natura fiduciaria delle transazioni che avvengono tra gli operatori. Il sistema si è andato diffondendo, a seguito dei massicci flussi migratori, principalmente tra le popolazioni dei Paesi islamici in Medio Oriente e in Africa, in India e nel Sud-Est asiatico³¹⁷. Questi sistemi tradizionali che si fondano sulla presenza fisica di mediatori, *broker*, corrieri ecc., hanno iniziato ad essere sostituiti da metodi alternativi, che prevedono l'utilizzo di più moderne tecnologie, sulla base di sistemi di pagamento digitali con i quali operare transazioni più veloci, anonime e capaci di movimentare flussi finanziari su base transnazionale.

In tempi più recenti, pur a fronte di un progressivo arretramento dello “*Stato Islamico*” sul piano militare, la minaccia del terrorismo internazionale continua a rimanere elevata in tutto il mondo e sembra riorientarsi verso nell'ambito del conflitto israelo-palestinese. Nel territorio europeo l'attenzione delle autorità deputate al contrasto al terrorismo e al suo finanziamento è rivolta soprattutto alla minaccia specifica dei cd. “lupi solitari” e dei combattenti stranieri di ritorno dal conflitto (*returnees*) e alle forme sempre più parcellizzate assunte dal fenomeno generale, che vede la presenza di piccole cellule autoctone, anche non direttamente collegate ai *network* internazionali. La maturazione di sentimenti religiosi radicali da parte di questi ultimi avviene nelle comunità e nei luoghi di aggregazione locali, talvolta all'interno di strutture detentive, o sempre più spesso, previo auto-indottrinamento, favorito dai *social network*.

Questa parcellizzazione della minaccia terroristica, unita alla particolare inclinazione delle nuove leve verso il *web*, ha fatto emergere il rischio circa la possibilità che gruppi terroristici possano finanziarsi ovvero finanziare le proprie cellule dormienti o lupi solitari, attraverso il ricorso ai *crypto-asset*. In realtà, come rileva il CNAS (*Center for a New American Security*), tra i più influenti *think tank* statunitensi nel settore dell'antiterrorismo, questi ultimi strumenti possono essere attrattivi per le organizzazioni terroristiche allo stesso modo di come lo possono essere per scopi legittimi³¹⁸.

³¹⁷ Per maggiori dettagli vds. il rapporto [Gruppo d'Azione Finanziaria Internazionale, *The role of hawala and other similar service providers in money laundering and terrorist financing*. Report, 2013.](#)

³¹⁸ Cfr. [Goldman Z.K. et al., *Terrorist use of virtual currencies: containing the potential threat*, Center for a New American Security, 2017.](#)

Il primo caso documentato di finanziamento al terrorismo tramite *crypto-asset*³¹⁹ è il “*fund the islamic struggle without leaving a trace*”, una pagina anonima apparsa nel 2012 nel *deep web*. La campagna di donazione fu totalmente vana, ricevendo l’equivalente di \$50, molto probabilmente trasferiti attraverso un impacciato tentativo di versamento posto in essere dai medesimi ideatori³²⁰.

Bisogna arrivare al 2014 per incontrare altri due casi documentati che appaiono presentare profili d’interesse per gli analisti. Il primo caso, in particolare, è quello di un sito, accessibile sempre sul *deep web* e pubblicizzato anche dalla rivista dell’Islamic State, “*Dabiq*”, che perseguiva lo scopo di vendere monete in oro, argento e rame utilizzate come mezzo di scambio all’interno dei territori occupati dall’ISIS. Oltre a mezzi di pagamento tradizionali il sito accettava anche pagamenti in *bitcoin*, che rappresentano un simbolo di antagonismo verso il sistema bancario occidentale. Proprio in quest’ottica, il “*Bitcoin a Sadaqat al-Jihad*” (*Bitcoin* è l’elemosina della jihad) si propone come il *white paper* jihadista dei *bitcoin*, introducendo gli *asset* virtuali come un’arma per abbattere il sistema bancario occidentale in assoluto anonimato³²¹. Il 2015 segna l’anno in cui prendono avvio le campagne di donazione che accettano *asset* virtuali direttamente riconducibili a gruppi terroristici: *Jahezona*, organizzata dall’*Ibn Taymiyya Media Center (ITMC)* - il reparto media del *Mujahideen Shura Council (MSC)*, un’alleanza di gruppi jihadisti salafiti della striscia di Gaza - ha iniziato ad accettare donazioni in *bitcoin*. *Jahezona* compare su canali pubblici di *Twitter* e *Telegram* e nei suoi *post* dichiara apertamente di aver bisogno di denaro per acquistare armi. All’inizio, la compagna è sembrata di scarsa portata, ricevendo più o meno l’equivalente di \$500, ma nel 2018, il nuovo indirizzo *bitcoin* (pubblicato sulla pagina *Telegram*) mostra 15 transazioni, due delle quali rispettivamente di \$289.273,87 e \$123.020,68. Nel 2016 un affiliato all’*Islamic State Hacking Division* (un’unità informatica di Daesh) ha chiesto un riscatto di

³¹⁹ Per i casi descritti nel presente paragrafo si è fatto riferimento alle informazioni riportate da Cfr. Barone D.B., *Criptovalute e Jihad: Propaganda, ideologia e comunicazione*, cit..

³²⁰ [Azani E. e Liv N., Jihadists’ Use of Virtual Currency, IDC Herzliya – ICT International Institute for CounterTerrorism, 2018.](#)

³²¹ L’articolo cita i pilastri e i principi dell’Islam che sono alla base delle campagne di raccolta fondi jihadiste:

- *Zakat*, una sorta di tassa utilizzata per donare una quota delle proprie disponibilità (solitamente il 2.5%, percentuale che aumenta in tempi di guerra);
- *Sadaqa*, la carità volontaria;
- *Jhad bil maal*, donazioni verso i *mujahideen*.

2 *bitcoin* (al tempo \$500) ad un *e-commerce* dell'*Illinois* per rimuovere un *virus* dai suoi sistemi. Nel 2017, pochi giorni dopo la perdita delle roccaforti dell'*IS* in Siria, *Al Sadaqah* (la carità), chiede esplicitamente denaro per finanziare la battaglia dei *mujahideen* in Siria contro il regime di Assad. Lo stesso anno in Indonesia Bahrin Naim, considerato l'ideatore dell'attentato terroristico del 2016 a Giacarta, è stato indagato di aver donato *bitcoin* per sostenere operazioni terroristiche per *Daesh* in Indonesia. Nel 2018, il *Malhama Tactical team*, gruppo di mercenari fiancheggiatori di organizzazioni islamiche estremiste, a seguito della morte del proprio *leader* causata da un bombardamento russo, ha richiesto donazioni in *bitcoin* per l'acquisto di armi, munizioni e provviste per i combattenti. Nel 2021, l'Ufficio nazionale israeliano per il finanziamento del contrasto al terrorismo (*NBCFT*) ha sequestrato diversi indirizzi di *crypto-asset* riferiti a *blockchain* associate a campagne di donazioni portate avanti dall'organizzazione terroristica *Hamas*. L'ordine di sequestro dimostra come *Hamas* abbia raccolto donazioni anche in *Tether*, *TRON*, *Cardano*, *XRP* e *DOGE*, cercando di liberarsi dalla dipendenza da *bitcoin* dopo che il Dipartimento di Giustizia degli Stati Uniti aveva annunciato il sequestro di \$2 milioni in *bitcoin* da parte di importanti gruppi terroristici, tra cui *al-Qaeda*, *ISIS* e la stessa *Hamas* nell'agosto 2020.

A livello di *enforcement* a livello globale, le iniziative di monitoraggio dei rischi di finanziamento del terrorismo sono proseguite allo scopo di individuare efficaci strategie per il rafforzamento della prevenzione e del contrasto del finanziamento del terrorismo. Nel 2018 il GAFI ha aggiornato l'*Operational Plan* antiterrorismo adottato nel 2016 per le attività del GAFI stesso e dei Paesi membri, nella cornice della *Strategy on combatting terrorism financing*, elaborata nel 2016. Sempre nel 2018 il GAFI ha pubblicato un rapporto dedicato al finanziamento delle attività di reclutamento per attività terroristiche³²², che approfondisce le modalità di finanziamento di iniziative di propaganda volte a favorire la radicalizzazione e l'affiliazione. L'azione di contrasto al finanziamento del terrorismo è proseguita, in Europa, in linea con l'*Action Plan* adottato dalla Commissione nel 2016 (*Communication from the Commission to the EU Parliament and the Council on an Action Plan for Strengthening the Fight against Terrorism Financing* (COM (2016) 50). Tra le molteplici linee di azione

³²² Vds. [Gruppo d'Azione Finanziaria Internazionale, *Financing of recruitment for terrorist purposes*, 2018.](#)

individuare figurano il rafforzamento della cooperazione tra autorità competenti (in particolare le FIU) e la prevenzione dell'anonimato nelle transazioni finanziarie.

7. Usi illeciti di *NFT* per finalità di riciclaggio e finanziamento al terrorismo

I *Non-Fungible Token*, come abbiamo osservato, hanno la capacità di creare rarità (nel senso di non fungibilità) ad un qualsiasi oggetto fisico o virtuale attraverso certificati di proprietà garantiti tramite *smart contract*. Da un punto di vista più strettamente giuridico possiamo affermare che il valore dell'*NFT* è dato dalla sua irripetibilità e dalla fiducia che intercorre tra le parti (venditore e acquirente), fondata sul fatto che quell'opera associata all'*NFT* non ha copie simili ed è unica. I settori coinvolti sono i più svariati: dall'arte al *gaming*, dalla musica alla moda e al mercato del lusso.

Coloro che desiderano acquistare un'opera di arte digitale possono seguire diverse strade, in quanto molti operatori del settore hanno iniziato a guardare con interesse a tale segmento del mercato potendosi peraltro rivolgere a piattaforme che ne agevolano la creazione, la collocazione sul mercato e la vendita al pubblico anche attraverso aste tradizionali. Tuttavia, bisogna considerare che rispetto ai *crypto-asset* come il *bitcoin*, gli *NFT* non risentono dell'oscillazione del mercato, in quanto sono appunto considerati risorse digitali uniche, non fungibili appunto, per cui il loro valore è puramente soggettivo e dipende da un singolo scambio tra un cedente e un cessionario. Le vendite di pezzi di arte digitale associati a *NFT* hanno oramai raggiunto valutazioni simili a quelle di opere artistiche tradizionali.

Secondo un recente *report* del Dipartimento del Tesoro statunitense³²³, nei primi tre mesi del 2021, gli scambi di *NFT* ha generato la cifra di \$1,5 miliardi, ammontare che è cresciuto del 2,6% rispetto al trimestre precedente. Il *report* sottolinea come la popolarità degli *NFT* stia crescendo rapidamente tra gli operatori del mercato dell'arte tradizionale ed in particolare tra le case d'asta, che hanno incontrato l'interesse di moltissimi utenti, tra i quali si potrebbero celare organizzazioni criminali interessate a riciclare proventi di natura illecita (rappresentati sia da *crypto-asset* che da valuta tradizionale) prendendo parte alla negoziazione degli *NFT*. Peraltro, il procedimento seguito dai riciclatori potrebbe coinvolgere operazioni di *wash*

³²³ Cfr. [Department of The Treasury, Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art, 2022.](#)

trading, che riguarda transazioni in cui in cui il venditore agisce anche come compratore, con l'intento di eseguire ripetuti scambi tra *wallet* nella disponibilità di una stessa organizzazione criminale. L'effetto è quello di compiere un vero e proprio arbitraggio di natura finanziaria, ossia una speculazione tesa a incrementare i volumi di vendita di un determinato bene e, di conseguenza, il relativo prezzo. Una volta ceduto, a prezzi gonfiati, ad operatori terzi (convinti dal volume degli scambi precedenti che quel bene sia particolarmente prezioso), gli *NFT* determinano plusvalenze del tutto lecite che possono a questo punto essere convertite in denaro.

In merito, il *report* del Tesoro statunitense evidenzia come «*questi tipi di contratti [ndr. Smart contract] possono costituire un incentivo a manipolare il mercato in cui l'opera d'arte è scambiata ripetutamente in un breve periodo. Sebbene ciò garantisca che gli artisti vengono compensati per la loro opera dopo la prima vendita, l'attività di scambio può favorire il riciclaggio di denaro, poiché l'incentivo a negoziare può essere potenzialmente superiore all'incentivo a verificare l'identità dell'acquirente dell'opera*». Il *report* qualifica le operazioni di *wash trading*, come attività di auto-riciclaggio, attraverso cui i criminali possono acquistare un *NFT* con fondi illeciti e procedere ad effettuare transazioni con sé stessi per creare *record* di vendite sulla *blockchain*. Gli *NFT* finirebbero per essere venduti, in ultima istanza, ad un individuo inconsapevole che ricompenserebbe il criminale con fondi puliti. Peraltro, evidenzia sempre il *report*, si deve considerare che è anche possibile procedere a transazioni dirette *peer-to-peer* di un'opera digitale protetta da *NFT* senza il coinvolgimento di un intermediario e senza la necessità che le stesse siano registrate o meno su un registro pubblico. Parliamo di opere digitali intrinsecamente più facili da trasferire tra le parti interessate, che non hanno bisogno di spostarsi fisicamente da un luogo ad un altro, né di trasportare il bene, che per sua natura è immateriale, né di avvalersi di servizi di spedizione, assicurazione, di dogana, ecc. La possibilità di trasferire gli *NFT* sul *web*, senza la preoccupazione delle distanze geografiche che richiederebbero l'attraversamento dei confini reali di uno Stato, rende tali strumenti particolarmente appetibili per coloro che cercano di ripulire proventi di origine illecita, in quanto il costo del riciclaggio risulta quasi azzerato (se si escludono gli oneri relativi alle commissioni) dal momento che il movimento

di valore si realizza senza incorrere in potenziali costi finanziari, normativi o investigativi, tipici dei traffici commerciali tradizionali.

In tale contesto, il GAFI, che ha continuato a svolgere analisi sui rischi di riciclaggio connessi ai *virtual asset*, nel 2022 ha pubblicato un resoconto in cui vengono evidenziate le criticità legate agli strumenti di *DeFi* e ai *token* non fungibili. Rischi che vengono denunciati da più parti e che sono legati alle evidenze circa l'incremento dell'utilizzo degli *NFT* proprio per finalità di riciclaggio. In particolare, le indagini e gli studi più recenti mostrano chiaramente come il controvalore delle cripto-attività trasmesse da indirizzi, coinvolti in attività criminose, in direzione dei mercati degli *NFT*, è aumentato in modo significativo nell'ultimo periodo.

Analogamente, sul versante della lotta contro il finanziamento al terrorismo (*CFT*), si è osservato come l'estrema fluidità e l'intrinseca sicurezza di tali strumenti abbia spinto diverse organizzazioni di matrice terroristica ad avvalersene, sia come fonte e/o canale di ossigenazione finanziaria sia come metodo innovativo per attività di proselitismo.

In tale contesto, come riportato in un recente rapporto della *Elliptic*³²⁴, sebbene movimenti come *al-Qaeda*, *ISIS* e *Hamas* si siano avvalsi in diverse occasioni di finanziamenti basati su *crypto-asset*, queste organizzazioni operano soprattutto con strumenti di tipo tradizionali poiché sono localizzate in aree in cui l'accesso a *Internet* e ai servizi finanziari e interbancari è particolarmente limitato. Il rischio che il finanziamento terroristico basato su *crypto-asset* possa estendersi anche agli *NFT* permane quindi relativamente basso. Eppure, in questa sede appare opportuno evidenziare che le transazioni di *token* non fungibili di alto valore possano garantire un facile mezzo per aggirare i fragili presidi normativi, non solo in materia di antiriciclaggio (*AML*), ma anche in tema di contrasto al finanziamento al terrorismo (*CFT*). Ciò è ancor più vero vista la presenza di iniziative speculative condotte in modo opaco che investono i mercati degli *NFT* sia le diffuse lacune normative esistenti a livello tanto europeo che internazionale. D'altronde, l'utilizzo degli *NFT* si presta per sua natura alla raccolta di fondi anche per finalità militari, a prescindere dalla bontà delle iniziative che possono avere connotazioni aggressive (in conflitti armati) e finanche terroristiche (in attacchi eversivi mirati), ma anche difensive e, più in generale, benefiche. Ad esempio, sono stati documentati

³²⁴ Cfr. [Elliptic, *NFTs and Financial Crime*, 2022](#).

casi in cui le forze separatiste filorusse nell'Ucraina orientale, abbiano fatto ricorso alla raccolta di fondi anche attraverso tali strumenti, con la finalità appunto di agevolare l'invasione russa nel *Donbass*³²⁵. Nello stesso tempo, ampio risalto è stato dato alla raccolta fondi operata dal governo e dall'esercito ucraino in *crypto-asset*, *NFT* e *stablecoin*. Le donazioni includono anche un'unica transazione di \$1,86 milioni, che proviene da ricavi generati dalla vendita di *NFT*, creati da Julian Assange e dall'artista Pak ed associati all'immagine della bandiera ucraina³²⁶. Questa stessa doppia valenza, sempre a titolo esemplificativo, è stato possibile riscontrarla anche in altre aree di crisi come l'Afghanistan. Più in particolare, recentemente, è stato rilevato un *NFT* creato con funzioni contro-narrative e di propaganda da parte di organizzazioni terroristiche. Diffuso da un simpatizzante pro-*ISIS* per esaltare un recente attacco condotto da militanti islamici ai danni di una postazione talebana in Afghanistan³²⁷, il *token* digitale era associato all'emblema dello Stato Islamico. Nello stesso periodo veniva reso noto che l'*UNHCR* (Agenzia delle Nazioni Unite per i Rifugiati), per celebrare il suo 70° anniversario ha lanciato la prima collezione di *NFT* di beneficenza per raccogliere fondi per l'Afghanistan, grazie all'opera di un noto fumettista siro-palestinese³²⁸. Si potrebbero operare moltissimi altri esempi di come organizzazioni terroristiche abbiano fatto ricorso al mercato degli *NFT* per finalità ostili (*Hamas* in Israele, e più in particolare le Brigate *al-Qassam*, l'organizzazione terroristica *al-Ikhwa* in Siria e così via), ma altrettanto potremmo fare pensando alle numerose iniziative di raccolte fondi attraverso il lancio di opere associate a *NFT* per finalità sociali e filantropiche, per scopi di pace o per sostenere iniziative di cooperazione internazionale allo sviluppo.

8. Il quadro giuridico di contrasto al riciclaggio (*AML*) e al finanziamento del terrorismo (*CFT*)

8.1. Le avvertenze del Gruppo d'Azione Finanziaria Internazionale (GAFI)

Come sopra evidenziato, l'opera regolatoria ha perseguito dapprima finalità di natura pubblicistica e di deterrenza legate principalmente al contrasto del riciclaggio di denaro

³²⁵ Vds. [Ruocco T., *NFT, così il terrorismo li usa per finanziarsi*, 2022.](#)

³²⁶ Vds. [Paliotta A. P., *Guerra in Ucraina: ecco come criptovalute, NFT e crowdfunding finanziano la resistenza*, 2022.](#)

³²⁷ [Talley L., *Islamic State Turns to NFTs to Spread Terror Message*, Wall Street Journal, 2022.](#)

³²⁸ Cfr. [UNHCR, *Meet the Syrian cartoonist behind UNHCR's first-ever NFT fundraiser*, 2021.](#)

illecito e del finanziamento del terrorismo, muovendo da una serie di dati empirici da cui andava via via emergendo come il mondo dei *crypto-asset* avesse in effetti consentito di integrare nuove forme di illecito, grazie alla scarsa tracciabilità delle transazioni da parte degli organismi deputati al controllo³²⁹.

Sulla base di simili premesse, si è innestata l'opera del Legislatore sia italiano che internazionale di cui appare utile ripercorrere le principali tappe, con il fine precipuo di comprendere la natura più profonda delle dinamiche del fenomeno e come lo stesso sia stato disciplinato da parte dei regolatori domestici ed internazionali.

In tale contesto va precisato che, sia in ambito G20 che in sede europea, i regolatori si avvalgono dell'opera del Gruppo d'Azione Finanziaria Internazionale (GAFI)³³⁰, organismo deputato al contrasto del riciclaggio e del finanziamento al terrorismo che, con i suoi 39 membri, tra cui la Commissione Europea, si occupa di monitorare il livello di armonizzazione agli standard globali dei vari Paesi, collaborando, tra gli altri, con la Banca Mondiale, il Fondo Monetario Internazionale (FMI), la Banca Centrale Europea (BCE), l'Organizzazione

³²⁹ Cfr. [Sturzo L., Bitcoin e riciclaggio 2.0, Diritto Penale Contemporaneo, 2018](#), p. 20. Su simili posizioni vds. ACCINNI G. P., *Profili di rilevanza penale delle criptovalute (nella riforma della disciplina antiriciclaggio)*, Archivio Penale, 2018, n. 1, p. 13, che ha inquadrato il fenomeno nei termini che seguono: «le *crypto-currencies* garantiscono un livello di anonimato assai maggiore rispetto alle ordinarie transazioni bancarie, non solo poiché il loro protocollo di funzionamento non richiede l'identificazione o la verifica della reale identità dei detentori dei portafogli elettronici, ma perché (...) esistono numerosi tools che consentono di massimizzare la privacy degli utenti (ad es. i servizi di mixing) e delle valute virtuali (ad es. Monero o ZCash) che sono completamente anonime». L'autore cita il noto caso di riciclaggio Liberty Reserve, «ancora oggi il maggior caso di riciclaggio online mai verificatosi. Nel corso del maggio 2013 il Dipartimento di Giustizia degli Stati Uniti d'America ha accusato la Società Liberty Reserve, ente di intermediazione mobiliare con sede in Costa Rica, di aver concorso nel riciclaggio di 6 miliardi di dollari di profitti illeciti. In particolare, le indagini avevano fatto emergere come siffatta società fosse stata costituita al solo fine di fornire supporto ad associazioni criminali interessate a riciclare i proventi rinvenienti dalla clonazione di carte di credito, furti di identità, reati informatici, narcotraffico e pornografia minorile, consentendogli di porre in essere transazioni anonime e non rintracciabili. (...) Più in dettaglio, per conseguire il proprio "oggetto sociale" la società usava emettere una propria moneta virtuale, il Liberty Dollar, che periodicamente veniva quotato in dollari statunitensi. (...) All'atto dell'inchiesta Liberty Reserve risultava perciò pienamente operativa in paesi quali l'Australia, Cipro, la Cina, Hong Kong, il Marocco, la Russia e la Spagna, tanto che le indagini che hanno condotto infine allo shut down del sistema hanno richiesto la collaborazione di ben 18 giurisdizioni sparse in tutto il mondo». Ancora: «un altro esempio (...) è poi rappresentato dal noto caso Silk Road (...) che operava nel dark web e consentiva ai propri utenti di acquistare e vendere droga, armi, dati personali trafugati e altre merci di carattere illecito in concorso con organizzazioni di narcotrafficianti, di hackers e di altri soggetti dediti al riciclaggio. (...) il sito perseguiva l'anonimato dei propri clienti operando nel dark web ed accettando in pagamento solo Bitcoin».

³³⁰ Il Gruppo d'Azione Finanziaria Internazionale (GAFI) o Financial Action Task Force (FATF), è un organismo intergovernativo, istituito dal G7 nel luglio 1989 allo scopo di promuovere strategie volte al contrasto del riciclaggio di capitali a livello nazionale e internazionale mediante l'adozione di appropriate misure da parte di tutti i Paesi che ne sono membri. Competenze successivamente estese anche alle tematiche del finanziamento del terrorismo e della proliferazione di armi di distruzione di massa.

delle Nazioni Unite (ONU), il Comitato di Basilea per la vigilanza bancaria e il Gruppo Egmont.

Le stesse Direttive europee in materia di antiriciclaggio, come vedremo a breve, hanno recepito le raccomandazioni del GAFI. Si tratta in particolare, delle quaranta raccomandazioni originariamente formulate nel 1990 al fine di contrastare l'uso improprio dei sistemi finanziari per riciclare i proventi del narcotraffico. Sono state, poi, revisionate per la prima volta nel 1996, al fine di riflettere l'evoluzione delle tendenze e delle tecniche del riciclaggio ed estendere il proprio raggio d'azione al di là del contrasto del riciclaggio dei proventi del narcotraffico. Nel corso di una riunione plenaria tenutasi a pochi giorni di distanza dagli attentati dell'11 settembre 2001, il GAFI ha ampliato il proprio mandato al contrasto del finanziamento del terrorismo, elaborando gli indirizzi normativi e i principi guida per dare concreta attuazione alle Risoluzioni dell'ONU. Nell'occasione, ha emanato 8 Raccomandazioni Speciali (introducendo la nona dal 2004) dedicate specificamente al finanziamento del terrorismo. Il GAFI ha successivamente, e a più riprese, revisionato le proprie raccomandazioni³³¹. In materia di *crypto-asset*, il GAFI è stato tra i primi organismi internazionali ad intervenire. Nel 2014, in particolare, ha pubblicato un documento dal titolo: “*Virtual currencies: key definitions and potential AML/CFT risks*”³³². Tuttavia, il *report* non reca una compiuta disciplina, ma propone un primo *conceptual framework for understanding and addressing the anti-money laundering/countering the financing of terrorism*, associato ai sistemi di pagamento basati su cripto-attività (all'epoca qualificate come criptovalute) che vengono definite come «una rappresentazione digitale di valore che può essere scambiata digitalmente e funziona come (1) mezzo di scambio; e/o (2) unità di conto; e/o (3) riserva di valore, ma non ha corso legale (cioè, se offerta a un creditore, è un'offerta di pagamento

³³¹ L'ultimo *updated* è del febbraio 2023, [Gruppo d'Azione Finanziaria Internazionale, International standards on combating money laundering and the financing of terrorism & proliferation – FATF Recommendations, 2023](#).

³³² Vds. [Gruppo d'Azione Finanziaria Internazionale, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 2014](#). Il documento espone le prime preoccupazioni sul fenomeno affermando che «le valute virtuali convertibili che possono essere scambiate con denaro reale o con altre valute virtuali sono potenzialmente vulnerabili al riciclaggio di denaro e all'abuso di finanziamento del terrorismo per molte delle ragioni identificate nella guida NPPS del 2013. In primo luogo, possono consentire un maggiore anonimato rispetto ai tradizionali metodi di pagamento non in contanti. I sistemi di valute virtuali possono essere scambiati su Internet, sono generalmente caratterizzati da rapporti con i clienti non faccia a faccia e possono consentire finanziamenti anonimi (...). Possono anche consentire trasferimenti anonimi, se il mittente e il destinatario non sono adeguatamente identificati.», *ivi*, pag. 11.

valida e legale) in nessuna giurisdizione. Non è emessa né garantita da alcuna giurisdizione e svolge le funzioni di cui sopra solo in base a un accordo all'interno della comunità degli utenti della valuta virtuale. La valuta virtuale si distingue dalla valuta fiat (anche detta "valuta reale", "denaro reale" o "valuta nazionale"), che è la moneta e la carta-moneta di un Paese che ha corso legale, circola ed è abitualmente utilizzata e accettata come mezzo di scambio nel Paese di emissione»³³³.

Il GAFI ha poi ulteriormente sviluppato la propria posizione con le raccomandazioni contenute nel *report* del giugno del 2015, dal titolo “*Guidance for a risk-based approach virtual currencies*”³³⁴, il cui *focus* è incentrato sugli *exchanger points of intersection* con il sistema finanziario regolamentato, fornendo delle linee di condotta in merito all’identificazione e alla mitigazione dei rischi associati ai *crypto-asset*, all’applicazione dei requisiti di licenza/registrazione, nonché all’attuazione di una supervisione efficace, che adotti anche sanzioni dissuasive e strumenti di controllo che abbiano accesso alla cooperazione internazionale. Nelle proprie raccomandazioni, il GAFI ha anche evidenziato come sia i governi che il settore privato abbiano chiesto maggiore chiarezza in ordine agli *standard AML* (*anti-money laundering*) e *CFT* (*countering the financing of terrorism*). Ha infatti rilevato come i *crypto-asset* (la locuzione utilizzata è *virtual-asset*³³⁵) possano essere impiegati per gli scambi e per finalità di investimento, così individuando le attività meritevoli di attenzione per la prevenzione dei rischi di riciclaggio e di finanziamento del terrorismo. Per la gestione e la mitigazione dei rischi è opportuno che i prestatori di servizi relativi all’utilizzo di *asset* virtuali siano sottoposti alle normative nazionali di prevenzione, a regimi di licenza o registrazione e a controlli di *compliance*.

Nella plenaria di ottobre 2018, il GAFI ha introdotto *standard* internazionali in materia di *crypto-asset*, apportando modifiche al “Glossario” e alla Raccomandazione n. 15. In

³³³ Il GAFI ha svolto un ruolo pionieristico nel cercare di definire gli aspetti connessi agli adempimenti antiriciclaggio in relazione alle transazioni con *asset* virtuali, muovendo da un assunto, secondo il quale, nonostante l’iniziale utilizzo equivoco dei termini “criptovaluta” o “criptomoneta”, ci troviamo di fronte ad una “non moneta”, ossia all’espressione digitale di un valore suscettibile di una valutazione economica da parte di coloro che ne accettano la negoziazione che in quanto tale non può essere esclusa dal complesso regolamentare in materia *AML* e *CFT*.

³³⁴ [Gruppo d’Azione Finanziaria Internazionale, *Guidance for a risk-based approach virtual currencies*, 2015.](#)

³³⁵ Si veda il nuovo testo della Raccomandazione n. 15 e il Glossario allegato alle Raccomandazioni del GAFI per le definizioni di *virtual asset* e *virtual asset service provider* (illustrato *infra*).

particolare, le revisioni sono state elaborate, anche su impulso del G20, proprio per promuovere l'attuazione di presidi idonei a contenere i rischi di riciclaggio e di finanziamento del terrorismo connessi all'uso di *virtual/crypto-asset*.

L'Organizzazione ha poi revisionato la Raccomandazione n. 15, inerente ai rischi di riciclaggio connessi con le cd. nuove tecnologie. L'intervento ha riguardato gli obblighi gravanti sui prestatori di servizi connessi con il settore delle valute virtuali (*virtual asset services provider – VASP*), quali possibili presidi per il monitoraggio dei flussi finanziari sospetti e, in quanto tali, sottoponibili agli obblighi di licenza e registrazione presso un albo speciale nazionale, con il duplice fine di consentire il monitoraggio e contenere il fenomeno dell'anonimato delle transazioni effettuate attraverso essi. Il criterio prescelto al fine di individuare il perimetro dei soggetti rilevanti a fini antiriciclaggio ha riguardo alla tipologia di attività svolta. Nell'ambito dei *VASP* sono inclusi i soggetti, non altrimenti disciplinati dalle Raccomandazioni, che svolgono professionalmente una delle attività seguenti: conversione tra *virtual asset* e valute legali; conversione tra *virtual asset*; trasferimento di *virtual asset*; custodia e/o amministrazione di *virtual asset* o di strumenti che ne consentono il controllo; partecipazione e fornitura di servizi finanziari relativi all'offerta e/o alla vendita di *virtual asset* (il riferimento è alle *Initial Coin Offerings – ICOs*).

Gli obblighi di registrazione dovrebbero essere adempiuti avendo riguardo alla giurisdizione del Paese nel quale gli stessi *VASP* sono stati istituiti o, nel caso in cui il *provider* sia una persona fisica, nel luogo dove viene condotta l'attività prevalente di erogazione del servizio (*place of business*). Non è, invece, richiesta la registrazione qualora i *VASP* siano già classificati - nel Paese di insediamento - come istituzioni finanziarie e, in quanto tali, già sottoposti a specifici obblighi nazionali. Il GAFI si è raccomandato, inoltre, di adottare pertinenti misure legali e regolamentari al fine di evitare che criminali o loro associati possano detenere o essere i beneficiari effettivi di un interesse significativo o di una partecipazione rilevante, oltre che svolgere una funzione di gestione in un *VASP*.

Al fine di monitorare il rispetto delle regole e il livello di *compliance* nei settori *AML* e *CFT*, poi, i *VASP* dovrebbero essere sottoposti alla vigilanza di un'Autorità nazionale competente diversa da un organismo di autoregolamentazione (*Self-Regulatory Body*), dotata di adeguati poteri di supervisione, monitoraggio ed ispezione, nonché di richiesta di informazioni

sull'attività esercitata ed in grado di irrogare sanzioni di natura civile, amministrativa e penale, incluso il ritiro della licenza di esercizio dell'attività.

In merito alle misure preventive, infine, dovranno trovare applicazione le speciali misure previste dai *FATF Standard n. 10-21*, concernenti, tra l'altro, l'adeguata verifica della clientela e la raccolta di informazioni sul beneficiario effettivo della transazione³³⁶.

L'Italia si è allineata a tali raccomandazioni, adeguando la propria disciplina antiriciclaggio al fenomeno delle cripto-attività per mezzo del D. Lgs. n. 90/2017, con cui sono state adottate modifiche al D. Lgs. n. 231/2007 attraverso l'introduzione di previsioni che hanno sostanzialmente anticipato l'intervento dell'Unione Europea, che ha affrontato il tema in argomento solo nel 2018, con l'emanazione della V Direttiva antiriciclaggio (Direttiva UE 843/2018 del 30 maggio 2018). Il quadro di recepimento italiano è stato, dunque, completato con il D. Lgs. n.125/2019. Successivamente, nel giugno 2019, il GAFI ha emanato una nota interpretativa alla Raccomandazione n. 15 per chiarire ulteriormente come applicare i requisiti GAFI in relazione ai *virtual asset* e ai *VASP*³³⁷, in particolare per quanto riguarda:

- l'applicazione dell'approccio basato sul rischio in relazione alle attività o ad operazioni svolte con *virtual asset* da parte dei *VASP*;
- la supervisione o monitoraggio dei *VASP* per scopi *AML/CFT*;
- aspetti connessi con licenze e/o registrazioni;
- misure preventive, come gli obblighi di *due diligence* da parte della clientela, la tenuta dei registri e la segnalazione di operazioni sospette, ecc.;
- sanzioni e altre *enforcement measures*;
- la cooperazione internazionale.

Ancora, nel giugno 2019, sulla scorta di tali indicazioni, il GAFI ha aggiornato le proprie linee guida del 2015 attraverso il documento "*Virtual assets and virtual asset service*

³³⁶ In tale ottica, qualora le transazioni effettuate dai *VASP* superino la soglia dei 15.000 euro/dollari, occorrerà procedere agli obblighi di adeguata verifica della clientela (*customer due diligence*). I *VASP* che hanno generato le transazioni devono conseguentemente rilevare e conservare le informazioni su chi ha ordinato l'operazione e sui beneficiari della stessa, esibendole a richiesta delle autorità competenti, anche se non strettamente connesse alla specifica transazione monitorata.

³³⁷ Un'ulteriore revisione della Raccomandazione n. 15 è intervenuta nel giugno 2021.

providers - Guidance for a risk-based approach”³³⁸, nel quale si evidenzia l’esigenza che gli Stati, i *VASP* e le altre entità coinvolte nelle attività su *virtual asset* comprendano i rischi *AML/CFT* associati alle loro attività e intervengano con appropriate misure di attenuazione. In particolare, la Guida illustra esempi di indicatori di rischio che dovrebbero essere considerati avuto riguardo a quei fattori che potrebbero offuscare ulteriormente le transazioni o impedire la capacità dei *VASP* di identificare i clienti. In tale contesto, particolarmente interessanti appaiono le indicazioni fornite proprio in favore dei *VASP*: è raccomandata l’adozione di una visione olistica delle informazioni (*holistic view of the information*) ottenute nel contesto dell’applicazione delle misure *CDD* (“*Customer Due Diligence*”), che potrebbero includere sia informazioni tradizionali sia informazioni non convenzionali. In tal senso, i *VASP* e le altre entità obbligate dovrebbero predisporre un appropriato profilo di rischio del cliente, così da poter adattare il livello e il tipo di monitoraggio potenzialmente necessario, che consenta ai *VASP* di poter decidere se stabilire, continuare o interrompere la relazione con il cliente. I profili di rischio possono focalizzarsi a livello del cliente (ad esempio, natura e volume dell’attività di *trading*, origine dei fondi virtuali depositati, ecc.) o a livello di *cluster* di clienti aventi caratteristiche omogenee. Se un *VASP* avesse contezza che alcuni *virtual asset* presentano rischi *AML/CFT*, dovrebbe procedere a stilare la propria “*blacklist wallet addresses*”.

8.2. *Crypto-asset e normativa antiriciclaggio: dalla IV Direttiva AMLD alle successive V e VI e al loro recepimento.*

In materia di antiriciclaggio è utile premettere come l’Unione Europea sia intervenuta a partire dalla prima Direttiva 91/308/CE del Consiglio (recepita in Italia con la legge n. 197 del 1991), che definiva il riciclaggio dei proventi di attività illecite soprattutto in relazione ai reati connessi con il traffico di stupefacenti ed imponeva obblighi soltanto verso il settore finanziario³³⁹. Con la seconda Direttiva 2001/97/CE del Parlamento Europeo e del Consiglio

³³⁸ Vds. [Gruppo d’Azione Finanziaria Internazionale, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, 2019.](#)

³³⁹ La Direttiva, in particolare, riprendeva la definizione di riciclaggio introdotta nella Convenzione delle Nazioni Unite del 1998 contro il traffico illecito di stupefacenti, elencando fra le azioni tipiche del riciclatore:

- la conversione e il trasferimento di beni di provenienza criminosa, allo scopo di occultarne l’origine illecita o di aiutare chiunque sia coinvolto in tale attività delittuose;

(recepita in Italia con la legge n. 56 del 2004) è stato ampliato l'ambito di applicazione della precedente, per quanto concerne la tipologia di reati (così da introdurre una definizione più estesa del riciclaggio, fondata su una gamma più vasta di reati "base" o "presupposto"), le professioni e le attività coinvolte³⁴⁰. Le prime due direttive antiriciclaggio, così come le successive, hanno recepito in ambito europeo le raccomandazioni del GAFI, come nel tempo emendate ed integrate. Il Parlamento Europeo e il Consiglio, proprio al fine di allineare la normativa *AML* alle raccomandazioni del GAFI, così come riviste ed ampliate nel 2003, ha adottato la terza Direttiva antiriciclaggio 2005/60/CE, unitamente alla Direttiva 2006/70/CE che ne reca le misure di esecuzione (entrambe recepite in Italia con il D. Lgs. n. 231/2007)³⁴¹. Queste ultime sono state poi abrogate a mezzo della quarta Direttiva antiriciclaggio, n. 2015/849/UE (recepita in Italia con il D. Lgs. 90/2017), che si è allineata agli *standard* internazionali rimodulati dal GAFI nel febbraio 2012³⁴².

-
- la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, titolarità dei beni o diritti sugli stessi, effettuata nella consapevolezza che detti beni provengono da attività criminose;
 - l'acquisto, la detenzione o l'utilizzo di beni di cui è nota, al momento della loro ricezione, la provenienza illecita;
 - la partecipazione ad uno degli atti di cui ai punti precedenti, l'associazione per commettere tali atti, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolarne l'esecuzione.

In Dottrina vds. Quattrocioni B., *Norme, regole e prassi nell'economia dell'antiriciclaggio internazionale*, Torino, 2017; Cenci P., *La nuova normativa antiriciclaggio - Direttive comunitarie e normativa nazionale*, Cedam, 2010, p. 9; Monteverde S., *Attuazione della direttiva CEE in materia di riciclaggio, Diritto Penale e Processo*, 1997, n. 8, p. 925.

³⁴⁰ Cfr. Cassese E. e Costanzo P., *Il recepimento della seconda direttiva comunitaria "antiriciclaggio"*, *Giornale di Diritto Amministrativo*, 2004, n. 5, p. 495; Carano A. e Salerno S., *D. Lgs 20 febbraio 2004, n. 56: l'attuazione della seconda Direttiva europea nella strategia antiriciclaggio e le novità procedurali e sanzionatorie*, *Il Fisco*, 2004, n. 42, p. 7146.

³⁴¹ Cfr. [Starola L., Il riciclaggio nel d.lgs. 231/2007. Nozione, ambito operativo e soggetti destinatari. Il nuovo diritto delle società, ODCEC, 2011](#), p. 27 e ss.; Cassese E. e Costanzo P., *La terza direttiva comunitaria in materia di antiriciclaggio e antiterrorismo*, *Giornale di Diritto Amministrativo* n.1, 2006, p. 5; Querqui M. e Verrocchi G., *La delega legislativa per il recepimento della direttiva n. 60/2005/CE in materia di contrasto al riciclaggio ed al finanziamento del terrorismo internazionale*, *Il Fisco*, 2006, n. 9, p. 1324; Fisicaro E., *Antiriciclaggio e terza direttiva UE. Obblighi a carico dei professionisti intermediari finanziari e operatori non finanziari alla luce del D.lgs. 231/2007*, Giuffrè, 2008.

³⁴² Cfr. [Bizioli G. e Salvatore P., Il titolare effettivo dei trust esteri dopo il recepimento della IV direttiva antiriciclaggio, Boll. Trib. d'Inf., 2020](#), p. 655 e ss.; Capolupo S., *Modifiche alla normativa antiriciclaggio e lotta ai paradisi fiscali*, *Il Fisco*, 2016, p. 4455; [Giacometti T. e Formenti O., La nuova disciplina in materia di prevenzione del riciclaggio e di finanziamento del terrorismo \(d.lgs. 25 maggio 2017, n. 90\), Dir. Pen. Cont., 2017](#), n. 7-8, p. 195; Krogh M., *Gli obblighi e le nuove sanzioni antiriciclaggio nel D.lgs. 25 maggio 2017, n.90*, *Il Notariato*, 2017, p. 523; Tramontano G. et al., *La IV direttiva antiriciclaggio e antiterrorismo. I nuovi obblighi per gli intermediari finanziari e i professionisti*, Aracne, 2016.

In questo stesso periodo molte entità istituzionali avevano iniziato a mettere in guardia dai pericoli insiti ai *crypto-asset*. Nel mese di giugno del 2014, ad esempio, il GAFI aveva assunto una dura presa di posizione, nel report “*Virtual Currencies - Key Definitions and Potential AML/CFT Risks*”, su cui ci siamo già soffermati. Nonostante ciò, la IV Direttiva non affrontava ancora il tema dei *crypto-asset*, questione sulla quale andavano comunque consolidandosi le prime prese di posizione da parte degli Organismi di vigilanza europei che, nel giugno 2016, portarono alla presentazione, da parte della Commissione Europea, di una proposta emendativa. La maggiore preoccupazione era legata al fatto che, per il tramite di piattaforme *on line*, gruppi terroristici o riciclatori di organizzazioni criminali potessero essere in grado di trasferire denaro verso il sistema finanziario dell’Unione o all’interno delle reti degli *asset* virtuali dissimulando i trasferimenti digitali o beneficiando di un certo livello di anonimato. Di qui la «fondamentale importanza di ampliare l’ambito di applicazione della direttiva (UE) 2015/849 in modo da includere i prestatori di servizi (...) e i prestatori di servizi di portafoglio digitale», nonché l’esigenza che le autorità competenti siano in grado «di monitorare, attraverso i soggetti obbligati, l’uso delle valute virtuali». Monitoraggio che «consentirebbe un approccio equilibrato e proporzionale, salvaguardando i progressi tecnici e l’elevato livello di trasparenza raggiunto in materia di finanziamenti alternativi e imprenditorialità sociale»³⁴³. In tale quadro, è stata adottata la quinta Direttiva antiriciclaggio (Direttiva 2018/843/UE), che ha modificato ed integrato significativamente il testo della Direttiva 849/2015/UE. A distanza di pochi mesi è stata adottata la sesta Direttiva antiriciclaggio, Direttiva 2018/1673/UE, che si pone l’obiettivo di contrastare il riciclaggio mediante il diritto penale, consentendo una cooperazione transfrontaliera fra le Autorità competenti più efficiente e più rapida³⁴⁴.

³⁴³ Così il *Considerando* n. 8 della Direttiva UE 2018/843/UE, relativa alla prevenzione dell’uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo che modifica le direttive 2009/138/CE e 2013/36/UE. Vds. anche il *Considerando* n. (9): «per contrastare i rischi legati all’anonimato, le unità nazionali di informazione finanziaria (FIU) dovrebbero poter ottenere informazioni che consentano loro di associare gli indirizzi della valuta virtuale all’identità del proprietario di tale valuta».

³⁴⁴ L’art. 3 della VI Direttiva, in particolare, si occupa di definire le condotte ascrivibili al riciclaggio, nei termini che seguono:

a) la conversione o il trasferimento di beni, effettuati essendo nella consapevolezza che i beni provengono da un’attività criminosa, allo scopo di occultare o dissimulare l’origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche della propria condotta;

Ulteriore questione da riportare sul piano sovranazionale è l'approvazione del nuovo Regolamento sui dati informativi che accompagnano, con finalità antiriciclaggio, i trasferimenti di fondi e determinate crypto-attività. In poche parole, *«scopo del regolamento è garantire la piena tracciabilità dei crypto patrimoni³⁴⁵ al pari di qualsiasi altra operazione finanziaria. Il documento, approvato a larga maggioranza in sede plenaria, rappresenta un importante strumento di contrasto ai fenomeni di riciclaggio e di finanziamento al terrorismo perché estende alle operazioni in crypto-attività la cd. travel rule³⁴⁶, già presente nella finanza tradizionale, che prevede che le informazioni sull'origine e sul beneficiario finale dei crypto-asset “viaggino” con la transazione e siano conservate da entrambi i partecipanti al trasferimento³⁴⁷»*.

Venendo all'esame della normativa domestica per come derivata dalla regolamentazione europea, occorre premettere che uno dei problemi principali con i quali il Legislatore nazionale si è trovato a misurarsi è stato di tipo prettamente definitorio ed ha riguardato proprio l'inquadramento del concetto di *crypto-asset* (successivamente, qualificati dalla normativa antiriciclaggio europea come “*virtual currencies*”)³⁴⁸. In un simile scenario, a

b) l'occultamento o la dissimulazione della reale natura, della provenienza, dell'ubicazione, della disposizione, del movimento, della proprietà dei beni o dei diritti sugli stessi nella consapevolezza che i beni provengono da un'attività criminosa;

c) l'acquisto, la detenzione o l'utilizzazione di beni nella consapevolezza, al momento della loro ricezione, che i beni provengono da un'attività criminosa.

³⁴⁵ Nello specifico i trasferimenti di crypto-attività, come *bitcoin* e *token* di moneta elettronica.

³⁴⁶ «La Travel Rule del GAFI, nota anche come Raccomandazione GAFI n. 16, obbliga le imprese a registrare e divulgare le informazioni dei partecipanti (ordinanti e beneficiari) a una transazione. Questa regola, originariamente applicabile solo alle banche, è stata estesa nel 2019 per richiedere anche ai VASP di registrare e divulgare le informazioni relative alle transazioni di criptovalute. Di conseguenza, molti Paesi osservatori hanno iniziato a incorporare la Travel Rule nelle loro direttive locali in materia di antiriciclaggio. Parte della Travel Rule richiedeva ai Paesi di garantire che le istituzioni finanziarie monitorassero i trasferimenti allo scopo di individuare quelli privi delle informazioni richieste sull'ordinante e/o sul beneficiario. Purtroppo, le soluzioni tecnologiche per implementare la Travel Rule sono limitate e (...) manca ancora l'interoperabilità tra le soluzioni tecniche e le giurisdizioni. Queste tecniche di applicazione frammentate rappresenteranno una sfida per la supervisione e il monitoraggio dei crypto-asset rispetto alle normative nel breve termine e potrebbero richiedere molti anni per essere standardizzate. Questo processo lungo anni è preoccupante, data la crescita dinamica e i rapidi sviluppi tecnologici degli asset crittografici, anche se il settore sta attivamente sviluppando standard per affrontare questa lacuna. Anche se la vigilanza e il monitoraggio coerenti fossero possibili in alcune giurisdizioni, è improbabile che lo siano in tutte, il che potrebbe comportare ulteriori asimmetrie informative e di applicazione». [World Economic Forum, Pathways to the Regulation of Crypto-Assets: A Global Approach, White Paper, 2023.](#)

³⁴⁷ [Marvulli E., Ue, il Parlamento estende le travel rules alle crypto-attività, Fisco Oggi, 2023.](#)

³⁴⁸ Secondo la V Direttiva antiriciclaggio per *virtual currencies* deve intendersi «una rappresentazione di valore digitale che non è emessa o garantita da una Banca Centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da

mezzo della legge di delegazione europea del 12 agosto 2016, n. 170, all'articolo 15³⁴⁹, il Parlamento italiano ha conferito al Governo la delega legislativa all'attuazione nell'ordinamento italiano della predetta IV Direttiva, attesa anche la necessità di conformarlo a quanto previsto dal Regolamento 2015/847/UE del Parlamento Europeo e del Consiglio, datato 20 maggio 2015, riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il Regolamento 1781/2006/CE: *«l'obiettivo dichiarato era quello di puntare ad una gestione mirata ed efficace delle politiche di contrasto all'utilizzo del sistema economico finanziario per fini illegali»*³⁵⁰. In effetti, tra i principi e criteri direttivi che il Governo era tenuto a seguire nell'esercizio della delega, figurava la finalità di orientare e gestire efficacemente le politiche di contrasto dell'utilizzo del sistema economico e finanziario per fini illegali, oltre che di graduare i controlli e le procedure strumentali all'attuazione delle medesime politiche in funzione del rischio di riciclaggio dei proventi di

persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente». Si deve precisare come, all'epoca, il dibattito sulla qualificazione della natura delle cripto-attività fosse tutt'altro che sopito e verteva essenzialmente sulla di considerarle o meno come valute. Si notava, invero, come si avesse a che fare con uno strumento digitale utilizzabile nello spazio virtuale, dunque sicuramente altro rispetto a quello avente corso legale, non assimilabile né al concetto di moneta *fiat* né a quello di moneta elettronica. Per moneta elettronica, in effetti, secondo la definizione fornita dal Testo Unico Bancario, è ancora oggi da intendere il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso per effettuare operazioni di pagamento e che sia accettato da persone fisiche e giuridiche diverse dall'emittente. In tale contesto, vi è chi ritiene che *«la moneta virtuale si colloca, dunque, in uno spazio intermedio tra moneta fisica ed elettronica, nel tentativo di assumerne i rispettivi vantaggi»*. Così [Sturzo L., Bitcoin e riciclaggio 2.0, Diritto Penale Contemporaneo, 2018](#), p. 20; Amato M. e Fantacci L., *Per un pugno di Bitcoin. Rischi e opportunità delle valute virtuali*, Bocconi University Press, 2016. Vds. anche [Passarelli N., Bitcoin e antiriciclaggio, Sicurezza Nazionale, 2016](#), il quale evidenzia che se vero che la moneta corrente presenta il duplice vantaggio dell'accessibilità e dell'anonimato e se vero che la moneta elettronica ha il merito di essere di più agevole utilizzo, consentendo pagamenti anche a distanza, si può allora affermare che *«il sistema Bitcoin ambisce proprio ad inserirsi a cavallo fra queste due monete, traendone i rispettivi vantaggi e, per tale motivo, viene definito come contante digitale, in quanto consente sia di effettuare pagamenti a distanza sia di essere anonimo (o meglio... pseudonimo) e di non sopportare commissioni di intermediazione»*. Cfr. ancora Carbone M. et al., *Le nuove regole antiriciclaggio*, IPSOA, 2021, p. 683.

³⁴⁹ Delega al Governo per il recepimento della Direttiva 2015/849/UE del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o di finanziamento del terrorismo, che modifica il Regolamento 648/2012/UE del Parlamento Europeo e del Consiglio e che abroga la Direttiva 2006/60/CE del Parlamento Europeo e del Consiglio e la Direttiva 2006/70/CE della Commissione, e per l'attuazione del Regolamento 2015/847/UE del Parlamento Europeo e del Consiglio, del 20 maggio 2015, riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il Regolamento 1781/2006/CE.

³⁵⁰ In relazione ai contenuti della legge di delegazione, la dottrina ha avuto modo di osservare come *«tale modello, a differenza di quelli fin qui adottati dall'Unione europea, si caratterizza non tanto e non solo per la spiccata finalità preventiva, quanto piuttosto per il fatto di fare propria una diversa concezione del rischio riciclaggio basata su una sorta di differenziazione del rischio stesso»* (Vds. Carbone M. et al., *Le nuove regole antiriciclaggio*, IPSOA, 2021, pp. 727 ss.).

attività criminose e di finanziamento del terrorismo³⁵¹. L'intervento normativo è stato improntato ad un "*risk based approach*", teso alla valutazione ed identificazione del rischio insito nell'esercizio di attività economico finanziarie, anche per mezzo dell'attività di vigilanza degli Organismi deputati al controllo³⁵².

A mezzo del decreto legislativo n. 90 del 2017³⁵³ l'Italia ha così dato attuazione alla Direttiva europea con una certa lungimiranza, tanto da anticipare, proprio con riferimento al tema dei *crypto-asset*, quelli che sarebbero stati, più avanti, i contenuti della V Direttiva antiriciclaggio: «*con un'azione sorprendentemente avanguardista rispetto alla normazione europea, il legislatore, anticipando le previsioni dettate dalla Fourth Directive Anti Money Laundering, ha proceduto anzitutto a prevedere e definire la qualifica di cambia valute virtuali, ad imporre in capo a questi l'obbligo di iscrizione in apposita sezione del registro di cambia valute, ed infine ad inserirli tra i soggetti destinatari degli obblighi antiriciclaggio, in forza del d. lgs n. 231/2007*»³⁵⁴.

Vale la pena soffermarsi su tale intervento normativo giacché, nel contesto appena descritto, il Legislatore italiano ha modificato la normativa antiriciclaggio intervenendo anche sulla materia delle "*valute virtuali*" (o cripto-attività che dir si voglia), in un duplice senso: anzitutto, definendone il concetto³⁵⁵, ed in un secondo momento regolando l'attività dei

³⁵¹ Interessante notare sin da ora come la delega indicasse che tale adeguamento sarebbe dovuto avvenire nel rispetto dei principi e della normativa nazionale ed europea in materia di tutela della riservatezza e protezione dei dati personali. Di qui l'annosa questione della compatibilità della normativa con il nuovo sistema di protezione del dato delineato dal *GDPR*.

³⁵² Vds. Carbone M. *et al.*, *Le nuove regole antiriciclaggio*, IPSOA, 2021, p. 728' i quali osservano come l'emanazione del decreto legislativo "*denoti l'avvenuta presa di coscienza da parte del legislatore nazionale circa la pericolosità dell'anonimato delle transazioni finanziarie effettuate mediante criptovaluta, di cui Bitcoin risulta essere una, sebbene celeberrima, species*".

³⁵³ Recante l'attuazione della Direttiva 2015/849/UE relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante la modifica delle direttive 2005/60/CE e 2006/70/CE e l'attuazione del Regolamento 2015/847/UE riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il Regolamento 1781/2006/CE. Il decreto rimodula il D. Lgs. n. 231/2007, introducendo diverse innovazioni che principalmente riguardano i soggetti destinatari degli obblighi, l'attività di registrazione, le comunicazioni alle competenti Autorità, la nozione di titolare effettivo, le misure di adeguata verifica della clientela, i controlli, gli obblighi di conservazione e le sanzioni. La seconda parte del decreto interviene sul D. Lgs. n. 109/2007 (in tema di antiterrorismo) e su altre disposizioni in materia valutaria e finanziaria.

³⁵⁴ [Sturzo L., Bitcoin e riciclaggio 2.0, Diritto Penale Contemporaneo, 2018](#), p. 27.

³⁵⁵ Come abbiamo evidenziato nel secondo capitolo, la terminologia "*valute virtuali*" contenuta nel D.lgs. 231/2007 è considerata sinonimo delle locuzioni "*Crypto-asset/Cripto-attività*" e "*Virtual asset*"; in particolare quest'ultima è la formulazione adottata dal GAFI nei nuovi *standard* per la prevenzione del riciclaggio e del finanziamento del terrorismo.

prestatori di servizi digitali, ora sottoposti agli obblighi già in vigore per altri operatori del settore finanziario³⁵⁶. Più precisamente, la valuta virtuale, ai sensi dell'art. 1, comma 2, lett. qq) del novellato D. Lgs. n. 231/2007 (su cui interviene il D. Lgs. n. 90/2017), è definita come la *«rappresentazione digitale di valore, non emessa da una Banca Centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente»*. Per quanto concerne, invece, i prestatori di servizi, l'art. 1, comma 2, lett. f) del novellato decreto 231 del 2007, così ora si esprime: *«prestatori di servizi relativi all'utilizzo di valuta virtuale: ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale»*. Per effetto di tale intervento, i prestatori di servizi collegati all'utilizzo di valuta virtuale sono stati inclusi tra i destinatari degli obblighi antiriciclaggio (sull'adeguata verifica della clientela, la segnalazione di operazioni sospette ecc.), limitatamente allo svolgimento di attività di conversione di valute virtuali da o in valute aventi corso forzoso. Già all'indomani della pubblicazione del decreto legislativo, tuttavia, da più parti è stata sottolineata una certa incompiutezza del dato normativo, che si andavano a sommare alle diverse carenze già evidenziate in relazione alla IV Direttiva. In particolare, *«le modifiche apportate dal d.lgs. n. 90/2017 al d.lgs. n. 231/2007, pur apparendo di grande innovazione, non sembrano poi in realtà così idonee a contrastare un fenomeno la cui espansione cammina di pari passo alla crescita del valore di mercato della criptovaluta in questione»*, dal momento che, inevitabilmente, *«porre il presidio antiriciclaggio in relazione a soggetti eventualmente, forse probabilmente, ma non certamente, ricompresi nella transazione non servirà ad affievolire l'elevata minaccia di riciclaggio intrinsecamente presente nelle caratteristiche del bitcoin»*³⁵⁷.

In sostanza, la normativa nazionale del 2017, trovava applicazione nei confronti dei prestatori di servizi relativi all'utilizzo di valuta virtuale *«limitatamente allo svolgimento dell'attività*

³⁵⁶ Per approfondimenti e considerazioni critiche sul tema all'attenzione, cfr. Sarzana di S. Ippolito F. e Nicotra M., *Diritto della blockchain, intelligenza artificiale e IoT*, IPSOA, 2018, pp. 162 ss.; Pacillo V., *Le valute virtuali alla luce della V Direttiva Antiriciclaggio*, Riv. Trim. Dir. Trib., nn. 3-4, 2018, p. 631.

³⁵⁷ Vds. [Sturzo L., Bitcoin e riciclaggio 2.0, Diritto Penale Contemporaneo, 2018](#), p. 30.

di conversione di valute virtuali da ovvero in valute aventi corso forzoso», in tal modo, includendo nel perimetro di applicazione soggettiva della normativa solo gli erogatori di servizi di exchange e non anche gli altri prestatori di servizi, come i fornitori di servizi connessi a digital wallet, ovvero specializzati nella prestazione di servizi di crittografia per la custodia di valori virtuali. In particolare, erano stati estesi ai soli exchange gli obblighi previsti per i cambiavalute ai sensi dell'art. 17-bis del D. Lgs. n. 141/2010, da attuarsi per mezzo dell'iscrizione in una sezione speciale (poi istituita il 16 maggio 2022³⁵⁸) del Registro tenuto dall'Organismo di cui all'art. 128-undecies del TUB, il cd. OAM (Organismo per la gestione degli elenchi degli agenti in attività finanziaria e dei mediatori creditizi).

Le carenze del dato normativo non venivano individuate solo nella marginalità o eventualità del ruolo svolto dagli scambiatori di valuta virtuale ma anche nel fatto che «il Bitcoin profitto del reato presupposto non dovrà necessariamente essere scambiato in valuta reale, ben potendo continuare a circolare indisturbato nel mondo virtuale ovvero essere scambiato con ulteriori valute convertibili, che potrebbero a loro volta trovare la via d'uscita senza passare per i soggetti obbligati»³⁵⁹.

D'altra parte, negli stessi termini era intervenuta anche la Banca Centrale Europea il 12 ottobre 2016, nell'ambito del proprio *«Parere su una proposta di direttiva del Parlamento europeo e del Consiglio che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica la Direttiva 2009/10/CE»³⁶⁰*. In tale contesto va ad inserirsi, in data 30 maggio 2018,

³⁵⁸ Come ribadito in precedenza, i VASP in possesso di requisiti minimali sono oggi tenuti ad iscriversi nel registro dei cambiavalute, secondo le modalità stabilite dal decreto del Ministero dell'Economia e delle Finanze del 13 gennaio 2022. In particolare, il decreto stabilisce che l'attività di VASP è riservata ai soggetti con sede legale in Italia o ai soggetti UE con stabile organizzazione in Italia, non essendo ammessa l'operatività nella forma della libera prestazione di servizi.

³⁵⁹ [Sturzo L., Bitcoin e riciclaggio 2.0, Diritto Penale Contemporaneo, 2018.](#)

³⁶⁰ La BCE ha formulato, infatti, diverse osservazioni in merito alla regolamentazione di piattaforme di cambio di valute virtuali e prestatori di servizio di portafoglio digitale, oltre che ai registri centrali di banca e conti di pagamento. In particolare, ha espresso un giudizio positivo in relazione all'ampliamento dei soggetti obbligati all'applicazione della Direttiva 2015/849/UE per includervi i prestatori di servizio la cui attività principale e professionale consiste nella fornitura di servizi di cambio tra valute virtuali e valute legali, oltre che i prestatori di servizi di portafoglio digitali che offrono servizi di custodia delle credenziali necessarie per accedere alle valute virtuali, ed in relazione alla registrazione dei prestatori dei registri di cambio tra valute virtuali e valute legali ed i prestatori di servizio di portafoglio digitale. Ad avviso della BCE, tali disposizioni si sarebbero rivelate quanto mai utili poiché *«i terroristi e le altre organizzazioni criminali possono attualmente trasferire denaro all'interno delle reti delle valute virtuali dissimulando i trasferimenti o beneficiando di un certo livello di anonimato su tali piattaforme»*, nella misura in cui l'utilizzo delle valute virtuali presenterebbe rischi ancor

la V Direttiva antiriciclaggio, n. 2018/843 del Parlamento Europeo e del Consiglio³⁶¹. L'Unione Europea ha, in questa sede, affermato di aver sentito la necessità di intervenire in materia giacché *«i recenti attentati terroristici hanno evidenziato l'emergere di nuove tendenze, in particolare per quanto riguarda le modalità con cui i gruppi terroristici finanziano e svolgono le proprie operazioni. Taluni servizi basati sulle moderne tecnologie stanno diventando sempre più popolari come sistemi finanziari alternativi, considerando che restano al di fuori dell'ambito di applicazione del diritto dell'Unione o che beneficiano di deroghe all'applicazione di obblighi giuridici che potrebbero essere non più giustificate»*. Di qui, la presa d'atto che, *«per stare al passo con queste nuove tendenze è opportuno adottare ulteriori misure volte a garantire la maggiore trasparenza delle operazioni finanziarie, delle società e degli altri soggetti giuridici, nonché dei trust e degli istituti giuridici aventi assetto o funzioni affini a quelli del trust, allo scopo di migliorare l'attuale quadro di prevenzione e di contrastare più efficacemente il finanziamento del terrorismo»*³⁶². La nuova Direttiva si muove, dunque, nella direzione di assicurare ancor più trasparenza al contesto economico-finanziario e, per quanto di più stretto interesse in questa sede, ha il pregio di aver provveduto ad estendere il rispetto degli obblighi antiriciclaggio anche ai *wallet provider*, oltre che agli *exchange*, ossia i cambia valute virtuali ³⁶³, motivo per il quale ci si attendono ulteriori passi avanti nel contrasto ai fenomeni criminali legati ai *crypto-asset*³⁶⁴.

maggiori rispetto ai mezzi di pagamento tradizionali poiché la trasferibilità della valuta virtuale è limitata solo dalle capacità delle reti e delle infrastrutture informatiche che vi sono alla base

³⁶¹ Che modifica la Direttiva 2015/849/UE relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE.

³⁶² Ivi, *Considerando* n. 2.

³⁶³ Oltre alla definizione, che abbiamo già evidenziato, di “valuta virtuale”, la Direttiva offre ulteriori spunti per chiarirne la natura. Nel *Considerando* n. 10 si precisa che *«le valute virtuali non dovrebbero essere confuse con la moneta elettronica quale definita all'articolo 2, punto 2, della direttiva 2009/110/CE del Parlamento europeo e del Consiglio con il più ampio concetto di “fondi” di cui all'articolo 4, punto 25, della direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, con il valore monetario utilizzato per eseguire operazioni di pagamento di cui all'articolo 3, lettere k) e l), della direttiva (UE) 2015/2366, né con le valute di gioco che possono essere utilizzate esclusivamente all'interno di un determinato ambiente di gioco. Sebbene le valute virtuali possano essere spesso utilizzate come mezzo di pagamento, potrebbero essere usate anche per altri scopi e avere impiego più ampio, ad esempio come mezzo di scambio, di investimento, come prodotti di riserva di valore o essere utilizzate in casinò online. L'obiettivo della presente direttiva è coprire tutti i possibili usi delle valute virtuali»*.

³⁶⁴ Come appare evidente, il presupposto della registrazione non elimina il problema dell'anonimato di tali strumenti di negoziazione digitale, dal momento che gli utenti potrebbero effettuare operazioni anche senza ricorrere a tali operatori. Per tale motivo, il *Considerando* n. 9 della V Direttiva antiriciclaggio afferma che, per

L'ultimo intervento italiano che, nel contesto appena descritto, è d'obbligo segnalare, riguarda, pertanto, il decreto legislativo n. 125 del 2019, recante appunto modifiche ed integrazioni ai D. Lgs. nn. 90 e 92 del 2017, ed attuativo della Direttiva 2018/843/UE. La novella introduce, questa volta, anche la definizione normativa della categoria degli operatori che offrono servizi di portafoglio digitale, ossia dei *VASP*, prevedendo che anch'essi siano assoggettati alla disciplina di cui al Titolo I della legge 231/2007. In particolare, l'art. 1, comma 1, lettera g) li identifica nelle "*persone fisiche o giuridiche che forniscono a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private al fine di detenere, memorizzare e trasferire valute virtuali*" (definizione assai ampia mutuata dalla stessa Direttiva).

In tale quadro, si innestano, infine, diverse iniziative in ambito UE tese a riformare profondamente l'intero impianto regolamentare in tema *AML/CFT*. Il 7 maggio 2020, in particolare, la Commissione ha presentato un piano d'azione per una politica integrata dell'Unione in materia di prevenzione del riciclaggio di denaro e del finanziamento del terrorismo. Con tale piano d'azione la Commissione si è impegnata ad attuare sei pilastri, che richiedono l'adozione di un pacchetto *AML/CFT* composto da quattro proposte legislative che comprendono:

- una proposta di regolamento relativo alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio e finanziamento del terrorismo (cd. *AMLR VI*);
- una proposta di direttiva che stabilisce i meccanismi che gli Stati membri dovrebbero istituire per prevenire l'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che abroga la Direttiva 2015/849/UE;
- una proposta di regolamento che istituisce un'autorità dell'UE per la lotta contro il riciclaggio e il finanziamento del terrorismo ("*AMLA*");
- una proposta di rifusione del Regolamento 2015/847/UE che estende i requisiti di tracciabilità alle crypto-attività.

contrastare i rischi legati all'anonimato, le Unità nazionali di Informazione Finanziaria (*Financial Intelligence Unit*) dovrebbero poter ottenere informazioni che consentano loro di associare gli indirizzi della valuta virtuale all'identità del proprietario di tale valuta. È, inoltre, evidenziata la possibilità di consentire agli utenti di presentare, su base volontaria, un'autodichiarazione alle autorità designate.

Avuto riguardo alla prima proposta, questa non si limita a trasferire le disposizioni dalla vigente Direttiva *AML/CFT* all'interno di un Regolamento, ma indica una serie di modifiche sostanziali al fine di conseguire un maggiore livello di armonizzazione e convergenza nell'applicazione delle norme *AML/CFT* in tutta l'UE. È possibile al momento tracciare le seguenti linee di intervento:

- al fine di mitigare rischi nuovi ed emergenti, l'elenco dei soggetti obbligati è ampliato per includere i fornitori di servizi per le cripto-attività ma anche altri settori quali le piattaforme di *crowdfunding* e gli operatori che prestano servizi di migrazione;
- per garantire un'applicazione coerente delle norme in tutto il mercato interno, sono chiariti gli obblighi e i requisiti relativi a politiche, controlli e procedure interni, anche nel caso dei gruppi, e le misure di adeguata verifica della clientela sono rese più dettagliate, con obblighi più chiari in funzione del livello di rischio del cliente;
- gli obblighi relativi ai Paesi terzi sono riesaminati per garantire l'applicazione di misure rafforzate di adeguata verifica ai Paesi che rappresentano una minaccia per il sistema finanziario dell'Unione;
- gli obblighi relativi alle persone politicamente esposte sono oggetto di chiarimenti di minore entità, in particolare per quanto riguarda la definizione di persona politicamente esposta;
- gli obblighi in materia di titolarità effettiva sono semplificati per garantire un adeguato livello di trasparenza in tutta l'Unione e sono introdotti nuovi obblighi in relazione ai fiduciari e ai soggetti stranieri per mitigare il rischio che i criminali si nascondano dietro livelli intermedi;
- per orientare più chiaramente la segnalazione di operazioni sospette, sono chiariti gli indicatori di rischio che fanno sorgere sospetti, mentre gli obblighi di comunicazione e la condivisione di informazioni tra privati rimangono immutati;
- al fine di garantire la piena coerenza con le norme dell'UE in materia di protezione dei dati, sono introdotti obblighi in relazione al trattamento di determinate categorie di dati personali ed è previsto un termine più breve per la conservazione dei dati personali;

- le misure volte a mitigare l'abuso degli strumenti al portatore sono rafforzate ed è inserita una disposizione che limita l'uso di denaro contante per le operazioni di importo elevato, alla luce del comprovato scarso effetto dell'attuale approccio che fa affidamento sui soggetti che commerciano beni per l'attuazione degli obblighi in materia di *AML/CFT* in relazione ai pagamenti in contanti di importo elevato.

Per quanto di più stretto interesse, l'inclusione dei fornitori di servizi per le cripto-attività tra i soggetti cui si applicano le norme *AML/CFT* e l'introduzione di obblighi di informazione per i trasferimenti di attività virtuali integreranno il pacchetto sulla finanza digitale del 24 settembre 2020, assicurando la piena coerenza tra il quadro dell'UE e le norme del GAFI.

SEZIONE 2. TASSAZIONE: COME I CASP DOVRANNO GESTIRE IL TRATTAMENTO FISCALE DELLE CRIPTO-ATTIVITÀ

1. Introduzione su tassazione in Italia e in Europa

Dinanzi a fenomeni in larga parte non ancora regolamentati in modo organico, lungo l'elaborato è stato evidenziato che sono in corso a livello internazionale ed europeo lavori per disegnare un nuovo insieme di regole e di controlli per i prodotti crittografici (e relativi "ecosistemi"), ma la loro entrata a regime richiederà ancora tempo³⁶⁵.

Sebbene la prospettiva *AML/CFT* abbia permeato la disciplina dei *CASP*, una minuziosa attenzione nella lettura del *MiCA* (artt. 85 e 110 del testo)³⁶⁶ ci permette di desumere che tali *provider* dovranno attrezzarsi anche sul piano del diritto tributario nazionale, unitamente a riferimenti normativi sovranazionali. Volendo essere precisi, il testo appena richiamato non impone esplicitamente oneri fiscali in capo ai fornitori di cripto-attività operanti nell'UE, bensì contempla un sistema di vigilanza più ampio che promuova la sorveglianza delle cripto-attività anche su altri fronti, includendo per l'appunto la cooperazione con le autorità fiscali. In ultima istanza, ciò porta a presumere la ragionevole necessità per i *CASP* di non farsi trovare impreparati da questo punto di vista.

Peraltro, in un contesto tecnologico dove le cripto-attività sono in rapida evoluzione, anche i responsabili delle politiche fiscali sono ancora in una fase di valutazione delle loro

³⁶⁵ Sul punto si richiama l'Intervento di [Perrazzelli A., Vice Direttrice Generale della Banca d'Italia, Le iniziative regolamentari per il Fintech: a che punto siamo?](#), Università degli Studi dell'Insubria. Laboratorio di Finanza Digitale, 4 maggio 2021. Per quanto riguarda specificamente i *crypto-asset*, in attesa dell'applicazione del [Regolamento del Parlamento Europeo e del Consiglio relativo ai mercati delle cripto-attività e che modifica i Regolamenti 1093/2010/UE e 1095/2010/UE e le Direttive 2013/36/UE e 2019/1937/UE \(c.d. MiCA\)](#), tali ultimi "prodotti" continueranno a non essere regolamentati nella maggior parte delle giurisdizioni. Sul punto, in data 25 maggio 2023, l'Autorità europea degli strumenti finanziari e dei mercati (*ESMA*), ha rilasciato una dichiarazione pubblica per mettere in guardia gli investitori dai rischi che si presentano quando le imprese di investimento offrono prodotti e/o servizi finanziari non regolamentati.

³⁶⁶ L'art. 85 recita così: «Se un emittente di cripto-attività, compresi i token collegati ad attività o i token di moneta elettronica, o un fornitore di servizi per le cripto-attività svolge attività diverse da quelle contemplate dal presente regolamento, le autorità competenti cooperano con le autorità responsabili della vigilanza o della sorveglianza di tali altre attività come previsto dal pertinente diritto dell'Unione o nazionale, comprese le autorità fiscali». Di simile tenore l'art. 110: «Se un emittente di token collegati ad attività significativi o un emittente di token di moneta elettronica significativi svolge attività diverse da quelle contemplate dal presente regolamento, l'ABE coopera con le autorità responsabili della vigilanza o della sorveglianza di tali altre attività come previsto dal pertinente diritto dell'Unione o nazionale, comprese le autorità fiscali».

implicazioni che restano in gran parte inesplorate, ancorché costituiscano un aspetto importante del quadro normativo complessivo.

Dal punto di vista ricognitivo assume particolare interesse un rapporto OCSE in cui si rileva che su 43 Paesi esaminati dallo stesso organismo, 30 hanno una legislazione interna che regola il fenomeno delle valute virtuali³⁶⁷. Ai fini delle imposte sui redditi, il rapporto pone in evidenza il fatto che la maggior parte dei Paesi considera le valute virtuali un *asset* tassandolo in maniera analoga ad altre forme di beni immateriali. Nello specifico, le attività di *mining* e di scambio sono tassate principalmente come *capital gains*, all'infuori di una minoranza di Paesi che distingue le attività commerciali dalle attività personali o occasionali. Ulteriori differenze vengono riscontrate in ordine all'individuazione delle fattispecie imponibili: mentre la maggior parte dei Paesi ritiene imponibile tutte le forme di scambio di cripto-attività, in altri gli scambi sono considerati esenti se non addirittura esclusi dalla tassazione. Una maggior coerenza viene, invece, riscontrata in ordine al trattamento delle cripto-attività ai fini delle imposte sui consumi, rispetto al quale si nota una tendenziale esenzione o esclusione delle relative operazioni. Con particolare riferimento all'Europa, attualmente solo cinque Stati membri dell'UE su 27 hanno adottato disposizioni giuridiche specifiche sulla tassazione delle cripto-attività mentre 19 Stati membri dispongono di orientamenti amministrativi sulla tassazione delle cripto-attività³⁶⁸. Mantenendo ancora un'ottica comparata, un recente *report* di *Coincub* fotografa «molte differenze tra Paese e Paese riguardo la tassazione crypto. Tali differenze non riguardano solo l'aliquota fiscale, ma anche in generale le norme fiscali, le eventuali soglie di esenzione o gli obblighi dichiarativi, financo la natura stessa delle criptovalute considerate come asset finanziari o come proprietà. Ma anche concentrandosi solo sulle aliquote con cui vengono tassate le eventuali plusvalenze è emerso un quadro molto variegato»³⁶⁹. La Figura 15 offre uno scorcio globale «di tutti i Paesi del mondo a cui è associata la percentuale di tassazione dell'aliquota principale per chi detiene criptovalute per lunghi

³⁶⁷ [OCSE, *Taxing Virtual Currencies. An Overview of Tax Treatments and Emerging Tax Policy Issues*, 2020.](#)

³⁶⁸ Cfr. [Parlamento europeo, *Impatto delle nuove tecnologie sulla tassazione: cripto-attività e blockchain*, Risoluzione del Parlamento europeo del 4 ottobre 2022 sull'impatto delle nuove tecnologie sulla tassazione: cripto-attività e blockchain \(2021/2201\(INI\)\), 2022.](#)

³⁶⁹ [Cavicchioli M., *Dove la tassazione crypto è più favorevole?*, The Cryptonomist, 2023.](#)

periodi»³⁷⁰. La mappatura consente di osservare molteplici categorie:

- Paesi a zero tasse sulle crypto-attività con prospettive altamente positive;
- Bassa tassazione (inferiore al 19%) con prospettive positive;
- Tassazione media 20-29%, *crypto-friendly*;
- Tassazione medio-alta 30%-40%, ma con agevolazioni a lungo termine³⁷¹;
- Elevata tassazione sulle crypto-attività (30%, 40% e oltre), senza nessuna concessione.

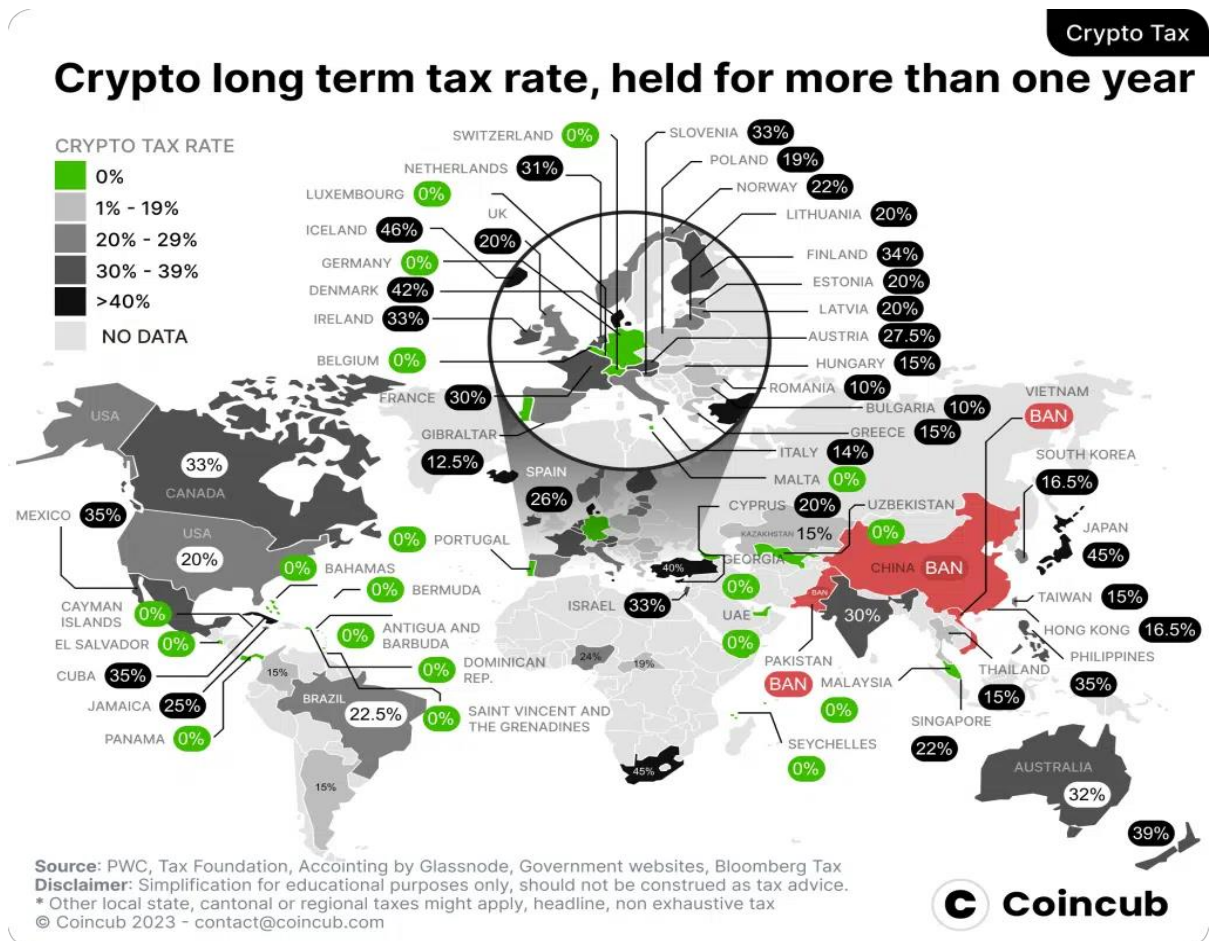


Figura 15 – Fonte: [Coincub, Crypto Tax Report, 2023](#).

³⁷⁰ [Cavicchioli M., Dove la tassazione crypto è più favorevole?, The Cryptonomist, 2023](#). «Ovvero non riguarda chi fa trading vendendo le crypto meno di 12 mesi dopo averle acquistate, ma chi invece le acquista per tenerle in portafoglio (i cosiddetti holder)».

³⁷¹ [Coincub, Crypto Tax Report, 2023](#). «L'Italia ha adottato politiche fiscali di nuova concezione volte ad attrarre individui con un elevato patrimonio netto. Il risultato è un sistema fiscale complesso e in continuo sviluppo. I guadagni provenienti dall'Italia sono tassabili come reddito, con un'esenzione fiscale per i guadagni in criptovalute che non superano l'enorme cifra di 51.000 euro, mentre i redditi e i guadagni esteri possono

Concentrando l'attenzione sui Paesi componenti l'Unione Europea, sebbene sia pacifico che la potestà impositiva sia prerogativa di ciascun Stato membro, non si può non notare come vi siano notevoli differenze di tassazione che possono ragionevolmente indurre un *provider* a registrare la propria attività in un determinato Paese europeo esclusivamente in base alla convenienza fiscale. In altri termini, questa circostanza sembra potenzialmente incidere in termini concorrenziali all'interno del mercato digitale unico, in cui determinati *CASP* possono beneficiare di un trattamento fiscale migliore rispetto ad altri.

Da questi brevi sintetici cenni appare evidente che allo stato attuale non esista un approccio coordinato ed armonico riguardante la tassazione delle cripto-attività, tant'è che i vari Paesi hanno adottato un'ampia gamma di regolamentazioni al riguardo. Invero, proprio considerando la portata globale dei fenomeni connessi con le transazioni in cripto-attività, il relativo trattamento fiscale richiederebbe uno sforzo maggiore a livello internazionale per disciplinare meglio, e secondo principi di equità, l'imposizione dell'economia digitale, così come ampiamente indicato nella Risoluzione del Parlamento UE del 4 ottobre 2022 *sull'impatto delle nuove tecnologie sulla tassazione: cripto-attività e blockchain*³⁷².

Infatti, le particolari caratteristiche del fenomeno *crypto* (decentralizzazione³⁷³, disintermediazione, pseudo-anonimato, eterogeneità delle forme concretamente assunte³⁷⁴ ecc.) acuiscono le tensioni di un settore, quello tributario, in cui i principi – di natura prettamente materiale e territoriale - che sono alla base della sovranità impositiva dei singoli Stati, appaiono progressivamente perdere di forza non riuscendo più a garantire che la potestà impositiva possa esercitarsi verso tutte le manifestazioni di ricchezza, a maggior ragione se queste sono caratterizzate dall'immaterialità dei processi e dall'assoluta

essere esentati dalle imposte italiane. Per gli scambi di criptovalute a lungo termine i contribuenti italiani potrebbero essere motivati a detenere le criptovalute più a lungo per beneficiare dell'"imposta sostitutiva sul reddito" sul 14% del valore degli asset detenuti al 1° gennaio del prossimo anno, anziché sul costo al momento dell'acquisto».

³⁷² Il Parlamento europeo ritiene che la politica fiscale debba essere integrata in un solido quadro normativo per le cripto-attività e debba essere coerente con altri aspetti politici, tra cui la trasparenza fiscale e i requisiti giuridici, finanziari e di protezione dei consumatori.

³⁷³ Come precedentemente accennato, il mondo delle cripto-attività si fonda su processi che si muovono su *DLT*, il che rende più difficile ricorrere in maniera centralizzata ad intermediari per assistere le autorità fiscali.

³⁷⁴ La natura ibrida di tali prodotti e l'intrinseca connotazione transfrontaliera del fenomeno renderebbero opportuna una regolamentazione "*cross-settoriale*", uniforme a livello europeo.

manca di un radicamento territoriale³⁷⁵. Tanto è vero che il Parlamento Europeo ha già sottolineato che *«le attuali norme internazionali in materia di imposta sulle società non sono più adeguate nel contesto della digitalizzazione e della globalizzazione dell'economia»* e che *«gli sviluppi della digitalizzazione e una maggiore dipendenza dalle attività immateriali e il loro aumento nelle catene del valore creano prospettive e sfide in termini di tracciabilità delle operazioni economiche e degli eventi imponibili, compresa la possibilità di pratiche di elusione fiscale, in particolare quando tali operazioni sono transfrontaliere o hanno luogo al di fuori dell'Unione»*.

Le preoccupazioni espresse dal Parlamento Europeo in ordine alle nuove sfide sollevate dal fenomeno *crypto* trovano ragion d'essere nelle dinamiche innovative delle cripto-attività imposte dall'evoluzione tecnologica. Dalla parziale e sintetica panoramica delle cripto-attività emerge che siamo di fronte ad una materia in continua evoluzione perché legata anche all'impiego di tecnologie che sono a loro volta in continuo progredire e i cui potenziali sviluppi non sono assolutamente immaginabili allo stato attuale.

In questo senso, occorre prendere altresì atto che la complessità del fenomeno non consente di qualificare “in astratto” e “a priori” le varie fattispecie riscontrabili nella realtà fenomenica. Peraltro, come abbiamo avuto modo di evidenziare nei precedenti paragrafi, a causa dell'eterogeneità e varietà delle forme assumibili, le cripto-attività non hanno natura omogenea e qualificazione giuridica certa (non tutte le cripto-attività hanno ad esempio natura finanziaria). Pertanto, la loro qualificazione, ai fini dell'imposizione, non può che avvenire in concreto e caso per caso, tenuto conto delle caratteristiche funzionali e del concreto utilizzo³⁷⁶.

Chiarito che il concetto di cripto-attività ricomprende una vasta ed eterogenea gamma di rappresentazioni digitali dalle funzioni più disparate, spesso diverse fra loro, occorre sin da ora evidenziare che le difficoltà sono proprio legate alla capacità di individuare definizioni univoche che non riguardino solo il profilo oggettivo, connesso con il concetto stesso di cripto-attività, ma anche quello soggettivo con riguardo, da un lato agli utenti finali³⁷⁷ e

³⁷⁵ Gli operatori dell'economia digitale possono infatti svolgere attività commerciali significative ovunque senza stabilirvi una presenza fisica e, per l'effetto, le imposte versate in una giurisdizione non riflettono più il valore e gli utili ivi creati.

³⁷⁶ L'approccio è condiviso dall'Agenzia delle Entrate nella circolare sulle criptovalute.

³⁷⁷ Che poi sono coloro che dovrebbero sopportare l'onere tributario

dall'altro tutti quei soggetti che forniscono servizi di cripto-attività (*Crypto-Asset Service Provider, CASP*) che si trovano in una posizione privilegiata per la raccolta e la verifica delle informazioni sugli stessi utenti necessarie per valutare l'utilizzo delle cripto-attività che possono essere utilizzate a fini di pagamento o di investimento .

All'interno di questo complesso quadro si inserisce la scelta del Legislatore domestico di approntare in piena autonomia una speciale disciplina tributaria allo scopo di rendere la normativa fiscale coerente con l'evoluzione delle diverse tipologie di cripto-attività presenti nel sistema.

2. La disciplina fiscale delle cripto-attività in Italia: l'imposta sul reddito delle persone fisiche (Irpef)

In ambito nazionale il primo pronunciamento sul tema della fiscalità delle cripto-attività si rileva nella risoluzione dell'Agenzia delle entrate n. 72/E in data 2 settembre 2016, avente ad oggetto il trattamento fiscale applicabile alle società che svolgono attività di servizi relativi a valute virtuali³⁷⁸. La risoluzione in parola riguarda una istanza di interpello presentata ai sensi dell'art. 11 della L. n. 212/2000 (c.d. "Statuto dei diritti del contribuente") nell'ambito della quale un contribuente, per il tramite di una società a responsabilità limitata, intendeva svolgere operazioni di acquisto e vendita di *bitcoin* e, pertanto, chiedeva di conoscere il corretto trattamento fiscale sia ai fini dell'imposta sul valore aggiunto sia ai fini delle imposte dirette.

Preliminarmente, l'Agenzia qualifica la circolazione dei *bitcoin* quale «*sistema di pagamento decentralizzato, che utilizza una rete di soggetti paritari (peer to peer) non soggetto ad alcuna disciplina regolamentare specifica né ad una Autorità centrale che ne governa la stabilità nella circolazione*».

³⁷⁸ In dottrina vds. Capaccioli S., *Criptovalute e Bitcoin: un'analisi giuridica*, 2015; Capaccioli S., *Bitcoin: le operazioni di cambio con valuta a corso legale sono prestazioni di servizio esenti*, Fisco, 2015 ; Capaccioli S., *Riciclaggio, antiriciclaggio e Bitcoin*, *Il Fisco*, 2014, n. 46, p. 4561; Claps P. e Pignatelli M., *L'acquisto e la vendita per conto terzi di "Bitcoin" non sconta l'IVA ma rileva ai fini IRES ed IRAP*, *Corr. trib.*, 2016, n. 40, p. 3075; Corasaniti G., *Il trattamento tributario dei Bitcoin tra obblighi antiriciclaggio e monitoraggio fiscale*, cit.; Ferrari E., *Bitcoin e criptovalute: la moneta virtuale tra Fisco e antiriciclaggio*, *Il fisco*, 2018, 9, p. 861 e ss; Magliocco A., *Bitcoin e tassazione*, in *Strumenti finanziari e fiscalità*, 2016, p. 22; Palumbo G., *Il trattamento tributario dei «Bitcoin»*, *Dir. Prat. Trib.*, 2016, 1, p. 279 e ss.; Piasente M., *Esenzione IVA per i "Bitcoin": la strada indicata dalla Corte UE interpretando la nozione "divise"*, *Corr. Trib.*, 2016.

Parimenti, la risoluzione cita la sentenza della Corte di Giustizia dell'Unione Europea quale imprescindibile pronunciamento sul trattamento ai fini dell'imposta sul valore aggiunto, costituendo «*necessariamente un punto di riferimento sul piano della disciplina fiscale applicabile alle monete virtuali e, nello specifico, ai bitcoin*».

D'altra parte, il caso analizzato dai giudici della Corte Europea si mostrava davvero simile a quello che la stessa Agenzia delle Entrate si trovava ad affrontare, inerente a un *exchange* che svolgeva attività di cessione ed acquisto di valuta virtuale, sempre *bitcoin*, in cambio di valuta tradizionale. Anche in quella situazione il compenso per l'attività era determinato in misura pari al margine differenziale fra il prezzo che il cliente paga per l'acquisto di un'unità di moneta virtuale e la migliore quotazione dello stesso *bitcoin* sul mercato.

Conformandosi all'orientamento proprio del giudice europeo, l'Agenzia ha qualificato, ai fini dell'imposta sul valore aggiunto, l'attività della società istante quale prestazione di servizi esenti da imposta ai sensi dell'articolo 10, comma 1, n. 3), del D.P.R. n. 633/1972. Coerentemente all'inquadramento giurisprudenziale europeo, l'Agenzia delle entrate ha ritenuto che la società istante dovesse essere assoggettata ad imposizione diretta per le componenti positive di reddito derivanti dalla attività di intermediazione nell'acquisto e vendita di *bitcoin*, al netto di quelle negative riferite a detta attività. Nel caso in esame, l'Agenzia ha evidenziato che:

- il cliente, in caso di ordine di acquistare, provvede ad anticipare le risorse finanziarie alla società che, concluso l'acquisto di *bitcoin*, registra nel *wallet* del cliente i codici relativi ai *bitcoin* acquistati;
- la società, in caso di ordine di vendere, preleva dal cliente i *bitcoin* e gli trasferisce, al completamento delle operazioni di vendita, la somma pattuita.

Il guadagno (o la perdita) di competenza della società³⁷⁹ è imputabile ai ricavi (o ai costi) di esercizio, che concorrono quali elementi positivi (o negativi) alla formazione della base imponibile da assoggettare a tassazione ai fini delle imposte dirette (Ires ed Irap).

³⁷⁹ Derivante dalla differenza (positiva o negativa) tra i prezzi di acquisto sostenuti dall'istante e costi di acquisto a cui si è impegnato il cliente (nel caso in cui quest'ultimo abbia affidato alla società l'incarico a comprare) o

I *bitcoin* che permangono nella disponibilità della società a fine esercizio devono invece essere valutati secondo il cambio vigente alla data di chiusura dell'esercizio e tale valutazione acquisisce rilievo ai fini fiscali in ragione dell'art. 9 del TUIR, facendo pertanto riferimento al valore normale rinvenibile sulla base della media delle quotazioni ufficiali riportate nelle piattaforme *on line* ove sono compravenduti i *bitcoin*. Sul punto, emergono chiari segnali di criticità legati, oltre che alla estrema volatilità dei prezzi di riferimento (anche giornalmente), all'assenza di un sistema di rilevazione ufficiale che comporta possibili fenomeni di arbitraggio nelle quotazioni dei singoli mercati.

Al contempo, ancorché in via incidentale, nella citata risoluzione n. 72/E l'Agenzia si esprime in ordine agli aspetti di tassazione ai fini delle imposte dirette per le persone fisiche che detengono *bitcoin* al di fuori dell'attività di impresa, ricordando che le operazioni a pronti (acquisti e vendite) di valuta non generano redditi imponibili mancando la finalità speculativa.

Purtuttavia, non si è esclusa la possibilità di generare un reddito diverso³⁸⁰ ai sensi dell'art. 67, comma 1, lett. *c-ter*), del TUIR. Tale disposizione contempla la sottoposizione a tassazione delle plusvalenze derivanti dalla cessione a titolo oneroso di valute, ma l'imponibilità delle operazioni sulle valute estere è riferita esclusivamente a quelle operazioni tassativamente riportate nella lett. *c-ter*) che si intendono come espressive, per presunzione di legge, di una attività di investimento (cioè, il prelievo della valuta da depositi o conti correnti ovvero la sua cessione a termine). D'altro canto, non sono mai rilevanti le cessioni a pronti delle valute, mancando appunto la finalità speculativa.

In tal senso si è espressa la stessa Agenzia delle entrate – Direzione Regionale Lombardia, nella risposta (non pubblicata) all'interpello n. 956-39/2018 relativo all'istanza presentata

tra prezzi di vendita praticati dall'istante e ricavi di vendita garantiti al cliente (nel caso di affidamento di incarico a vendere).

³⁸⁰ Nella categoria denominata "redditi diversi", disciplinata dal TUIR, il Legislatore ha concentrato una serie di casistiche reddituali eterogenee, non riconducibili alle fattispecie tipiche, ossia alle categorie caratterizzate dalla derivazione dei redditi considerati da una fonte produttiva omogenea. In particolare, la accennata eterogeneità delle ipotesi contemplate dall'art. 67 del TUIR è una diretta conseguenza delle finalità proprie della categoria reddituale in esame, che sono quelle di assoggettare ad imposizione i redditi nei cui confronti non si sia verificato almeno uno dei presupposti necessari per la riconduzione nell'ambito delle altre categorie reddituali previste dal Legislatore. Tra i redditi diversi vi sono anche alcuni redditi di natura finanziaria e, in special modo, quelli derivanti da operazioni finanziarie che possono dar luogo a risultati sia positivi che negativi (guadagni o perdite) in relazione al verificarsi di eventi incerti e aleatori (c.d. *capital gains*).

da un contribuente privato investitore che nel 2013 aveva acquistato alcuni *bitcoin* su una piattaforma *exchange* e nel 2017 ne aveva utilizzati una parte al fine di acquistare oro da investimento da un intermediario estero che ammetteva il pagamento con moneta virtuale. Con tale istanza veniva chiesto all'Agenzia delle entrate il corretto trattamento fiscale della plusvalenza realizzata con l'acquisto dell'oro tramite *bitcoin*³⁸¹.

Preliminarmente, l'Agenzia delle entrate esordisce rappresentando che in «*attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006*», è stato adottato il D.Lgs. n. 90/2017, in vigore dal 4 luglio 2017. L'art. 1 del suddetto decreto legislativo ha sostituito, tra l'altro, l'art. 1 del D. Lgs. n. 231/2007 introducendo la nozione di “*valuta virtuale*”. In particolare, il novellato art. 1, comma 2, lettera *qq*), del D. Lgs. n. 231/2007, definisce “*valuta virtuale*” «*la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi è trasferita, archiviata e negoziata elettronicamente*». In altri termini, il Legislatore riconosce normativamente l'utilizzo delle valute virtuali come strumento di pagamento alternativo a quelli tradizionalmente utilizzati nello scambio di beni e servizi ovvero definisce tale “*strumento di pagamento*” quale «*rappresentazione digitale di valore*”, “*trasferita, archiviata e negoziata elettronicamente*». Nell'assimilare la cessione di cripto-attività a quella di «*valute estere rinvenienti da depositi e conti correnti*», l'Agenzia consente applicazione l'art. 67 del già menzionato TUIR, a mente del quale, al comma 1-ter: «*le plusvalenze derivanti dalla cessione a titolo oneroso di valute estere rinvenienti da depositi e conti correnti concorrono a formare il reddito a condizione che nel periodo d'imposta la giacenza dei depositi e dei conti correnti complessivamente intrattenuti dal contribuente, calcolata*

³⁸¹ Vds. Angelucci P. e Bracchi A., *Tassazione e monitoraggio fiscale delle criptovalute. Analisi dei recenti chiarimenti forniti dall'Agenzia delle Entrate – Direzione Regionale della Lombardia nella risposta (non pubblicata) all'interpello n. 956-39/2018*”.

secondo il cambio vigente all'inizio del periodo di riferimento sia superiore ad euro 51.645,69 per almeno sette giorni lavorativi continui».

Conseguentemente, le cessioni a pronti di *crypto-asset* sono tassate a titolo di reddito diverso solo qualora la “giacenza media” del corrispondente *wallet* superi il controvalore di € 51.645,69 per almeno sette giorni lavorativi continui nel periodo d'imposta. Inoltre, in ordine alla determinazione di un'eventuale plusvalenza derivante dal prelievo dal *wallet* che abbia superato la predetta giacenza media, si deve prendere in riferimento il costo di acquisto, considerando – nella quantificazione delle plusvalenze/minusvalenze – cedute per prime le valute acquisite in data più recente (art. 67, comma 1-bis, del TUIR). La plusvalenza conseguita (al netto di eventuali minusvalenze scomputabili) va inserita nel quadro RT della dichiarazione annuale, utilizzando il criterio LIFO in caso di vendite parziali e liquidando la relativa imposta sostitutiva del 26%. Il costo, se non documentabile, può essere calcolato dividendo l'importo del bonifico effettuato all'*exchange* per il numero di *crypto-asset* acquistati. Per ciò che attiene al calcolo della plusvalenza, si applicano le regole dell'art. 68, comma 6, del TUIR, che individua la plusvalenza fiscalmente riconosciuta nella differenza tra il corrispettivo percepito a seguito della cessione e il valore di acquisto.

Ultimo punto attiene alla rilevanza dei *crypto-asset* ai fini degli obblighi di monitoraggio fiscale previsti dal D.L. n. 167/90. Sul tema, *«l'Agenzia delle Entrate, partendo sempre dall'assunzione che le valute virtuali siano equiparabili alle valute estere, si esprime a favore della riconducibilità di tale fenomeno nell'ambito della disciplina del monitoraggio fiscale; e ciò stante l'inclusione – in linea con i principi generali indicati nella circolare n. 38/E/2013 – delle valute estere tra le attività finanziarie estere. Ne consegue che, secondo l'Agenzia delle Entrate, tutti i soggetti che detengono bitcoin (e in generale criptovalute) al di fuori del circuito degli intermediari residenti, devono monitorare detti investimenti nel quadro RW della dichiarazione dei redditi»*³⁸².

Attesa l'applicabilità dei principi generali che regolano le operazioni aventi ad oggetto valute tradizionali nonché le disposizioni in materia di antiriciclaggio anche alle valute

³⁸² Cancelliere F. e Tardini A., *Risposta (non pubblica) all'interpello n. 956-39/2018: profili fiscali della detenzione di criptovalute da parte di persone fisiche residenti in Italia.*

virtuali, l'Agenzia ritiene che anche le valute virtuali debbano essere oggetto di comunicazione attraverso il citato quadro RW, indicando alla colonna 3 ("*codice individuazione bene*") il codice 14 – "*Altre attività estere di natura finanziaria*". Il controvalore in euro della valuta virtuale detenuta al 31 dicembre del periodo di riferimento deve essere determinato al cambio indicato a tale data sul sito dove il contribuente ha acquistato la valuta virtuale. Negli anni successivi, il contribuente dovrà indicare il controvalore detenuto alla fine di ciascun anno o alla data di vendita nel caso di valuta virtuale vendute in corso d'anno.

Anche il Tribunale Amministrativo del Lazio si è recentemente pronunciato sul trattamento fiscale delle cripto-attività, con sentenza n. 1077 del 27 gennaio 2020³⁸³. Il giudice amministrativo definisce le valute virtuali come «*rappresentazioni digitali di valori*»³⁸⁴, ribadendo la riconducibilità delle stesse ai redditi diversi ai sensi dell'art. 67 del TUIR. Il caso riguardava un ricorso di legittimità proposto da due associazioni contro due provvedimenti dell'Agenzia delle Entrate³⁸⁵ relativi all'obbligo di indicazione nel quadro RW della dichiarazione dei redditi degli *asset* crittografici detenuti.

Le associazioni hanno agito sostenendo che le valute virtuali sono dei meri "*contenitori astratti vuoti*", che si prestano, eventualmente, ad essere riempiti di dati e trasmessi ad altri utenti.

Dunque, l'Agenzia delle Entrate avrebbe assoggettato le valute virtuali all'obbligo di dichiarazione dei redditi senza una previsione legislativa specifica, e senza previa adeguata informazione al contribuente.

La decisione del TAR evidenzia un ulteriore orientamento del panorama giuridico italiano sulla materia, attribuendo rilievo all'aspetto funzionale: il TAR, infatti, assoggetta ad imposizione non il mero possesso di valute virtuali ma il loro diverso utilizzo fintantoché questo generi materia imponibile. In altri termini, ciò che è assoggettato a tassazione non è la moneta virtuale come mezzo finanziario in sé, ma l'utilizzo che se ne fa della stessa.

Argomenta il TAR nel senso che è dirimente la circostanza che la modifica del D.L. n. 167/1990, operata per il tramite del D. Lgs. n. 90/2017, ha esplicitamente inserito l'utilizzo

³⁸³ Il testo della sentenza è rinvenibile al [sito](#) della Giustizia Amministrativa.

³⁸⁴ Cfr. normativa antiriciclaggio, D.lgs. 231/2007.

³⁸⁵ Prot. nn. 23596/2019 e 85457/2019.

delle “*monete virtuali*” tra le operazioni relative ai trasferimenti da e per l’estero, rilevanti ai fini del relativo monitoraggio *ex art. 1* del D.L. n. 167/1990.

L’art. 1 citato opera sotto un duplice profilo, oggettivo e soggettivo: sotto il profilo oggettivo, assoggetta espressamente al monitoraggio sia l’utilizzo delle valute virtuali che l’utilizzo di “mezzi di pagamento” (distinti dalle prime e definiti all’art. 1, comma 2, lett. “s” del D. Lgs. n. 231/2007); sotto quello soggettivo, ai suddetti obblighi di monitoraggio sono tenuti sia gli operatori finanziari che gli operatori non finanziari. Su queste premesse, il TAR ha ritenuto infondate le doglianze del ricorrente secondo le quali le valute virtuali non dovrebbero essere dichiarate nel quadro RW perché non espressamente elencate nell’art. 4: la nozione di investimenti esteri, valevole ai fini del monitoraggio, è definita all’art. 1 del medesimo decreto legge, che concorre a definire la nozione degli “investimenti all’estero” e di “attività estere di natura finanziaria”, includendo in esse anche investimenti ed attività mediante impiego di valute virtuali.

Per ultimo, sostiene il TAR, l’art. 1 assoggetta agli obblighi di monitoraggio sia gli operatori finanziari che quelli non finanziari; pertanto, irrilevante è la tesi secondo cui le monete virtuali sarebbero “mezzi di pagamento” (e non valute), perché la disposizione di cui all’art. 1 è relativa alle operazioni compiute sia con valute virtuali sia con mezzi di pagamento in quanto tali.

Fino al 2023, quindi, il trattamento fiscale del fenomeno *crypto* è stato risolto dall’Amministrazione finanziaria in via del tutto interpretativa, profittando del fatto che la poliedrica natura delle cripto-attività consentiva di sussumere diverse tipologie di attività nelle fattispecie imponibili tratte dall’art. 67 del TUIR, con l’effetto, tuttavia di rendere applicabile ai redditi derivanti dalle relative cessioni norme impositive differenti³⁸⁶.

Tuttavia, fin dall’inizio erano evidenti le criticità e le problematiche sollevate da un simile incedere al punto tale da richiedere l’introduzione di una speciale disciplina.

L’esigenza di una disciplina *ad hoc* per le cripto-attività è stata di recente espressa anche dalla Banca d’Italia nella “*Comunicazione della Banca d’Italia in materia di tecnologie*

³⁸⁶ Cfr. Arginelli P., *La tassazione di bitcoin e cripto-attività e la Costituzione*, Bitcoin e cripto-attività, Il Sole 24 Ore, 2023, p. 64, il quale tiene ad evidenziare che l’applicazione delle pregresse disposizioni normative poteva comportare l’imponibilità anche delle c.d. operazioni *crypto-to-crypto* che sono, invece, attualmente escluse dalla tassazione.

decentralizzate nella finanza e crypto-attività” del giugno 2022. Nel documento, la Banca d’Italia ha ritenuto opportuno evidenziare che sotto il profilo fiscale «è avvertita la necessità di definire discipline ad hoc che conferiscano certezza agli operatori e agli investitori», dal momento all’epoca il Paese non era dotato di una disciplina tributaria specifica ma basata «sull’applicazione, in via interpretativa, di norme dettate per altre tipologie di operazioni e attività». In prospettiva, sottolineava il documento, «appare opportuno favorire un bilanciamento tra la considerazione delle peculiarità del settore e le esigenze di coerenza fra la disciplina fiscale delle crypto-attività e quella di altri cespiti, nonché con l’ordinamento giuridico in generale, anche per motivi di equità di trattamento».

Come osservato da attenta dottrina, le maggiori criticità riguardavano le persone fisiche e non tanto le imprese. Infatti, per queste ultime l’operatività in crypto-attività trova(va) di regola riscontro nelle registrazioni contabili e la rilevanza fiscale passa(va) attraverso il c.d. “principio di derivazione rafforzata” sancito dall’art. 83, del TUIR³⁸⁷.

Allo stimolo della Banca d’Italia ha risposto il Legislatore che con la Legge 29 dicembre 2022, n. 197 (Legge di bilancio 2023) ha introdotto all’art. 1, commi 126-147, una disciplina tributaria relativa alle crypto-attività. In particolare, colmando un vuoto normativo³⁸⁸, la novella legislativa ha introdotto specifiche disposizioni in ordine alla tassazione delle operazioni relative alle crypto-attività, disciplinando nel seguente ordine: la tassazione a titolo di redditi diversi delle plusvalenze e degli altri proventi realizzati nell’ambito di operazioni relative alle crypto-attività, l’applicazione di un’imposta

³⁸⁷ Cfr. Ghiselli F., *Giù le tasse ma con stile!*, Franco Angeli, 2019, il quale tiene comunque a precisare che la determinazione del reddito d’impresa trova complicazioni nel fatto che nessuno di tali principi (nazionali ed internazionali) dispone di regole specifiche per la rilevazione e valutazione in bilancio delle “crypto-attività”.

³⁸⁸ Come prima indicato, in assenza di una specifica disciplina, precedentemente all’intervento legislativo la regolamentazione fiscale delle crypto-attività era tratta esclusivamente dagli orientamenti giurisprudenziali e dall’interpretazione offerta dai documenti di prassi dell’Agenzia delle Entrate. Tra quest’ultimi si segnala: la Risoluzione n. 72/E del 2 settembre 2016, la risposta ad interpello n. 788 del 24 novembre 2021, la risposta ad interpello DRE Lombardia n. 956/39/2018, la risposta n. 110 del 20 aprile 2020, la risposta ad interpello n. 397 del 1° agosto 2022. Tra i primi, invece, si segnala a livello nazionale nella recente sentenza della Corte di cassazione n. 44378 del 22 novembre 2022 ed a livello europeo la sentenza del 22 ottobre 2015, nella causa *Hedqvist*, C-264/14, della Corte di giustizia dell’Unione Europea.

sostitutiva³⁸⁹, la concorrenza delle cripto-attività alla formazione del reddito ai fini IRES e IRAP, la possibilità di rivalutare le cripto-attività, la possibilità di effettuare una *voluntary disclosure* per la detenzione di cripto-attività non dichiarate alla data del 31 dicembre 2021, l'applicazione dell'imposta di bollo ai rapporti aventi ad oggetto cripto-attività o di un'imposta sul valore³⁹⁰.

Secondo la nuova disciplina, le plusvalenze realizzate e gli altri proventi percepiti (al di fuori dell'attività d'impresa o di lavoro autonomo) per effetto di operazioni aventi ad oggetto dette cripto-attività, sono assoggettate ad imposizione (aliquota d'imposta 26%), a titolo di reddito diverso, in capo alle persone fisiche³⁹¹.

Per quanto riguarda l'Irpef, il Legislatore ha di fatto confermato la collocazione dei proventi derivanti dalla cripto-attività all'interno dei redditi di natura finanziaria, stabilendo che *«sono redditi diversi se non costituiscono redditi di capitale ovvero se non sono conseguiti nell'esercizio di arti e professioni o di imprese commerciali o da società in nome collettivo e in accomandita semplice, né in relazione alla qualità di lavoratore dipendente: (...) le plusvalenze e gli altri proventi realizzati mediante rimborso o cessione a titolo oneroso, permuta o detenzione di cripto-attività, comunque denominate, non inferiori complessivamente a 2.000 euro nel periodo d'imposta»*. Quindi, il Legislatore si è premurato di fornire una definizione fiscale di cripto-attività stabilendo che con tale termine si intende *«una rappresentazione digitale di valore o di diritti che possono essere trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga»*. Come anticipato, la definizione fiscale di cripto-attività contenuta nella lettera c-sexies) all'art. 67, comma 1, TUIR³⁹², ha mutuato la nozione codificata nel

³⁸⁹ Modificando gli artt. 5, 6 e 7 del D.lgs. n. 461/1997, la Legge di bilancio 2023 ha praticamente riorganizzando la tassazione dei redditi diversi di natura finanziaria rivedendo il regime della dichiarazione, il regime del risparmio amministrato e il regime del risparmio gestito.

³⁹⁰ Tra gli effetti prodotti dalla nuova disciplina si rilava il cambio di rotta rispetto agli orientamenti espressi in sede di prassi dall'Agenzia delle Entrate secondo la quale eventuali plusvalenze relative alle valute virtuali dovevano assimilarsi a quelle relative alle valute estere, ai sensi della lett. c-ter) dell'art. 67 del TUIR.

³⁹¹ Analoga disciplina si applica agli enti non commerciali per i redditi conseguiti al di fuori dell'attività d'impresa, alle società semplici ed equiparate ai sensi dell'art. 5 del TUIR. ed ai soggetti esteri senza stabile organizzazione in Italia per i redditi ivi prodotti ai sensi dell'art. 23 del TUIR.

³⁹² L'attuale testo normativo è stato introdotto con la Legge di Bilancio 2023 (L. 197 del 29/12/2022) che è intervenuta a regolamentare ai fini fiscali il settore delle cripto-attività, il cui regime di tassazione lasciava agli operatori non solo svariati dubbi applicativi, ma anche ampi spazi di possibile evasione ed occultamento di imponibili.

Regolamento *MiCA*, per cui in sede esegetica del fenomeno in questione ci pare utile fare riferimento anche alla corrispondente definizione europea, sebbene occorra fin d'ora osservare che la nozione fiscale non prevede le specifiche esclusioni previste dal *MiCA*³⁹³. Ciò potrebbe implicare innanzitutto che, analogamente a quanto avvenuto in sede di *MiCA*, nella definizione fiscale possano rientrare tutte quelle rappresentazioni digitali di valore o di diritti che non sono suscettibili di rientrare in una definizione di strumento finanziario³⁹⁴. In quest'ottica di idee, pare che l'Amministrazione finanziaria consideri in termini del tutto residuali la disciplina di recente introduzione³⁹⁵. Trattasi evidentemente di una posizione che al momento non trova alcun esplicito riferimento normativo³⁹⁶.

L'ampia formulazione della norma consente, in via introduttiva, di annoverare tra le cripto-attività la gran parte dei "prodotti digitali" che utilizzano i registri distribuiti³⁹⁷. Come già schematicamente nel secondo capitolo, vi rientrano sicuramente *crypto-asset* come, ad esempio, *bitcoin*, *ethereum*, e gli *stablecoin* quali *USD Tether*, *USD Coin*. Allo stesso modo, rientrano nella nozione di cripto-attività anche gli *NFT* e la Finanza Decentralizzata meglio conosciuta come *DeFi*³⁹⁸.

La scelta operata dal Legislatore si discosta, quindi, da quella operata in sede di normativa antiriciclaggio, sia in termini terminologici, avendo individuato l'oggetto di definizione

³⁹³ Cfr. circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate, la quale espressamente evidenzia che nell'ottica della nuova disciplina fiscale delle cripto-attività, le attività che non costituiscono investimenti di natura strettamente finanziaria debbono essere disciplinate secondo i dettami dell'art. 67, comma 1, lettere da c) a c-*quinquies*) del TUIR.

³⁹⁴ In tal senso la circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate, nella quale viene evidenziato che la nozione di cripto-attività è volta ad individuare una serie di attività che non costituiscono investimenti di natura strettamente finanziaria, la cui disciplina è già contenuta nelle lettere da c) a c-*quinquies*) del comma 1 dell'articolo 67 del TUIR.

³⁹⁵ Nello specifico la circolare sulle criptovalute stabilisce che la disciplina fiscale introdotta in materia di cripto-attività ha carattere residuale.

³⁹⁶ Contrariamente a quanto si riscontra sul piano fiscale, la proposta di Regolamento *MiCA* dal quale è mutuato la nozione di cripto-attività recita espressamente che «*Le cripto-attività assimilabili a "strumenti finanziari" quali definiti all'articolo 4, paragrafo 1, punto 15, della direttiva 2014/65/UE dovrebbero pertanto continuare a essere disciplinate dalla vigente legislazione generale dell'Unione, compresa la direttiva 2014/65/UE, indipendentemente dalla tecnologia utilizzata per la loro emissione o il loro trasferimento*».

³⁹⁷ Per Capaccioli S., *La tassazione delle attività digitali*, 2023, p. 240, la definizione tributaria introdotta nell'ordinamento domestico costituisce una nozione "quasi omnicomprensiva", potendovi ricomprendere i *NFT*, la *DeFi* e i *token* sottesi alle *Decentralized Autonomous Organization*.

³⁹⁸ Cfr. Capaccioli S. e Deotto D., *Disciplina tributaria delle cripto-attività: novità in chiaroscuro*, il Fisco, n. 4/23, p. 315 e ss.

con il termine “valuta virtuale” anziché “cripto-attività” che di approccio metodologico, avendo definito le valute virtuali con approccio di tipo funzionale.

In sede di disciplina, è stato in estrema sintesi previsto che ai fini Irpef le plusvalenze e gli altri proventi derivanti da cripto-attività debbano essere tassate con un'aliquota del 26% a condizione che nel periodo d'imposta esse raggiungano complessivamente il valore di €2.000. Anche in termini di fattispecie imponibile, come facilmente rilevabile, la formulazione della norma è molto ampia facendoci rientrare ogni fenomeno reddituale riconducibile alla “detenzione”, “rimborso”, “permuta” e “cessione a titolo oneroso” di cripto-attività. Sul punto, la circolare sulle criptovalute dispone che rientrano nella categoria reddituale dei redditi diversi, i proventi e le plusvalenze derivanti dalle seguenti operazioni in *cripto-attività*:

- cessione a pronti, permuta (a condizioni che abbiano diverse caratteristiche e funzioni) e rimborsi di cripto-attività;
- cessione a termine di cripto-attività non costituenti strumenti finanziari in forma digitale³⁹⁹;
- attività di *staking*;
- cessione a titolo oneroso di *utility token*. A tal proposito, viene espressamente escluso che l'acquisto del bene o servizio a prezzo scontato per effetto dell'esercizio del diritto possa costituire reddito;
- cessione di *NFT* già “emessi”⁴⁰⁰.

Così facendo l'Amministrazione finanziaria prende una posizione ufficiale sulle fattispecie imponibili di più semplice soluzione, lasciando di fatto l'interprete nell'incertezza di fronte alle fattispecie più complesse.

³⁹⁹ La circolare sulle criptovalute ribadisce l'estraneità degli investimenti di natura strettamente finanziaria (cc.dd. *investment token* o *security token*) dall'ambito applicativo della disciplina in argomento, corrispondendo a strumenti finanziari previsti dalla *MiFID II*.

⁴⁰⁰ In merito, la circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate, precisa che la cessione degli *NFT* da parte dell'autore fuori dall'esercizio d'impresa, costituisce reddito di lavoro autonomo ai sensi e per gli effetti dell'art. 53, comma 2, lettera b), del TUIR ovvero redditi diversi ai sensi dell'art. 67, comma 1, lettera l), dello stesso testo unico.

Iniziando dalla fattispecie di “rimborso di crypto-attività”, in dottrina è stato evidenziato che il concetto di “rimborso” non si addice propriamente a tutte le crypto-attività, potendolo a prima vista escludersi nel caso delle criptovalute ed ammetterlo per talune tipologie di *token* rappresentativi⁴⁰¹.

Anche il riferimento alla “detenzione” è foriero di incertezze applicative. La dottrina che si è per prima occupata di esaminare la novella legislativa considera il riferimento alla “detenzione” come una sorta di chiusura del sistema, inteso ad attrarre nei redditi diversi proventi altrimenti non inquadrabili (*Airdrop, Decentralized Finance, Faucet, Play to earn*, etc.), di natura e provenienza eterogenea. Allo stesso tempo, la stessa dottrina evidenzia la difficoltà di individuare la fattispecie impositiva dato che sovente l’utente non ha alcuna conoscenza (e talvolta conoscibilità senza interventi tecnici) dell’esistenza del provento⁴⁰². Ciò non toglie il fatto che il riferimento alla mera detenzione contrasta con la regola generale sulla fiscalità dei beni che impone l’imposizione solamente all’atto del realizzo.

Un’ulteriore fattispecie impositiva è stata ravvisata nella “permuta”, con esclusione dall’ambito applicativo dell’imposta dell’operazione di scambio aventi ad oggetto “*cripto-attività aventi eguali caratteristiche e funzioni*”. Anche in questo caso, per la dottrina più avveduta la formula utilizzata dal Legislatore è foriera di incertezze applicative stante il fatto che in teoria nessuna crypto-attività è uguale alle altre⁴⁰³ e che la loro eterogeneità rende il riferimento del tutto inconferente⁴⁰⁴. Sul punto, è stato sostenuto che nelle intenzioni del Legislatore la permuta tra crypto-attività non assume rilevanza fiscale, mentre

⁴⁰¹ Per Capaccioli S., *La tassazione delle attività digitali*, 2023, p. 241, la nozione di “rimborso” potrebbe assumere un significato a-tecnico, includendovi forme di ristoro in caso di truffe o di sostituzione di *token*, senza che ciò possa integrare il concetto di permuta. A sottolineare il fatto che si tratti di un’ipotesi piuttosto infrequente anche Avella F., *L’Irpef sulle crypto-attività dopo la legge di Bilancio 2023*, in *Bitcoin e crypto-attività*, Il Sole 24 ore, 2023, p. 67.

⁴⁰² Cfr. Capaccioli S. e Deotto D., *Disciplina tributaria delle crypto-attività: novità in chiaroscuro*, Il Fisco, n. 4, 2023, p. 315 e ss.

⁴⁰³ Cfr. Capaccioli S., *La tassazione delle attività digitali*, 2023, p. 241.

⁴⁰⁴ Cfr. Capaccioli S. e Deotto D., *Disciplina tributaria delle crypto-attività: novità in chiaroscuro*, Il Fisco, n. 4, 2023, p. 315 e ss.. Secondo gli autori chi ha scritto la norma voleva intendere - come risulta dai documenti accompagnatori - che non assumono rilevanza «*lo scambio tra valute virtuali, mentre assume rilevanza fiscale l’utilizzo di una crypto-attività per l’acquisto di un bene o un servizio o di una altra tipologia di crypto-attività (ad esempio utilizzo di una crypto currency per acquistare un Non Fungible Token) o la conversione di una crypto currency in euro o in valuta estera*». Nutrono, invece, forti dubbi, gli stessi autori rispetto alla rilevanza fiscale in termini di plusvalenza dell’operazione di acquisto di un *NFT* attraverso l’utilizzo di una valuta virtuale come per esempio *ether*.

il passaggio da valuta virtuale a valuta *fiat*, oppure l'utilizzo della valuta per acquistare beni o servizi assume rilevanza fiscale⁴⁰⁵

Ai fini applicativi, in dottrina l'espressione "*aventi eguali caratteristiche e funzioni*" è stata valorizzata collegando il concetto di "funzione" alla distinzione tra rappresentazioni digitali di valori e rappresentazioni digitali di diritti, ed il concetto di "caratteristiche" all'utilizzo della tecnologia di registro distribuito o di tecnologia analoga⁴⁰⁶.

La fattispecie della cessione a titolo oneroso, invece, trova un esplicito riferimento normativo nell'art. 9, comma 5 del TUIR ai sensi del quale *«ai fini delle imposte sui redditi le disposizioni relative alle cessioni a titolo oneroso valgono anche per gli atti a titolo oneroso che importano costituzione o trasferimento di diritti reali di godimento e per i conferimenti in società»*. Una volta tratteggiate le fattispecie imponibili, è utile richiamare talune ipotesi astrattamente non riconducibili a quest'ultime. Sulla base della lettera della disposizione, infatti, è evidente come talune operazioni che tipicamente interessano le cripto-attività rimangano fuori dalla portata applicativa della norma. Nel caso, ad esempio, del trasferimento di cripto-attività da una tipologia di *wallet* ad un'altra dello stesso contribuente non si verifica alcuna delle fattispecie impositive tratteggiate dalla norma. Di converso, invece, rimangono dubbi sul trattamento fiscale degli ammanchi di cripto-attività per perdita o furto delle chiavi private dei *wallet*, attacchi informatici o truffe nei confronti degli *exchange* o altri operatori presso cui erano custodite cripto-attività, ecc.

La determinazione della base imponibile è, invece, disciplinata dal nuovo comma 9-bis dell'art. 68 del TUIR a mente del quale *«le plusvalenze di cui alla lettera c-sexies) del comma 1 dell'articolo 67 sono costituite dalla differenza tra il corrispettivo percepito ovvero il valore normale delle cripto-attività permutate e il costo o il valore di acquisto. Le plusvalenze di cui al primo periodo sono sommate algebricamente alle relative minusvalenze; se le minusvalenze sono superiori alle plusvalenze, per un importo superiore a 2.000 euro, l'eccedenza è riportata in deduzione integralmente dall'ammontare delle*

⁴⁰⁵ Cfr. Capaccioli S., *La tassazione delle attività digitali*, 2023, p. 241, il quale richiama la Relazione illustrativa alla legge nella parte in cui recita *«non assume rilevanza lo scambio tra valute virtuali, mentre assume rilevanza fiscale l'utilizzo di una cripto-attività per l'acquisto di un bene o un servizio o di una altra tipologia di cripto-attività (ad esempio, l'utilizzo di una criptocurrency per acquistare un non fungible token) o la conversione di una currency in euro o in valuta estera»*.

⁴⁰⁶ Cfr. Capaccioli S., *La tassazione delle attività digitali*, 2023, p. 242.

plusvalenze dei periodi successivi, ma non oltre il quarto, a condizione che sia indicata nella dichiarazione dei redditi relativa al periodo di imposta nel quale le minusvalenze sono state realizzate. Nel caso di acquisto per successione, si assume come costo il valore definito o, in mancanza, quello dichiarato agli effetti dell'imposta di successione. Nel caso di acquisto per donazione si assume come costo il costo del donante. Il costo o valore di acquisto è documentato con elementi certi e precisi a cura del contribuente; in mancanza il costo è pari a zero. I proventi derivanti dalla detenzione di cripto-attività percepiti nel periodo di imposta sono assoggettati a tassazione senza alcuna deduzione».

Rispetto agli altri redditi diversi, la norma non contempla la possibilità di scomputare gli oneri inerenti alla produzione di plusvalenze e minusvalenze come nel caso delle commissioni applicate dagli *exchange* centralizzati per le compravendite⁴⁰⁷.

Con riguardo alle operazioni di permuta di cripto-attività rilevanti fiscalmente, la circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate ritiene che il valore normale della cripto-attività ricevuta da prendere in considerazione sia quello rilevabile al momento sul sito in cui è avvenuto lo scambio.

Infine, le attività *staking* sembrano trovare un riferimento normativo nel comma 9-bis dell'art. 68 del TUIR, nella parte in cui recita *«i proventi derivanti dalla detenzione di cripto-attività percepiti nel periodo di imposta sono assoggettati a tassazione senza alcuna deduzione»*.

Con riferimento al diverso tema degli adempimenti, allo scopo di semplificare gli obblighi dichiarativi del contribuente – consentendogli di non indicare il reddito da cripto-attività nella dichiarazione fiscale – sono state apportate modifiche alla normativa relativa alle modalità di applicazione dell'imposta sostitutiva (D. Lgs. n. 461/97):

- estendendola ai redditi derivanti dalle cripto-attività;

⁴⁰⁷ Sul punto, Avella F., *L'Irpef sulle cripto-attività dopo la legge di Bilancio 2023, Bitcoin e cripto-attività* – Il Sole 24 Ore, 2023, p. 70 ritiene che gli oneri inerenti alla produzione di plusvalenze e minusvalenze debbano comunque essere scomputati. Di contrario avviso è la circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate

- consentendo la possibilità di assolvere gli obblighi fiscali per il tramite di terzi, aderendo ai regimi opzionali (rispetto al “regime dichiarativo”) del “risparmio amministrato” e del “risparmio gestito”.

In estrema sintesi⁴⁰⁸:

- attraverso il “regime dichiarativo” la tassazione avviene in sede di dichiarazione dei redditi, sommando algebricamente plusvalenze e minusvalenze generate dalle operazioni sulle crypto-attività;
- con il “risparmio amministrato” gli intermediari finanziari e gli operatori che gestiscono rapporti e i *wallet* debbono applicare l’imposta sostitutiva su ciascun reddito diverso realizzato ai sensi della lettera c-*sexies*) del comma 1 dell’articolo 67 del TUIR, indipendentemente dal superamento dei €2.000 previsti dalla stessa disposizione, considerando le eventuali minusvalenze in compensazione con le successive plusvalenze realizzate nel medesimo periodo d’imposta o in quelli successivi, ma non oltre il quarto;
- attraverso il “risparmio gestito” l’imposta sostitutiva viene applicata sul risultato netto della gestione maturata rimanendo indifferente il momento della sua effettiva percezione.

Come espressamente indicato dall’art. 21 della Legge n. 197/2022, la nuova disciplina trova applicazione a partire dal 1° gennaio 2023.

3. L’imposta sui redditi delle società (IRES)

Per i soggetti che realizzano un reddito d’impresa, l’art. 1, comma 131 ha inserito il comma 3-bis all’interno dell’art. 110 del TUIR, ove viene previsto che *«in deroga alle norme degli articoli precedenti del presente capo e ai commi da 1 a 1-ter del presente articolo, non*

⁴⁰⁸ Secondo la circolare 30/E del 27 ottobre 2023 dell’Agenzia delle Entrate, non è possibile compensare i redditi diversi di natura finanziaria di cui alle lettere da c) a c-*quinquies*) del comma 1 dell’articolo 67 del TUIR, con i redditi diversi derivanti dalle crypto-attività.

concorrono alla formazione del reddito i componenti positivi e negativi che risultano dalla valutazione delle cripto-attività alla data di chiusura del periodo di imposta a prescindere dall'imputazione al conto economico».

In tale maniera, si è proceduto a sterilizzare i fenomeni valutativi riguardanti le *cripto-attività*, a prescindere dalle modalità con cui esse sono iscritte in bilancio e dalla rilevazione a conto economico dei componenti (positivi o negativi) derivanti da detti fenomeni.

Pertanto, il Legislatore ha scelto per le cripto-attività un approccio simile a quello previsto per le operazioni in valuta. Se si escludono le disposizioni relative alla valutazione delle cripto-attività, le novità introdotte dalla Legge di bilancio 2023 non riguardano direttamente i redditi conseguiti nell'ambito dell'attività d'impresa, per cui si deduce che le fattispecie imponibili debbano essere disciplinate secondo le ordinarie regole sul reddito d'impresa. Di conseguenza, in forza del cd. principio di derivazione rafforzato, assumerà prioritariamente rilievo l'inquadramento contabile adottato, per cui è necessario preliminarmente esaminare il trattamento contabile delle cripto-attività.

3.1. Il trattamento contabile delle cripto-attività

Le modalità di contabilizzazione delle cripto-attività rappresentano un aspetto importante del procedimento di redazione di un bilancio veritiero e corretto, con evidenti riflessi sul piano tributario. Le difficoltà in termini di inquadramento giuridico delle cripto-attività ha evidentemente influenzato la tematica relativa alla rappresentazione contabile delle stesse cripto-attività, tant'è che né a livello domestico né a livello internazionale è stato dedicato alcun chiarimento ufficiale sul corretto trattamento contabile delle cripto-attività⁴⁰⁹. In particolare, ad oggi non ci sono indicazioni in proposito né a livello codicistico, dato che gli articoli 2423 e ss. cod. civ. non dispongono alcunché sul tema, né a livello di *standard setter* nazionale ed internazionale, non avendo l'*OIC* e lo *IASB* ancora affrontato la tematica nei propri documenti ufficiali.

⁴⁰⁹ Cfr. Greco D. e Catinari E., *Criptovalute: spunti operativi alla luce della Manovra 2023*, Fiscalità e comm. inter., n. 3, 2023, p. 60 e ss, i quali osservano che nel mondo è possibile riscontrare differenti qualificazioni giuridiche attribuite alle valute virtuali (si va da Paesi che qualificano le criptovalute in termini di moneta a Paese che individuano in esse degli investimenti o vere e proprie *commodity*) con altrettanti diversi trattamenti contabili.

In verità, l'*IFRS Interpretations Committee* (Ic)⁴¹⁰, che interpreta i principi contabili internazionali – su richiesta dello *IASB* (*International Accounting Standards Board*) – si è espressa in merito al trattamento contabile da riservare alle cripto-attività. Specificando che le valute virtuali non sono sicuramente attività finanziarie in quanto non soddisfano le condizioni che inquadrano le predette attività nello *IAS 32*, nel *paper 12* del giugno del 2019 l'IC ha concluso a favore della qualificazione di tali *asset* come rimanenze, da contabilizzare secondo lo *IAS 2*⁴¹¹, se detenute per la vendita nell'ambito dell'attività ordinaria⁴¹², oppure – in caso contrario – come attività immateriali da contabilizzare secondo lo *IAS 38*. È evidente che la diversa scelta di classificazione contabile ha riflessi sia sul criterio di valutazione che, conseguentemente, sulla rappresentazione in bilancio. Nello specifico, lo *IAS 38* consente la scelta tra la valutazione al costo oppure al *fair value*, mentre lo *IAS 2*, consente l'iscrizione iniziale delle rimanenze in bilancio al costo e la successiva valutazione al minore tra il costo e il valore netto di realizzo. Contestualmente, in tale occasione è stato escluso che le valute virtuali potessero essere ricondotte alle nozioni di:

- ***financial asset***, in quanto non correlate ad un'attività sottostante o ad una controparte;
- ***moneta***, non attribuendo a chi le possiede il diritto contrattuale di ricevere denaro o altri *financial asset*;
- ***cash equivalent***, a causa dell'elevata instabilità di prezzo cui sono soggette che contrasta con le caratteristiche proprie di quest'ultimi ravvisabili principalmente nella possibilità di essere prontamente convertibili in un ammontare noto di denaro per far fronte ad impegni di liquidità e ridurre il rischio di insolvenza dell'ente che detiene tale

⁴¹⁰ Trattasi dell'organo interpretativo dell'*International Accounting Standards Board*. Il Comitato delle Interpretazioni collabora con il Consiglio per sostenere l'applicazione degli *IFRS*.

⁴¹¹ Tale trattamento viene messo in dubbio dalla *American Institute of Certified Public Accountants* (*AICPA*), in quanto le valute virtuali mancano di consistenza fisica. Nella pubblicazione "*Accounting for and auditing of digital assets*" del 2020 l'*AICPA* conclude quindi che le valute virtuali devono essere considerati "attività immateriali" ai fini contabili, indipendentemente dalla loro destinazione.

⁴¹² Tale inquadramento potrebbe valere ad esempio per gli operatori specializzati in criptovalute come *exchange* o i *wallet provider*, potenzialmente interessati a mantenere scorte di queste attività, oppure quelli che lo *IAS 2* definisce *commodity broker-traders*.

attività/passività.

Ciò stante, l'IC ha escluso che le cripto-attività possano avere natura monetaria e che possano dunque essere contabilizzati tra le disponibilità liquide o tra gli strumenti finanziari. Sul punto, occorre, comunque, osservare che l'orientamento sopra espresso dall'IC non pare sia più sufficiente a rappresentare l'odierna categoria criptovalutaria che è, peraltro, in continua ed incessante evoluzione⁴¹³.

Infine, occorre richiamare la posizione espressa dal *Financial Accounting Standards Board (FASB)* che nell'ambito del progetto “*Accounting for and Disclosure of Crypto Assets*” ha affermato che i *crypto-asset* vanno in ogni caso valutati al *fair value*, pur senza fornire alcuna specifica classificazione degli stessi⁴¹⁴. Allo stesso tempo, nel *Memorandum* del 1° settembre 2022 il *FASB* afferma che rientrano nell'ambito del progetto i *crypto-asset* che soddisfano la definizione di *intangible asset*, e ne sono esclusi gli *utility token* e i *non fungible token (NFT)*.

Sul piano nazionale, pur non registrandosi posizioni ufficiali, giova comunque richiamare le perplessità espressa dall'OIC in sede di *Tentative agenda decisions* del Comitato *IAS/IFRS* presentate in data 30 maggio 2019⁴¹⁵, sulla possibilità di ricondurre le *cryptocurrencies* ai beni immateriali, senza, tuttavia, proporre alcuna classificazione alternativa. A questo punto, posto che appare allo stato da escludere l'evenienza di qualificare le cripto-attività in termini di disponibilità liquide (*OIC 14*), crediti (*OIC 15*) o strumenti finanziari (*OIC 32*), e considerato che non ci sono sostanziali differenze in termini di definitori tra l'*OIC 24* (paragrafo 9) e lo *IAS 38* (paragrafi 8 e ss.), al pari di ciò che accade accostando l'*OIC 13* (paragrafo 4) e il citato *IAS 2*, nonostante le richiamate perplessità dell'OIC espresse nella discussione in seno al Comitato *IAS/IFRS*, in dottrina è stata sostenuta l'applicazione in via analogica dell'*OIC 24* e dell'*OIC 13* con possibilità di

⁴¹³ Per Pedotti P., *Gli aspetti contabili delle criptovalute*, in *Amministrazione e finanza*, n. 5, 2022, p. 35, la posizione assunta dallo *IASB Interpretation Committee* nel 2019, ad oggi forse non è più sufficiente a rappresentare le nuove valute in corso, e l'evoluzione sul tema a livello di *standard setter*.

⁴¹⁴ [FASB, Accounting for and Disclosure of Crypto Assets, 2023.](#)

⁴¹⁵ Cfr. [OIC, Re: IFRS Interpretations Committee tentative agenda decisions published in the March 2019 IFRIC update, 2019.](#)

trattare contabilmente le cripto-attività alternativamente come⁴¹⁶:

- “immobilizzazioni immateriali” laddove presentino la potenzialità di generare benefici economici lungo un arco temporale di più esercizi e siano destinate ad essere possedute come attività e non come beni per la vendita nel normale svolgimento dell’attività d’impresa;
- “rimanenze” laddove l’impresa le destini tipicamente alla vendita nel normale svolgimento della sua attività.

Questa prospettiva troverebbe altresì sostegno dal principio contabile nazionale n. 11, secondo cui *«laddove un principio contabile internazionale risulti conforme ai postulati previsti nell’OIC 11, e non vi siano altri OIC applicabili in via analogica, possa essere preso a riferimento dal redattore del bilancio nello stabilire di caso in caso una politica contabile appropriata»*. Tale modalità di contabilizzazione non sembra coincidere con la prassi amministrativa manifestata nella risoluzione n. 72/E del 2 settembre 2016 e nella successiva risposta n. 14 del 28 settembre 2018, dove l’Agenzia delle Entrate ha affermato che le valute virtuali dovrebbero essere trattate alla stregua di valute tradizionali anche ai fini contabili. Tuttavia, occorre osservare che la citata prassi si riferisce ad un periodo antecedente alla disciplina tributaria introdotta dalla Legge di bilancio 2023 e non rispecchia più per la gran parte l’assetto regolamentare introdotto dalla novella legislativa. Altra dottrina, quindi, sostiene che l’orientamento interno sia che le valute virtuali debbano essere invece classificate nel bilancio d’esercizio come immobilizzazioni finanziarie o attività finanziarie a breve termine, a seconda dell’utilizzo che l’utente intende farne, adottando per la scelta classificatoria un criterio di distinzione di tipo “funzionale”⁴¹⁷.

⁴¹⁶ Avella F., *L’imposizione diretta sulle cripto-attività per i soggetti passivi imprenditori, Bitcoin e cripto-attività*, Il Sole 24 ore, 2023, p. 105.

⁴¹⁷ Cfr. Greco D. e Catinari E., *Criptovalute: spunti operativi alla luce della Manovra 2023*, Fiscalità e comm. inter., n. 3, 2023, p. 60 e ss, per i quali la classificazione nel bilancio d’esercizio in termini di attività finanziarie dipende dall’effettiva finalità dell’acquisto delle valute virtuali che, a seconda dei casi, può comportare che queste siano mantenute nel patrimonio aziendale per un arco temporale più (nel qual caso andrebbero iscritte tra le “immobilizzazioni finanziarie”) o meno lungo (nel qual caso andrebbero iscritte tra le “Attività finanziarie che non costituiscono immobilizzazioni”). Gli autori precisano che qualora le criptovalute siano oggetto dell’attività d’impresa alla chiusura dell’esercizio esse vanno iscritte nella voce C), al numero I, dell’attivo patrimoniale denominata “Rimanenze”.

In conclusione, non esiste al momento un orientamento ufficiale. L'assenza di regole precise non è senza effetti in quanto la diversa classificazione e qualificazione incide sulla valutazione di tali attività, che può essere effettuata al costo di acquisto ovvero al valore di mercato (*fair value*), al lordo o al netto di oneri accessori, e sulla necessità di procedere o meno all'ammortamento.

3.2. La tassazione delle cripto-attività nell'ambito del reddito d'impresa

A questo punto, considerato che la normativa in tema di redditi d'impresa per ragioni sistematiche non contempla alcuna definizione di cripto-attività, si ritiene opportuno fare riferimento alla nozione recata nel più volte citato art. 67 del TUIR, nonostante la norma stessa si premuri di specificare che la definizione è resa «*ai fini della presente lettera*». Tale rinvio reca con sé le criticità riscontrate in sede di analisi con riferimento alle difficoltà di circoscrivere l'ampia portata applicativa della norma definitoria.

In tale occasione, è stato ritenuto che l'ambito applicativo della normativa non riguarda quelle rappresentazioni digitali suscettibili di rientrare in una definizione di strumento finanziario. Tale indirizzo esegetico non è privo di effetti, visto che in caso contrario potrebbe accadere che dinanzi, ad esempio, di un *security token* che abbia le caratteristiche tali da essere assimilabile alle azioni si correrebbe il rischio di poter applicare il regime di *participation exemption*.

Altrettanto scarna (per non dire inesistente) appare la normativa in ordine agli aspetti realizzativi della fattispecie che si occupa esplicitamente della sola valutazione delle cripto-attività, per cui occorrerà fare riferimento alle normali regole di determinazione del reddito d'impresa. A tal proposito, in assenza di una speciale normativa assumeranno rilievo il trattamento contabile concretamente assunto in virtù del principio di derivazione rafforzata ex art. 83 del TUIR, secondo il quale ai fini della determinazione del reddito d'impresa «*valgono, anche in deroga alle disposizioni dei successivi articoli della presente sezione, i criteri di qualificazione, imputazione temporale e classificazione in bilancio previsti dai rispettivi principi contabili*». Sul punto, si richiama l'esito (incerto) cui si è pervenuti nel precedente paragrafo in ordine al trattamento contabile delle cripto-attività. Sulla base della classificazione concretamente adottata in sede di bilancio delle cripto-attività, si

applicheranno quindi le seguenti disposizioni⁴¹⁸:

- per i beni immateriali e attività finanziarie immobilizzate, gli articoli 86 e 101 del TUIR;
- per le attività finanziarie attivo circolante o altre rimanenze, l'articolo 85 del TUIR.

In ogni caso, il valore fiscale delle crypto-attività è determinato applicando le previsioni di cui all'articolo 9 del TUIR. Nel caso specifico dei proventi derivanti dalla detenzione di crypto-attività (derivanti cioè da *staking*, *yieldfarming*, *savings*, *lockdrop*, ecc.), la dottrina ritiene che vadano tassati, quando accreditati nel *wallet* dell'impresa, quali sopravvenienze attive ex art. 88 TUIR⁴¹⁹. Seguendo tale orientamento, sul piano applicativo potranno verificarsi diverse ipotesi. Ad esempio, le cessioni degli *utility token* da parte della società emittente sono escluse dall'IRES qualora siano rappresentate contabilmente come una mera movimentazione finanziaria⁴²⁰.

Sotto l'aspetto valutativo, invece, la legge di bilancio 2023, apportando modifiche all'art. 110 del TUIR, ha stabilito che i componenti positivi e negativi che risultano dalla valutazione delle crypto-attività non concorrono alla formazione del reddito ai fini dell'imposta sul reddito delle società (IRES) e dell'imposta regionale sulle attività produttive (IRAP). A tal proposito, la circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate, l'Amministrazione finanziaria ha chiarito che sono fiscalmente irrilevanti le valutazioni operate in bilancio a prescindere dalle modalità di contabilizzazione delle crypto-attività. Conseguentemente, il contribuente sarà obbligato ad apportare le corrispondenti variazioni in aumento o in diminuzione, a seconda della circostanza che le crypto-attività siano rilevate in bilancio come dei beni immateriali, rimanenze di beni materiali o di attività finanziarie, attività finanziarie immobilizzate.

⁴¹⁸ In tal senso anche la circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate.

⁴¹⁹ Avella F., *L'imposizione diretta sulle crypto-attività per i soggetti passivi imprenditori, Bitcoin e crypto-attività*, Il Sole 24 ore, 2023, p. 101.

⁴²⁰ Cfr. circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate.

4. Altri redditi

Nell'ottica di considerare la nuova disciplina sulle cripto-attività in termini residuali, si ritiene tornino in generale applicabili le categorie reddituali proprie di ciascun bene/diritto secondo un'analisi *case by case* il cui corollario è la prevalenza della sostanza sulla forma. In tale ottica, ai compensi erogati dalla società emittente ai propri amministratori e dipendenti sotto forma di *token*, si renderà applicabile la disciplina dei redditi di lavoro dipendente di cui all'articolo 49 del TUIR nonché di redditi assimilati a quelli di lavoro dipendente di cui all'articolo 50, comma 1, lettera c-bis), del TUIR. Per tali redditi vale in generale il principio di onnicomprensività, per cui costituisce reddito imponibile per il dipendente, ovvero per l'amministratore di società *«tutte le somme ed i valori in genere a qualunque titolo percepiti nel periodo d'imposta, anche sotto forma di erogazioni liberali, in relazione al rapporto di lavoro»*. Pertanto, nel caso sopra prospettato, è stato ritenuto che le erogazioni costituiscono reddito di lavoro dipendente assoggettabile alla ritenuta d'acconto di cui all'art. 23 del d.P.R. 29 settembre 1973, n. 600, a condizione che il valore della remunerazione superi, per ciascun percettore, l'importo di € 258,23⁴²¹. Di converso, viene escluso che i *token* assegnati ad amministratori e dipendenti in corrispondenza delle prestazioni di lavoro possano essere considerati in via autonoma come reddito diverso.

Sulla stessa falsariga occorre affrontare il caso dei redditi derivanti dai cc.dd. *investment token* (o *security token*) e qualificabili come uno strumento finanziario, sui quali la circolare sulle criptovalute considera applicabili le disposizioni sui redditi di capitale di cui all'art. 44 del TUIR e sui redditi diversi di natura finanziaria di cui all'articolo 67, comma 1, lettere da c) a c-*quinquies*), del medesimo testo unico⁴²².

A titolo esemplificativo il documento di prassi in consultazione fa l'esempio delle azioni o quote di società emesse sotto forma di *cripto-attività*, ritenendo che la diversa rappresentazione digitale non muti la natura giuridica del corrispondente contratto di società e, per l'effetto, torna applicabile la norma di cui all'articolo 67, comma 1, lettere c) e c-*bis*), del TUIR. Medesime considerazioni valgono per le *cripto-attività* che

⁴²¹ Così la circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate.

⁴²² Sul punto viene richiamata la relazione illustrativa all'articolo 8 del D.L. n. 25 del 2023 la quale chiarisce che *«restano ferme la disciplina impositiva e le modalità di applicazione della stessa prevista per i corrispondenti strumenti finanziari non emessi in forma digitale»*.

costituiscono il sottostante di un contratto derivato (ad es. *contract for difference* o *future*), tassabili secondo la disciplina dell'articolo 67, comma 1, lett. *c-quater*). Sul punto, occorre tuttavia rilevare che in effetti l'orientamento dell'Amministrazione finanziaria non è scevro di incognite posto che il richiamato art. 67, comma 1, lettera *c-quater*), del TUIR non menziona espressamente i derivati su crypto-attività, a meno che non si voglia collocarli all'interno di "ogni altro parametro di natura finanziaria".

In altri termini, con riferimento a tali strumenti non trova applicazione la citata lettera *c-sexies*).

5. L'imposta sul valore aggiunto (IVA)

Le crypto-attività non sono oggetto di una disciplina speciale ai fini dell'IVA né a livello comunitario, tantomeno a livello domestico. Anche in termini di linee guida dell'UE si riscontra un'apprezzabile scarsità. A livello giurisprudenziale, poi, si registra un unico intervento della Corte di giustizia dell'Unione Europea la quale, con la sentenza del 22 ottobre 2015 nella causa *Hedqvist*, C-264/14, ha stabilito che lo scambio di *bitcoin* per una valuta tradizionale è una prestazione di servizi esente da Iva ai sensi dell'articolo 135, paragrafo 1, lettera e), della direttiva IVA, conferendo quindi alle valute virtuali "bidirezionali" lo stesso trattamento IVA delle valute tradizionali. Avendo trattato uno delle plurime forme che può assumere una crypto-attività (il *bitcoin*), sono evidenti i limiti di estensione dei principi di diritto ivi contenuti alle differenti tipologie di attività ed operazioni cui possono riferirsi tali prodotti.

Come più volte chiarito, infatti, le crypto-attività costituiscono una categoria eterogenea, di cui le crypto-valute sono solo una parte. Questa eterogeneità si è ampliata dal diffondersi di forme ibride, collocabili nell'intermezzo di due tipologie di crypto-attività, e di strumenti che nel tempo cambiano la loro natura originaria in base alle scelte operate dal possessore o al verificarsi di (in)determinate circostanze.

Tanto premesso, è evidente che anche (*a fortiori* considerata l'assenza di una speciale normativa) per il settore impositivo (analogamente a quanto avviene nelle imposte sui redditi) vale la regola di effettuare un'analisi *case by case*⁴²³, finalizzata a individuare e

⁴²³ Il cui corollario è la prevalenza della sostanza sulla forma.

valutare mediante un approccio *look through* la reale natura della cripto-attività, la sua funzione nella pratica e gli scopi per i quali è effettivamente utilizzata, andando dunque al di là del nome a esso attribuito dall'emittente anche per finalità commerciali⁴²⁴.

Trattasi del medesimo approccio adottato dall'OCSE nel documento “*Crypto-Asset Reporting Framework (CARF)*”⁴²⁵, approvato ad agosto 2022 e nella proposta di direttiva in materia di cooperazione amministrativa (DAC8). Sulla scorta di tale approccio, vengono di seguito analizzati i casi più frequenti nell'ordine indicato nella più volte menzionata circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate.

5.1. Cripto-attività e servizi connessi

Secondo la Corte di giustizia dell'Unione Europea (sentenza 22 ottobre 2015, causa C-264/14, *Hedqvist*), una *cripto-attività* si qualifica come valuta virtuale quando «*non ha altre finalità oltre a quella di un mezzo di pagamento e che essa sia accettata a tal fine da alcuni operatori*». Di conseguenza, come ribadito anche dal Comitato Iva in “*Guidelines resulting from the 120th meeting of 28 March 2022 - 1045*”, le operazioni aventi ad oggetto tale

⁴²⁴ Cfr. circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate, con richiamo all'OCSE - *Crypto-Asset Reporting Framework (CARF)*. «In molti casi i NFT sono commercializzati come oggetti da collezione. Questa funzione, tuttavia, non impedisce di per sé che un NFT possa essere utilizzato per scopi di pagamento o di investimento. È importante considerare la natura del NFT e la sua funzione nella pratica e non la terminologia o i termini di marketing utilizzati. I NFT che possono essere utilizzati a fini di pagamento o di investimento nella pratica sono *Crypto-Asset* rilevanti. I fornitori di servizi di segnalazione di *crypto-asset* devono quindi valutare caso per caso se un NFT non può essere usato per scopi di pagamento o di investimento, tenendo conto dell'uso comunemente accettato del *crypto-asset*. Gli NFT che sono scambiati su un mercato possono essere utilizzati per scopi di pagamento o di investimento e sono quindi da considerarsi *Crypto-Asset* rilevanti».

⁴²⁵ Si invita, pertanto, alla lettura del [OECD, Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard, 2022](#). «Alla luce del rapido sviluppo e della crescita del mercato dei *Crypto-Asset* e per garantire che i recenti guadagni in termini di trasparenza fiscale globale non vengano gradualmente erosi, nell'aprile 2021 il G20 ha incaricato l'OCSE di sviluppare un quadro che preveda lo scambio automatico di informazioni fiscalmente rilevanti sui *Crypto-Asset*. Nell'agosto 2022, l'OCSE ha approvato il *Crypto-Asset Reporting Framework (CARF)*, che prevede la comunicazione di informazioni fiscali sulle transazioni in *crypto-asset* in modo standardizzato, in vista dello scambio automatico di tali informazioni. Il CARF definisce gli *Asset* criptovalutari rilevanti nell'ambito di applicazione e gli intermediari e altri fornitori di servizi che saranno soggetti alla segnalazione. Nel fare ciò, il CARF incorpora i recenti sviluppi degli standard globali antiriciclaggio del Gruppo di azione finanziaria internazionale. In linea con il CRS, le procedure di due diligence richiedono l'identificazione dei clienti individuali e delle entità, nonché delle loro persone di controllo. Il CARF richiede una rendicontazione su base aggregata, suddivisa per tipo di *Crypto-Asset* e tipo di transazione. Nell'agosto 2022, l'OCSE ha inoltre approvato modifiche al CRS per far rientrare nell'ambito di applicazione alcuni prodotti di moneta elettronica e le valute digitali delle banche centrali. Alla luce del CARF, sono state apportate modifiche per garantire che gli investimenti indiretti in *crypto-asset* attraverso derivati e veicoli di investimento siano ora coperti dal CRS».

fenomeno sono in generale esenti ai fini Iva ai sensi dell'art. 135, par. 1, lett. e) della direttiva 2006/112/CE, trasfuso nell'art. 10, comma 1, n. 3) del D.P.R. n. 633/72⁴²⁶.

In ossequio a tale posizione, nella circolare sulle criptovalute si ritengono esenti da IVA, ai sensi dell'articolo 10, primo comma, n. 3) del decreto IVA, a nulla rilevando le modalità di determinazione e di pagamento del corrispettivo, le seguenti operazioni finanziarie quando effettuate a titolo oneroso:

- i servizi di *digital wallet*;
- il cambio di valuta tradizionale contro valuta virtuale;
- il *mining*;
- l'attività di *staking*.

Con riferimento all'attività di *mining*, l'Amministrazione finanziaria ritiene che l'operazione sia fuori campo IVA nelle ipotesi in cui non sia possibile riscontrare il carattere dell'onerosità della prestazione di servizi. Considerato che l'onerosità di una prestazione implica la sussistenza di un nesso diretto fra il servizio prestato e il corrispettivo ricevuto e che tale nesso risulta acclarato qualora tra il prestatore e il destinatario intercorra un rapporto giuridico nell'ambito del quale avvenga uno scambio di reciproche prestazioni e il compenso ricevuto dal prestatore costituisca il controvalore effettivo del servizio prestato al beneficiario, tale carattere sembra assente nelle ipotesi tipiche del *miner*, in cui viene corrisposta ad un soggetto una remunerazione, in via del tutto automatica, dal sistema, anziché da una controparte ben individuata, all'esito di un'attività che è liberamente esercitata e non costituisce oggetto di alcun obbligo giuridico.

Viceversa, nel caso di attività negozialmente regolamentate da parti ben individuate, tornano applicabili le ordinarie regole poste in materia IVA. Di conseguenza, al ricorrere di tutti i presupposti applicativi, il mining su cripto-attività diventa rilevante ai fini dell'imposta e sottoposto alla disciplina applicabile alla specifica cripto-attività.

⁴²⁶ Così nella circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate.

5.2. *Utility token e Hybrid token*

Le conclusioni del paragrafo precedente si estendono ai *token* (e i servizi a essi connessi) che vengono utilizzati per trasferire denaro e valori o come mezzo di pagamento. Invece, ai *security token* e ai servizi a essi connessi si applica comunemente il regime di esenzione di cui all'art. 10, primo comma, n. 4) del decreto Iva in quanto generalmente hanno natura di strumenti di investimento⁴²⁷.

Con riferimento agli *utility token*, invece, considerata la continua evoluzione che si registra nella specifica categoria, occorre operare valutando *case by case*. In tal modo, allora, si potrà, per esempio, applicare la disciplina IVA contenuta nella c.d. direttiva *Voucher*⁴²⁸, alle ipotesi in cui le caratteristiche dei *token* consentano di assimilarli ai *voucher*. Affinché ciò sia possibile è indispensabile riscontrare la ricorrenza degli elementi essenziali dei *voucher*, che vengono comunemente ravvisati: i) nell'obbligo imposto al potenziale fornitore di accettarli in contropartita alla cessione di beni/prestazione di servizi acquistata e ii) nell'indicazione dei beni/servizi cui darebbe diritto o dell'identità dei potenziali fornitori⁴²⁹. Nel diverso caso in cui i *token* dovessero assumere la natura di titoli di legittimazione di cui all'articolo 2002 c.c., ne muterebbero il relativo trattamento IVA con esclusione dall'applicazione dell'imposta. Da qui la necessità di effettuare un esame del caso specifico per stabilire se un *token* sia un *voucher* piuttosto che uno strumento di pagamento o altro. In generale, quindi, non occorre sempre e comunque ricondurre gli *utility token* nell'ambito della disciplina dei *voucher*⁴³⁰. A tal proposito, sul punto la circolare sulle criptovalute fa propria la posizione della Commissione UE la quale ritiene che un *utility token* non possa essere trattato come un *voucher* quando:

- opera come criptovaluta e quindi potrebbe essere preso in considerazione come un servizio di pagamento;
- non sono sufficientemente dettagliati i beni e/o i servizi cui darebbe diritto, o l'identità dei potenziali fornitori che partecipano alla filiera;

⁴²⁷ Cfr. circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate.

⁴²⁸ La disciplina comunitaria è stata recepita con il d.lgs. n. 141 del 2018.

⁴²⁹ Cfr. risposta a interpello n. 507 del 12 ottobre 2022.

⁴³⁰ Cfr. circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate.

- il suo scopo è passibile di modifica per cui la funzione dello strumento non è ben definita al momento della sua emissione.

5.3. Non Fungible Token (NFT)

Sulla falsariga metodologica finora adottata, l'individuazione della disciplina IVA applicabile ai *NFT* richiede un'analisi preliminare del regolamento negoziale associato ai *NFT* e delle modalità di circolazione, secondo il tipico approccio *case by case*.

Ebbene, considerato che l'*NFT* rappresenta il “veicolo” mediante il quale vengono trasferiti i beni, servizi e diritti che incorpora (c.d. “sottostanti”) nascenti originariamente in forma digitale o fisica, si applica la disciplina Iva relativa al sottostante⁴³¹. Per cui, se il sottostante è un *asset* digitale si applicano le regole Iva proprie dei servizi elettronici e dunque l'IVA diventa esigibile al momento del pagamento del corrispettivo⁴³². Se viceversa il sottostante è un bene materiale si applica la disciplina Iva relativa ai corrispondenti *asset*⁴³³.

6. Gli obblighi di monitoraggio fiscale

Dal 1° gennaio 2023, i possessori diretti o titolari effettivi secondo la normativa antiriciclaggio delle cripto-attività sono obbligati ad indicarle nel Quadro RW del modello Redditi in quanto sono potenzialmente suscettibili di produrre redditi da tassare in Italia a titolo di redditi diversi. Secondo la posizione assunta dall'Amministrazione finanziaria, l'adempimento degli obblighi imposti in tema di monitoraggio fiscale permane al di là dalle modalità di conservazione e archiviazione delle cripto-attività, e senza tener conto del fatto che siano detenute all'estero o in Italia. L'obbligo dichiarativo non sussiste per le cripto-attività affidate in gestione o in amministrazione agli intermediari residenti e per i contratti comunque conclusi attraverso il loro intervento, qualora i flussi finanziari e i redditi

⁴³¹ Cfr. circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate.

⁴³² La circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate tiene a precisare che nell'ipotesi in cui il sottostante è un'opera d'arte digitale la cessione del relativo *NFT* da parte dello stesso autore è fuori campo Iva per carenza del presupposto oggettivo.

⁴³³ La circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate non esclude, peraltro, che al ricorrere dei relativi presupposti, possa essere applicata la disciplina dei *voucher*, come può accadere nell'ipotesi in cui l'*NFT* incorpora servizi che l'acquirente ha diritto di fruire o il diritto a partecipare a una c.d. *community*.

derivanti da tali attività e contratti siano stati assoggettati a ritenuta o imposta sostitutiva dagli intermediari stessi.

7. Rideterminazione del valore delle cripto-attività

In forza della novella legislativa, il Legislatore ha concesso ai i soggetti che non hanno violato gli obblighi di monitoraggio fiscale, la possibilità di rideterminare il valore delle *cripto-attività* detenute alla data del 1° gennaio 2023. A tal fine, l'art. 1, comma 133, della L. n. 197/2022 ha previsto che *«agli effetti della determinazione delle plusvalenze e delle minusvalenze di cui alla lettera c-sexies) del comma 1 dell'articolo 67 del testo unico delle imposte sui redditi, di cui al decreto del Presidente della Repubblica 22 dicembre 1986, n. 917, introdotta dal comma 126, lettera a), del presente articolo, per ciascuna cripto-attività posseduta alla data del 1° gennaio 2023 può essere assunto, in luogo del costo o del valore di acquisto, il valore a tale data, determinato ai sensi dell'articolo 9 del citato testo unico, a condizione che il predetto valore sia assoggettato a un'imposta sostitutiva delle imposte sui redditi nella misura del 14 per cento».*

Sul punto, la circolare sulle criptovalute ha chiarito i seguenti punti:

- il valore al 1° gennaio 2023 va rilevato sulla piattaforma dove è stata acquistata la cripto-attività. In caso ciò non fosse possibile, si potrà fare riferimento ad analoga piattaforma dove le medesime cripto-attività sono negoziate;
- tale valore concorrerà al computo della plusvalenza realizzata nell'ambito delle operazioni fiscalmente rilevanti relative alle cripto-attività
- il nuovo valore preclude la possibilità di realizzare minusvalenze utilizzabili ai sensi del comma 9-bis dell'articolo 68 del TUIR;
- per perfezionare il regime agevolato in argomento, sarà necessario versare l'imposta sostitutiva per l'intero suo ammontare, ovvero in tre rate annuali di pari importo nei termini prestabiliti;
- il contribuente può avvalersi immediatamente del nuovo valore di acquisto ai fini della determinazione delle plusvalenze di cui all'articolo 67, comma 1, lettera c-sexies), del TUIR.

8. Regularizzazione delle cripto-attività

Le persone fisiche, gli enti non commerciali e le società semplici ed equiparate ai sensi dell'articolo 5 del TUIR, residenti in Italia che hanno omesso di indicare nella propria dichiarazione annuale dei redditi le cripto-attività detenute entro la data del 31 dicembre 2021, nonché i redditi sulle stesse realizzati, hanno la possibilità di presentare un'istanza di regolarizzazione⁴³⁴.

Nello specifico, nel primo caso è possibile regolarizzare la propria posizione versando la sanzione per l'omessa indicazione nel Quadro RW del modello Redditi, nella misura ridotta pari allo 0,5 per cento per ciascun anno del valore delle attività non dichiarate⁴³⁵.

I soggetti che hanno invece realizzato redditi nel periodo di riferimento possono regolarizzare la propria posizione attraverso la presentazione dell'istanza e il pagamento di un'imposta sostitutiva, nella misura del 3,5 per cento del valore delle cripto-attività detenute al termine di ciascun anno o al momento del realizzo, nonché di un'ulteriore somma, pari allo 0,5 per cento per ciascun anno del predetto valore, a titolo di sanzioni e interessi, per l'omessa indicazione nel Quadro RW del modello Redditi⁴³⁶.

9. Criticità emergenti e potenziali soluzioni

In sede di prassi, l'Amministrazione finanziaria ha preso atto che le cripto-attività si sono diffuse così rapidamente ed assumendo le forme più svariate da rendere difficile ricondurre il fenomeno ad unitarietà ovvero di *“qualificare “in astratto” e “a priori” le varie fattispecie riscontrabili sul mercato”*⁴³⁷. Infatti, si tratta di un fenomeno dalle forme poliedriche che, pur avendo in comune il fattore tecnologico, non ha natura omogenea né una qualificazione giuridica unica⁴³⁸.

Quanto precede è strettamente connesso al problema definitorio che resta uno degli ostacoli più rilevanti per una più chiara ed efficiente disciplina.

⁴³⁴ Cfr. comma 138 dell'art. 1 della legge 29 dicembre 2022, n. 197

⁴³⁵ Cfr. comma 139 dell'art. 1 della legge 29 dicembre 2022, n. 197

⁴³⁶ Cfr. comma 140 dell'art. 1 della legge 29 dicembre 2022, n. 197

⁴³⁷ Cfr. circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate.

⁴³⁸ Tant'è che, ad esempio, non tutte le cripto-attività possono essere collocate nell'ambito degli strumenti finanziari.

Difatti, l'ampia formulazione della norma definitoria inserita nell'art. 67 del TUIR rischia di attrarre nel suo ambito di applicazione *asset* che ricadono più correttamente in altre fattispecie impositive. È il caso di quegli *asset* fisici che potrebbero venire “*tokenizzati*” con il rischio di essere distolti dal proprio campo di imposizione. L'assenza di ulteriori specificazioni - come può essere la precisazione di escludere le valute virtuali emesse dalle autorità pubbliche o private - rende altresì possibile annoverare al suo interno anche ulteriori fenomeni quali le *CBDC*⁴³⁹, il cui trattamento fiscale non può essere certamente quello adottato per le cripto-attività in generale.

Così com'è confezionata la norma richiederà necessariamente uno sforzo interpretativo per delimitare l'ambito applicativo diretto principalmente a risolvere le inevitabili antinomie che sorgeranno in forza del crescente fenomeno della *tokenizzazione* della ricchezza. In tal senso, sembra muoversi in anticipo l'Amministrazione finanziaria che con la più volte citata circolare sulle criptovalute ha chiarito – seppur apoditticamente senza formulare alcuna argomentazione di sorta – che nella definizione fiscale di cripto-attività rientrano «*tutte quelle rappresentazioni digitali di valore o di diritti che non sono suscettibili di rientrare in una definizione civilistica di strumento finanziario*»⁴⁴⁰ specificando, altresì, che non rientrano nell'ambito applicativo della novella legislativa tutti quei redditi derivanti da cripto-attività suscumbibili nel concetto di strumento finanziario ai sensi della normativa *MiFID II*, a prescindere dal fatto che siano rappresentati digitalmente⁴⁴¹. Ebbene, pur apprezzando l'intervento chiarificatore dell'Amministrazione finanziaria non ci si può esimere dall'osservare che l'interpretazione fornitaci non trova alcun riferimento concreto in sede normativa, riducendosi, in assenza di argomentazioni giuridiche, ad un'astratta petizione di principio.

Ampliando lo sguardo, in una prospettiva sistematica, si colgono gli ulteriori limiti e criticità di una simile impostazione provocati dal carattere eterogeneo del fenomeno crypto. Ci riferiamo a quelle forme ibride di cripto-attività ossia a quegli strumenti che

⁴³⁹ Tali criticità sono state sollevate anche da Avella F., *L'Irpef sulle cripto-attività dopo la legge di Bilancio 2023*, in *Bitcoin e cripto-attività*, Il Sole 24 ore, 2023, p. 67.

⁴⁴⁰ Nella circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate viene espressamente indicato che la definizione di *cripto-attività* operata dal Legislatore fiscale è volta ad individuare una serie di attività che non costituiscono investimenti di natura strettamente finanziaria, la cui disciplina è già contenuta nelle lettere da c) a c-quinquies) del medesimo comma 1 dell'articolo 67 del TUIR.

⁴⁴¹ Cfr. circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate.

nascono come figura intermedia tra due tipologie di cripto-attività, per non dire di quelli che nascono in un modo per poi subire una modificazione in base alle scelte fatte dal possessore, dall'emittente o al verificarsi di (in)determinate circostanze. È fin troppo evidente che in questi casi lo sforzo dell'interprete è messo a dura prova e senza alcun riferimento normativo non crediamo si possano trovare valide e fondate soluzioni giuridiche.

In questo quadro incompleto una possibile soluzione parrebbe essere quella di considerare la norma in tema di cripto-attività in termini del tutto residuali, preferendo in prima battuta sostenere l'applicazione delle alternative disposizioni (in questi termini da considerare "speciali"), in modo tale da assicurare, con approccio sostanzialistico piuttosto che formale, un trattamento unico ai beni e diritti sostanzialmente simili in un'ottica di neutralità tecnologica.

Nel tratteggiare l'ambito applicativo della norma il Legislatore è stato più accorto nel caso delle operazioni *crypto-to-crypto*. In particolare, la nuova disciplina rende fiscalmente irrilevanti le operazioni *crypto-to-crypto*, purché avvengano tra cripto-attività «*aventi eguali caratteristiche e funzioni*». Però, anche in questo caso sono evidenti le difficoltà applicative, soprattutto considerando l'estrema eterogeneità del fenomeno per cui nessuna *crypto* è uguale alle altre. A ciò si aggiungano le ulteriori difficoltà riscontrabili nei casi di *crypto* ibride o di *crypto* che modificano le loro caratteristiche *in itinere*. In assenza di concreti riferimenti normativi si ritiene che possa valere la regola (poc'anzi menzionata) secondo cui bisogna effettuare un'analisi *case by case*, «*finalizzata a individuare e valutare (...) la reale natura della cripto-attività, la sua funzione nella pratica e gli scopi per i quali è effettivamente utilizzata, andando dunque al di là del nome a esso attribuito dall'emittente anche per finalità commerciali*»⁴⁴². Nello specifico, sarebbe forse opportuno valorizzare la distinzione comunemente accolta secondo il criterio della funzione

⁴⁴² Cfr. circolare 30/E del 27 ottobre 2023 dell'Agenzia delle Entrate.

economica dei *crypto-asset*, che individua quattro e diverse categorie: (i) *currency token*, (ii) *security token*⁴⁴³; (iii) *utility token* e (iv) *non-fungible token*⁴⁴⁴.

Sempre con riferimento alla sfera applicativa, le incertezze applicative aumentano se si considera che la nuova disciplina non si cura di definire il concetto di “cripto-attività” rilevante ai fini del reddito d’impresa. In questo caso, l’inquadramento giuridico sembra assumere maggior rilievo se si considera, ad esempio, che dinanzi ad un *security token* che abbia le caratteristiche tali da essere assimilabile alle azioni si porrebbe il dubbio sull’applicabilità o meno del regime di *participation exemption*. Le incertezze nel campo del reddito d’impresa aumentano se si considera che la tematica in ordine al trattamento contabile delle cripto-attività è stata a lungo trascurata dagli standard setter e dalle autorità nazionali, tant’è che ad oggi non esiste alcun documento ufficiale in merito. In questo senso, si auspica che da parte di tutte le parti interessate ci si attivi per fornire delle indicazioni agli operatori. Ecco allora che si ritiene ineludibile un intervento legislativo chiarificatore che fornisca una definizione di cripto-attività che tenga in debita considerazione la natura, le caratteristiche e la funzione di ciascuna forma di *crypto-asset*. Ulteriore fonte di incertezze sono le modalità di determinazione del reddito d’impresa prodotto dalle operazioni relative alle cripto-attività. Infatti, in tutti i casi in cui manchi l’erogazione in euro o altra valuta tradizionale, le plusvalenze, ricavi e sopravvenienze devono essere valorizzati al valore normale ex art. 9 del TUIR. Sul punto, la circolare sulle criptovalute è chiara se non fosse che si limita a confermare tale indicazione di sorta senza, tuttavia, specificare le concrete modalità di determinazione. Trattandosi di un settore soggetto a continue fluttuazioni, anche molto significative, ed in cui il prezzo delle cripto-attività differisce da *exchange* ad *exchange*, non esiste un unico prezzo di riferimento per cui resta difficile stabilire il valore normale. Una soluzione pratica potrebbe essere quella

⁴⁴³ In merito alle *security token* occorre ricordare che secondo l’orientamento indicato nella circolare sulle criptovalute non rientrano «nell’ambito di applicazione della lettera c-sexies) del comma 1 del citato articolo 67 del TUIR, i redditi derivanti dai cc.dd. *investment token* (o *security token*) che corrispondano ad uno strumento finanziario previsto dalla MiFID II, in quanto tali token devono essere considerati a tutti gli effetti strumenti finanziari, indipendentemente dalla circostanza che siano rappresentati digitalmente».

⁴⁴⁴ Cfr. Avella F., *L’Irpef sulle cripto-attività dopo la legge di Bilancio 2023*, in *Bitcoin e cripto-attività*, Il Sole 24 Ore, 2023, p. 6. L’autore pone il caso dello scambio di *stablecoin*, nella forma di individuata dal Regolamento MiCA di *electronic money token*, con *stablecoin* nella diversa forma di individuata dallo stesso Regolamento di *asset-referenced token*. Ebbene essendo diversamente dominate dal Regolamento sorgono dubbi sulla possibilità che possano essere ravvisati eguali caratteristiche e funzioni.

illustrata in sede di risoluzione n. 72/E del 2016, in cui si propone di fare «*riferimento alla media delle quotazioni ufficiali rinvenibili sulle piattaforme on line in cui avvengono le compravendite di bitcoin*». Tuttavia, trattasi di una soluzione parziale adottabile, appunto, per i *bitcoin* rispetto ai quali si riscontra nella realtà una movimentazione significativa. Di converso, negli altri casi occorrerà adottare un criterio differente che tenga in debita considerazione le caratteristiche proprie della cripto-attività oggetto di rilievo. Nel caso di permuta tra cripto-attività, ad esempio, si potrebbe assumere come valore normale quello rilevabile sul sito attraverso il quale è avvenuto lo scambio alla data in cui lo stesso è concluso⁴⁴⁵. Anche in questo caso, però, sarebbe utile una presa di posizione quantomeno da parte dell'Amministrazione finanziaria.

Foriero di incertezze costituisce altresì la specifica previsione per cui il costo o valore di acquisto delle cripto-attività debba essere documentato «*con elementi certi e precisi a cura del contribuente; in mancanza il costo è pari a zero*». Infatti, posto che costituisce regola generale per cui il costo debba essere sempre provato dal contribuente, la previsione di una specifica disposizione rischia di esporre gli stessi contribuenti a richieste connaturate da una più ampia discrezionalità, soprattutto in un settore in cui la reportistica fornita dagli *exchange* centralizzati consiste di file *excel* mentre non vi è una reportistica quando si opera su *exchange* decentralizzati⁴⁴⁶. Ciò stante, è evidente che per superare l'onere probatorio sarà richiesto al contribuente una maggior cura rispetto ai casi simili, procedendo a documentare e ricostruire con dettaglio qualsiasi operazione connessa anche indirettamente ad operazioni con le cripto-attività.

Infine, corre l'obbligo osservare che pur trovando applicazione a partire dal 1° gennaio 2023, il comma 127 della Legge n. 197/2022 prevede con norma di tipo transitorio che «*le plusvalenze relative a operazioni aventi a oggetto cripto-attività, comunque denominate, eseguite prima della data di entrata in vigore della presente legge si considerano realizzate ai sensi dell'art. 67 del Testo Unico delle imposte sui redditi, di cui al Decreto del Presidente della Repubblica 22 dicembre 1986, n. 917, e le relative minusvalenze realizzate*

⁴⁴⁵ Trattasi di un'evenienza suggerita dalla circolare sulle criptovalute ancorché con riferimento ai redditi diversi.

⁴⁴⁶ Cfr. Avella F., *L'Irpef sulle cripto-attività dopo la legge di Bilancio 2023*, in *Bitcoin e cripto-attività*, Il Sole 24 Ore, 2023, p. 70.

prima della medesima data possono essere portate in deduzione ai sensi dell'art. 68, comma 5, del medesimo Testo Unico. Ai fini della determinazione della plusvalenza si applica l'art. 68, comma 6, del predetto Testo Unico». Ebbene, dal tenore letterale della norma parrebbe che il Legislatore voglia applicare l'imposta anche a fattispecie impositive realizzatesi anteriormente all'introduzione della disciplina fiscale con evidenti effetti retroattivi. Nello specifico, la novella legislativa stabilisce che le plusvalenze relative ad operazioni sulle crypto-attività eseguite anteriormente a tale data debbano considerarsi comunque realizzate. Così com'è formulata, la norma "sposta" di fatto in avanti l'effetto (fiscale) del realizzato derogando alla regola generale valevole per le operazioni eseguite successivamente al 2022⁴⁴⁷. Innanzitutto, corre l'obbligo evidenziare che la disposizione non chiarisce il tempo esatto in cui si considererebbe realizzata l'operazione effettuata antecedentemente al 1° gennaio 2023, né l'intervallo temporale da monitorare rispetto alla data di esecuzione di siffatte operazioni. In quest'ultimo caso, è evidente che in assenza di precisi riferimenti si potrebbe paventare l'ipotesi (assurda) di considerare tutte le operazioni aventi ad oggetto le crypto-attività eseguite anteriormente all'entrata in vigore della disciplina senza alcun limite temporale con l'effetto, per esempio, di "tassare" plusvalenze realizzate 10 anni fa, in evidente violazione del principio di capacità contributiva.

In definitiva, pur apprezzando l'intervento novativo del Legislatore, corre l'obbligo di evidenziare che la scarsa disciplina regolatoria è gravida di incertezze solo in minima parte risolte celermente dal documento di prassi in elaborazione. A ciò si aggiunga che la natura ibrida delle *crypto* e l'intrinseca connotazione transfrontaliera del fenomeno richiederebbe un intervento normativo uniforme a livello europeo ed internazionale. Nel complesso, la disciplina tributaria di nuovo conio patisce l'inafferrabilità di un fenomeno difficilmente collocabile nelle tradizionali categorie giuridiche, in cui gli stessi interpreti si trovano di fronte alla primaria difficoltà di inquadrare giuridicamente il fenomeno delle crypto-attività, acuita dalle mutazioni continue e costanti dell'oggetto dell'analisi. Ad aggravare la

⁴⁴⁷ Per Capaccioli S. e Deotto D., *Disciplina tributaria delle crypto-attività: novità in chiaroscuro*, Il Fisco, n. 4, 2023, p. 315 e ss., la disposizione sembra assumere i connotati di una presunzione legale assoluta, e, per l'effetto, da ritenersi illegittima in quanto lesiva del diritto di difesa ex art. 24 Cost.

situazione contribuiscono gli stessi istituti giuridici tributari che in alcuni casi sono inadatti a leggere il nuovo fenomeno.

SEZIONE 3. AMBIENTE: DELUCIDAZIONI E SPUNTI NORMATIVI A FRONTE DEL DISPENDIO ENERGETICO GENERATO DA *CASP* E *DIGITAL ASSET*

1. Ambiente, cripto-attività e *CBDC*: un nesso problematico

Fino a pochi decenni orsono il cambiamento climatico e le sue conseguenze risultavano all'attenzione di pochi ecologisti ed esperti di settore, ma il non più così sporadico sopraggiungere di fenomeni naturali estremi ha reso la questione impellente in ambito politico ed economico⁴⁴⁸. Il tema non è di semplice definizione in quanto richiede l'implementazione di norme programmatiche di una tale portata da investire l'insieme dell'economia globale, oltre che lo stile di vita ed i consumi della popolazione del pianeta. Declinando il discorso nel contesto della finanza crittografica, vari ambienti scientifici, economici e politico-sociali si sono interrogate su come le cripto-attività si posizionino rispetto alla sostenibilità ambientale. Conseguentemente a primi studi e valutazioni che prendono in esame soprattutto il *bitcoin*, ciò che ne è uscito fuori è che le cripto-attività sono accusate di essere tutt'altro che ecosostenibili⁴⁴⁹. Tale percezione è acuita non solo da pubblicazioni scientifiche vertenti sul tema, ma anche dalla lettura dei documenti preparatori del *MiCA*, in cui è previsto l'obbligo in capo ai *CASP* di informare periodicamente l'*ESMA* in merito ai propri consumi così da misurarne l'impatto energetico. In aggiunta a ciò, come accennato nel primo capitolo, nel *Considerando* n. 7 del *MiCA* è esplicitato che «*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*

⁴⁴⁸ [Commissione Europea, Conseguenze dei cambiamenti climatici, Climate action, 2023.](#)

⁴⁴⁹ Vds. [Tavelli A., Bitcoin e sostenibilità ambientale: amici o nemici?, IARI – Istituto Analisi Relazioni Internazionali, 2023.](#) Stando ad alcune stime, il *mining* di *bitcoin* consuma circa 273 *Gigawatt* al giorno. Al riguardo si noti che la città di Tokyo consuma circa 210 *GWh* al giorno mentre l'intero Giappone consuma circa 2,7 *Terawatt* al giorno. Secondo le medesime stime, il consumo energetico annuale di produzione del *bitcoin* è superiore al consumo annuale di alcuni Paesi, come il Belgio, le Filippine od il Kazakhstan visto che consuma circa 100,4 *TWh* all'anno mentre i tre Paesi sopracitati circa 85, 90 e 92, rispettivamente. Ricomprendendo altre valutazioni, la sola rete *Bitcoin* consuma oltre 130 *TWh* l'anno che, sommate a tutte le altre *blockchain* che usano il *Proof of Work* come sistema di certificazione, porta i consumi mondiali a qualche migliaio di *TWh* l'anno. Molto più del consumo annuale dell'intera Italia. [Ruocco A., Ma è vero che il bitcoin consuma davvero tanta energia?, 2022;](#) [Tavelli A., Bitcoin e sostenibilità ambientale: amici o nemici?, 2023;](#) [Soldavini P., Le criptovalute sono energivore? Quanta energia serve per produrle e per gestirle?, 2 maggio 2022.](#)

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». In tale contesto, l'ESMA e l'EBA sono state chiamate ad elaborare progetti di norme tecniche di regolamentazione al fine di specificare «il contenuto, le metodologie e la presentazione delle informazioni in relazione agli indicatori di sostenibilità per quanto riguarda gli impatti negativi sul clima e altri effetti negativi connessi all'ambiente, nonché di delineare i principali indicatori energetici».

Pertanto, obiettivo di questa sezione è illustrare le principali questioni tecniche e organizzative che attanagliano i *CASP* (specie i *miner*) nell'erogazione dei loro servizi e che meriterebbero di essere tenute in considerazione per la stesura di nuove *policy* improntate sul versante energetico ed ambientale⁴⁵⁰. Inoltre, appare interessante notare come queste

⁴⁵⁰ Come afferma l'autore Ruocco, è tuttavia «essenziale distinguere tra consumo di elettricità e impronta ambientale. Il primo riguarda la quantità totale di elettricità utilizzata dal processo di mining. La seconda riguarda le implicazioni ambientali del mining. In definitiva, ciò che conta per l'ambiente non è il livello di consumo di elettricità in sé, ma l'intensità di carbonio delle fonti energetiche utilizzate per generare tale elettricità. Per esempio, a questo riguardo si noti che un chilowattora (kWh) di elettricità generato da una centrale a carbone ha un'impronta ambientale significativamente peggiore di un kWh di elettricità prodotto da un parco eolico. Di conseguenza, l'aumento (o la diminuzione) della domanda di energia elettrica non comporta automaticamente un aumento (o una diminuzione) proporzionale delle emissioni di anidride carbonica e di altri gas serra. I minatori di bitcoin e crypto-asset simili sono presenti in tutto il mondo e di conseguenza utilizzano un'ampia varietà di fonti energetiche. Un sondaggio di settore effettuato nel 2020 ha rilevato che i miner, in quanto in genere tributari dell'elettricità fornita da reti locali alimentate da una composizione variabile di fonti energetiche, presentavano anch'essi un mix di consumi energetici in gran parte costituito da energia prodotta dall'idroelettrico, dal carbone e dal gas naturale, ma utilizzano anche fonti tratte dal petrolio, dal nucleare e dalle fonti rinnovabili (eolica, solare e geotermica). Sebbene la divulgazione delle fonti energetiche stia diventando sempre più comune tra le strutture di hashing, l'esatto mix energetico dell'industria del mining rimane sconosciuto. Diversi studi hanno dimostrato che una quota crescente del consumo totale di elettricità proviene da fonti di energia rinnovabili come l'energia idroelettrica, solare o eolica. Tuttavia, le stime divergono notevolmente, variando da circa il 20%-30% del mix energetico totale a oltre il 70%. Una possibile spiegazione di queste discrepanze può essere trovata nella natura dinamica del mining, che fa fluttuare il mix energetico durante l'anno. Grazie alla relativa mobilità delle apparecchiature di mining, le strutture di hashing possono essere installate in tempi relativamente brevi altrove. Ciò ha portato alcuni minatori a preferire contratti di elettricità off-grid con centrali elettriche in aree remote per le quali i dati disponibili sono scarsi o inesistenti. Inoltre, in alcuni Paesi sono state osservate migrazioni stagionali tra regioni con profili energetici diversi; in particolare in Cina, dove i minatori, fino a poco tempo fa, si riversavano dalla Provincia settentrionale dello Xinjiang, ricca di carbone, alla Provincia Sud-occidentale del Sichuan per beneficiare di un surplus di energia idroelettrica a basso costo durante la stagione dei monsoni. Le stime che non hanno una dimensione temporale non sono in grado di cogliere queste sottigliezze. Tutto ciò che possono fornire è una visione parziale basata su un'unica istantanea in un momento specifico. Poiché il mix energetico del bitcoin non è statico, una corretta valutazione ambientale del mining richiede un monitoraggio e un'analisi continui. Poiché il mercato del mining sta subendo cambiamenti significativi in seguito al giro di vite imposto dal Governo cinese nel giugno 2021, sono necessarie ulteriori ricerche e dati per valutare come la redistribuzione globale dell'hashrate influisca sul mix energetico e sull'intensità di carbonio della rete». [Ruocco A., Ma è vero che il bitcoin consuma davvero tanta energia?, 2022.](#)

difficoltà non coinvolgano esclusivamente i *CASP*, ma anche colossi tecnologici che basano la propria potenza economica su imponenti e sofisticati *data center* o istituzioni nazionali e sovranazionali in procinto di implementare la propria moneta digitale a servizio dei cittadini e più in generale dei consumatori digitali.

Come accennato nel precedente capitolo, il *Proof-of-Work (PoW)* e il *Proof-of-Stake (PoS)* rappresentano due algoritmi largamente utilizzati per l'elaborazione delle transazioni e la creazione di nuovi blocchi in una *blockchain*. Andando più in profondità, è possibile notare come questi meccanismi differiscano nel funzionamento e, più in generale, nell'approccio di validazione:

- ***Proof-of-Work (PoW)***⁴⁵¹. Singoli validatori (*miner*) o gruppi (*mining pool*)⁴⁵² estraggono (*rectius*, “minano”) *crypto-asset* come *bitcoin* mediante il cd. *mining process*⁴⁵³. In base a questo specifico metodo, tutti i soggetti validatori competono tra loro nella rapida risoluzione di complessi calcoli matematici, con la finalità ultima di aggiudicarsi il diritto di creare un nuovo blocco nonché l'ottenimento di una commissione (*mining fee*)⁴⁵⁴ come ricompensa del notevole “sforzo lavorativo” e computazionale messo in atto. Per quest'ultima ragione, tale modalità di validazione dei blocchi è però da molti ritenuta altamente dispendiosa in termini energetici, ancorché molto sicura e decentralizzata.
- ***Proof-of-Stake (PoS)***⁴⁵⁵. A differenza del *PoW*, si tratta di un protocollo di validazione (definito anche *minting* o *forging*) che non fa leva sullo spirito agonistico dei lavoratori, bensì su quello collaborativo. In sostanza, «un gruppo di approver blocca una porzione considerevole dei propri token nativi per aggiudicarsi il diritto di approvare una transazione. Gli approver vengono selezionati da un algoritmo complesso, che guarda anche allo storico degli approver e quanto hanno messo in palio. Nel caso in cui un approver faccia un errore, perde una parte dei propri token e vede intaccato il suo

⁴⁵¹ La *blockchain* di *Bitcoin* si basa ad esempio sul meccanismo di consenso *Proof-of-Work (PoW)*.

⁴⁵² In pratica, una cooperativa di *miner* che mette insieme la propria potenza di calcolo e divide i profitti.

⁴⁵³ [AA.VV., Mining criptovalute e bitcoin: cos'è, come farlo \(cloud e non\) e guadagni, Blockchain4innovation, 2022.](#)

⁴⁵⁴ Per maggiori delucidazioni vds. [Scaling Parrots, Cosa sono le commissioni sulle transazioni Blockchain e perché esistono?, 2023](#) o [Grillo F., Proof-of-Work e impatto ambientale: problemi e potenziali soluzioni, Alma Mater Studiorum – Università di Bologna, 2020.](#)

⁴⁵⁵ Altri *crypto-asset* utilizzano, ad esempio, la *proof of stake* (la *Peercoin* è stata la prima).

storico, venendo penalizzato. La *proof-of-stake* è un meccanismo sicuro veloce e meno intenso dal punto di vista energetico, ed è al cuore del Merge di Ethereum, avvenuto nel corso del 2022»⁴⁵⁶. Perciò, affinché un nodo possa divenire *validator*, è necessario depositare una cauzione (*stake*) al fine di prendere (potenzialmente) parte al processo di validazione. Difatti, maggiore è la somma depositata, maggiore sarà la probabilità di essere selezionato come *minter* (o *forger*) del blocco successivo.

A ben vedere, la differenza tra i due algoritmi suesposti si ravvisa non solo nella diversa modalità di acquisizione del diritto ad elaborare le transazioni⁴⁵⁷, ma anche nel diverso dispendio energetico impiegato per soddisfare tale obiettivo. Questa veloce disamina non deve però frettolosamente convincerci che il protocollo *Proof-of-Stake* sia aprioristicamente migliore di quello *Proof-of-Work*⁴⁵⁸. Difatti, il *report* di *Kraken Intelligence* conclude dicendo che, «in definitiva, né PoW né PoS offrono una soluzione universale che si adatta a ogni caso d'uso della blockchain. Comprendere i compromessi che derivano dall'utilizzo di

⁴⁵⁶ Pagano F. e Soldavini P., *Il capitale decentralizzato: Blockchain, NFT, Metaverso*, Il Sole 24 Ore, 2022.

⁴⁵⁷ In questo ambito possono essere chiamati in molti modi: *validator*, *minter*, *forger*, *approver*, ecc.

⁴⁵⁸ [De Conno A., *Criptovalute e impatto ambientale: verso una nuova regolamentazione europea*, Altalex, 2022;](#) [Tumietto D., *Cripto-attività, ecco il regolamento MICA: le nuove regole da conoscere*, 2023.](#) Snocciolando alcuni dati, De Conno nota come il *Cambridge Center for Alternative Finance* dell'omonima università inglese abbia evidenziato nel suo *report* del 2018 che «l'attività di mining PoW può essere qualificata come ad alta intensità energetica, poiché richiede un enorme sforzo computazionale, e dunque un notevole consumo energetico. A titolo esemplificativo, basti pensare che, come evidenzia il report del 2018, i sei principali sistemi di criptovalute hanno da soli consumi energetici pari a quelli del Belgio (con riferimento all'anno 2016). Il rapporto a pone una specifica attenzione sulla dimensione ambientale dell'attività di mining, evidenziando peraltro come la valutazione del suo impatto sia un'attività articolata e a complessa, che può essere svolta secondo varie modalità e tenendo in considerazione vari aspetti: l'efficienza energetica degli strumenti utilizzati per l'attività "estrattiva", il confronto con gli strumenti finanziari "tradizionali", l'utilizzo o meno di fonti rinnovabili da parte dei miner, la percentuale di utilizzo di tali fonti e le ricadute che questo ha a livello locale; si pensi, a titolo esemplificativo, all'effetto che un incremento della richiesta di energia per le attività di mining potrebbe generare rispetto ai prezzi dell'energia in una regione in cui, ad esempio, l'accesso a fonti energetiche rinnovabili sia particolarmente agevole. In questo quadro, peraltro, un significativo ruolo è giocato anche dalla consapevolezza dei miner rispetto all'impatto ambientale della propria attività che, secondo il report del 2018, è ancora piuttosto limitata, a fronte invece di una maggiore attenzione alla possibilità di accedere a fonti energetiche affidabili e a costi contenuti. L'analisi è proseguita con il successivo rapporto del 2020, che ha evidenziato come, nonostante un incremento della trasparenza rispetto alla sostenibilità della "filiera produttiva" delle criptovalute e dell'attenzione a tale aspetto, il tema sia ancora fortemente dibattuto (e continui a richiedere una particolare attenzione). Il report del 2020, si concentra, in particolare, sull'utilizzo di energie rinnovabili, ed evidenzia come, sebbene il 76% dei miner usi anche queste ultime per la propria attività, esse rappresentano solo il 39% delle fonti energetiche utilizzate complessivamente per l'attività di mining a livello globale». [Cambridge Center for Alternative Finance \(CCAF\), *Cambridge Bitcoin Electricity Consumption Index*, University of Cambridge, 2018-2023.](#)

uno dei due è un passo fondamentale prima di decidere quale sia preferibile per un determinato caso d'uso. PoW offre in genere maggiori garanzie di sicurezza e decentralizzazione, sacrificando però un certo grado di scalabilità. PoS offre in genere una migliore scalabilità, sacrificando però un certo grado di sicurezza e decentralizzazione. La scelta migliore dipende da numerosi fattori, tra cui il caso d'uso principale di una determinata blockchain, come la resilienza del denaro sporco o la funzionalità degli smart contract»⁴⁵⁹.

Al netto delle osservazioni sinora condivise, è indubbio che la risoluzione di problemi matematici complessi costituisca un processo altamente energivoro e richieda un'enorme capacità di calcolo, resa possibile solo tramite dispositivi informatici particolarmente potenti e dotati di programmi in grado di compiere tale lavoro⁴⁶⁰. Per di più, oltre a sollevare motivazioni di carattere tecnico⁴⁶¹, una parte della comunità crittografica mette in luce le criticità supervisionali che un protocollo PoW implicitamente comporta. Ad esempio,

⁴⁵⁹ [Kraken Intelligence, PoW vs. PoS: Securing the Chain, Report, 2022](#). La riflessione succitata fa evidente riferimento al cd. trilemma, secondo cui risulta estremamente complicato per degli sviluppatori migliorare contestualmente scalabilità, sicurezza e decentralizzazione di una rete *blockchain*. In altri termini, se si intende rafforzare uno o due di questi aspetti, difficilmente si potrà ottenere lo stesso livello ottimale per il terzo.

⁴⁶⁰ [Tar A., Proof-of-Work, spiegata semplicemente, CoinTelegraph Italia, 2018](#).

⁴⁶¹ Il PoW presenta alcune criticità: i) la difficile scalabilità. Molti sostengono che la lentezza delle transazioni e le commissioni elevate stanno bloccando l'adozione su una grande scala della *blockchain*. Tuttavia, l'adozione di soluzioni *off-chain* (*Lightning Network*) o modifiche delle dimensioni del blocco (*Bitcoin Cash*) consentono di dipanare il problema; ii) vulnerabilità del 51%. In teoria, si verifica quando un gruppo di *miner* controlla più del 50% del potere di *hashing* della *blockchain* e poi assume il controllo su di esso. Tuttavia, è proprio l'enorme consumo di energia necessaria a scoraggiare coloro che intendono attaccare una determinata rete. Chiap G. *et al.*, *Blockchain. Tecnologie e applicazioni per il business*, Hoepli, 2022. Volendo vederla da una prospettiva speculare, Ci sono diversi fattori che pongono un limite alla crescita della domanda di energia di *crypto-asset*. In primo luogo, potrebbe non essere disponibile sul mercato un hardware funzionale sufficiente ad assorbire un aumento significativo di energia. Le apparecchiature più vecchie possono essere usurate o comunque non operative, mentre la produzione di nuove apparecchiature può essere ritardata o bloccata a causa della carenza di *chip* a livello globale. In secondo luogo, i minatori sono in concorrenza con altri utenti industriali e residenziali di elettricità, il che riduce il numero di risorse energetiche sfruttabili, abbondanti e a basso costo. Ciò include anche lo spazio di *hosting* limitato disponibile nelle regioni ricche di energia, che potrebbe esaurirsi rapidamente. In terzo luogo, la domanda di energia della rete criptovalutaria è vincolata anche dall'andamento futuro del prezzo dei *digital asset*: è ragionevole presumere che esista un limite naturale alla crescita del prezzo, che a sua volta pone un tetto alla spesa per l'elettricità. Una previsione credibile della futura domanda di energia di *bitcoin* necessita innanzitutto di una previsione accurata della futura traiettoria del prezzo di *bitcoin*. Inoltre, l'incertezza sugli sviluppi dell'*hashrate*, unitamente ad altri fattori di rete, complica ulteriormente la proiezione. Infine, i progressi tecnologici nell'*hardware* per il *mining* possono influenzare i cicli di sostituzione dell'*hardware* e causare cambiamenti significativi nell'inventario, con nuove macchine ad alta efficienza energetica che sostituiscono *hardware* più vecchi e meno efficienti. [Ruocco A., Ma è vero che il bitcoin consuma davvero tanta energia?, 2022](#); [Tavelli A., Bitcoin e sostenibilità ambientale: amici o nemici?, 2023](#).

Ruocco⁴⁶² spiega che in ambito di *PoW mining* i *server* devono rimanere sempre accesi e debitamente raffreddati⁴⁶³ e il consumo reale di elettricità non può essere misurato direttamente, bensì solo stimato⁴⁶⁴. Le ragioni alla base di questa constatazione sono molteplici: libertà generalmente concessa ai *miner* di agire sotto pseudonimo⁴⁶⁵; possibilità di usare «*diverse apparecchiature hardware con diverse efficienze energetiche, per le quali non esistono dati di vendita o di distribuzione affidabili*»⁴⁶⁶; sperequata resa energetica delle strutture di *hashing*⁴⁶⁷. In un mondo sempre più alla ricerca di soluzioni “*green*”, queste circostanze non fanno che pesare sommando le diverse attività messe in atto da un *CASP*. Tuttavia, alcuni espedienti sono stati escogitati per rendere meno vago l’effettivo consumo del *mining* facendo affidamento a determinati fattori quali la redditività prevista derivante dall’attività di estrazione o dai ricavi del *mining*, per natura molto volatili data la loro dipendenza dal prezzo degli *asset* digitali e dal contesto competitivo dinamico. Così facendo, i costi operativi potrebbero risultare prevedibili e determinabili principalmente dalle tariffe elettriche⁴⁶⁸. Approfondendo questo aspetto, secondo un’analisi condotta da *CoinGecko* (Figura 16), «*come minatore solista, è necessaria una media di 266.000 chilowattora (kWh) di elettricità per estrarre un singolo Bitcoin (BTC). Questo processo richiederebbe circa sette anni per essere completato, richiedendo un consumo mensile di elettricità di circa 143*

⁴⁶² *Ibidem*.

⁴⁶³ [Abbà M., Efficienza energetica dei data center: 6 piccoli aggiustamenti di successo, NetworkDigital360, 2023.](#)

⁴⁶⁴ [Ranocchiari M., Il consumo di acqua dei data center sta diventando un problema. Anche il Cloud ha sete, ma l'impronta idrica dei data center dipende dalla geografia, Materia Rinnovabile, 2023.](#)

⁴⁶⁵ Difatti, tali operatori non hanno il bisogno di identificarsi. Considerando che la *MiCA* contempla esclusivamente le persone giuridiche (dando piena libertà alla forma societaria da assumere), e non anche l’iscrizione di persone fisiche in appositi registri, tale scelta potrebbe essere rivista data la particolare incisività dei minatori sul fronte ambientale.

⁴⁶⁶ Ad esempio, le apparecchiature più vecchie possono rimanere inattive nei magazzini per molto tempo, fino a quando l’aumento dei ricavi del *mining* non giustifichi una riattivazione. [Ruocco A., Ma è vero che il bitcoin consuma davvero tanta energia?, 2022.](#); [Tavelli A., Bitcoin e sostenibilità ambientale: amici o nemici?, 2023.](#)

⁴⁶⁷ Ad esempio, quanta elettricità viene utilizzata per il raffreddamento rispetto al semplice funzionamento delle macchine. [Ruocco A., Ma è vero che il bitcoin consuma davvero tanta energia?, 2022.](#); [Tavelli A., Bitcoin e sostenibilità ambientale: amici o nemici?, 2023.](#)

⁴⁶⁸ L’aumento del prezzo e/o la diminuzione dei costi dell’elettricità portano generalmente ad un aumento del consumo di elettricità, poiché l’hardware meno efficiente tendenzialmente verrà ripristinato. Per converso, la diminuzione del prezzo e/o l’aumento dei costi dell’elettricità spingono verso una contrazione del consumo di elettricità, poiché l’hardware meno efficiente tende ad essere spento.

kWh. Per metterlo in prospettiva, questo consumo mensile di elettricità è circa un sesto di quello che una famiglia tipica negli Stati Uniti ha consumato nel 2021»⁴⁶⁹.

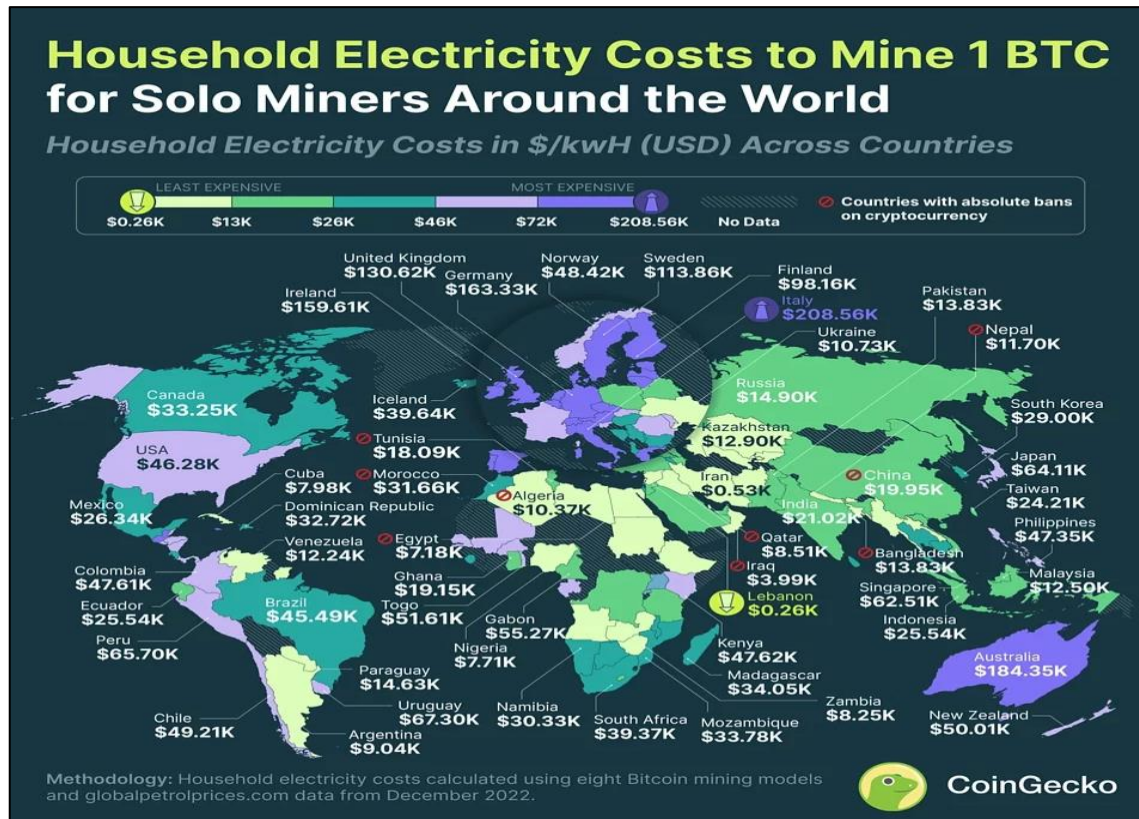


Figura 16 – Fonte: [Amase W., Household Electricity Costs to Mine 1 Bitcoin at Home, Around the World, CoinGecko, 2023.](#)

Altro dato interessante emerso dalla suesposta ricerca è che negli 82 Paesi in cui non risulta redditizio estrarre *bitcoin*, l'area più costosa per un *miner* è propria quella europea e l'Italia figura come Paese con il più alto costo dell'elettricità al mondo per minare un *bitcoin*. Seppure precisato che l'aumento dei prezzi dell'elettricità domestica all'interno della regione europea vada attribuito a vari fattori, tra cui l'impennata globale dei prezzi all'ingrosso dell'elettricità, emersa durante la pandemia di *COVID-19* e la crescente domanda internazionale, le ondate di calore del 2022 e l'invasione russa dell'Ucraina, che ha portato alla sospensione delle consegne di gas ad alcuni Stati membri dell'UE, l'analisi condotta ci

⁴⁶⁹ [Amase W., Household Electricity Costs to Mine 1 Bitcoin at Home, Around the World, CoinGecko, 2023.](#)

fa comunque comprendere come difficilmente i *miner* possano risultare attratti dal mercato europeo. E anche se lo fossero, vi sono evidenti sperequazioni nel mercato unionale interno secondo cui un *CASP* opterebbe per una specifica giurisdizione e non per un'altra, determinando, al pari di quanto detto nella sezione dedicata alla tassazione, un fattore d'interferenza sul piano concorrenziale da appianare il prima possibile.

Ulteriore aspetto da considerare, come fa notare correttamente Tavelli, «*visti gli elevati costi legati all'approvvigionamento elettrico, i miner tendono a migrare in territori in cui l'energia ha un costo più basso, in cui le normative in merito sono meno stringenti*»⁴⁷⁰ ed in cui il clima freddo consente di ridurre i consumi per il raffreddamento e lo smaltimento del calore prodotto. Per tale ragione, come asserisce Ruggiero⁴⁷¹, sono state cercate anche soluzioni impiantando *mining farm* in mare o agli estremi delle terre abitate. Tuttavia, anche laddove il clima è favorevole, ci si è scontrati con i consumi di energia elettrica, che hanno provocato lamentele da parte della popolazione residente visto che, in alcuni casi, le *mining farm* erano arrivate ad assorbire circa il 30% dell'energia totale disponibile⁴⁷². Inoltre, sebbene queste soluzioni estreme abbiano permesso di ridurre il costo per la produzione di 1 *bitcoin* da circa \$14.000 a circa \$5.000 cadauno e di aumentare gli ottimi margini di remunerazione per i *miner*, sono emersi seri dubbi di sostenibilità nel medio periodo. Infatti, tale redistribuzione geografica delle attività è risultata in netto contrasto con i piani di transizione ecologica che prevedono una riduzione sia del consumo di energia sia delle emissioni di CO².

Il quadro complessivo non appare dei migliori se accostato allo studio della testata britannica *Scientific Reports*, secondo cui «*quella della produzione di bitcoin sarebbe una delle industrie più inquinanti del pianeta. Stando alle stime dei ricercatori, basate sui costi economici delle emissioni di anidride carbonica, i danni climatici di ogni bitcoin generato*

⁴⁷⁰ [Tavelli A., Bitcoin e sostenibilità ambientale: amici o nemici?, IARI – Istituto Analisi Relazioni Internazionali, 2023.](#)

⁴⁷¹ [Ruggiero N., Criptovalute, come ridurre l'impatto ambientale: ecco le vie più promettenti, 2022.](#)

⁴⁷² Emblematica in questo senso è la migrazione di minatori (soprattutto cinesi) in Kazakhstan che agli inizi del 2022 si è imbattuta in un dispendio energetico di gravità tale da destabilizzare un intero Paese, oltre che reso ancor più schizofrenico un mercato volatile come quello dei *bitcoin*. [Volpicelli G. M., La crisi in Kazakhstan è un grosso problema per i miner di criptovalute, Wired, 2022;](#) [Carboni K., La crisi in Kazakhstan sta influenzando il mercato dei bitcoin, Wired, 2022;](#) [Cavicchioli M., Bitcoin, "the great mining migration" is underway, The Cryptonomist, 2022.](#)

nel 2021 hanno superato la cifra di \$11.300. Tra il 2016 e il 2021, i danni climatici medi sono stati pari al 35% del suo valore. La cifra sale vicino al 60% se si considera solo il periodo 2020/2021. Questi numeri collocano le cripto-attività vicino a industrie ad alto impatto ambientale come quello petrolifero o agroalimentare della carne mentre, complessivamente, i danni climatici globali provocati dal bitcoin tra il 2016 e il 2021 sono stati quantificati in \$12 miliardi»⁴⁷³. Le suestimate stime risultano valide anche nel caso di altre cripto-attività (*stablecoins* e *NFT*) visto che anch'esse fanno prevalentemente ricorso alla *PoW*. Non a caso, a fine 2021 si stimava che un *Non-Fungible Token (NFT)* su *Ethereum* (prima di passare alla *Proof of Stake*) fosse equivalente al consumo energetico di una *Tesla Model S 75* per percorrere circa 450 km⁴⁷⁴.

Sebbene a livello globale, relativamente alle cripto-attività, ci sia una crescente consapevolezza della necessità di considerare le implicazioni ambientali delle politiche finanziarie e monetarie, in pochi casi tali preoccupazioni sono state rivolte alla *Central Bank Digital Currency (CBDC)*. Questa angolazione consente di capire se le stesse valutazioni sinora fatte per i *crypto-asset* valgono anche per le valute digitali di Stato.

Solo a partire dal 2022 ha preso ad emergere una reale riflessione e un altrettanto reale dibattito circa l'impatto ambientale di tale *digital asset*. Il G7, la BCE e la Banca d'Inghilterra, nell'ambito delle loro iniziative di progettazione di *CBDC*, hanno infatti pubblicato principi o requisiti comprensivi della valutazione dell'impronta ecologica e, in tal modo, hanno stimolato l'avvio di un esame più approfondito sul tema⁴⁷⁵. Più nel dettaglio, il G7 nel suo rapporto "*Public Policy Principles for Retail Central Bank Digital Currencies*", delineando i principi fondamentali volti ad indirizzare l'esame ed il potenziale sviluppo della *CBDC*, ha raccomandato l'effettuazione di valutazioni circa il consumo energetico fin dalle prime fasi della progettazione e dell'implementazione cosicché l'utilizzo di energia di qualsiasi infrastruttura e architettura sia il più efficiente possibile, sostenendo in tal modo gli impegni condivisi della comunità internazionale per la transizione verso un'economia ad

⁴⁷³ [Forbes, Il Bitcoin come il petrolio e la carne bovina: tra il 2016 e il 2021 ha provocato danni climatici per 12 miliardi di dollari, 2022.](#)

⁴⁷⁴ [Stimolo S., Un NFT su Ethereum consuma energia quanto una Tesla, The Cryptonomist, 2021.](#)

⁴⁷⁵ [Panetta F., L'euro digitale e l'evoluzione del sistema finanziario, Intervento BCE, 2022; Avan-Nomayo O., Il governo del Regno Unito crea una task force dedicata alle CBDC, CoinTelegraph, 2021.](#)

impatto zero⁴⁷⁶. Contestualmente, nell'ottobre 2020, anche la BCE ha pubblicato un rapporto sull'Euro Digitale in cui si sottolinea che l'Eurosistema sosterrà in modo proattivo miglioramenti dei costi complessivi del sistema monetario e dei pagamenti e dell'impronta ecologica, ottenendo una maggiore efficienza energetica⁴⁷⁷.

Secondo un *paper* della Banca Mondiale, per identificare l'impatto ambientale della CBDC e valutare i potenziali rischi correlati, appare rilevante esaminare dal punto di vista ambientale la struttura e le caratteristiche intrinseche di tale *asset* digitale (soprattutto per quanto attiene alla sua produzione ed alla sua circolazione) e le sue differenze rispetto ad altri metodi di pagamento. Appare innanzitutto opportuno interrogarsi su quanta energia può potenzialmente utilizzare la CBDC e quali fattori tecnici nella progettazione della CBDC consumano più energia. Nella medesima ottica appare importante anche domandarsi se e per quale ragione la CBDC consuma meno energia rispetto ad altri metodi di pagamento nonché se ci sono lezioni utili che si possono trarre dall'introduzione e dallo sviluppo di altri metodi di pagamento.

Ciò premesso, è da rilevare che la CBDC, differentemente da altri *asset* digitali, «può fare uso dei sistemi di regolamento delle transazioni in tempo reale (RTGS) già attivi nell'ambito di alcuni sistemi bancari (UE, Australia, Ungheria, Hong Kong, Brasile) ovvero può essere progettata in una forma ibrida o, per meglio dire, correlata sia a un sistema RTGS centralizzato, sia a un sistema basato su blockchain centralizzata. Tale possibilità di scelta consente la ricerca di una ponderazione fra una pluralità di esigenze e priorità e, in primis, il livello di sicurezza del sistema, il costo di calcolo e conseguentemente il consumo energetico. I sistemi RTGS hanno raggiunto resilienza e prestazioni elevate, essendo da anni testati e utilizzati sul campo. Per converso, il punto di forza principale del sistema blockchain è l'assenza di un singolo punto di errore e, quindi, la possibilità di funzionare correttamente anche quando alcuni partecipanti alla rete sono malintenzionati. Questo vantaggio della tecnologia blockchain deriva dal meccanismo di consenso all'interno della sua struttura

⁴⁷⁶ [G7, G7 Public Policy Principles for Retail Central Bank Digital Currencies and G7 Finance Ministers and Central Bank Governors' Statement on Central Bank Digital Currencies and Digital Payments, Policy paper, 2021](#); Filippetta A., *Il rapporto del 13 ottobre 2021 dei Ministeri dell'Economia e delle Banche Centrali dei Paesi G7 "Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)"*, Atlante storico del diritto dei dati. Anni 2020-2022 Raccolta della rubrica Diritto e nuove tecnologie pubblicata sulla rivista Persona e Mercato dall'Osservatorio Giuridico sull'Innovazione Digitale, 2022.

⁴⁷⁷ [BCE, Report on a digital euro, 2020.](#)

distribuita. Tuttavia, rispetto ai sistemi basati su RTGS, i sistemi blockchain richiedono calcoli aggiuntivi per raggiungere il consenso e questo costo di calcolo influisce sul consumo energetico del sistema. Il costo varia a seconda del meccanismo di consenso adottato. Conseguentemente, dopo aver scelto la tecnologia più consona al tipo di progettazione prestabilita per l'infrastruttura di una CBDC, bisogna scegliere il meccanismo di consenso appropriato che soddisfi gli obiettivi generali del sistema. Esistono vari meccanismi di consenso con caratteristiche diverse che influenzano i diversi livelli di consumo energetico. Oltre al suo meccanismo di funzionamento intrinseco, anche il numero e la distribuzione dei partecipanti ad un'infrastruttura blockchain possono influire sui consumi energetici a seconda dei protocolli di consenso. Ad esempio, il costo di calcolo aumenta in modo lineare con l'aumentare del numero di partecipanti durante la convalida, ma aumenta in modo esponenziale nel caso di utilizzo di protocolli di consenso basati su Practical Byzantine Fault Tolerance (PBFT). Limitare il numero di partecipanti può far risparmiare energia, soprattutto per i meccanismi basati su PBFT, ma ciò ridurrà i vantaggi in termini di sicurezza e moltiplicherà le vulnerabilità agli attacchi. Inoltre, dal punto di vista della distribuzione, avere molti nodi all'interno di un singolo spazio, o gestiti da una singola entità, non offre un grande vantaggio in termini di sicurezza e può essere un singolo punto di errore. Tuttavia, la partecipazione di molte entità diverse come operatori di nodo può anche comportare costi di gestione elevati e problemi relativi alla privacy oltre alle implicazioni ambientali»⁴⁷⁸.

⁴⁷⁸ [Lee S., Park J., *Environmental Implications of a Central Bank Digital Currency \(CBDC\)*, World Bank Group Korea Office, Innovation and Technology Note Series, July 2022, note series number 8.](#) «Passando ad un esame comparativo dell'impronta ambientale della CBDC rispetto ai differenti sistemi di pagamento sono in primo luogo da rammentare gli esiti di alcune recenti indagini. Infatti, un recente studio condotto dalla banca centrale dei Paesi Bassi circa l'impatto ambientale dei pagamenti con carta di debito ha rilevato che l'impatto ecologico totale di un pagamento in contanti è 1,5 volte superiore a quello di un pagamento con carta di debito. Inoltre, nello studio del 2021 "Measuring the Environmental Impact of Cryptocurrency", Ripple, una società di protocollo di pagamento basata su blockchain, ha misurato l'impatto ambientale di crypto-asset, contanti e carte di credito (Visa e Mastercard) finendo per stimare che questi ultimi utilizzano meno energia rispetto alle risorse blockchain ed ai contanti è 1,5 volte superiore a quello di un pagamento con carta di debito. Inoltre, nello studio del 2021 "Measuring the Environmental Impact of Cryptocurrency", Ripple, una società di protocollo di pagamento basata su blockchain, ha misurato l'impatto ambientale di crypto-asset, contanti e carte di credito (Visa e Mastercard) finendo per stimare che questi ultimi utilizzano meno energia rispetto alle risorse blockchain ed ai contanti. Tracciare il consumo di energia durante l'intero ciclo di vita della carta moneta è difficile perché il processo varia a seconda del Paese e dell'uso delle materie prime. Ciononostante, sono stati condotti vari studi al riguardo adottando una pluralità di metodologie. Ad esempio, lo studio del 2018 di S. Rochemont "A cashless society: benefits, risks, issues" si è focalizzato sulla stampa e sulla circolazione

In conclusione, appare possibile evidenziare che, visto che la credibilità e l'affidabilità della CBDC si fonda sulla fiducia di cui godono le Banche Centrali, questo *digital asset* non ha bisogno di ricorrere ad una struttura tecnologica implicante un sistema di consenso ad alta intensità energetica o agli energivori meccanismi di *mining* utilizzati dalle altre *crypto*. Pertanto, in linea di massima, a differenza delle cripto-attività, la CBDC presenta un impatto ambientale variabile a seconda delle scelte operate in fase di progettazione del sistema e, quindi, a seconda delle scelte tecnologiche adottate per bilanciare diverse priorità, con la possibilità di renderla relativamente poco energivora⁴⁷⁹.

2. Tendenze evolutive del mercato criptovalutario e potenziali soluzioni al problema della pesante impronta ambientale ed energetica del *mining*

Preso coscienza del notevole impatto ambientale dei *bitcoin* e di buona parte dei *crypto-asset*, è d'uopo comprendere come le autorità di regolamentazione di tutto il mondo si siano mosse (o intendano muoversi rispetto al tema della sostenibilità). Più nel dettaglio, a partire dal 2013, in Cina, la limitata regolamentazione del settore di produzione di energia elettrica ha spinto numerosi imprenditori locali a conquistare una posizione dominante nella “produzione” globale di *crypto-asset* (prevalentemente *bitcoin*) nonostante, da anni, non fosse permesso alcuno scambio legale di *bitcoin* e le Autorità fossero ostili a tali prodotti crittografici, sia per ragioni di controllo della moneta locale, sia per finalità di tutela ambientale e perseguimento di obiettivi climatici, in ultimo sposate anche dal Partito Comunista Cinese. Ruocco precisa che questi minatori tendevano a muovere la sede delle proprie attività a seconda della stagione e così, nei mesi estivi si portavano in località

delle banconote e, dopo aver individuato i costi energetici medi della stampa di banconote e della rete di sportelli bancomat negli Stati Uniti, ha concluso che la rete di carte, comprese le carte di debito e di credito, consuma molta meno elettricità rispetto ad altri metodi di pagamento ovvero le cripto-attività e la carta moneta. Tenuto conto degli esiti dei predetti studi appare quindi possibile rilevare che, mentre la rete di carte è il sistema di pagamento con il minor impatto ambientale dal punto di vista del consumo energetico, il metodo di pagamento con le caratteristiche e l'infrastruttura più simili alla rete di carte di debito/credito è in linea di massima rappresentato dalla CBDC». Sempre ripreso da [Lee S., Park J., *Environmental Implications of a Central Bank Digital Currency \(CBDC\)*, World Bank Group Korea Office, Innovation and Technology Note Series, July 2022, note series number 8.](#) Si vedano per ulteriori approfondimenti: Ripple, *Measuring the Environmental Impact of Cryptocurrency*, 2021. [Rochemont, \(An addendum to\) A cashless society: benefits, risks, issues – Environmental sustainability of a cashless society](#), Institute and Faculty of Actuaries, 2018.

⁴⁷⁹ [Lee S., Park J., *Environmental Implications of a Central Bank Digital Currency \(CBDC\)*, World Bank Group Korea Office, Innovation and Technology Note Series, July 2022, note series number 8.](#)

adiacenti ai produttori di energia idroelettrica nelle province montuose del Sichuan e dello Yunnan, che convertono neve e piogge in elettricità. In inverno, invece, i *miner* trasferivano i computer nello Xinjiang e nella Mongolia interna, dove si estrae carbone e dove pertanto il costo dell'elettricità è relativamente vantaggioso⁴⁸⁰. Tale stato di cose al limite della legalità è continuato sino alla primavera 2021, quando le Autorità cinesi ha diffuso un primo studio dedicato alla CBDC nazionale e, nelle more di una sua futura introduzione, hanno preso a sostenere attivamente una criptovaluta nazionale, lo *yuan* digitale. Visto che la nuova valuta digitale si è affiancata alla valuta corrente, le istituzioni cinesi responsabili della vigilanza delle banche e dell'industria dei pagamenti hanno con maggior forza imposto a chi opera nella finanza del Paese a non effettuare operazioni con altre criptovalute, inclusi il *trading* e la conversione di valute fiat in monete digitali mentre hanno spinto numerose *mining farm* a chiudere e a delocalizzare le loro attività in altri Stati. Così, ad esempio, dopo aver recuperato a livello nazionale oltre 50 Terawattora di energia (ovvero una quantità tale da alimentare una città con più di un milione di abitanti), una delle Province più povere del Paese, il Guizhou, ha deciso di sfruttare l'energia liberata dai *miner* per sostenere la riconversione ecologica procedendo all'installazione di più di 4.000 stazioni di ricarica per veicoli elettrici ed incentivando l'acquisto di auto elettriche⁴⁸¹.

Nel frattempo, in Europa, come correttamente descritto da De Conno, *«l'attenzione rispetto all'impronta energetica ed all'impatto ambientale del sistema delle c.d. cripto-attività è progressivamente emersa a livello comunitario, nel quadro di una più ampia riflessione sui rischi collegati alle cripto-attività e all'assenza di una regolamentazione europea di tale sistema. Il 14 marzo 2022, la Commissione per i problemi economici e monetari del Parlamento Europeo (ECON) ha adottato la propria posizione negoziale sul testo della proposta di Regolamento MiCA in materia di cripto-attività. La proposta era stata pubblicata dalla Commissione Europea nel settembre 2020, nel quadro della strategia europea sulla finanza digitale, per poi essere successivamente rivista dal Consiglio d'Europa nel novembre 2021, e mira a fornire una regolamentazione a livello europeo delle attività in*

⁴⁸⁰ [Ruocco A., Ma è vero che il bitcoin consuma davvero tanta energia?, 2022.](#)

⁴⁸¹ [Oropallo, D., La Cina sostiene la sua criptovaluta, banna le altre e il bitcoin crolla, 2021.,; Oropallo D., In Cina l'energia del mining è riutilizzata per scopi ecosostenibili, 2021.](#)

materia di criptovalute, a partire da una tassonomia puntuale di queste ultime. Nello specifico, tale quadro normativo mira a raggiungere una maggiore chiarezza a livello comunitario, poiché, sebbene alcuni Stati membri già dispongano di una legislazione nazionale per le cripto-attività, non vi è ancora alcun quadro normativo specifico a livello dell'UE. Si punta così a colmare una lacuna individuata nella legislazione vigente dell'UE, per non ostacolare l'uso di nuovi strumenti finanziari digitali garantendo però, al tempo stesso, che tali nuove tecnologie e prodotti rientrino nell'ambito di applicazione della regolamentazione finanziaria e degli accordi in materia di gestione dei rischi operativi delle imprese attive nell'UE. La Commissione ECON ha chiesto alla Commissione Europea di includere, entro il 1° gennaio 2025, qualsiasi attività di mining di criptovalute nella tassonomia della finanza sostenibile dell'UE. Quest'ultima è stata introdotta con il Regolamento 2020/852/UE, allo scopo di contribuire al raggiungimento degli obiettivi climatici ed energetici dell'UE per il 2030 e di quelli del Green Deal europeo facendo leva su un settore chiave, ovvero quello degli investimenti finanziari. Il Regolamento ha dunque previsto la creazione di un sistema di classificazione comune per le attività economiche sostenibili, allo scopo di fornire una guida per gli investitori e le imprese, favorendo così investimenti coerenti con gli obiettivi delle politiche di sostenibilità europee. Entro il 2025, dunque, il Regolamento in materia di tassonomia della finanza sostenibile potrebbe essere destinato ad ampliarsi, includendo anche le attività di connesse all'estrazione di criptovalute. Con la propria delibera, peraltro, la Commissione ECON ha optato per un regime meno rigoroso rispetto a quello previsto nella precedente versione della proposta di Regolamento, fortemente contestato dagli operatori nel settore delle criptovalute. Tale versione prevedeva infatti l'inserimento, nel Regolamento MiCA, di stringenti requisiti di sostenibilità ambientale per le cripto-attività che utilizzano meccanismi particolarmente impattanti sul piano energetico, come il "Proof-of-Work" (PoW). La proposta prevedeva l'adozione di un piano di eliminazione graduale dei sistemi di mining più impattanti, con la transizione verso protocolli di validazione più sostenibili, come il c.d. "Proof-of-Stake" (PoS). Alcuni emendamenti al Regolamento prevedevano inoltre un obbligo per i prestatori dei servizi relativi alle criptovalute (exchange) e gestori di piattaforme di trading) di escludere dalla gamma dei prodotti offerti le valute virtuali non rispondenti ai criteri di

valutazione della sostenibilità degli investimenti ESG (Environmental, Social and Governance). Successivamente, nel giugno 2022, la presidenza del Consiglio e il Parlamento Europeo hanno raggiunto un accordo provvisorio in merito alla proposta di Regolamento MiCA. Per quanto riguarda la questione dell'impatto ambientale dell'attività di mining, in base al nuovo testo della proposta gli operatori del mercato delle cripto-attività saranno tenuti a dichiarare le informazioni sulla loro impronta ambientale e climatica. All'Autorità europea degli strumenti finanziari e dei mercati (ESMA) è stato invece attribuito il compito di elaborare progetti di norme tecniche di regolamentazione riguardanti il contenuto, le metodologie e la presentazione delle informazioni relative ai principali effetti negativi sull'ambiente e sul clima, mentre la Commissione Europea dovrà presentare, entro due anni, una relazione sull'impatto ambientale delle cripto-attività e sull'introduzione di norme minime di sostenibilità obbligatorie per i meccanismi di consenso, compreso il già citato *Proof-of-Work*⁴⁸²».

Il 20 aprile 2023 il Parlamento Europeo ha approvato il Regolamento MiCA che mira ad introdurre un quadro giuridico completo che armonizzerà i requisiti normativi per i servizi legati alle criptovalute in tutta Europa e, ricomprendendo vari aspetti, impone ai fornitori di servizi significativi di rendere noto l'impatto ambientale dei *crypto-asset* che offrono ai clienti in un'ottica di riduzione dell'impronta di carbonio delle cripto-valute⁴⁸³.

Il 9 giugno 2023, infine, la Gazzetta Ufficiale dell'Unione Europea ha pubblicato due dispositivi destinati a inquadrare l'emissione, la diffusione e lo scambio di *token* e *cryptocurrency*: il Regolamento 2023/1114/UE, altresì noto come regolamento MiCA ed il Regolamento 2023/1113/UE, anche conosciuto come *TFR Transfer of Funds Regulation*⁴⁸⁴. Mentre l'UE ha proceduto alla definizione ed approvazione della suesposta normativa, anche negli Stati Uniti, le Autorità non hanno mancato di dimostrare attenzione per i *crypto-asset* e per la loro pesante impronta energetica ed ambientale. Infatti, alcuni Stati americani hanno preso provvedimenti per incoraggiare il *mining* di criptovalute a basso consumo energetico. Il quotidiano specializzato *The Cryptonomist* riporta ad esempio che «lo Stato del Kentucky

⁴⁸² [De Conno A., Criptovalute e impatto ambientale: verso una nuova regolamentazione europea, Altalex, 2022;](#) [Tumietto D., Cripto-attività, ecco il regolamento MICA: le nuove regole da conoscere, 2023.](#)

⁴⁸³ [Garavaglia R., Cripto-asset: MiCAR approvato dal Parlamento europeo, 2023.](#)

⁴⁸⁴ [Garavaglia R., Regolamento \(UE\) 2023/1113: un'analisi delle disposizioni relative ai trasferimenti di fondi e cripto-attività, 2023.](#)

ha introdotto incentivi fiscali per i minatori di criptovalute che utilizzano fonti di energia rinnovabile e lo Stato del Texas è noto per le sue abbondanti risorse di energia rinnovabile, che hanno attratto i minatori di criptovalute alla ricerca di energia sostenibile e a basso costo»⁴⁸⁵. A livello federale, l'Amministrazione Biden, dopo essersi fatta promotrice di controverse proposte normative volte ad accrescere i requisiti di rendicontazione per le transazioni *crypto* e una maggiore supervisione delle borse e dei depositari di *crypto-asset*, ha ricompreso nella sua proposta di bilancio federale per il 2024 una disposizione che prevedeva di tassare fino al 30% dei costi di elettricità sostenuti dai minatori di criptovalute (tassa sulla *Digital Asset Mining Energy - DAME*) visto che il consumo di energia richiesto per il *mining* risultava significativo e visto che l'elevato utilizzo di energia elettrica del *mining* poteva comportare una tensione sulle reti elettriche locali, un conseguente aumento dei costi per i consumatori e, in alcuni casi, persino dei *blackout*. Tassando il consumo energetico del *mining* il Governo sperava inoltre di incoraggiare i minatori ad adottare pratiche e tecnologie più efficienti dal punto di vista energetico. Il gettito generato dalla tassa avrebbe potuto essere utilizzato per finanziare la ricerca sulle fonti energetiche alternative e per mitigare l'impatto economico del *mining* di *bitcoin* sulle reti elettriche locali⁴⁸⁶.

Di fronte a tale iniziativa⁴⁸⁷, tuttavia, si sono levate varie voci critiche che hanno rimarcato che tale tassazione avrebbe potuto portare a un esodo dei minatori dagli Stati Uniti. Secondo

⁴⁸⁵ [Porcelli A., Il Presidente Biden nella proposta di bilancio federale propone la tassazione del 30% per il mining di Bitcoin, 2023.](#)

⁴⁸⁶ [Erb K. P., White House Proposes 30% Energy Tax To Address Environmental Crypto Mining Costs, Forbes, 2023.](#)

⁴⁸⁷ Va detto che questa condizione non è di esclusivo appannaggio statunitense, ma assume diverse sfaccettature e contorni strategici specifici in vari Paesi del mondo: i) ad esempio in Iran, grazie alle abbondanti risorse naturali e all'accesso all'elettricità a basso costo, l'industria mineraria è un settore in crescita. L'Iran ospita il 4,5% del *mining* globale di *Bitcoin*, da cui ricava centinaia di milioni di dollari. Il Paese ha riconosciuto l'attività mineraria come legale nel 2019 e ha imposto l'obbligo di licenza mineraria nel 2022. Il governo trae profitto dalla fornitura di elettricità a prezzi più alti, concede esenzioni fiscali ai minatori e si procura i beni estratti per i pagamenti delle importazioni. Il rapporto tra i minatori e il governo, tuttavia, è sempre stato conflittuale. Durante i periodi di picco della domanda di elettricità, il governo ha smesso di fornire energia elettrica alle miniere. Inoltre, il governo ha regolarmente adottato misure restrittive nei confronti dei minatori che operano "illegalmente" sfruttando l'elettricità gratuita o sovvenzionata, anche se spesso usata come pretesto per ulteriori tasse da parte del governo. A causa di questi fattori, l'attività mineraria iraniana è instabile e la sua quota mensile può scendere dal 4,5% allo 0,12% in pochi mesi. Tuttavia, il Paese non dispone di un ambiente normativo adeguato per i fornitori di servizi di *asset* virtuali (*VASP*), il che rende il paese pieno di truffe criptovalutarie; ii) nel 2023, il governo kenyota ha rivelato una proposta per introdurre una tassa del 3% sui beni digitali nell'anno finanziario 2023-2024. La proposta prevede anche di tassare la monetizzazione degli *asset* digitali con un prelievo del 15%. L'imposta potrebbe indicare una forma di riconoscimento dei beni digitali da parte del governo. Sebbene sia troppo presto per valutare il successo di questa iniziativa, essa ha già aperto la strada a una

gli oppositori, infatti, con molti Paesi che offrono regimi fiscali più favorevoli per i minatori di criptovalute, come costi di elettricità più bassi o addirittura agevolazioni fiscali, la tassa avrebbe potuto rendere gli Stati Uniti meno competitivi nell'industria globale delle criptovalute. Alcuni sostenitori dell'imposta hanno d'altra parte controbattuto sostenendo che in realtà tale tassa avrebbe potuto giovare agli Stati Uniti nel lungo periodo, incoraggiando l'innovazione nelle tecnologie di *crypto mining* ad alta efficienza energetica.

Dopo aver alimentato un serrato dibattito, con un sorprendente colpo di scena, la proposta di una tassa sulla *DAME* è stata infine rimossa dal tavolo dell'accordo sul tetto del debito degli Stati Uniti raggiunto dal Presidente Biden ed il Presidente della Camera Kevin McCarthy. La rimozione della tassa, oltre a rappresentare una vittoria per i suoi avversari, indica il riconoscimento dell'importanza del settore delle criptovalute e la volontà di favorirne la crescita. La decisione di non imporre la tassa riflette inoltre una comprensione più sfumata delle preoccupazioni ambientali legate al *mining* e suggerisce che gli Stati Uniti stanno optando per un approccio cauto, consentendo al settore di prosperare pur tenendo d'occhio il suo impatto. È probabile che si svolgeranno ulteriori discussioni e negoziati per sviluppare un quadro normativo completo che risponda alle preoccupazioni senza ostacolare il progresso tecnologico⁴⁸⁸.

A margine rispetto alle suddette iniziative politico-normative, anche la comunità *crypto*, non è rimasta indifferente alla crescente consapevolezza da parte dell'opinione pubblica della

potenziale collaborazione tra le autorità di regolamentazione e *VASP*; iii) in Kirghizistan sono previste anche norme regolanti l'attività dei *miner*, i quali hanno l'obbligo di registrarsi, avere un proprio *hardware*, un *virtual wallet* attivo nonché alimentazione elettrica di qualità adeguata nei locali adibiti all'attività. Inoltre, devono pagare una tariffa elettrica maggiorata; iv) invece in Nigeria, nonostante numerose circolari e *crypto ban* espliciti da parte della Banca Centrale, nel 2023 il governo nigeriano ha introdotto una nuova legge per tassare i guadagni sui beni digitali come le criptovalute. Nello specifico, la legge è entrata in vigore lo scorso maggio ed introduce una tassazione del 10% sulle plusvalenze derivanti dalla cessazione di beni digitali, comprese le criptovalute; v) la legge slovena sui servizi e i sistemi di pagamento ha stabilito che le criptovalute non sono una valuta virtuale né un bene monetario. Tuttavia, i fornitori di criptovalute, come gli *exchange* e i *trader*, sono considerati istituzioni finanziarie per garantire la conformità con la legge antiriciclaggio. L'imposta sul reddito delle persone fisiche si applica al reddito ottenuto sotto forma di criptovaluta o dal *crypto mining*. Tuttavia, le plusvalenze ricevute dal *trading* non sono soggette all'imposta sul reddito; vi) nel settembre 2020, il Venezuela ha legalizzato il *mining* di *bitcoin* e ha annunciato che avrebbe concesso licenze di "mineraggio" attraverso un apposito registro chiamato "Integral Miners Registry" (*RIM*). In effetti, tutte le attività di *mining* devono essere esercitate attraverso il "National Mining Pool" (*NMP*) per mezzo del quale il governo supervisiona e distribuisce i guadagni ottenuti dalle attività di mining. Coloro che opereranno al di fuori di questo *NMP* saranno penalizzati.

⁴⁸⁸ [Porcelli A., Il Presidente Biden nella proposta di bilancio federale propone la tassazione del 30% per il mining di Bitcoin, 2023](#); [Porcelli A., L'accordo sul tetto del debito USA blocca la tassa del 30% sul mining di Bitcoin, 2023](#).

pesante impronta ambientale delle criptovalute. Nell'ecosistema *bitcoin* sono infatti emerse diverse iniziative private focalizzate sulla trasparenza e sull'impegno a "decarbonizzare" il *mining* entro un orizzonte temporale preciso. Molte società minerarie quotate in borsa hanno già fatto da apripista divulgando informazioni sulle proprie strutture, sui propri *mix* energetici e sui propri sforzi di sostenibilità. Contestualmente, alcune imprese attive nel settore delle criptovalute senza essere direttamente coinvolte nel *mining* quali i gestori di patrimoni e le borse valori hanno iniziato a compensare le proprie emissioni con crediti di carbonio⁴⁸⁹. L'insieme di tali iniziative hanno accresciuto la consapevolezza ambientale nel settore e, conseguentemente, hanno spinto le società minerarie a rivedere le loro strategie di approvvigionamento energetico ed a prendere provvedimenti per ridurre la loro impronta di carbonio. Così, negli ultimi anni, molti grandi minatori si sono impegnati a minimizzare l'uso di energia non rinnovabile, favorendo sempre di più l'energia sostenibile. Negli Stati Uniti, il Paese con la maggior quantità di *mining* di *bitcoin*, esiste addirittura un'associazione di minatori specificamente dedicata alla sostituzione dell'energia non rinnovabile utilizzata nel *mining* con energia sostenibile⁴⁹⁰.

In tale quadro, una menzione particolare merita un'iniziativa intrapresa nella primavera del 2023 dalla società statunitense *Tether*, società emittente e gestore della *stablecoin* più diffusa al mondo, l'*USDT*. *Tether* ha infatti deciso di investire parte delle sue risorse nella produzione di energia sostenibile da utilizzare per il *mining* di *bitcoin* in Uruguay, in collaborazione con una società autorizzata locale. I punti di forza dell'Uruguay nel settore delle energie rinnovabili rendono il Paese un luogo ideale per l'iniziativa visto che il 94% dell'elettricità prodotta nel Paese già proviene da fonti rinnovabili. Inoltre, grazie a significativi investimenti nelle infrastrutture energetiche, il Paese già dispone inoltre di una solida rete elettrica in grado di soddisfare le esigenze dell'industria moderna⁴⁹¹.

Accanto all'iniziativa di *Tether* in Uruguay, specie negli USA, sono comparse sul mercato una serie di nuove criptovalute alternative che fanno della sostenibilità la loro ragion d'essere (*SolarCoin*, *BitGreen*, *Cardano*, *Ripple*) e di "criptovalute ecologiche" che funzionano

⁴⁸⁹ [DeRoche M. et al., *The Energy Bomb: How Proof-of-Work Cryptocurrency Mining Worsens the Climate Crisis and Harms Communities Now*, 2022.](#)

⁴⁹⁰ [Ruggiero N., *Criptovalute, come ridurre l'impatto ambientale: ecco le vie più promettenti*, 2022.](#)

⁴⁹¹ [Leonardo C., *La stablecoin Tether verso il mining di Bitcoin sostenibile*, 2023.](#)

utilizzando fonti di energia rinnovabile per l'estrazione di criptovalute⁴⁹². Fra le predette iniziative, il blog "Criptonotizia" ne rammenta alcune a titolo d'esempio:

- **Ecocoin** ha adottato un algoritmo di consenso che richiede una quantità di energia elettrica molto più bassa rispetto alle altre criptovalute;
- **Carboncoin** è una criptovaluta che utilizza l'algoritmo di consenso *PoS (Proof of Stake)*, che richiede meno energia rispetto al *PoW (Proof of Work)* utilizzato da *Bitcoin*. Inoltre, per ogni unità di *Carboncoin* estratta, viene piantato un albero per compensare le emissioni di CO²;
- **Golem** è una piattaforma di *cloud computing* che si è impegnata ad utilizzare fonti di energia rinnovabile quali, in primo luogo, l'energia solare;
- **Grovecoin GRV**, dopo aver sposato la mission di fornire soluzioni sostenibili per l'agricoltura, il commercio al dettaglio e per la tecnologia, ha introdotto la criptovaluta *Grove coin* che punta sulla sostenibilità e sulla connessione al mondo reale attraverso un ecosistema composto da *GroveBlockchain*, *GroveSwap*, *GroveKeeper* e *GroveX*;
- **Gridcoin (GRC)** è una criptovaluta che premia i partecipanti al progetto di calcolo distribuito BOINC (*Berkeley Open Infrastructure for Network Computing*) con monete virtuali. BOINC è un progetto di ricerca scientifica che utilizza la potenza di calcolo di computer condivisi da tutto il mondo per risolvere problemi complessi. Gridcoin utilizza questo sistema per rendere più efficiente il processo di creazione di nuove monete, riducendo l'impatto ambientale delle criptovalute;
- **Chia (XCH)** è una criptovaluta che riduce il consumo di energia necessario per la produzione facendo ricorso ad un algoritmo di consenso *Proof of Space e Time (PoST)* ovvero un algoritmo che sfrutta lo spazio di archiviazione su disco invece della potenza di calcolo per la creazione di nuove monete;
- **Hedera (HBAR)**, oltre ad utilizzare solo energia rinnovabile per la produzione di criptovalute, fa ricorso al protocollo di consenso *Hashgraph* ovvero un protocollo fondato su un algoritmo di consenso asincrono che consente la convalida delle transazioni in modo molto rapido ed efficiente;

⁴⁹² [AA.VV., Criptovalute ecologiche: come funzionano e perché sono importanti, 2023](#); Wright T., Tether inizierà a minare Bitcoin in Uruguay, Cointelegraph, 2023.

- **Energy Web Token (EWT)** è una criptovaluta che ha sposato l'obiettivo di rivoluzionare il settore energetico utilizzando la tecnologia *blockchain*. A tale fine, *EWT*, oltre ad utilizzare un sistema di consenso *Proof of Authority (PoA)* che richiede meno potenza di calcolo rispetto al *PoW*, premia gli utenti che utilizzano fonti di energia rinnovabile per la produzione di energia elettrica;
- **Nano (XNO)**, al fine di ovviare agli elevati consumi energetici legati ai protocolli di consenso *PoW*, utilizza per validare le transazioni un protocollo di consenso asincrono (*AoS*);
- **IOTA (MIOTA)**, per le medesime ragioni, al posto della *blockchain*, ha adottato la tecnologia *Tangle* ovvero ha deciso di ricorrere ad un sistema in cui le transazioni sono validate dagli utenti stessi attraverso un sistema di verifica reciproca;
- **Cardano (ADA)**, sempre al fine di ovviare ai costi ambientali imposti dai sistemi basati sul *PoW*, ha adottato il protocollo di consenso *Ouroboros*. Inoltre, mossa da finalità di tutela ambientale e consapevole delle potenzialità offerte dalla sua architettura modulare, ha sposato l'obiettivo di diventare una piattaforma per le applicazioni decentralizzate (*dApps*) che utilizzano energia rinnovabile;
- **Tezos (XTZ)** ha adottato un protocollo di consenso *PoS* e, forte della sua architettura modulare, ha anch'essa assunto l'obiettivo di diventare una piattaforma per le applicazioni decentralizzate che utilizzano energia rinnovabile;
- **Stellar (XLM)**, oltre ad utilizzare fonti di energia rinnovabile per il *mining*, ricorre ad un protocollo di consenso federato per validare le transazioni⁴⁹³.

Interessante notare come il tratteggiato fenomeno delle “criptovalute ecologiche” abbia interessato anche altri Paesi, Italia inclusa. Ad esempio, in Trentino, è stata fondata la *start up* “*Alps Blockchain Srl*” con la *mission* di creare un ponte tra la tecnologia della *blockchain* e il mondo delle fonti rinnovabili e così rendere più sostenibile e accessibile il *mining* in Italia. *Alps Blockchain* ha a tal fine sviluppato sistemi innovativi per realizzare *mining farm* alimentate unicamente da fonti di energia pulite, progettando e installando i propri calcolatori all'interno di centrali idroelettriche (attualmente 18 e in prospettiva 32) performanti e a ridotto impatto ambientale. L'iniziativa ha peraltro dato nuova vita a varie centrali

⁴⁹³ *Ibidem*.

idroelettriche italiane, garantendo flussi di cassa da poter impiegare per il *revamping* di impianti in molti casi necessitanti ristrutturazioni ed ammodernamenti. Il *business model* adottato è quello dell'autoconsumo visto che parte dell'energia prodotta, in esubero o altrimenti destinata all'immissione nella rete nazionale, viene riciclata e destinata al consumo interno per la *mining farm*⁴⁹⁴.

Come ogni tecnologia emergente, le “criptovalute ecologiche” presentano vantaggi e svantaggi rispetto alle criptovalute tradizionali. Alcuni dei principali vantaggi sono rappresentati dal loro impatto ambientale ridotto frutto del ricorso per il *mining* a fonti di energia rinnovabile, dal loro impegno teso a promuovere l'adozione di fonti di energia rinnovabile e dalla loro attività di mobilitazione della comunità crypto nella creazione di una criptovaluta più sostenibile e responsabile dal punto di vista ambientale. Per converso, i principali svantaggi delle criptovalute ecologiche appaiono essere in primo luogo legati alla loro maggiore complessità tecnologica rispetto alle criptovalute tradizionali e, quindi, alla relativamente minore facilità di adozione da parte di nuovi utenti. Inoltre, almeno allo stato attuale, molte criptovalute ecologiche presentano limitazioni di utilizzo, la loro accettazione è inferiore ed offrono relativamente meno opportunità di investimento.

Di fronte all'emergere delle suddette prospettive di limitare l'impatto climatico-ambientale dell'attività di *mining* di criptovalute, alcuni studiosi hanno approfondito il tema realizzando degli studi volti a meglio indirizzare le scelte politico-amministrative ed industriali. Ad esempio, Aliehyaei e colleghi hanno recentemente ultimato uno studio in cui hanno innanzitutto calcolato l'ammontare dei consumi di energia elettrica per la produzione di *bitcoin* e del prezzo base di *bitcoin*. Su tale base, i predetti autori hanno proceduto a delineare: quattro scenari di produzione di *bitcoin* mediante elettricità fornita da fonti energetiche non rinnovabili corredati ad una stima della quantità di sostanze inquinanti emesse e dei connessi costi sociali; uno scenario di produzione di *bitcoin* attraverso fonti di energia rinnovabile. L'insieme dei dati così raccolti ed elaborati ha quindi permesso di proporre uno scenario utile a rispondere a due fondamentali interrogativi, ovvero: a quale prezzo la produzione di *bitcoin*

⁴⁹⁴ [Fondazione Finanza etica, Criptovalute e tecnologia blockchain, Capire la finanza, n.26, 2022.](#)

è *cost-effective* per i governi? qual è la fonte di energia rinnovabile migliore per produrre *bitcoin*?⁴⁹⁵.

Per finalità simili anche Cross T. del Reed College di Portland e Bailey A.M. del Yale-NUS College si sono impegnati nello studio intitolato “*Carbon-neutral bitcoin for Nation States*” in cui – dopo aver rammentato che nel 2021 ha affiancato al dollaro il *bitcoin* come moneta di riferimento e dopo aver rilevato che l’adozione, sia come moneta a corso legale che come riserva di tesoreria, di *bitcoin* da parte di Stati aumenta la redditività dell’estrazione di *bitcoin* ad alta intensità energetica, creando significative emissioni di carbonio – si analizzano i metodi di introduzione del *bitcoin* come moneta di Stato mitigando o eliminando le conseguenti emissioni di carbonio. I due ricercatori, infatti, hanno esaminato tre possibili soluzioni: una basata sulla regolamentazione/tassazione, una sulla compensazione del carbonio emesso e, infine, una sull’estrazione a emissioni zero condotta o sostenuta dallo Stato. Dopo aver evidenziato i vantaggi di quest’ultima soluzione, la ricerca non ha poi mancato di:

- porre a confronto due modalità di realizzarla ovvero la modalità secondo cui lo Stato estrae tutte le sue riserve di *bitcoin* e la modalità secondo cui la percentuale di *mining* di *bitcoin* realizzata dallo Stato è pari a quella dell’insieme delle sue disponibilità di *bitcoin*;
- fornire elementi a favore di quest’ultima modalità;
- giungere infine alla conclusione che uno Stato può adottare *bitcoin* in modo *carbon-neutral* con un investimento relativamente piccolo nel *mining carbon neutral* (ai livelli attuali del *mining* di *bitcoin* e dei prezzi dei *bitcoin*, sarebbe sufficiente un’allocazione annuale di circa l’1% delle disponibilità di *bitcoin* dello Stato per il *mining* per generare un rendimento positivo)⁴⁹⁶.

Ritornando a quanto accennato nella parte iniziale di questa sezione, è da evidenziare che, negli ultimi anni, la ricerca di una minore impronta energetica ed ambientale ha riguardato la realizzazione e l’impiego di algoritmi più efficienti (come il *PoS*) ovvero sia meno energivori e più veloci nel risolvere le transazioni sulla *blockchain*, soprattutto nella *DeFi*. Il tema vero,

⁴⁹⁵ [Aliehyaei M. et al., Development a policy for the production of Bitcoins with renewable energy sources, Future Energy Vol.3, pp.16-23, 2023.](#)

⁴⁹⁶ [Cross T. and Andrew M. Bailey, Carbon-neutral bitcoin for nation states, Financial Cryptography and Data Security, Springer International Publishing, 2022.](#)

che il settore ha subito affrontato, è che, pur lavorando sull'efficienza, il *proof of work*, per sua natura, è ancora oggi il sistema più sicuro, inviolabile e non influenzabile ma anche il più energivoro. Sono nati quindi nuovi concetti, tra cui *Algo* con *Algorand*, che lavora sul “*proof of stake*”, o *Ethereum 2.0*, che ha creato il suo *consensus layer* (pur sempre un “*proof of stake*”), molto adatti al concetto *DeFi*, per semplificare e ridurre al minimo i tempi e le capacità di calcolo per validare un blocco. Non si compete più tra chi arriva per primo a risolvere un complicato algoritmo (“*proof of work*” stile *bitcoin*) ma si collabora alla soluzione di un problema semplificato (“*proof of stake*” stile *Algorand*) guadagnando in termini di consumi e velocità. Ciò comporta, secondo alcuni, la perdita di unicità e non replicabilità del sistema di *bitcoin*, quindi l'esposizione a rischi concreti sulla veridicità della certificazione del blocco. Come ribadisce Ruggiero, *«questa nuova generazione di algoritmi riesce a ridurre i consumi energetici anche del 90% ed oltre e transare in 4-5 secondi sulla blockchain: una velocità di transazione che eliminerebbe alla fonte la possibilità per malintenzionati di influenzare il sistema. In particolare, il 15 settembre 2022, Ethereum ha compiuto la transizione verso un protocollo basato su “proof of stake”, vale a dire sul consenso prestato dai possessori di valute che le mettono in staking, a disposizione per questo utilizzo. In questo modo la criptovaluta numero due, la piattaforma che abilita lo sviluppo di smart contract, stablecoin e finanza decentralizzata, ha praticamente azzerato il consumo energetico (attualmente stimato a circa 0,0026 TWh/anno, sull'intera rete globale). Nel 2022, prima della transizione, il consumo energetico di Ethereum oscillava tra i 46,31 TW e i 93,98 TW all'anno. Tale transizione ha tuttavia fatto emergere anche aspetti negativi: la community ha espresso timori in merito all'incremento del livello di centralizzazione del network. L'aspetto della centralizzazione è diventato evidente subito dopo la transizione, dato che il 46,15% dei nodi per l'archiviazione dei dati, l'elaborazione delle transazioni e l'aggiunta di nuovi blocchi sulla blockchain apparteneva a soltanto due indirizzi. Sebbene i sostenitori di Ethereum sostengano che chiunque possieda 32 ETH può diventare un validatore, non si tratta affatto di una cifra esigua (al momento 32 ETH equivalgono a \$52.000)»*⁴⁹⁷.

⁴⁹⁷ [Ruggiero N., Criptovalute, come ridurre l'impatto ambientale: ecco le vie più promettenti, 2022.](#) Per ulteriori dati e approfondimenti vds. [Sarkar A., I consumi di Ethereum sono diminuiti del 99,9% dopo il Merge, 2022.](#)

Circa le prospettive offerte dall'introduzione e adozione di nuovi algoritmi di consenso meno energivori è interessante rammentare un recente studio a carattere econometrico dei ricercatori indiani Sapra e Shaikh volto a meglio identificare i fattori specifici del mercato e del *mining* responsabili dell'enorme consumo di energia dei *bitcoin* (ovvero quali sono le variabili significative del *mining* e *trading* che portano a un aumento del consumo di energia dei *bitcoin* e in che modo queste variabili sono correlate al consumo di energia dei *bitcoin*) così da avanzare a politici ed investitori possibili misure utili a ridurre l'impronta climatico-ambientale del settore d'attività. In sintesi, risultati ottenuti dai predetti ricercatori dimostrano che *Ethereum 2.0* si comporta come un sostituto dei *bitcoin* aprendo la strada ai Governi per l'adozione di iniziative di promozione di criptovalute ad alta efficienza energetica presso gli investitori interessati e di regolamentazione del mining attraverso criteri d'efficienza energetica⁴⁹⁸.

Secondo sempre il parere di Ruggiero, se lavorare sui consumi è una delle strade per rendere sostenibile il mondo delle criptovalute ai fini degli obiettivi *ESG* (*environmental, social, governance*), l'altra strada è utilizzare il calore prodotto in eccesso per alimentare altri ecosistemi ed integrare il mondo digital delle criptovalute con ambienti fisici e produzioni reali⁴⁹⁹. L'altra frontiera per rendere sostenibile una industria molto energivora è utilizzare fonti rinnovabili disponibili in grandi quantità e potenze come l'eolico od il fotovoltaico e, meglio ancora, l'idroelettrico, disponibile in maniera costante 24 ore al giorno. Tale tipologia di approvvigionamento energetico non ha lo stesso impatto ambientale di quella derivata da fonti fossili, ma è pur sempre sottratta ad altri utilizzi: se il fornitore di energia elettrica non usa rinnovabili, in grossa parte si sta solo spostando il consumo da un settore all'altro, senza ridurre l'impatto complessivo indotto dai *miner*. Quindi ci si sta avviando verso una configurazione di attività industriali diverse, l'una al servizio dell'altra, per creare un ecosistema *green* rispondente agli obiettivi *ESG*. Un ecosistema che vede insieme impianti di produzione di energia elettrica per centinaia di *MWh*/anno da fonti rinnovabili a servizio esclusivo di grandi *mining farm*. Il calore di questi impianti viene dissipato per alimentare

⁴⁹⁸ [Sapra N. e Shaikh I., *Impact of Bitcoin mining and crypto market determinants on Bitcoin-based energy consumption*, *Managerial Finance*, 2023.](#)

⁴⁹⁹ Ne sono esempi: il riscaldamento delle serre per la produzione di frutta e ortaggi, oppure il teleriscaldamento di una piccola comunità o tutte quelle applicazioni dove è necessaria una discreta quantità di calore prodotto costantemente durante l'intera giornata.

attività produttive di beni di consumo o beni industriali come, ad esempio, prodotti da serra. Il tutto possibilmente localizzato in Paesi dove la legislazione è snella, fiscalmente accettabile, burocraticamente molto veloce nel rilasciare le autorizzazioni necessarie alle opere industriali, possibilmente con clima freddo tutto l'anno e grandi spazi inutilizzati a disposizione. Altri requisiti richiesti sono la presenza di fonti di energia rinnovabili, meglio se idroelettrico, una buona rete logistica e di trasporto per commercializzare i prodotti “non digitali” ma anche una ottima infrastruttura di telecomunicazioni, per collegare la *mining farm* all'internet globale e gestire i miliardi di transazioni necessari in tempi brevissimi⁵⁰⁰.

A questo riguardo appare degno di attenzione il caso texano. Infatti, al fine di approfittare dei bassi prezzi dell'energia garantiti dal poco regolamentato mercato texano (prodotta, tra l'altro, per quasi il 20% mediante fonti rinnovabili), da qualche anno alcune compagnie di *mining* nordamericane si sono stabilite in Texas. Ora per questi *miner* si stanno prospettando due interessanti strade:

- la prima consiste nello stipulare contratti di fornitura a lungo termine tra *miner* e *provider* di energia che consentono ai primi di acquistare elettricità a un prezzo fisso per anni; così, quando la domanda di energia elettrica raggiunge il picco, i *miner* potrebbero rivendere la loro energia in eccesso alle centrali;
- la seconda consiste nell'utilizzo di *bitcoin* come *grid resource* per regolamentare della domanda di energia elettrica; infatti la capacità delle infrastrutture energetiche texane è compromessa dalla difficoltà di inviare in modo economico l'energia dai siti di produzione al consumatore.

Similmente a quanto traspare nel predetto caso, nell'ambito di una recente riflessione sui *bitcoin*, Rudd ha evidenziato come la pur energivora attività di *mining* possa comunque risultare in linea e funzionale con gli obiettivi climatico-ambientali rimarcando come detti consumi energetici, in quanto flessibili sotto il profilo temporale e geografico, possano favorire:

⁵⁰⁰ [Ruggiero N., Criptovalute, come ridurre l'impatto ambientale: ecco le vie più promettenti, 2022.](#)

- un più efficiente sfruttamento dell'energia nel corso delle 24 ore (specie nel corso delle fasce orarie a bassa domanda di energia) e, quindi, maggiori utili per le compagnie che gestiscono le reti elettriche e maggiori risorse disponibili per il potenziamento delle reti nonché per la realizzazione di impianti di produzione elettrica *green*;
- uno sfruttamento *in loco* di fonti di metano (gas serra particolarmente impattante quando rilasciato in atmosfera) situate in aree geografiche remote e, di conseguenza, con costi di collegamento e valorizzazione energetica allo stato proibitivi⁵⁰¹.

In conclusione, la prospettiva ambientale costituisce ormai una questione imprescindibile per poter meglio inquadrare il fenomeno dei *CASP* e, più in generale, quello *crypto*.

⁵⁰¹ [Rudd M.A., Bitcoin is full of surprises, Challenges 14\(2\) 27, 2023.](#)

SEZIONE 4. *PRIVACY*: UNA NUOVA FONTE DI ONERI CHE I CASP DOVRANNO CONSIDERARE IN FUTURO?

1. Considerazioni preliminari: i termini del rapporto tra privacy e finanza digitale

È di recente pubblicazione il testo della Relazione annuale dell'Autorità Garante per la protezione dei dati personali, dal titolo *“Il potere dell'innovazione e la solitudine digitale. La protezione dei dati a tutela della persona”*. Le sfide odierne che attraversano la materia della protezione del dato personale sono sotto gli occhi di ogni osservatore e gli Organi preposti sono impegnati a darne rinnovata disciplina giacché *«con l'urgenza delle più forti istanze democratiche emerge, (...), progressivamente più chiara, la necessità di uno statuto, giuridico ma anche etico, delle nanotecnologie, che ne promuova massimamente lo sviluppo, ma al servizio della persona, della solidarietà, dei diritti fondamentali»*⁵⁰². Il bilancio degli anni segnati dall'entrata in vigore del Regolamento 2016/679/UE, Regolamento generale sulla protezione dei dati (meglio noto come *GDPR – General Data Protection Regulation*) lascia all'interprete la chiara necessità di perseguire nella strada tracciata per il rinnovamento delle modalità di tutela del dato personale e della riservatezza delle persone fisiche⁵⁰³.

Uno sguardo attento alle dinamiche unionali non può mancare di scorgere le molteplici declinazioni che il predetto concetto sta assumendo, pure nelle intenzioni del regolatore sovranazionale. In via segnata, ci si riferisce alle novelle che di recente stanno distinguendo

⁵⁰² [Garante per la protezione dei dati personali \(GPDP\), *Il potere dell'innovazione e la solitudine digitale. La protezione dei dati a tutela della persona, Relazione del Presidente Pasquale Stanzone – 2022, 2023.*](#)

⁵⁰³ Sulle indagini giuridiche condotte intorno al tema della riservatezza e della tutela del dato personale si rinvia, senza pretesa di esaustività, a: Cerri A., *Riservatezza (diritto alla)*, in Enc. Giur. XXVII, 1995; Pardolesi R., *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e continuità*, in Pardolesi R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, vol. I, 2003; [Califano L., *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati*, in Califano L., Colapietro C. *Innovazione tecnologica e valore della persona*, 2017; Pollicino O. – Resta F., *Visibilità del potere, riservatezza individuale e tecnologia digitale. Il bilanciamento delineato dalla Corte*, in *Diritto dell'Informazione e dell'Informatica* \(II\) fasc. 1, 2019, pp. 110-121; \[Frosini T. E., *Il costituzionalismo nella società tecnologica, Liber Amicorum per Pasquale Costanzo*, vol. I, 2020.\]\(#\)](#)

In giurisprudenza, si rinvia alla lettura di Corte cost. n. 19/2020, che così ha affermato al *Considerato* in diritto, pt. 3.1: *«La giurisprudenza della Corte di giustizia dell'Unione europea ha influenzato lo stesso legislatore europeo, che ha avviato un ampio processo di revisione del quadro di regole in materia di protezione dei dati personali, concluso con l'emanazione di un unico corpus normativo di carattere generale, costituito dal Regolamento 2016/679/UE, divenuto efficace successivamente ai fatti dai quali originano le questioni di legittimità costituzionale in esame, ma tenuto in debita considerazione dal giudice a quo. Esso detta le regole fondamentali per il trattamento dei dati personali, nozione che include anche la trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione dei dati (art. 4, comma 1, numero 2)»*.

la cd. *politica europea del digitale*, specie a mezzo degli ultimi Regolamenti in materia di *Data Governance*, *Digital Services* e *Digital Markets*. In particolare, a voler mutuare la catalogazione di recente svolta dalla Banca d'Italia⁵⁰⁴:

- a) il Regolamento 2022/868/UE, in tema di *governance europea del dato*, ha dettato le disposizioni utili all'utilizzo, in modo sicuro, da parte delle imprese dei dati detenuti dagli enti pubblici, nel caso in cui ciò si rivelasse necessario per la fornitura di un servizio di interesse generale;
- b) il Regolamento 2022/1925/UE, in materia di *mercati digitali*, disciplina l'attività svolta dalle imprese che svolgono servizi di intermediazione su piattaforme digitali;
- c) il Regolamento 2022/2554/UE, in materia di *resilienza digitale*, che detta nuove regole di resilienza per gli operatori finanziari del settore digitale, quindi banche, imprese di investimento ed assicurazioni;
- d) il Regolamento 2022/2065/UE, in materia di *servizi di intermediazione digitale*, ha dettato i profili di responsabilità per l'utilizzo dei dati dei soggetti a favore dei quali è svolta l'attività di intermediazione, imponendo pure l'istituzione di autorità nazionali di controllo in materia.

Nell'era di una digitalizzazione che sempre più influenza le dinamiche dell'interazione umana, i termini del bilanciamento tra «*Stato e mercato, persona e tecnica, libertà e*

⁵⁰⁴ [Banca d'Italia, Relazione del Responsabile della Protezione dei Dati. Anno 2022, 2023](#). V. in particolare, p. 4 e ss. A p. 6, poi, il report della collaborazione intrapresa con il Garante della Protezione dei Dati personali: «Lo svolgimento di compiti di sorveglianza in materia di protezione dei dati personali nell'attività dell'Istituto implica il coinvolgimento del RPD nelle forme di collaborazione con il Garante privacy e nelle richieste da questo rivolte alla Banca. Al quadro delle relazioni in argomento va in particolare ascritta l'iniziativa, promossa dal Garante privacy, volta a costituire una rete dei RPD del settore bancario, per acquisire conoscenza dei fenomeni di effettiva rilevanza nel comparto e individuare possibili profili di coordinamento con l'Autorità in materia di protezione dei dati personali: a tale network è stato invitato a partecipare anche il RPD della Banca. Nell'anno la funzione del RPD ha anche collaborato a un'analisi approfondita della compliance con la normativa sulla protezione dei dati personali sollecitata dal Garante privacy sull'Anagrafe dei Soggetti gestita dalla Banca: sono state fornite articolate informazioni su ampiezza del trattamento effettuato, specifiche finalità perseguite, natura dei dati personali oggetto di trattamento, modalità di raccolta, base giuridica nel quadro delle fonti che disciplinano i poteri della Banca alla luce dell'art. 6, par. 3, lett. b), del GDPR e dell'art. 2-ter del Codice privacy, nonché sul rispetto degli altri principi posti dal GDPR e dell'esercizio dei diritti da parte degli interessati. Va segnalata infine la cooperazione prestata dal RPD nell'ottemperanza a due richieste di informazioni rivolte alla Banca dal Garante privacy ai sensi dell'art. 157 Codice privacy».

*innovazione»*⁵⁰⁵ ambiscono a farsi maggiormente definiti. La stessa regolamentazione si sforza di superare il più stretto tecnicismo per lasciare spazio ad un linguaggio aperto, oltre che a formulazioni che aspirano a conservare margini interpretativi, a fronte di una realtà digitale in costante evoluzione. A ben considerare, si tratta di tecniche di normazione necessarie al fine di evitare l'ingabbiamento del fenomeno tecnologico all'interno di certe categorie giuridiche, che il Legislatore europeo persegue attraverso la semplificazione dei moduli organizzativi e il controllo dell'applicazione tecnica. Difatti, *«nel rinnovato contesto sociale dell'informazione, la Rete si propone come una risorsa non rivale nel consumo e non escludibile, abilitante nuovi ecosistemi digitali per il pieno sviluppo delle attività economiche e sociali dell'individuo, suggestivamente ascritti nel cd. Paradigma dell'accesso»*⁵⁰⁶.

In ultima istanza, in un contesto in cui lo sviluppo del digitale consente l'accesso ad ogni tipo di informazione, la cd. *esplosione della tecnica* richiede una costante misurazione con il paradigma di valore dato dall'intimità individuale. La persona fisica è ormai *online* in ogni sfaccettatura della propria esistenza ed i diritti di libertà del singolo, stando alle considerazioni della dottrina, vivono una dimensione ulteriore e rinnovata. Questo perché *«il percorso di costruzione del diritto alla protezione dei dati personali si intreccia con il parallelo crescente sviluppo dell'innovazione tecnologica delle comunicazioni elettroniche»*⁵⁰⁷. Non stupisce quindi come la protezione della riservatezza sia divenuta una pista di riferimento costante di ogni intervento di regolazione condotto su svariati aspetti dell'attività umana. A tal proposito, è significativo un recente intervento della Corte Costituzionale, pronunciatisi sulla disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, all'articolo 14, commi 1-bis e 1-ter, del decreto legislativo 14 marzo 2013,

⁵⁰⁵ [Garante per la protezione dei dati personali \(GPDP\), ult. op. cit. pag. 5.](#)

⁵⁰⁶ [Farina M., Il diritto all'oblio nella governance dell'identificazione, Federalismi.it, 2020.](#) Ancora, a pag. 3: *«la governance dell'identificazione, come operazione di associazione effettuata da soggetti terzi (nel caso di specie, i service provider), costituisce campo di analisi privilegiato. Infatti, sebbene la Rete consenta la massima esplicitazione dei diritti della personalità, la disseminazione - nonché la fisiologica permanenza - di dati personali spuri, inesatti, incompleti e spesso non più pertinenti, rischia di minare l'integrità dell'individuo, imprimendo al tradizionale monadismo identitario una nuova dimensione dinamica».*

⁵⁰⁷ [Califano L., Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati, Editoriale scientifica, 2017,](#) cit., p. 9 e ss.

n. 33⁵⁰⁸. Dette disposizioni prevedevano, in particolare, la pubblicazione dei dati di cui all'articolo 14, comma 1, lettere c) ed f) dello stesso decreto legislativo, anche nei confronti dei titolari di incarichi dirigenziali (si trattava di particolari tipologie di compensi percepiti in ragione dell'incarico)⁵⁰⁹. Con sentenza n. 20/2019, il Giudice delle leggi ha quindi condotto un'interessante analisi relativa agli effetti della «*pubblicazione di massicce quantità di dati*»⁵¹⁰, anche nell'ottica di una proporzionalità del mezzo rispetto al fine perseguito. La Corte ha evidenziato come «*i diritti inviolabili dell'uomo e la libertà personale risulterebbero lesi da obblighi di pubblicazione funzionali bensì ad esigenze di trasparenza amministrativa, ma non idonei a scongiurare la diffusione di dati sensibili, per un verso superflui ai fini perseguiti dalla disciplina, per altro verso suscettibili di interpretazioni distorte*»⁵¹¹.

⁵⁰⁸ Con ordinanza del 19 settembre 2017, il Tribunale amministrativo regionale del Lazio, sezione prima quater, ha sollevato, in riferimento agli [artt. 2, 3, 13 e 117, primo comma, della Costituzione](#) – quest'ultimo in relazione agli [artt. 7, 8 e 52 della Carta dei diritti fondamentali dell'Unione europea \(CDFUE\)](#), proclamata a Nizza il 7 dicembre 2000 e adattata a Strasburgo il 12 dicembre 2007, all'[art. 8 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali \(CEDU\)](#), firmata a Roma il 4 novembre 1950, ratificata e resa esecutiva con la [legge 4 agosto 1955, n. 848](#), all'[art. 5 della Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale](#), adottata a Strasburgo il 28 gennaio 1981, ratificata e resa esecutiva con la [legge 21 febbraio 1989, n. 98](#), nonché agli artt. 6, paragrafo 1, lettera c), 7, lettere c) ed e), e 8, paragrafi 1 e 4, della [Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati](#) – questioni di legittimità costituzionale dell'[art. 14, commi 1-bis e 1-ter, del decreto legislativo 14 marzo 2013, n. 33 \(Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni\)](#).

⁵⁰⁹ In particolare: «e) gli altri eventuali incarichi con oneri a carico della finanza pubblica e l'indicazione dei compensi spettanti; f) le dichiarazioni di cui all'[articolo 2, della legge 5 luglio 1982, n. 441](#), nonché le attestazioni e dichiarazioni di cui agli articoli 3 e 4 della medesima legge, come modificata dal presente decreto, limitatamente al soggetto, al coniuge non separato e ai parenti entro il secondo grado, ove gli stessi vi consentano. Viene in ogni caso data evidenza al mancato consenso. Alle informazioni di cui alla presente lettera concernenti soggetti diversi dal titolare dell'organo di indirizzo politico non si applicano le disposizioni di cui all'articolo 7».

⁵¹⁰ *Ibidem*, Considerato in diritto, pt. 1.2.

⁵¹¹ Sul punto, cfr. [Colapietro C., Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione, Federalismi, n. 14, 13 maggio 2020](#).

Così osserva l'A. a p. 64: «*La trasparenza e la privacy rappresentano due elementi essenziali per mantenere in buona salute la vita democratica di uno Stato. Si tratta, infatti, di due forze tutt'altro che conflittuali, ma anzi complementari, la cui azione combinata permette allo stesso tempo di preservare la libertà dei privati dagli abusi del potere e di favorire la libera partecipazione dei cittadini, i quali possono informarsi sull'azione della pubblica amministrazione, celando però gli aspetti della propria vita privata che, se rivelati, potrebbero potenzialmente condurre a conseguenze indesiderate e talvolta discriminatorie. (...) È bene ricordare, del resto, che, secondo la concezione di Westin, la dittatura è il sistema in cui l'individuo è completamente trasparente e l'azione dello Stato è coperta dalla massima riservatezza, mentre la democrazia è il sistema in cui l'azione dello Stato è ispirata al massimo livello di trasparenza e l'individuo è protetto dal massimo livello di privacy rispetto alle informazioni che lo riguardano*».

Come ha osservato attenta dottrina, è vero che la normativa sulla trasparenza ben può generare delle criticità in relazione alla sfera di riservatezza della persona fisica, valore costituzionalmente tutelato⁵¹². D'altra parte, è il "grado di misurazione dell'intrusione" a consentire il mantenimento di un punto di equilibrio tra le contrapposte esigenze: *«non si può ignorare come la trasparenza sia correlata non esclusivamente ai due articoli innanzi richiamati, ma all'intero sistema costituzionale, e quindi: all'art. 1 Cost., in quanto connaturata al principio democratico; artt. 2 e 3 Cost., se si assume la prospettiva di un'amministrazione pubblica che agisca per permettere il pieno sviluppo della persona umana nella sua dimensione sociale; all'art. 21 Cost., dal momento che esso comporta non solo la libertà di informare, ma anche il diritto dei cittadini ad essere informati; all'art. 28 Cost., che prevede da un lato il dovere dei funzionari di "dare pubblico conto", cui dall'altro corrisponde specularmente il diritto dei cittadini di «rendersi conto»; all'art. 54 Cost., che conforma alla disciplina e all'onore l'esercizio delle funzioni pubbliche e implica, dunque, un diritto ad una buona amministrazione»*⁵¹³.

In relazione a tanto, emerge con forza la portata dei principi di pertinenza e non eccedenza in tema di trattamento dei dati personali che, oltre ad essere già fortemente tutelati dalla normativa interna, sono *«presidiati dalle norme europee, primarie e derivate, indicate quali parametri interposti»*. Ad avviso della Corte Costituzionale, detti principi devono assurgere a disposizioni idonee non tanto (e non solo) alla regolazione della fattispecie, ma come *«criteri di riferimento per effettuare una ponderazione della conformità della disciplina censurata, mostrando di intendere che tale operazione sia di segno diverso dalla semplice applicazione o non applicazione di una norma al fatto»*⁵¹⁴.

D'altronde, giungendo al cuore dell'argomentazione che maggiormente interseca le finalità di questa trattazione, il diritto alla riservatezza si fronteggia con quello alla trasparenza *«soprattutto nel nuovo scenario digitale»*: è questo un ambito con il quale non si può mancare di confrontarsi, attesa l'evidenza della pericolosità di una indiscriminata diffusione e/o circolazione delle informazioni. Se è vero che la sola ed effettiva trasparenza del dato

⁵¹² *Ibidem*, p. 65.

⁵¹³ Colapietro C., *Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione*, *Federalismi*, n. 14, 2020, p. 68.

⁵¹⁴ *Ivi*, Considerato in diritto, pt. 2.1.

consente la realizzazione dei principi costituzionali legati al diritto di conoscere e rimanere informati, nell'ottica invece della realizzazione della massima democraticità del sistema e partecipazione del cittadino alla vita pubblica, l'interprete non può non confrontarsi con gli effetti scatenati dalla circolazione dei dati sul *web* nei confronti del diritto di ciascun individuo a conservare massimamente intatta la propria sfera di libertà personale, al riparo da intromissioni indiscrete e trattamenti illeciti⁵¹⁵.

Nel tempo, simili considerazioni hanno subito un'ulteriore declinazione in termini di massima valorizzazione di diritto all'oblio, tutelato ai sensi dell'articolo 17 del *GDPR*. In via segnata, l'interessato conserva il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano, senza ingiustificato ritardo; parimenti, nel caso in cui sussista una delle condizioni riportate al comma 1 del già citato articolo 17⁵¹⁶, lo stesso titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati

⁵¹⁵ Ivi, Considerato in diritto, pt. 3.1: «La Corte di giustizia dell'Unione europea ha ripetutamente affermato che le esigenze di controllo democratico non possono travolgere il diritto fondamentale alla riservatezza delle persone fisiche, dovendo sempre essere rispettato il principio di proporzionalità, definito cardine della tutela dei dati personali: deroghe e limitazioni alla protezione dei dati personali devono perciò operare nei limiti dello stretto necessario, e prima di ricorrervi occorre ipotizzare misure che determinino la minor lesione, per le persone fisiche, del suddetto diritto fondamentale e che, nel contempo, contribuiscano in maniera efficace al raggiungimento dei confliggenti obiettivi di trasparenza, in quanto legittimamente perseguiti ([sentenze 20 maggio 2003, nelle cause riunite C-465/00, C-138/01 e C-139/01, Österreichischer Rundfunk et al.](#), e [9 novembre 2010, nelle cause riunite C-92/09 e 93/09, Volker und Markus Schecke GbR e Eifert](#))». In dottrina, si rinvia alla lettura dei seguenti contributi. [Ruggeri A., La Consulta rimette a punto i rapporti tra diritto eurounitario e diritto interno con una pronuncia in chiaroscuro \(a prima lettura di Corte cost. n. 20 del 2019\), in Giur. Cost., Studi 2019/I, 113](#); [Fanti V., La trasparenza amministrativa tra principi costituzionali e valori dell'ordinamento europeo: a margine di una recente sentenza della Corte costituzionale \(n. 20/2019\), Federalismi.it](#); [Nicotra I., Privacy vs. trasparenza, il Parlamento tace e il punto di equilibrio lo trova la Corte, Federalismi.it](#); [Scaccia G., Corte costituzionale e doppia pregiudizialità: la priorità del giudizio incidentale oltre la Carta dei diritti?, Forum di Quaderni Costituzionali](#); [Pollicino O. e Repetto G., Not to be Push Aside: the Italian Constitutional Court and the European Court of Justice, Verfassungsblog, 2019](#); [Catalano S., Doppia pregiudizialità una svolta opportuna della Corte costituzionale, Federalismi.it, 2019](#).

⁵¹⁶ Ossia, se: «a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1».

In dottrina, si rimanda a Morelli M., *Oblio (diritto all')*, Enc. Dir., VI, 2002; Pizzetti F., *Il prisma del diritto all'oblio*, Pizzetti F. (a cura di), *Il caso del diritto all'oblio*, 2003; Mezzanotte M., *Il diritto all'oblio. Contributo allo studio della privacy storica*, 2009. Si veda anche il contributo di M. Farina, *Il diritto all'oblio nella governance dell'identificazione*, cit.

personali conservati. Ciò che si intende significare è la necessità di analizzare le tematiche concernenti il trattamento del dato anche in termini di tutela della dimensione “negativa” della conservazione dello stesso. In particolare, il dato personale non dovrebbe rimanere conservato a tempo indeterminato, ma quanto meno dovrebbe essere cancellabile a richiesta dell’individuo nel caso in cui costui ritenesse che lo stesso non rappresenti più l’attualità della propria condizione, né incarni l’immagine che la persona fisica intende conservare presso la collettività. Di qui i procedimenti di deindicizzazione, oggi assicurati dai motori di ricerca anche a seguito delle importanti pronunce della Corte di Giustizia dell’Unione Europea, nel noto caso C-131/12, *Google Spain*, del 13 maggio 2014⁵¹⁷.

D’altronde, ciò che presenta indiscutibili profili di interesse è pure la dimensione territoriale assunta dall’argomento⁵¹⁸: la garanzia dell’oblio dei propri dati *online* sembrerebbe mantenere la stessa estensione delle giurisdizioni chiamate a farlo valere⁵¹⁹. Se è vero che le procedure di indicizzazione condotte dai motori di ricerca hanno la capacità di integrare un trattamento del dato personale, l’interessato dovrebbe allora avere il diritto di rivolgersi al gestore della procedura di *index* ed ottenere, ai sensi della dedicata normativa a tutela della *privacy*, la rimozione dei contenuti che facciano riferimento alla propria persona, per come richiamati pure dalle pagine *web* cui il motore di ricerca rimanda. Nella successiva pronuncia

⁵¹⁷ Per una suggestione sulle più recenti riforme, v. [Marini M., Oblio, deindicizzazione e processo penale: dal diritto europolitano alla riforma Cartabia, Sistema Penale n. 1/2023.](#)

⁵¹⁸ Si veda, su una linea di argomentazione simile, quanto riportato anche in sede di [Regolamento cd. DORA – Digital Operational Resilience Act, Regolamento 2022/2554/UE del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa per il settore finanziario](#), che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011: «*In una relazione del 2020 incentrata sul rischio informatico sistemico, il Comitato europeo per il rischio sistemico (CERS) ha ribadito che l’attuale elevato livello di interconnessione tra entità finanziarie, mercati finanziari e infrastrutture del mercato finanziario, e in particolare l’interdipendenza dei rispettivi sistemi di ICT, potrebbe costituire una potenziale vulnerabilità sistemica dal momento che incidenti informatici localizzati potrebbero rapidamente diffondersi da una qualunque delle circa 22 000 entità finanziarie dell’Unione all’intero sistema finanziario, senza trovare alcun ostacolo nelle frontiere geografiche. Gravi violazioni delle ICT che si verificano nel settore finanziario non si limitano a colpire entità finanziarie isolate, bensì spianano anche la strada alla propagazione di vulnerabilità localizzate attraverso tutti i canali di trasmissione finanziaria e possono provocare conseguenze avverse per la stabilità del sistema finanziario dell’Unione, dando luogo ad esempio a pressanti richieste di rimborsi e a una generale perdita di fiducia nei mercati finanziari*», Considerando n. 3.

⁵¹⁹ Cfr. [Sica S. e D’Antonio V., La procedura di de-indicizzazione, in Resta G., Zeno-Zencovich V. \(a cura di\), Il diritto all’oblio dopo la sentenza Google Spain, 2015; Pardolesi R., L’ombra del tempo e \(il diritto al\)l’oblio, Quest. Giust., 2017; Comella C., Indice, sommari, ricerche e aspetti tecnici della de-indicizzazione, Diritto dell’informatica, 2014.](#)

Google CNIL, resa dalla Grande Sezione il 24 settembre 2019 (C-507/17)⁵²⁰ il giudice unionale ha più specificamente affrontato la questione dell'estensione territoriale del diritto in argomento. In particolare, la de-indicizzazione dei contenuti *online* relativi alla sfera individuale di chi veda integrati i requisiti per procedervi potrebbe essere effettuata soltanto nel contesto delle versioni dei motori di ricerca operanti negli Stati membri dell'Unione Europea, nei quali è in vigore la stessa normativa in materia di trattamento dei dati personali. Taluni hanno osservato come «*ne deriva, evidentemente, la circoscrizione della tutela del diritto all'oblio (largamente inteso) e pertanto un affievolimento della sua portata, specie avuto riguardo alla facilità con cui colui che sia realmente interessato alla ricerca di una determinata informazione (deindicizzata solo localmente) può giungerci mediante semplici aggiramenti tecnici (ad es.: l'utilizzo di un server proxy)*»⁵²¹. Insomma, ciò che ci si chiede è quale debba essere la reale portata che una effettiva protezione del dato personale possa assumere, specie nel caso in cui il riferimento sia a scenari di massima globalizzazione, in contesti in cui il dato è allocato su *server* ubicati presso Paesi che hanno giurisdizioni che non osservano gli stessi *standard* europei di protezione della *privacy* individuale. A ben opinare, la questione della comunicabilità delle tutele negli ordinamenti costituisce uno degli argomenti centrali quando si tratta delle materie della riservatezza e della protezione della sfera individuale, intorno a cui continua a discutersi molto.

D'altra parte, come detto poc'anzi, all'esito del lungo percorso giurisprudenziale il Legislatore europeo ha provveduto a recepire nell'ambito del *GDPR* il cd. diritto all'oblio, dandone disciplina positiva all'articolo 17 ed operandone un preciso bilanciamento con i principi della *necessarietà del trattamento*. Infatti, si legge al comma 3 che «*i paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: a) per l'esercizio del*

⁵²⁰ Cfr. Astone M.A., *Right to be forgotten e il discutibile ruolo dei gestori online e dei motori di ricerca*, *Giornale di diritto amministrativo*, 2020; v. anche [Bevilacqua G., La dimensione territoriale dell'oblio, Federalismi.it, 2019.](#)

In particolare l'autore osserva che «*delineare l'ambito geografico di applicazione del diritto alla deindicizzazione significa imbattersi in due tendenze della prassi sostanzialmente opposte: una – quella che incontra il sostegno della Grande sezione della Corte di giustizia nel caso Google CNIL – è in favore di una deindicizzazione limitata al territorio europeo; l'altra – quella che invece incontra il sostegno delle autorità garanti della protezione dei dati personali e della Corte Suprema canadese – è in favore di una deindicizzazione extraterritoriale*», p. 4.

⁵²¹ [Marini M., Oblio, deindicizzazione e processo penale: dal diritto eurolunitario alla riforma Cartabia, cit., p. 14.](#)

diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria»⁵²².

All'esito di queste note introduttive, vale in ultimo accennare ad una questione che pare aver impattato sul settore delle transazioni digitali e, in particolare, sull'accessibilità al dato personale di chi si muove nell'area del credito digitale. Infatti, in disparte quanto sinora osservato in relazione al trattamento del dato personale all'interno di mercati regolamentati, si sta affacciando sempre più sulla scena una modalità di transazione anonima condotta a mezzo di cripto-attività, oggi sempre più impiegate per gli acquisti e le vendite con la promessa di una nuova dimensione di sicurezza delle transazioni, verificate e controllate a mezzo di una successione di catene di trasmissione, unitamente ad una sorta di anonimato delle stesse.

Come largamente dimostrato nelle precedenti sezioni, la criminalità organizzata pare aver guardato a simili strumenti come opportunità per eludere i controlli antiriciclaggio e dare nuova vita ai proventi delle proprie attività illecite, investendoli in svariate attività. Di qui,

⁵²² Disposizione così commentata dalla citata dottrina. V., infatti, [Marini M., Oblio, deindicizzazione e processo penale: dal diritto eurounitario alla riforma Cartabia](#), cit., p. 16: «rileva anzitutto notare come il legislatore eurounitario manchi di fornirne una definizione e, in realtà, trascuri altrettanto di dettarne una disciplina specifica. Invero, recependo in parte alcuni insegnamenti della sentenza Google/Spain, la norma si limita a prevedere, al primo paragrafo, un elenco di casi in cui il soggetto ha il diritto di chiedere al titolare del trattamento la «cancellazione dei dati che lo riguardano senza ingiustificato ritardo». Nell'ultimo paragrafo, il terzo, poi, vi è un catalogo che contempla situazioni, in presenza delle quali il diritto alla cancellazione non può trovare sede. Tra questi, la prima lettera prevede proprio il diritto alla libertà di espressione e di informazione. Ebbene, come si nota, v'è una carenza di completezza e precisione: nulla viene meglio determinato in merito ai diversi principi elaborati dalla giurisprudenza lussemburghese in primis e dalle corti nazionali degli Stati membri in secundis».

l'altra faccia della medaglia della pubblicità del dato personale di chi conduce una transazione. Se da un lato, osservando ogni regolamentazione in materia di liceità del trattamento, la trasparenza consente una pervasività di controlli (soprattutto dal punto di vista dell'antiriciclaggio), dall'altro lato la deriva verso modalità di transazioni anonimizzate (e potenzialmente condotte a fini illeciti) accentua l'esigenza di una rinnovata gestione dei moduli di tutela della *privacy*, che non deve tuttavia farsi così pervasiva da scardinare i sistemi di controllo che presidiano un sistema democratico.

In tal misura, diviene ancora più chiaro quanto sinora osservato in relazione all'esigenza di regolamentare uno spazio digitale che potrebbe essere foriero di operazioni finanziarie rivolte ai fini più vari. Il progresso della tecnica, accompagnato all'inevitabile passaggio verso un sistema di valuta digitale, dovrebbe procedere di pari passo con la proporzionale e contestuale regolamentazione del trattamento del dato personale. Ciò sia al fine di arginare iniziative di iper-normazione del digitale che potrebbero stridere con le primarie esigenze di protezione della riservatezza e della libertà individuale sia allo scopo di evitare il prodursi di zone franche, nelle maglie delle quali la criminalità riesca ad inserirsi per condurre transazioni su circuiti virtuali del tutto privi di controllo. Quella della *privacy* è una dimensione che va trattata nella prospettiva del parallelo sviluppo delle “*cyber technology*”, senza che possa ambirsi a costituire un modello immutabile di trattamento del dato. Il bilanciamento tra le esigenze prima individuate si fa ancora più forte se proiettato nel *cyber*-spazio, dimensione sì a-territoriale e, per certi versi, de-regolamentata.

A ragione di tutto quanto premesso, le pagine che seguono saranno dedicate anzitutto ad un'analisi dello “stato dell'arte”: come funziona, oggi, un trattamento del dato finanziario online? Quali sono gli spazi rimessi alle banche (ormai sempre più virtuali) nella gestione del dato dei propri clienti?. In un secondo momento, sarà condotta un'indagine parallela relativa ai *digital asset*: da un lato, saranno analizzate le dinamiche d'impiego dei *crypto-asset* che consentono un'anonimizzazione delle transazioni; dall'altro, saranno valutati gli impatti della “reazione statuale” a questo fenomeno, per mezzo della produzione di *CBDC*. Approdando al termine di questo paragrafo, è quanto mai attuale il pensiero di Frosini ormai qualche anno addietro, ossia che «*quello che è stato definito “l'orizzonte giuridico dell'Internet” continua sempre più ad allargare e ampliare il suo panorama teorico e*

pratico. Non c'è settore del diritto che non sia investito e coinvolto: dal diritto civile dei contratti e delle transazioni concluse tramite computer, al diritto penale dei reati informatici e delle frodi elettroniche; dal diritto amministrativo dello e-government e dell'amministrazione digitale, al diritto processuale del c.d. "processo telematico" e della razionalizzazione informatica del sistema processuale. Si assiste, a seguito dell'affermarsi della tecnologia, a un nuovo modo di essere del diritto e, conseguentemente, a un processo di metamorfosi della figura del giurista come umanista in quella del giurista tecnologico. Il cui compito è quello di farsi interprete delle trasformazioni che si stanno verificando nella società sulla base dello sviluppo della tecnologia, e dell'impatto che questa sta avendo sul diritto, sui diritti»⁵²³.

2. Le modalità di trattamento del dato bancario: normativa in vigore e prospettive di sviluppo

Per scendere in maggior grado di dettaglio è necessario soffermarsi ad approfondire le modalità di regolamentazione dei rapporti tra finanza digitale e *privacy*. La questione della indebita diffusione di informazioni bancarie, oltre che del tracciamento delle operazioni condotte sui circuiti finanziari, costituisce una tematica che non può essere ignorata. A tal proposito, rimane ancora oggi particolarmente significativo l'intervento condotto dall'Autorità Garante per la protezione dei dati personali, a mezzo del provvedimento n. 192 del 2011, con cui ha prescritto le misure che i titolari del trattamento debbono adottare per il tracciamento delle operazioni bancarie effettuate – anche in forma indebita – dai cd. *incaricati di trattamento*, nei riguardi dei dati di patrimonio dei propri clienti.

A titolo di significativo precedente, pare utile citare anche il provvedimento della stessa Autorità indipendente sempre in tema di riservatezza dei dati bancari. Nell'occasione, rilevata l'illiceità del trattamento dei dati personali effettuato dalla banca nei confronti di un proprio cliente, il Garante prescriveva allo stesso istituto di credito il rafforzamento delle

⁵²³ [Frosini T. E., *Il diritto costituzionale di accesso a Internet*, Rivista AIC, n. 1/2011, 2010., p. 1.](#) «Emergono, infatti, dalla coscienza sociale, e a seguito dello sviluppo tecnologico, dei "nuovi diritti" fondamentali, i quali, sebbene non godano di un loro esplicito riconoscimento normativo, hanno un forte e chiaro "tono costituzionale", che li colloca, implicitamente, all'interno della costituzione, riservando all'interprete il compito di estrapolarli da essa (...)».

misure di sicurezza *«idonee a garantire la scrupolosa vigilanza sull’operato degli incaricati e a sensibilizzarli al rispetto delle istituzioni loro impartite in occasione di specifiche iniziative di formazione del personale»*⁵²⁴. Com’è ben evidente, si tratta di adempimenti che hanno subito una decisa spinta innovativa a seguito dell’entrata in vigore del *GDPR* già menzionato, inasprendo il trattamento sanzionatorio connesso alla violazione del regime delle tutele. Perciò, ai fini di una migliore comprensione dei concetti che si introdurranno di qui a breve, è necessario analizzare la portata del Regolamento in materia di *General Data Protection*, tenendo ben presente che lo stesso:

- a) *stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati* (articolo 1, par. 1);
- b) *si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi* (articolo 2, par. 1);
- c) *si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione* (articolo 3, par. 1);
- d) intende per “dato personale”: *«qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale»* (articolo 4, par. 1, n. 1));
- e) intende per “titolare del trattamento”: *«la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento*

⁵²⁴ Cfr. [Garante per la protezione dei dati personali, Provvedimento n. 1715015, 2010.](#)

sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri» (articolo 4, par. 1, n. 7));

- f) intende, per “responsabile del trattamento”: «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento» (articolo 4, par. 1, n. 8))⁵²⁵.

Svolte le doverose premesse, ciò che più strettamente interessa è l'analisi di compatibilità della terminologia e dei concetti introdotti in sede unionale, per mezzo della regolamentazione appena citata, rispetto al contesto della gestione dell'informazione finanziaria. L'istituto bancario costituisce nella dinamica della nuova configurazione europea della protezione del dato personale, un Titolare di trattamento, cui l'art. 24 del *GDPR* affida la messa in atto di misure tecniche e organizzative adeguate a garantire che il trattamento sia effettuato conformemente al Regolamento 2016/679/UE in parola. Si tratta di misure che richiedono una costante implementazione ed aggiornamento, nella prospettiva di massima conservazione della disciplina regolamentare cui si faceva cenno in apertura.

L'organizzazione di sicurezza del dato che le banche hanno dovuto approntare, peraltro, si è dovuto necessariamente conformare ai principi dettati in materia di *adeguatezza al rischio*, declinato – ad esempio – nei ben noti concetti della *pseudonimizzazione*, *cifratura del dato personale*, *capacità di tempestivo ripristino dell'accesso in caso di incidente fisico o tecnico*. Sono, questi, solo alcuni dei criteri dettati dall'articolo 32 del *GDPR*. La pseudonimizzazione, più nello specifico, ha costituito un concetto dalla portata

⁵²⁵ In relazione a tanto, si rinvia all'articolo 28 del *GDPR*: «Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento».

effettivamente rivoluzionaria nell'ambito dell'organizzazione della gestione del dato personale. Si legga, al *Considerando* n. 28 del *GDPR*, come «l'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati». Nella specie, ciò che si vuole intendere sono i termini di una gestione del dato personale stesso in una maniera che gli stessi, ai sensi dell'articolo 4, par. 1, lett. 5), del Regolamento in disamina, «non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile». Tant'è vero che all'articolo 32 del Regolamento in argomento, la già menzionata tecnica è associata a quella della cifratura, come modalità per assicurare la «Sicurezza del trattamento»⁵²⁶.

Infatti, se è vero che un dato completamente anonimo non potrebbe soddisfare i requisiti per integrare un dato personale (con quanto ne discende ai fini del relativo trattamento), diversi sono i termini della questione laddove il dato personale non è reso anonimo, ma è «pseudonimizzato». Stando a quanto citato nel *Considerando* n. 26 premesso al *GDPR*, anche il dato pseudonimizzato è considerato un'informazione relativa ad una persona fisica identificabile. L'incentivo che il Regolamento accorda alla pseudonimizzazione del dato (cfr. articolo 25 del *GDPR*) è da leggersi in uno con quel principio di minimizzazione del

⁵²⁶ Cfr. articolo 32 *GDPR*: «1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri».

trattamento, ossia con l'idea che il dato personale debba essere conservato nella sola misura in cui sia utile al trattamento effettuato. Ogni altra informazione aggiuntiva, o comunque non utile ai fini di quanto perseguito e dichiarato dal titolare del trattamento, non dovrebbe essere passibile di detenzione da parte di quest'ultimo. L'ottica è quella di un costante bilanciamento tra mezzo e fine, che permea ormai ogni regolamentazione sovranazionale in materia di utilizzo di un dato riconducibile in qualche maniera ad una persona fisica⁵²⁷.

Accompagnano lo scenario di controllo predisposto dal *GDPR* anche specifiche previsioni in materia di «comunicazione di una violazione di dati personali all'autorità di controllo e all'interessato, nonché di valutazione d'impatto sulla protezione del dato». In tal senso, un notevole rafforzamento hanno subito le procedure in tema di informativa chiara e trasparente alla clientela e al pubblico degli investitori⁵²⁸.

⁵²⁷ Così recita l'articolo 25, par. 1 del Regolamento in menzione: «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati». Tant'è vero che, al par. 2: «Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica».

⁵²⁸ Per approfondimenti sul più recente dibattito giurisprudenziale in tema di contratti di investimento si rinvia alla lettura, tra gli altri, di: [Cesiano D., Gli obblighi dell'intermediario finanziario nella prestazione dei servizi di investimento dagli orientamenti della giurisprudenza di merito alle Sezioni Unite, Rivista di Diritto Societario, fasc. 3, 2008](#); [Acierno M., I diritti dell'investitore nella giurisprudenza di legittimità, Questione Giustizia n. 3, 2017](#). Si legga, in ult. op. cit.: «l'orientamento sopra illustrato, tuttavia, è stato sottoposto a revisione critica all'interno della stessa Corte proprio sotto il profilo della funzione peculiare della forma scritta nei contratti d'intermediazione finanziaria, non riducibile a quella classica, mutuata dall'art. 1325 cod. civ. Secondo l'ordinanza interlocutoria n. 10447 del 2017 la ratio del requisito, in tutti i contratti caratterizzati da asimmetria informativa, s'individua nello scopo di mettere il contraente più debole a conoscenza del contenuto del contratto. In particolare, deve escludersi il rilievo strutturale della forma, tradizionalmente collegato alla ponderazione del contenuto dell'accordo ed a consacrare la rilevanza sociale del regolamento negoziale. La funzione prevalente se non esclusiva della forma scritta consiste, pertanto, nella preventiva documentazione delle condizioni contrattuali, in modo da rendere edotto il cliente delle clausole predisposte dall'intermediario. Così funzionalizzato l'obbligo di documentazione, consegue che, ai fini della tutela della corretta informazione del cliente, non è necessaria la doppia sottoscrizione del documento contrattuale e ci si deve chiedere se per ritenere assolto il compito dell'intermediario sia sufficiente la consegna al cliente del prospetto redatto dalla banca, oppure se sia necessario che venga documentata l'intera operazione negoziale comprensiva delle sottoscrizioni di entrambe le parti».

Ancora, si rinvia alla lettura di Valitutti A., *Il contratto di intermediazione finanziaria privo di forma scritta: nullità selettiva o abuso del diritto?*, Atti del Convegno "Questioni di diritto civile all'esame delle Sezioni Unite – Nullità selettiva" presso la Corte Suprema di Cassazione, 2019. Interessante riportare il passaggio a p. 7:

La rinnovata centralità assunta dall'interessato-cliente (persona fisica) rispetto alla possibilità di accedere, controllare, rettificare o chiedere la cancellazione dei dati personali che lo riguardano, invero, si esplica in una serie di *diritti* riconosciuti dal *GDPR* stesso, sì che ogni notizia fornita al titolare del trattamento sia sempre fornita in maniera consapevole e sia costantemente verificabile. Tali diritti sono enucleati, a favore di chi ne richiedesse l'approfondimento, al Capo III della normativa europea (articoli 12 – 23). L'articolo 12 del Regolamento, nello specifico, fonda un regime di «*informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato*». Ogni relazione con l'interessato dovrà, in tal misura, avvenire in una forma che sia concisa, trasparente, intellegibile e facilmente accessibile, in ossequio alla piena controllabilità dell'informazione cui si faceva cenno poc'anzi⁵²⁹.

«Posto che la nullità, sul piano generale, riveste i caratteri di un rimedio contro modalità di esplicazione dell'autonomia privata valutate dall'ordinamento come in contrasto con dati normativi, non può revocarsi in dubbio che nell'ambito delle cd. nullità di protezione – nelle quali rientrano il disposto degli artt. 36 cod. cons. e 23 d.lgs. n. 58 del 1998 – il nesso tra validità e tutela si atteggi in un modo particolare. Ed invero, non può del pari revocarsi in dubbio che siffatta forma di nullità – qualunque ne sia la causa, il difetto di forma ex art. 23 t.u.f. o altra fattispecie di nullità protettiva – intrattenga con la dinamica della selettività un rapporto di tipo strutturale. Nel senso che è solo «la nullità di protezione, e non altre, che rende la dinamica selettiva anche solo astrattamente ipotizzabile». Ed è del tutto evidente che le caratteristiche definitorie del vizio in esame hanno notevoli ricadute sulle condizioni di esperibilità dell'exceptio doli generalis».

⁵²⁹ Per approfondimenti, si rinvia alle [Informazioni di base – La trasparenza delle condizioni contrattuali](#) rese dalla Banca d'Italia nel progetto [L'economia per tutti – la Banca d'Italia per la cultura finanziaria](#). Si legga: «Perché una disciplina di "Trasparenza"? Quando si parla di "trasparenza delle operazioni e dei servizi bancari e finanziari" si intende un insieme di regole volte ad assicurare ai clienti un'informazione corretta, chiara ed esauriente che agevoli la comprensione delle caratteristiche, dei rischi e dei costi dei prodotti finanziari offerti e ne consenta la facile confrontabilità con altre offerte. Può accadere infatti che la documentazione elaborata dagli intermediari, sebbene completa nei contenuti, risulti difficile da leggere e capire, soprattutto se si è poco esperti di credito o finanza, per la quantità di informazioni fornite, per la loro complessità e tecnicità o per l'uso di un linguaggio non sempre facilmente comprensibile. La Banca d'Italia ha emanato disposizioni su "Trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti" anche con il contributo delle segnalazioni ricevute dall'utenza bancaria e finanziaria» (Provvedimento del 9.2.2011 che integra il Provvedimento del 29.7.2009). «Le previsioni definiscono standard minimi e generali di redazione dei documenti informativi predisposti per la clientela (struttura dei documenti, informazioni essenziali da fornire, scelte lessicali, standardizzazione di alcune tipologie di contratti più diffusi) e introducono per gli intermediari bancari e finanziari, anche per la commercializzazione dei servizi bancari tradizionali, obblighi di natura organizzativa ovvero di controllo per il rispetto della disciplina di trasparenza e la correttezza nei rapporti con l'utenza». E ancora, in termini di maggiore chiarezza: «Le nuove regole sono finalizzate al rafforzamento della tutela della clientela e al miglioramento della correttezza dei rapporti tra intermediari e clienti e si ispirano ai seguenti principi.

Semplificazione della documentazione messa a disposizione della clientela: ciò comporta semplificazione e snellimento dei contenuti e semplicità e chiarezza del linguaggio da adattare al livello di cultura finanziaria delle differenti fasce di clientela, anche in relazione al prodotto proposto. Per i prodotti più diffusi come i conti correnti e i mutui è prevista l'adozione di schemi "standard" predisposti dalla Banca d'Italia. Correttezza, completezza e comprensibilità delle informazioni da rendere: informazioni sintetiche, essenziali ed esaurienti

Anche avvalendosi del sempre più efficace supporto informatico, l'istituto bancario ha la possibilità di trattare il dato anche in modo aggregato o con procedure automatizzate. Di qui, le tutele più stringenti assicurate dallo stesso *GDPR*. L'articolo 22 del testo regolamentare si occupa – specificamente – della disciplina dei processi decisionali automatizzati relativi alla persona fisica, ivi compresa la profilazione. Secondo la disposizione, *«l'interessato ha il diritto di non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona»*.

D'altronde, il Regolamento in menzione prevede anche una serie di figure, direttamente deputate non solo a fornire consulenza al Titolare e al Responsabile del trattamento, ma anche a sorvegliarne l'osservanza e l'applicazione, eventualmente fornendo un parere in merito alla valutazione d'impatto sulla stessa protezione dei dati. Il riferimento è ai cd. Responsabili della protezione dei dati (RPD). Nell'ottica della regolamentazione in analisi, la collaborazione fra i tre soggetti appena menzionati costituisce il fulcro della corretta gestione del dato personale (cfr. articolo 38 *GDPR*)⁵³⁰. Ciò detto, va pure evidenziato come la pervasiva diffusione delle nuove tecnologie abbia ormai creato inedite porte d'accesso per nuovi soggetti sul mercato del credito. Le cd. *nuove banche*, digitalizzate, delocalizzate e

consentono al cliente di capire le caratteristiche, i rischi e i costi del prodotto e forniscono la chiara illustrazione dei suoi diritti; l'introduzione di guide pratiche offre un supporto concreto per la comprensione dei prodotti e dei servizi più diffusi. Comparabilità delle offerte: per rendere immediata ed effettiva la comparabilità, la struttura dei documenti riporta le informazioni in un ordine logico e di priorità adatto alle necessità informative del cliente e a facilitare la comprensione e il confronto con prodotti analoghi; per i costi, la raffrontabilità è agevolata dalla estensione agli affidamenti e ai conti correnti destinati alla clientela al dettaglio dell'uso di indicatori sintetici di costo».

⁵³⁰ Questo il testo dell'articolo 38: «1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. 2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica. 3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento. 4. Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento. 5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri. 6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi».

completamente virtuali, hanno rivoluzionato il tradizionale rapporto fra cliente ed intermediario finanziario. Lo scambio di dati richiesto, su piattaforma digitale, dai nuovi attori della finanza ha nel tempo condotto l'interprete ad interrogarsi sulla compatibilità di tali modalità di raccolta e conservazione del dato con i principi costituzionali legati alla tutela della riservatezza dell'individuo.

Così si è espressa anche la Banca d'Italia nella Relazione del Responsabile della Protezione dei Dati per il 2022⁵³¹ in cui afferma che *«l'attività del RPD deve tener conto della progressiva digitalizzazione e delocalizzazione delle informazioni che determinano rischi nuovi ed esigenza di presidi di sicurezza più raffinati nell'azione di protezione degli interessati. La tutela dei dati delle persone fisiche, come delineata dal GDPR, costituisce per le organizzazioni pubbliche e private un obbligo giuridico, del cui adempimento sono tenute a rendere conto; ma nello stesso tempo essa rappresenta nel settore pubblico anche un impegno etico, dal cui assolvimento dipendono i beni immateriali della reputazione della PA e della fiducia del cittadino»*. Non è un caso che l'ultima regolamentazione in materia di tutela del dato personale abbia ormai traslato il concetto di *privacy* all'interno dell'architettura informatica dei sistemi: di qui, il conio dei concetti di *privacy by design* e *privacy by default*. Si tratta di definizioni che per certi versi sembrano aver rivoluzionato l'approccio alla protezione del dato, anticipandone la tutela sin dalla fase di progettazione del sistema dedicato a trattarlo. In particolare, con *privacy by design* s'intende, l'adozione – da parte del titolare del trattamento – di misure tecniche e organizzative adatte a dare attuazione ai principi dettati in materia di *privacy* dallo stesso Regolamento europeo. Del pari, il concetto di *privacy by default* prevede che per impostazione predefinita i sistemi di trattamento gestiscano i dati personali nella sola misura necessaria e sufficiente per le finalità previste ed enucleate dal trattamento stesso. In sostanza, i dati raccolti non devono essere

⁵³¹ [Banca d'Italia, Relazione del Responsabile della Protezione dei Dati. Anno 2022, 2023](#). «Il disegno del legislatore comunitario, che postula l'*accountability* di ogni titolare di trattamento di dati personali, impone per diffuso convincimento uno stile di conduzione delle attività che presuppone una costante attenzione alla tutela dei dati personali, espressa da una coerente ideazione e impostazione dei processi di lavoro, dalla valutazione del rischio di violazione nei confronti delle persone e dalla scelta delle misure di sicurezza tecniche e organizzative ritenute adatte a contenere il rischio. Lo scenario si arricchisce della persistenza di sfide sempre aperte per le amministrazioni pubbliche, nei diversi ambiti di supervisione o di regolazione, quali il bilanciamento della sicurezza dei dati e del presidio sull'accesso agli stessi con gli obblighi di semplificazione e trasparenza o la promozione della fiducia degli utenti attraverso l'educazione al controllo sulle informazioni che riguardano la propria persona e la propria identità».

eccedenti rispetto allo scopo per il quale sono detenuti, né – a corollario – essere conservati per un periodo superiore a quanto strettamente necessario alla realizzazione degli stessi scopi. Lo *European Data Protection Board* si è, al riguardo, preoccupato di dettare alcune Linee guida in argomento⁵³², osservando che *«l'obbligo principale consiste nel predisporre misure adeguate e garanzie necessarie che permettano un'attuazione efficace dei principi della protezione dei dati e, di conseguenza, dei diritti e delle libertà degli interessati fin dalla progettazione e per impostazione predefinita»*⁵³³.

Sulla scorta di quanto detto, non sembrano residuare dubbi sulla necessità mutuare i termini delle stesse valutazioni di compatibilità circa l'applicabilità dei principi in materia di titolarità del trattamento di cui si è fatta ampia menzione fino a questo momento, anche rispetto ai nuovi soggetti di mercato. Del resto, significativo appare il dettato dell'articolo 35 del *GDPR*, il quale disciplina l'ipotesi di un tipo di trattamento che *preveda l'uso di nuove tecnologie* e che, *«considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche»*. In simile occasione, prima di procedere al trattamento, il titolare è chiamato ad effettuare una valutazione dell'impatto di tale nuova modalità di gestione del dato con le previsioni dettate in materia di protezione dei dati personali. Detta valutazione deve, in ogni caso, contenere la

⁵³² [European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.](#)

⁵³³ Si legga, in particolare, a p. 4: *«In un mondo sempre più digitale, il rispetto dei requisiti della protezione dei dati fin dalla progettazione e della protezione per impostazione predefinita svolge un ruolo cruciale nel promuovere la tutela della vita privata e la protezione dei dati nella società. È pertanto fondamentale che i titolari del trattamento prendano sul serio questa responsabilità e si attengano agli obblighi del RGPD quando progettano i rispettivi trattamenti. Le presenti linee guida forniscono orientamenti generali sull'obbligo di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita (in appresso «DPbDD») stabilito dall'articolo 25 del RGPD. La DPbDD costituisce un obbligo per tutti i titolari del trattamento, indipendentemente dalle dimensioni e dalla complessità del trattamento stesso. Per poter attuare la DPbDD, è di cruciale importanza che il titolare comprenda i principi della protezione dei dati nonché i diritti e le libertà dell'interessato»*. Ancora, di particolare interesse a p. 5: *«Le linee guida sono incentrate sull'attuazione, da parte dei titolari del trattamento, della DPbDD in virtù dell'obbligo di cui all'articolo 25 del RGPD. Anche altri attori, quali i responsabili del trattamento e i produttori di prodotti, servizi e applicazioni (in prosieguo: «produttori»), che non sono direttamente contemplati dall'articolo 25, possono trovare utili queste linee guida in vista della creazione di prodotti e servizi conformi al RGPD che consentano ai titolari del trattamento di adempiere ai propri obblighi in materia di protezione dei dati. Il considerando 78 del RGPD aggiunge che la DPbDD dovrebbe essere presa in considerazione nell'ambito degli appalti pubblici. Sebbene tutti i titolari abbiano il dovere di integrare la DPbDD nelle attività di trattamento, questa disposizione incentiva l'adozione dei principi di protezione dei dati nella misura in cui le pubbliche amministrazioni dovrebbero dare il buon esempio. Il titolare è tenuto ad assicurare il rispetto degli obblighi di DPbDD in relazione al trattamento svolto dai rispettivi responsabili e sub-responsabili e, pertanto, deve tenerne conto quando stipula contratti con tali soggetti»*.

«a) descrizione sistematica dei trattamenti previsti e delle finalità del trattamento (...); b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati (...); d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento (...)»⁵³⁴. Sul punto, sia consentito rinviare al maggiore approfondimento condotto nel paragrafo che segue, laddove saranno meglio analizzate le nuove, recenti implicazioni che il discorso ha avuto in materia di operatori finanziari del digitale.

3. Regolamento *DORA* – *Digital Operational Resilience Act*: le nuove frontiere della tutela della *privacy* nel settore finanziario

Risale al 27 dicembre 2022 la pubblicazione in Gazzetta Ufficiale dell’Unione Europea del Regolamento 2022/2554/UE del Parlamento Europeo e del Consiglio del 14 dicembre 2022, in materia di resilienza operativa digitale per il settore finanziario, conosciuto con l’acronimo di *DORA* (*Digital Operational Resilience Act*). Più nello specifico, l’atto normativo si rivolge a tutti le entità finanziarie che operano nel digitale. In realtà, oltre ai classici intermediari quali banche, imprese di investimento ed assicurazioni, in questo quadro vengono ricompresi anche i *Crypto-Asset Service Provider*, specie nella forma di emittenti di *Asset-Referenced Token* (*ART*)⁵³⁵. Perciò, quanto verrà detto in seguito farà automaticamente riferimento anche a questi nuovi soggetti *crypto*.

L’intervento del Legislatore europeo prende le mosse dalla rilevanza ormai assunta nell’era digitale dalle tecnologie dell’informazione e della comunicazione (cd. *ICT* – *Information Communication Technology*), le quali sostengono, oggi, ogni sistema complesso impiegato nelle quotidiane attività. In particolare, «(le stesse) mantengono in funzione i principali settori delle nostre economie, tra cui il settore finanziario, e migliorano il funzionamento del mercato interno (...) L’uso onnipresente dei sistemi di *ICT* e l’elevata digitalizzazione e connettività sono oggi caratteristiche fondamentali delle attività delle entità finanziarie dell’Unione». Tuttavia, emerge l’evidenza per cui «la loro resilienza digitale deve ancora

⁵³⁴ Articolo 35, comma 7, del Regolamento generale sulla protezione dei dati personali.

⁵³⁵ [Elteste U. e Nietsch T., Exploring DORA: EU tightens IT Security rules for the financial sector, targeting “critical” third-party providers, K&L Gates Hub, 2023.](#)

*essere affrontata e integrata in maniera più efficace nei loro quadri operativi di portata più ampia»⁵³⁶. Oggi la digitalizzazione riguarda l'intero sistema dei pagamenti, che dal cartaceo/contante sono oramai trasmutati in una dimensione digitale. La compensazione, il regolamento dei titoli, la negoziazione elettronica e algoritmica, le operazioni di prestito e finanziamento, la *peer-to-peer finance*, la gestione dei crediti e le operazioni di *back office*, del pari, hanno subito una quasi completa digitalizzazione. Insomma, «non solo l'intero settore finanziario è diventato in larga misura digitale, ma la digitalizzazione ha anche reso più marcate le interconnessioni e le dipendenze all'interno del settore e nei confronti di fornitori terzi di infrastrutture e servizi»⁵³⁷. Sul punto, già dal 2019 si sono susseguiti diversi alert da parte delle istituzioni preposte, in relazione alla necessità di adottare approcci coerenti alla migliore gestione del rischio informatico nel settore finanziario cosicché la resilienza operativa digitale nel settore dei servizi del credito e della finanza venisse potenziata a livello unionale⁵³⁸. Messa in questa prospettiva, obiettivo del Regolamento*

⁵³⁶ [Regolamento DORA](#), Considerando n. 1.

⁵³⁷ *Ivi*, Considerando n. 2.

⁵³⁸ Il riferimento è ai pareri tecnici dell'[EBA \(Autorità bancaria europea\)](#), istituita dal [Regolamento 1093/2010/UE](#) del Parlamento Europeo e del Consiglio, dell'[EIOPA \(Autorità europea delle assicurazioni e delle pensioni aziendali e professionali\)](#) istituita dal [Regolamento 1094/2010/UE](#) del Parlamento europeo e del Consiglio; dell'[ESMA \(Autorità europea degli strumenti finanziari e dei mercati\)](#) istituita dal [Regolamento 1095/2010/UE](#) del Parlamento europeo e del Consiglio. La questione, a parere del Regolatore europeo, pare comunque originare dal fatto che «il settore finanziario dell'Unione è regolamentato da un codice unico ed è disciplinato da un sistema europeo di vigilanza finanziaria. Le disposizioni sulla resilienza operativa digitale e sulla sicurezza delle ICT non sono tuttavia ancora armonizzate in maniera completa o coerente, benché nell'era digitale la resilienza operativa digitale sia un elemento fondamentale della stabilità finanziaria e dell'integrità del mercato, non meno importante, ad esempio, delle norme comuni riguardanti gli aspetti prudenziali o la condotta sul mercato. Sarebbe quindi opportuno perfezionare il codice unico e il sistema di vigilanza per coprire anche la resilienza operativa digitale, rafforzando i mandati delle autorità competenti per consentire loro di vigilare sulla gestione dei rischi informatici nel settore finanziario al fine di proteggere l'integrità e l'efficienza del mercato interno ed agevolarne il regolare funzionamento», Considerando n. 8. In particolare: «Ad oggi, dal momento che le disposizioni sui rischi informatici sono state trattate in modo soltanto parziale a livello di Unione, esistono carenze o sovrapposizioni in settori importanti, come la segnalazione degli incidenti connessi alle ICT e i test di resilienza operativa digitale, nonché incoerenze dovute alla divergenza delle norme nazionali o al sovrapporsi di norme la cui applicazione risulta inefficiente sotto il profilo dei costi. Si tratta di una situazione particolarmente dannosa per un settore come quello finanziario, che si contraddistingue per l'intenso ricorso alle ICT poiché i rischi tecnologici non conoscono frontiere e il settore finanziario offre i suoi servizi su base transfrontaliera sia all'interno che all'esterno dell'Unione. Le singole entità finanziarie che sono attive a livello transfrontaliero o detengono varie autorizzazioni (ad esempio, un'entità finanziaria può detenere autorizzazioni a operare quale banca, impresa di investimento e istituto di pagamento, ciascuna delle quali rilasciata da una diversa autorità competente in uno o più Stati membri) devono superare autonomamente sfide operative poste dai rischi informatici e dalla necessità di mitigare gli impatti

DORA è quello di conseguire un livello comune elevato di resilienza operativa digitale, stabilendo una serie di obblighi uniformi relativi alla sicurezza dei sistemi informatici e delle reti, che sostengono i processi commerciali delle entità finanziarie⁵³⁹.

Non potendo soffermare oltre questa trattazione rispetto alle novità connesse all'applicazione del citato Regolamento, ciò che ora più strettamente interessa riguarda gli impatti a livello di protezione del dato personale delle persone fisiche di fronte a sistemi finanziari che si fanno sempre più interconnessi, soprattutto all'esito dell'entrata in vigore del *Digital Operational Resilience Act* (che sarà applicabile a decorrere dal 17 gennaio 2025). Se da un lato pare indiscutibile il dovere di sottolineare gli evidenti vantaggi connessi alla digitalizzazione del settore bancario e finanziario, dall'altro gli operatori di mercato e comunità giuseconomica si sono interrogati sui possibili impatti di una circolazione delle informazioni *online* così pervasiva. In tal senso, il Regolamento *DORA* dovrebbe avere l'ambizione di operare un intervento a tutto tondo, capace di effettuare una sorta di integrazione delle tutele in materia di trattamento del dato persona che dovrebbe assicurare la piena protezione delle informazioni circolanti nel campo delle operazioni digitali.

In merito all'impianto normativo innestato sul tema, vi è parte della dottrina che al contempo spende parole positive e caute, constatando che *«il DORA e il GDPR sono testi giuridici che, seppur tra loro diversi, sono essenziali e complementari per salvaguardare la privacy e garantire la sicurezza informatica del settore finanziario digitale nell'UE. Al contempo, essi pongono sfide e complessità per le FE (Financial Entities, NDR) e i loro fornitori terzi di servizi ICT, che dovranno adottare (e aggiornare, con riferimento al GDPR) piani di adeguamento che tengano conto delle peculiarità di entrambi i quadri giuridici. Le FE (e i fornitori di servizi ICT soggetti al DORA) dovrebbero quindi prendere in considerazione la possibilità di integrare la gestione del rischio ICT e i principi di protezione dei dati in un unico processo decisionale. Una strategia e un approccio integrati possono facilitare la conformità al GDPR e al DORA, e allo stesso tempo ridurre il livello di esposizione al rischio»*⁵⁴⁰. In altri termini, si tratta di operare lungo una traccia di ripensamento delle tutele

avversi degli incidenti connessi alle ICT in maniera coerente ed efficiente sotto il profilo dei costi», Considerando n. 10.

⁵³⁹ Regolamento *DORA*, Articolo 1.

⁵⁴⁰ [Olivi G. e Venditti A., Tra DORA e GDPR: cybersecurity e privacy nel settore bancario, Diritto Bancario, 2023.](#)

approntate per il dato personale, che dovrebbero ora procedere in parallelo anche in relazione alle offerte del mercato finanziario digitalizzato. Quest'ultima esigenza si avverte ancor più alla lettura dello stesso Regolamento. Ad esempio, laddove l'invito del *DORA* è quello di *«incoraggiare le entità finanziarie a scambiarsi reciprocamente informazioni e analisi delle minacce informatiche e a sfruttare collettivamente, sul piano strategico, tattico e operativo, le conoscenze e le esperienze pratiche che hanno acquisito a livello individuale al fine di accrescere le proprie capacità di valutare e monitorare adeguatamente le minacce informatiche»*⁵⁴¹, gli aspetti connessi alla tutela del profilo della riservatezza del dato sono immediatamente presi in considerazione. Difatti, *«essi dovrebbero operare sulla base del ricorso a una o più basi giuridiche stabilite all'articolo 6 di tale regolamento, ad esempio nel contesto del trattamento dei dati personali necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, ai sensi dell'articolo 6, paragrafo 1, lettera f), dello stesso regolamento, nonché nel contesto del trattamento dei dati personali necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento»*⁵⁴². Si aggiunga inoltre che, laddove il Regolamento *DORA* si occupa di delineare le modalità del *«monitoraggio, da parte di un'entità finanziaria, dei rischi informatici derivanti da terzi»*⁵⁴³, la prescrizione è immediatamente quella di verificare la presenza di *«disposizioni contrattuali che specificano in che modo il fornitore terzo di servizi ITC garantisce l'accessibilità, la disponibilità, l'integrità, la sicurezza e la protezione dei dati personali; disposizioni che stabiliscono le pertinenti garanzie per consentire l'accesso, il ripristino e la restituzione dei dati in caso di insolvenza, risoluzione o cessazione dell'operatività del fornitore terzo di servizi ITC, nonché disposizioni che impongono al fornitore terzo di servizi ITC di prestare assistenza in caso di incidenti connessi alle ITC in relazione ai servizi forniti, senza costi supplementari oppure a un costo stabilito ex ante»*⁵⁴⁴. Perciò, la gestione dei rischi informatici derivanti da terzi rappresenta una delle maggiori aree di regolamentazione imposta dal Regolamento *DORA* alle entità finanziarie.

Le stesse, stando al dettato di cui all'articolo 28, sono chiamate alla gestione dei rischi

⁵⁴¹ Regolamento *DORA*, Considerando n. 34.

⁵⁴² *Ibidem*.

⁵⁴³ Regolamento *DORA*, Considerando n. 71.

⁵⁴⁴ *Ibidem*.

informatici derivanti da terzi *«quali componenti integranti dei rischi informatici nel contesto del proprio quadro per la gestione di detti rischi di cui all'articolo 6, paragrafo 1 (...)»*, in conformità ad una serie di principi fondamentali (dettati, peraltro, per la *solida gestione* dei predetti rischi). Più in particolare, le entità finanziarie sono chiamate a stabilire clausole che consentano la risoluzione degli accordi contrattuali per l'utilizzo di servizi *ICT* nel caso in cui *«punti deboli del fornitore terzo di servizi TIC emersi riguardo alla sua gestione complessiva dei rischi informatici e, in particolare, nel modo in cui il fornitore garantisce la disponibilità, autenticità, integrità e riservatezza dei dati, siano essi dati personali o altrimenti sensibili, oppure dei dati non personali»*⁵⁴⁵. Insomma, il compito ora assegnato agli operatori finanziari implica valutazioni in punto di:

- a) gestione dei rischi delle *ITC*;
- b) gestione degli incidenti connessi alle *ITC*⁵⁴⁶;
- c) test di resilienza operativa digitale⁵⁴⁷;
- d) condivisione dati ed informazioni in relazione a vulnerabilità e minacce informatiche;
- e) gestione dei rischi informatici derivanti da *Third Provider*⁵⁴⁸.

In ciascuno di simili scenari dovrà essere fornita dedicata analisi e tutela alle modalità d'impatto sul dato personale trattato, nella stessa ottica integrata di cui si parlava in apertura del presente paragrafo.

⁵⁴⁵ Regolamento DORA, articolo 28, "Principi generali", paragrafo 7, lettera c).

⁵⁴⁶ Il Regolamento definisce "Incidente connesso alle *ICT*" *«un singolo evento, o una serie di eventi collegati non programmati dall'entità finanziaria, che compromette la sicurezza dei sistemi informatici e di rete e ha un impatto avverso sulla disponibilità, autenticità, integrità o riservatezza dei dati o sui servizi forniti dall'entità finanziaria»* (articolo 1, par. 1, n. 8)).

⁵⁴⁷ Il Regolamento definisce la "Resilienza Operativa Digitale" come *«la capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi TIC, l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza dei sistemi informatici e di rete utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità, anche in occasione di perturbazioni»* (articolo 3, par. 1, n. 1)).

⁵⁴⁸ Il Regolamento definisce i "Rischi informatici derivanti da terze parti" come *«rischi relativi alle TIC cui un'entità finanziaria può essere esposta in relazione al ricorso, da parte di questa, a servizi TIC offerti da fornitori terzi o da subappaltatori di tali fornitori, anche mediante accordi di esternalizzazione»*.

Si rinvia, per approfondimenti che esulano da questa parte della trattazione, alla lettura del contributo di [Lio O., Paganelli C., Tulliani M., Regolamento DORA: ecco cosa devono fare le aziende del settore finanziario per adeguarsi, Agenda Digitale, 2023.](#)

4. Privacy e valuta digitale: il concetto della anonimizzazione delle transazioni e i profili di rischio

Nella complessità del discorso sinora intavolato in merito al rapporto tra *privacy* e finanza digitale, devono ora esaminarsi più attentamente le questioni introdotte dai *digital asset*. Si pensi al recentissimo caso *Worldcoin*, dai più ritenuto emblematico in considerazione dei profili di rischio legati al trattamento del dato personale dell'utente che si muove nell'articolato sistema delle criptovalute. Si tratta di una valuta creata da una società nota con il nome di *Tools for Humanity*, utilizzabile dagli utenti all'esito dell'esperimento di una serie di *controlli di sicurezza*, tra cui la scansione dell'iride. Allo stato attuale, come e dove siano conservati simili dati non è ancora chiaro⁵⁴⁹. Stando alle dichiarazioni dell'azienda riportate dalla fonte appena citata, la scansione dovrebbe servire «a dimostrare di essere una persona (e quindi non un bot) distinta rispetto agli altri esseri umani. A loro volta, le aziende di social media e le altre piattaforme online saranno in grado di verificare l'autenticità degli utenti, eliminando così le azioni dannose a opera dei bot, dallo spam alle frodi, fino alla diffusione di disinformazione»⁵⁵⁰.

Al netto dei progressi apportati dalla crittografia al settore finanziario, ampiamente ricordato in questo elaborato, diversi sono i profili di rischio che gli operatori di settore non hanno mancato di sottolineare le insidie derivanti dall'utilizzo di cripto-attività. Da un lato, infatti, il carattere relativamente anonimo di simili strumenti di pagamento ha consentito a parte della criminalità di avvalersi di una rinnovata modalità di impiego e riciclo del denaro proveniente da attività illecite. Dall'altro, l'assenza di un quadro regolamentare che definisca i termini e le tutele a fronte del ricorso a strumenti di pagamento sì strutturati ha esposto gli utenti della prima ora a rischi di ingenti perdite economiche, nonché a frodi connesse al fallimento o all'improvvisa sospensione dei servizi delle piattaforme di gestione dei portafogli digitali. Visto da questa angolazione, il settore bancario tradizionale non ha che potuto guardare con netto sfavore all'introduzione e alla circolazione delle cripto-attività, anche alla luce della totale decentralizzazione della gestione delle stesse, capaci di eliminare qualsiasi funzione di

⁵⁴⁹ Persino la stampa si è interessata alla vicenda: [Khalili J., Vi fareste scansionare l'iride in cambio di una criptovaluta?, Wired, 2023.](#)

⁵⁵⁰ *Ivi.*

intermediazione rimessa agli istituti di credito e agli intermediari finanziari.

D'altra parte, i sistemi di pagamento digitale legati ai *crypto-asset* avrebbero mancato di mantenere le proprie promesse: queste sono state le parole spese in un discorso del dott. Fabio Panetta, membro dell'*Executive Board della Banca Centrale Europea (BCE)*⁵⁵¹. Pertanto, conviene prendere atto di un simile fallimento per analizzare le novità, anche in termini di "innovazione dell'anonimizzazione", promesse dalle valute digitali.

Al fine di meglio comprendere le problematiche collegate alla protezione dei dati personali, è necessario considerare due aspetti rilevanti. *In primis* (i) l'identificazione del soggetto che si occupa della determinazione delle modalità in cui vengono trattati i dati personali e, in secondo luogo, (ii) l'individuazione del soggetto che si occupa di controllare il modo in cui i dati sono conservati e gestiti⁵⁵². In tal senso, v'è anche chi ha osservato come «queste distinzioni preliminari hanno ricadute in materia di data protection, con la conseguenza che un giudizio sulla compatibilità tra i registri distribuiti e il GDPR va preferibilmente formulato sulla base di un'analisi dettagliata caso per caso che tenga conto del design tecnico specifico e dello specifico assetto di governance: le blockchain non sono tutte compatibili o incompatibili con la disciplina sulla protezione dei dati, giacché ogni uso della tecnologia deve essere esaminato in base alle proprie caratteristiche»⁵⁵³.

È recente la presentazione, in Italia, della proposta di legge d'iniziativa di un numero di deputati, con ad oggetto il «divieto di utilizzo delle criptovalute che impiegano tecniche di

⁵⁵¹ [Panetta F., *Paradise lost? How crypto failed to deliver on its promises and what to do about it*, 23 giugno 2023](#), contributo della BCE reperibile anche sotto forma di [slides](#). «Oggi sosterrò che, a causa dei loro limiti, le criptovalute non si sono sviluppate in una forma di finanza innovativa e robusta, ma si sono trasformate in una forma deleteria. L'ecosistema delle criptovalute è pieno di fallimenti del mercato e di externalità negative, ed è destinato a subire ulteriori sconvolgimenti del mercato a meno che non vengano messe in atto adeguate tutele normative. I politici dovrebbero diffidare dal sostenere un'industria che finora non ha prodotto alcun beneficio per la società e che sta cercando sempre più di integrarsi nel sistema finanziario tradizionale, sia per acquisire legittimità come parte di tale sistema sia per appoggiarsi ad esso. Le autorità di regolamentazione dovrebbero invece sottoporre le criptovalute a standard normativi rigorosi, affrontare il loro costo sociale e trattare i modelli di criptovaluta non validi per quello che sono realmente: una forma di gioco d'azzardo. Ciò potrebbe indurre l'ecosistema a compiere maggiori sforzi per fornire un valore autentico nel campo della finanza digitale».

⁵⁵² Zambardino F, *La blockchain e la protezione dei dati personali: una tecnologia privacy compliant by design?*, 2 EJPLT, 2022, pp. 136-152.

⁵⁵³ [Pellecchia E., *GDPR e tecnologie blockchain: prospettive di evoluzione di un rapporto complesso*, 2021](#); Navaretta E., Ricci L., Villani A. (a cura di): *Il potere della tecnica e la funzione del diritto: un'analisi interdisciplinare di blockchain* – in *Vol. I Blockchain, democrazia e tutela dei diritti fondamentali*, p. 149 e ss.

anonimizzazione totale nelle transazioni economiche»⁵⁵⁴. In quell'occasione, si era posto l'accento sulla cd. tecnologia zero-knowledge; infatti, sulla Relazione d'accompagnamento alla Proposta si leggeva che «la ricerca in materia crittografica sta abilitando una nuova generazione di criptovalute che utilizza, per la dimostrazione delle transazioni, anche metodi crittografici chiamati “a conoscenza zero”. Una criptovaluta con sistemi di dimostrazione a conoscenza zero assicura, su una rete decentralizzata che utilizza una blockchain pubblica, una confidenzialità totale dei pagamenti celando, in ogni transazione, l'ammontare, il soggetto pagatore e il soggetto pagato. Le transazioni possono essere verificate esclusivamente se in possesso di una chiave di visualizzazione che, per ogni transazione, è nella disponibilità esclusiva del soggetto pagatore e del soggetto pagato. In questo modo, si realizza un sistema di pagamento totalmente anonimo che, a differenza del danaro contante, consente trasferimenti di valuta da un capo all'altro del mondo in tempo reale, senza possibilità di conoscere la provenienza dello stesso a una eventuale conversione in moneta fiat». Insomma, diverse questioni sono state messe in luce in questo ambito ed è questo un discorso che non può essere affrontato se non in parallelo alle considerazioni effettuate in materia di antiriciclaggio. Le stesse regole OCSE hanno dato risalto alla necessità di rendere pubblici gli intermediari degli scambi in valuta digitale, ossia chi rende servizi al pubblico utili a facilitare le transazioni in asset criptati⁵⁵⁵, su piattaforme di trading online.

Nel chiudere il paragrafo, sembra significativo citare una significativa considerazione svolta dalla Banca Centrale Europea, la quale ha dimostrato che *«i venditori preferiscono sempre utilizzare questi token per i depositi quando sono disponibili, perché così possono sfuggire alla cattura delle banche. In altre parole, nel nostro ambiente la disintermediazione ha luogo perché il settore bancario non è competitivo e i token della piattaforma disciplinano le banche nella competizione»⁵⁵⁶.*

⁵⁵⁴ [Camera dei deputati – XVII legislatura, Proposta di legge d'iniziativa dei Deputati Quintarelli, Mucci, Dambruoso, Galgano, Librandi, Menorello, Monchiero, Vargiu, Catalano, Basso, Carrozza, Dallai e Marzano, presentata il 26 ottobre 2016.](#)

⁵⁵⁵ [OCSE, Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard, 2022](#), p. 11: «Come si è detto, gli intermediari e gli altri fornitori di servizi che facilitano gli scambi tra crypto-asset rilevanti, nonché tra crypto-asset rilevanti e valute fiat, svolgono un ruolo centrale nel mercato dei crypto-asset. Pertanto, si propone che le entità o le persone fisiche che, come attività commerciale, forniscono servizi per effettuare transazioni di scambio in crypto-asset rilevanti, per o per conto dei clienti, siano considerate fornitori di servizi di segnalazione di crypto-asset ai sensi del CARF».

⁵⁵⁶ [BCE, Working Paper: the digital economy, privacy and CBDC – N. 2662, maggio 2022](#), p. 34.

5. Privacy e CBDC: verso la regolamentazione della valuta digitale. Quali (nuovi) impatti sulla riservatezza delle persone fisiche?

«Pensiamo alla CBDC come a una versione elettronica del contante. Nel nostro contesto, ciò significa che la CBDC consente ai venditori di effettuare vendite online senza rivelare il loro tipo alla banca. Di conseguenza, i venditori possono ora scegliere anche uno schema di commercio online-CBDC (ON-CBDC)», così si è di recente espressa la BCE⁵⁵⁷.

Come accennato in apertura, vale quindi la pena spendere alcune considerazioni circa l'avvento delle cd. *Central Bank Digital Currency* e le modalità con cui simili circuiti gestiscono il dato della persona fisica. Si tratta, a ben vedere, della diffusione di un *token* che ha caratteristiche simili alla criptovaluta; la differenza, in questo contesto, deriva dal fatto che l'emissione è riconducibile alla Banca Centrale del singolo Paese (ed il legame sarà, quindi, intrattenuto con la valuta avente corso legale nello stesso Paese).

D'altronde, è affermazione della Consob quella per cui *«guardato, tuttavia, come fase primordiale di un più ampio processo di sperimentazione tecnologica e finanziaria, le criptovalute e, più in generale, la distributed ledger technology potrebbero utilmente porre le basi per dar vita a soluzioni capaci di rendere più efficiente o, secondo i più ottimisti, di trasformare radicalmente l'attuale sistema economico»*⁵⁵⁸. Tanto che *«sembra, al riguardo, auspicabile che le autorità calibrino i contenuti delle future regolazioni in modo da affrontare adeguatamente i rischi, senza, tuttavia, soffocare oltremodo l'innovazione. Gli organismi internazionali stanno giocando un ruolo importante nell'identificazione e nella valutazione dei rischi posti dalle valute virtuali e potrebbero senz'altro contribuire a facilitare il processo di sviluppo e di affinamento delle politiche regolatorie a livello nazionale»*⁵⁵⁹.

Insomma, sembra che l'originario sfavore connesso all'impiego di simili prodotti tecnico-finanziari possa lasciare il passo ad un loro assorbimento nelle modalità di pagamento in uso agli stessi Stati, implementandone gli aspetti positivi e assoggettando a adeguata

⁵⁵⁷ Ahnert T. et al., *ECB Working Paper Series. The digital economy, privacy and CBDC* – N. 2662, maggio 2022, p. 21.

⁵⁵⁸ Cfr. Consob, *Le criptovalute: cosa sono e quali rischi si corrono*, *Le conoscenze finanziarie e di base*, 2023.

⁵⁵⁹ *Ibidem*.

regolamentazione quelli che sinora hanno mostrato i profili di maggiore criticità. Tant'è vero che le Banche Centrali, di recente, stanno implementando lo sviluppo di tale moneta, quasi in reazione al grande successo ottenuto – a livello mondiale – dalle valute virtuali (o cripto-valute), onde arginarne le criticità, soprattutto in punto di controllo delle dinamiche di circolazione.

Come già accennato in precedenza, pure la Banca Centrale Europea (BCE) ha allo studio, in collaborazione con le Banche Centrali nazionali facenti parte dell'Eurosistema, l'introduzione di un cd. Euro Digitale, rappresentando *«un passo necessario per assicurare che il nostro sistema monetario sia preparato a un futuro digitale. Sarà ampiamente accessibile e semplice da utilizzare, garantendo al tempo stesso la privacy, al pari del contante»*⁵⁶⁰. A ben pensarci, l'iniziativa assunta da Francoforte si rivela in linea con l'andamento generale in tema di digitalizzazione dei pagamenti. La stessa pandemia da *COVID-19*, nell'incentivare l'utilizzo degli scambi *online*, ha trascinato gli utenti in una dimensione sempre più digitale. Difatti, *«non si può ignorare quanto sta accadendo: l'uso del contante come mezzo di pagamento è in calo in molte parti del mondo, inclusa l'Europa. Con il passaggio a un'economia digitale, l'introduzione del contante in forma digitale è quindi il passo più logico da compiere»*⁵⁶¹. In relazione a ciò, pare allora d'obbligo chiedersi quali potranno essere gli impatti in termini di tutela della riservatezza delle persone fisiche che faranno uso di simili sistemi di pagamento. È infatti evidente che l'avvento di una forma di valuta digitale, pubblica e riconosciuta dagli Stati, debba ricondurre al centro del discorso quello dell'identificabilità e tracciabilità di una transazione.

D'altronde, la migliore tutela della *privacy* non potrà essere ignorata in tale frangente giacché quest'ultima *«sarà un tratto distintivo dell'euro digitale. La BCE non avrà accesso né ai dati personali degli utenti né alle loro scelte di pagamento. La possibilità di pagare offline garantirà un grado di protezione dei dati superiore a quello di qualsiasi altro metodo di pagamento digitale oggi disponibile»*⁵⁶². Su questo versante, diversa dottrina si è già occupata di analizzare i termini di una possibile relazione di compatibilità tra l'utilizzo delle tecnologie *blockchain* e la regolamentazione dettata dal *GDPR* in tema di "trattamento"

⁵⁶⁰ [Panetta F., Dombrovskis V., Perché l'Europa ha bisogno di un euro digitale, 2023.](#)

⁵⁶¹ *Ibidem.*

⁵⁶² *Ibidem.*

(anche automatizzato) dei dati personali. Se è vero che vi sono «*talune caratteristiche delle blockchain le renderebbero incompatibili con il GDPR: tra queste, l'impossibilità di individuare un titolare del trattamento, l'impossibilità di applicare i diritti dell'interessato, l'inconciliabilità con il diritto di cancellazione, il contrasto con il principio di minimizzazione del trattamento*»⁵⁶³, si è comunque creduto di poterne valorizzare gli aspetti maggiormente innovativi, al fine di sfruttarne le possibilità sul lato statuale⁵⁶⁴. Di qui, allora, l'eventualità dell'introduzione di un *e-Euro* entro i prossimi quattro anni, stando alle dichiarazioni rese dall'*Executive Board* della BCE, di cui si è fatta menzione sopra.

Una simile “reazione istituzionale” al fenomeno della valuta digitale è stato letto anche in termini di “sfida” all’iniziativa assunta dai colossi del web (cd. *Big Tech*) di creare una propria moneta. In questi termini si è espressa l’Autorità garante per la protezione dei dati personali, asserendo che «*la sfida lanciata da Facebook con la valuta alternativa è l'ennesimo segnale di una vera emergenza democratica legata alla società digitale. I colossi del web hanno oggi volumi di transazioni paragonabili a quelle di molti Stati, trattano alla pari con i governi, fanno con loro accordi non solo commerciali, e adesso battono anche moneta. Quote immense di potere stanno via via passando di mano dagli Stati a soggetti privati. Se il settore non sarà vincolato in fretta a principi di governance democratica, rischiamo di consegnare un'ampia fetta dei nostri diritti a un pugno di monarchie digitali, fondate sul potere dei dati*»⁵⁶⁵. La cd. *questione di potere* da cui ha messo in guardia l’Autorità indipendente, in effetti, sembra destinata a delineare una contrapposizione sempre più marcata tra Stato e mercato, con rilevanti impatti in punto di detenzione del dato. Il *potere del dato* è infatti la ricchezza accumulata, nei termini della società dell’informazione, da chi ha la capacità di raccoglierne di più. Le *Big Tech*, con le loro colossali possibilità di *storage*,

⁵⁶³ *Ivi*, p. 155.

⁵⁶⁴ Cfr. [BCE, ECB Working Paper Series: The digital economy, privacy and CBDC, at a panel on the future of crypto at the 22nd BIS Annual Conference, Basel, 2023](#). Si legga, nella dichiarazione di intenti: «*Studiamo un modello di intermediazione finanziaria, scelta di pagamento e privacy nell'economia digitale. I pagamenti digitali consentono ai commercianti di vendere beni online, ma rivelano anche informazioni alle banche. Al contrario, il contante garantisce l'anonimato, ma limita la distribuzione a luoghi offline meno efficienti. In equilibrio, i commercianti scambiano i guadagni di efficienza derivanti dalla distribuzione online (con i pagamenti digitali) e le rendite informative derivanti dal mantenimento dell'anonimato (con il contante). L'introduzione della moneta digitale della banca centrale (CBDC) aumenta il benessere perché riduce i problemi di privacy associati alla distribuzione online. I gettoni di pagamento emessi dalle piattaforme digitali escludono la CBDC, a meno che quest'ultima non faciliti la condivisione dei dati*».

⁵⁶⁵ [Soro A., Criptovalute. Con la moneta i big del web diventano Stati-padroni, Il Mattino, 2019](#).

sono in grado oggi di accumulare un numero indefinito di informazioni relative a qualsiasi aspetto della vita quotidiana degli individui che navigano il web e che, più o meno consapevolmente, gliele forniscono. Ciononostante, *«il punto vero della questione è che chi possiede la piattaforma nella quale si svolgono gli scambi monetari, è lo stesso soggetto che possiede le informazioni di miliardi di persone. Parliamo di soggetti che attraverso quelle informazioni hanno sviluppato un crescente potere di persuasione e di predizione e che tendenzialmente potrebbero sviluppare un sistema infettato dai gerani della discriminazione. Se una piattaforma decide di estromettere un certo soggetto o una certa categoria di persone dal suo sistema di pagamento privato, che fine fanno i loro diritti? Chi li tutela?»*⁵⁶⁶. In tal misura, mai come in questi ultimi anni è emersa la necessità di una regolamentazione della gestione di simili informazioni. Le ripercussioni sono evidenti: si pensi alla parabola degli acquirenti di moneta digitale o degli investitori in criptovalute che, da un giorno all'altro, hanno visto sparire le piattaforme di gestione dei loro portafogli digitali. Un problema così acceso come la tutela dei diritti fa peraltro il paio con la capacità del singolo di gestire il flusso dei propri dati personali, secondo le chiare regole dettate dalla normativa GDPR. La garanzia della riservatezza delle informazioni diffuse sul web, allora, deve essere qui letta non più come anonimizzazione delle transazioni (a tutto favore degli scopi illeciti che di queste vogliono farsi) ma come tutela del soggetto-consumatore che si serve del web a fini di investimento⁵⁶⁷. Non si può, allora, che guardare con rinnovata attesa all'intenzione dell'Eurozona di regolare da sé la possibile emissione di una valuta digitale, che tenti quantomeno di arginare il proliferare di dati nelle maglie di *Internet*.

⁵⁶⁶ *Ibidem*. V. anche, sullo stesso argomento, Intervento di Soro A., *Big data e libertà nella dimensione digitale*, 28 agosto 2018. Interessante il passaggio che si riporta: «Se, a proposito dei Big Data, si è parlato di quarta rivoluzione (pur con tutti i limiti che assumono questo tipo di periodizzazioni), è essenzialmente per gli effetti dirompenti determinati dalle loro caratteristiche addizionali di volume delle informazioni- di mole così rilevante da essere stoccate prevalentemente con il cloud- velocità dell'analisi cui sono sottoposti, eterogeneità di fonti, formato e struttura (potendo essere strutturati o meno), attendibilità. È la regola delle 4 v: volume, velocità, varietà, veridicità, caratteristiche che ne generano una quinta: valore, profitto».

Si tratta, infatti, di «soggetti dotati di eccezionale potere tecnologico (che) rischiano di creare enormi asimmetrie rispetto al mercato regolato. Di conseguenza bisognerà alzare la guardia. Non è un problema di settore, ma di equilibri di potere. La società digitale rischia di determinare una vera emergenza, che chiama in causa i futuri equilibri della nostra democrazia». Vds. [Soro A., Criptovalute. Con la moneta i big del web diventano Statipadroni, cit.](#)

⁵⁶⁷ Soro A., *Democrazia e potere dei dati. Libertà, algoritmi, umanesimo digitale*, Baldini + Castoldi 2019.

RIFLESSIONI CONCLUSIVE

Giunti al termine del lavoro, si raccoglieranno gli aspetti salienti dell'elaborato, cui seguiranno delle riflessioni conclusive.

Il **primo capitolo** è stato speso per dare un'illustrazione – il più lineare possibile – dei fattori che hanno portato allo sdoppiamento della *TradFi* in “*crypto financial system*”. Nello specifico, in un clima di generale sfiducia a seguito della Grande Recessione e la contestuale ondata di cambiamento apportato dal fenomeno *FinTech*, si è visto come le *crypto technology* (*DLT, blockchain e smart contract*) abbiano rimodulato in maniera più o meno significativa la natura dei capisaldi della finanza tradizionale (fiducia, sistemi di pagamento ed intermediari). La ricomposizione di questi nuovi elementi, alla stregua del sistema finanziario *mainstream*, ha determinato la creazione di un perimetro crittografico succedaneo e separato, al cui interno si possono individuare grossomodo due macro-dimensioni: *CeFi* e *DeFi*. In merito a ciò, è stato opportunamente puntualizzato come la linea di demarcazione che le separa appaia piuttosto labile, tanto da portare all'attenzione di chi legge la ragionevole opzione di concepire – almeno allo stato attuale – l'ecosistema *crypto* come un'unica dimensione centralizzata-decentralizzata (*CeDeFi*), punto d'incontro realistico in cui gli approcci e le peculiarità di *CeFi* e *DeFi* si mescolano, sintetizzando le migliori funzionalità di entrambe. Tale circostanza si riflette peraltro nella “duplice anima” insita nei *Crypto-Asset Service Provider* e nei servizi da loro erogati.

Sulla scorta di questa constatazione, ci si è posti la **prima domanda di ricerca**, chiedendosi se e come questa intrinseca “dualità” procuri nocimento al sistema finanziario *mainstream*. Ebbene, gli elementi raccolti fanno ritenere che quanto dedotto in sede di apertura della tesi sia stato correttamente percepito giacché il “*crypto financial system*”, qualora non opportunamente controllato, può rivelarsi una seria minaccia per la tutela degli investitori, l'integrità del mercato e – in ultima istanza – la stabilità finanziaria.

Metodologicamente parlando, si è innanzitutto proceduto a verificare l'effettiva esistenza di un legame tra i due paradigmi (*TradFi* e il *crypto system*). Segnatamente, rilevanti autorità di settore come la Banca dei Regolamenti Internazionali (*Bank of International Settlement, BIS*), il Consiglio per la Stabilità Finanziaria (*Financial Stability Board, FSB*), il Fondo

Monetario Internazionale (*International Monetary Fund, IMF*), l'OCSE (*Organization for Economic Co-operation and Development, OECD*), lo *European Systemic Risk Board (ESRB)* o la *Banque de France*, convergono tutte sul fatto che il legame intercorrente tra economia reale, finanza tradizionale e mercato criptovalutario esiste, ma al momento risulta limitato. Una volta assodata l'esistenza del rapporto tra *TradFi* e "*crypto financial system*" e misuratane la consistenza, il passo successivo è stato capire in che modo si strutturasse. A tal riguardo, sono stati individuati dei punti di contatto che, tramite la mediazione dei *CASP*, costituiscono dei viadotti problematici tra finanza decentralizzata e sistema finanziario tradizionale:

- 1) **Consumatori *retail***;
- 2) **Le *stablecoin***;
- 3) **Esposizioni bancarie**;
- 4) **La tokenizzazione dei crediti su beni fisici.**

A riprova di quanto riportato sopra, i fallimenti avvenuti Oltremare rappresentano un'ulteriore cartina al tornasole che dimostrano l'interconnessione (e quindi i rischi di contagio) tra questi paradigmi. Per rendere visibilmente apprezzabile la situazione, si è ricorsi a una *timeline* per registrare l'effetto-valanga determinatosi nel 2022, *annus horribilis* per il mercato criptovalutario:

- **Maggio 2022:** collasso dell'ecosistema *crypto Terra (LUNA)* e *Terra USD (UST)*;
- **Giugno/luglio 2022:** fallimenti di *Three Arrows Capital* (o *3AC*), *Celsius Network* e *Voyager Digital*;
- **Novembre/dicembre 2022:** fallimenti di *FTX*, *Alameda Research*, *BlockFi* e *Core Scientific Group*;
- **Gennaio 2023:** fallimento di *Genesis Global HoldCo*;

- **Marzo 2023:** crisi delle banche regionali statunitensi (*Silicon Valley Bank (SVB)*, *Silvergate Bank*, *Signature Bank* e *First Republic Bank*).

In aggiunta, gli eventi sopraelencati dischiudono le molteplici criticità che si celano dietro i fallimenti dei vari *exchange*: resilienza digitale poco sviluppata a fronte di attacchi cibernetici; costi energetici insostenibili; tecniche aggressive poste in essere dagli investitori; dipendenti con *know-how* non all'altezza della situazione; modelli di *business* non solidi; scarsa applicazione dei criteri prudenziali; depositi non assicurati; forte esposizione ad *asset* particolarmente rischiosi; incauta e/o negligente gestione societaria; problemi di liquidità; insolvenza e via discorrendo. Arner e colleghi riuniscono questo ventaglio di criticità sotto il nome di *"financialization of crypto"*, rimarcando con tale espressione che *«le criptovalute non sono né speciali né immuni e sono arrivate a presentare tutti i problemi classici della finanza tradizionale. Con l'evoluzione dell'ecosistema delle criptovalute, sono emersi i fallimenti del mercato e le esternalità della finanza tradizionale»*.

A integrazione di quanto sinora osservato, il lavoro di Aquilina ed altri autori nel Bollettino n. 66 del *BIS* dichiara senza troppi giri di parole che, *«dopo il fallimento di alcune importanti società di criptovalute, affrontare i rischi dei mercati delle criptovalute è diventata una questione politica più urgente. I mercati dei crypto-asset hanno già attraversato boom e disastri in passato, e finora i fallimenti non hanno portato a un contagio più ampio che ha minacciato la stabilità finanziaria. L'ecosistema crittografico e le funzioni di "finanza ombra" che esso svolge, attraverso entità finanziarie centralizzate (CeFi) e protocolli di finanza decentralizzata (DeFi), condividono molte delle vulnerabilità note della finanza tradizionale (TradFi). Ma diversi fattori esacerbano i rischi standard. Si tratta di un'elevata leva finanziaria, di disallineamenti di liquidità e di scadenze e di sostanziali asimmetrie informative. Le risposte politiche dovrebbero considerare come affrontare queste fonti di rischio in modo appropriato, data la natura senza confini delle criptovalute»*.

In sintesi, per via delle sue dimensioni ridotte e alle limitate interconnessioni con la *TradFi*, l'ecosistema crittografico non ha al momento le proprietà necessarie per destabilizzare incisivamente il sistema finanziario nel suo complesso. Tuttavia, rilevanti autorità di settore

affermano nitidamente che questa interconnessione tenderà a intensificarsi in futuro. In base a questo ragionamento, l'accelerazione nella regolamentazione di strutture politiche sui *CASP* potrebbe essere il passo-chiave per ridurre, o quanto meno contrastare, i contagi che sono oggettivamente emersi nella realtà finanziaria. Tutto ciò si traduce senza mezzi termini in un monito impellente per i legislatori di virare verso un approccio regolatorio (il più possibile armonizzato a livello internazionale) specificatamente dedicato al tema dei *CASP*; e non meramente contenitivo come messo in atto dal regolatore statunitense, il quale ha pagato a proprie spese la propria convinzione di poter contenere le criticità realizzate dai *provider* facendo esclusivo affidamento su leggi finanziarie preesistenti.

D'inverso, su questo punto, gran parte dei Paesi europei hanno dimostrato di avere un grado di maturità e resilienza strutturale maggiori. Con ogni probabilità ciò è dovuto *in primis* all'accoglimento tempestivo delle raccomandazioni del GAFI, implementando nei propri ordinamenti nazionali presidi *ad hoc* per i *Virtual Asset Service Provider (VASP)*. In seconda battuta, l'introduzione del *MiCA* ha dato nuovo slancio alla protezione del mercato dei prodotti crittografici, da un lato, imponendo maggiori oneri a tali soggetti (ora denominati *CASP*) e, dall'altro, armonizzando 27 ordinamenti diversi sul tema così da rendere il mercato unico più chiaro e attrattivo per i *provider*.

Dunque, per tutte queste ragioni, una maggiore stabilità finanziaria a livello infrastrutturale e sistemico richiede che le giurisdizioni nazionali prendano innanzitutto coscienza dei rischi insiti nella non-regolamentazione dei fornitori di crypto-attività e provvedano pertanto ad arricchire nei propri ordinamenti gli opportuni presidi giuridici per meglio salvaguardare la tenuta del proprio Sistema-Paese su questo fronte.

Dopo aver messo a confronto sistema finanziario tradizionale e il “*crypto financial system*”, il **secondo capitolo** si è addentrato nell'ecosistema crittografico, analizzando rispettivamente i prodotti circolanti (*digital asset*) e soprattutto i soggetti che vi abitano (*CASP*).

Con riferimento ai profili oggettivi, sono state sinteticamente passate in rassegna le fondamentali tecnologie di base ravvisabili nella *Distributed Ledger Technology*, *blockchain* e *smart contract*. In maniera altrettanto succinta sono stati descritti rapidamente *crypto-asset* e *Central Bank Digital Currency (CBDC)*. Con riferimento ai primi, sono state

messe in luce le difficoltà che si stanno registrando sul piano definitorio e tassonomico; in relazione al secondo macro-gruppo, sono state invece illustrate le principali ragioni alla base dell'adozione delle valute digitali di Stato nonché le diverse tipologie di *design* che le Banche Centrali stanno prendendo in considerazione per emetterle.

Con riguardo invece ai profili soggettivi, invece, si è operata un'approfondita analisi giuridica dei *Crypto-Asset Service Provider* e delle cripto-attività, alla luce del Regolamento *MiCA*. Mantenendo il filo del discorso sull'ultimo punto, la Regolamentazione vertente sui *Markets in Crypto-Assets* ha il pregio di sveltare nel panorama globale della regolamentazione *crypto* per via della sua trasversalità di trattazione. A parere di chi scrive, sebbene la struttura ricalchi in molti aspetti quella della *MiFID II* (specie con riferimento alla qualificazione dei servizi), la normativa *MiCA* si preoccupa di imbrigliare i *CASP* imponendo oneri di eterogenea natura. Finalità ultima di questo approccio è far sì, come fanno notare Daga e Buscema, che i *crypto provider* «dimostrino di possedere:

- *personale con le competenze necessarie per assolvere alla proprie responsabilità;*
- *garantire la continuità e la regolarità nell'erogazione dei servizi ai clienti;*
- *stabilire politiche efficaci di continuità operativa e disaster recovery;*
- *disporre di meccanismi di controllo interno e di procedure efficaci per la valutazione dei rischi;*
- *disporre di sistemi e procedure per proteggere la sicurezza, integrità e riservatezza delle informazioni;*
- *conservare i registri di tutti i servizi degli ordini e delle transazioni effettuate;*
- *disporre sistemi e procedure di monitoraggio per evitare abusi di mercato ed essere in grado di segnalare immediatamente qualsiasi sospetto alla propria autorità competente».*

Oltre a ciò, nonostante dalla lettura di questo elaborato emerga con evidenza una prospettiva orientata prettamente alla disciplina nazionale ed europea, non si è mancato di riportare lo stato di normazione dei fornitori di cripto-attività a livello globale attraverso una ricerca empirica personalmente svolta. L'esito di quest'ultima indagine ha messo in evidenza alcune interessanti considerazioni che peraltro si allineano coerentemente con quanto già osservato nel primo capitolo:

- la regolamentazione dei *CASP* presenta una diffusione a macchia di leopardo, in cui svettano gli Stati dell'area geografica europea;
- l'assenza di univocità terminologica se da un lato è sintomo di una forte discrezionalità all'interno di ogni giurisdizione, dall'altro inficia negativamente in merito alla possibilità di costruire una regolamentazione concordata a livello internazionale;
- la supervisione di questi soggetti appare largamente scoperta rispetto alla totalità delle giurisdizioni prese in esame;
- l'Europa, sia intesa nella sua accezione geografica che con riferimento all'ambito UE, sembra procedere speditamente rispetto agli altri continenti e l'approvazione del *MiCA* sembra consolidare questo primato;
- nella stragrande maggioranza dei Paesi non si riesce a cogliere con chiarezza se i *CASP* siano degli intermediari finanziari o una categoria a sé, dal momento che si rinvencono esempi nell'uno e nell'altro senso.

Quest'ultima constatazione si ricollega adeguatamente alla **seconda domanda di ricerca**: possono i *CASP* considerarsi una categoria a sé di soggetti mediatori? In altri termini, siamo in presenza di soggetti aventi una propria e precisa identità al punto tale da differenziarsi dai soggetti bancari e finanziari e costituire una nuova *species* nel panorama dell'intermediazione? In ragione della peculiarità dei servizi offerti, dall'elevato profilo tecnologico e da una spiccata tendenza all'innovazione continua, i *CASP* danno l'impressione di possedere caratteristiche talmente peculiari da potersi teoricamente distaccare dai soggetti bancari e finanziari e costituire una nuova *species* nel panorama finanziario. Difatti, tali *provider* non sembrano essere perfettamente sovrapponibili agli intermediari finanziari, quanto meno rispetto a determinati servizi, come, per esempio, la custodia o il controllo, per conto di clienti, delle cripto-attività o dei mezzi di accesso a tali cripto-attività (chiavi crittografiche private). Del resto, si tratta invero di una problematica che viene rimarcata anche da Troiano, asserendo che «*in dottrina, si rilevava come risultasse difficoltoso identificare un concetto unitario di attività finanziaria nel quale ricondurre ipotetici tratti comuni delle singole attività riservate agli intermediari in parola, trattandosi di attività tra*

loro diverse nei presupposti finanziari, nella causa e nelle modalità di svolgimento; l'unico elemento comune veniva rinvenuto nella finalità di economicità». D'altro canto, la categoria dei *CASP* va considerata a tutti gli effetti una “*financial entity*”, ai sensi dell'art. 1 del Regolamento *DORA*. Tuttavia, a parere di chi scrive, questa constatazione può risultare agevole solo attraverso una lettura combinata delle varie normative europee ricomprese sotto un'unica prospettiva. Qualora invece tale ragionamento si basasse esclusivamente sulla lettura del *MiCA*, va allora ammesso come vi siano non poche difficoltà nel giungere alla medesima conclusione.

Chiaramente, una simile ricostruzione ha sollevato e continua a sollevare – al pari delle altre lamentate carenze regolatorie – significative criticità dal punto di vista della necessaria qualificazione normativa e disciplina delle relative attività. Solo grazie a interventi sovranazionali, infatti, sta prendendo forma un quadro di regole in grado di assicurare al sistema in argomento un insieme di regole giuridiche che possano infondere nei consumatori un sufficiente grado di fiducia verso questa assai peculiare categoria di “intermediari”. In tale ottica, non può essere obliterato un cenno all'applicabilità nei confronti dei *CASP* (in qualità di prestatori di servizi relativi all'utilizzo di valuta virtuale) della disciplina antiriciclaggio nonché, a far data dal 30 dicembre 2024, del più volte citato Regolamento 2023/1114/UE del Parlamento Europeo e del Consiglio relativo proprio ai mercati delle cripto-attività.

Va da sé che, pur in assenza di una sostanziale assimilazione in senso definitorio e di qualificazione giuridica, la direzione ineluttabile da seguire non potrà non tradursi in una sorta di osmosi di regole, procedure autorizzatorie e metodiche e autorità di controllo, in guisa da consentire l'approntamento di sistemi di tutela del risparmio e dei mercati e, in ultima analisi, dei consumatori.

Da ultimo, il **terzo capitolo** è sceso ancora di più nel dettaglio analizzando l'impatto dei *CASP* e delle cripto-attività in relazione all'intero quadro normativo europeo e/o domestico. Obiettivo di questa parte finale della trattazione consisteva nel rispondere alla **terza domanda di ricerca**, in cui ci si è chiesti se il complesso delle suevocate norme europee circoscriventi l'*habitat* dei *CASP* sia riuscito a regolamentare esaurientemente tutti i possibili profili di criticità. E nell'eventualità che qualcosa sia sfuggito, tentare di convertire il potenziale *vulnus* individuato in spunti di riflessione o suggerimenti condivisibili sul piano

legislativo. Per fare ciò ci si è concentrati su materie di estrema rilevanza come l'antiriciclaggio, la tassazione, l'ambiente e la *privacy*. Formulando delle sintetiche valutazioni, si afferma quanto segue:

- **Antiriciclaggio:** gli sforzi impiegati dal GAFI nel promuovere il recepimento delle proprie raccomandazioni (in tema *VASP*) nelle discipline domestiche di antiriciclaggio di tutto il mondo hanno senza dubbio contribuito a rendere solido e compatto il legame tra prestatori di cripto-attività e settore *AML/CFT*. Se da un punto di vista della normazione, dunque, i *CASP* risultano pressoché blindati, a parere di chi scrive le criticità sorgono soprattutto in capo a chi dovrà supervisionare tali operazioni. La problematica di fondo risiede nella constatazione che le autorità di vigilanza di settore non sono, nella maggioranza dei casi, adeguatamente attrezzate da un punto di vista tecnologico per il monitoraggio dei *crypto-asset* rispetto alle normative nel breve termine e potrebbero volerci molti anni per standardizzare queste procedure. Secondo il GAFI, questa circostanza è preoccupante, «*data la crescita dinamica e i rapidi sviluppi tecnologici degli asset crittografici, anche se il settore sta attivamente sviluppando standard per affrontare questa lacuna. Anche se la vigilanza e il monitoraggio coerenti fossero possibili in alcune giurisdizioni, è improbabile che lo siano in tutte, il che potrebbe comportare ulteriori asimmetrie informative e di applicazione*». Pertanto, bisognerebbe prendere in considerazione l'idea di non concentrarsi eccessivamente sul trasferire il “nuovo nel vecchio”, ma anche permettere che il “vecchio entri nel nuovo”. Traducendo in termini più chiari, non bisogna preoccuparsi solamente di catturare l'innovazione (come le cripto-attività, nel caso *de quo*) e ricondurla in uno schema normativo preesistente o istituito *ad hoc*, ma vi è la complementare necessità di promuovere una svolta tecnico-informatica delle Amministrazioni pubbliche, specie nel settore *crypto*. Insomma, bisogna irrobustire i poteri di vigilanza ad un nuovo livello cosicché le autorità possano veramente atteggiarsi a *RegTech*, inglesismo al momento più teorico che concreto. Volendo fare esempi pratici, potrebbe essere utile istituire a livello istituzionale un *digital wallet* per ogni Amministrazione (come già avviene nel contesto statunitense e in altre giurisdizioni del mondo) o un nodo *blockchain* per poter accedere direttamente sulla rete;

- **Tassazione:** pur apprezzando l'intervento novativo del Legislatore nazionale, corre l'obbligo di evidenziare che la scarsa disciplina regolatoria è gravida di incertezze solo in minima parte risolte dal documento di prassi in elaborazione. Nel complesso, la disciplina tributaria di nuovo conio patisce l'inafferrabilità di un fenomeno difficilmente collocabile nelle tradizionali categorie giuridiche, in cui gli stessi interpreti si trovano di fronte alla primaria difficoltà di inquadrare giuridicamente il fenomeno delle cripto-attività, acuita dalle mutazioni continue e costanti dell'oggetto dell'analisi. Inoltre, per quanto sia pacifico che ogni Paese membro dell'UE abbia il diritto di gestire la trattazione fiscale delle cripto-attività come meglio crede, a rendere il tutto più complicato è la totale assenza di allineamento in questo senso. Di fronte a tassazioni differenti all'interno di un unico mercato digitale, un *provider* è ragionevolmente indotto a volersi registrare in un determinato Paese europeo esclusivamente in base alla convenienza fiscale. Non è difficile immaginare come questa circostanza possa potenzialmente incidere in termini concorrenziali. Sarebbe dunque auspicabile un'armonizzazione fiscale delle cripto-attività o una qualsiasi altro espediente orientato in tal senso, seppure di difficile realizzazione. Inoltre, in ragione della sua minatura transfrontaliera, risultano quantomai necessarie politiche transnazionali integrate e uniformi che permettano di regolamentare in maniera univoca le cripto-attività sul piano fiscale europeo;
- **Ambiente:** in questo ambito va certamente riconosciuto il merito delle istituzioni europee di includere il tema della sostenibilità ambientale, imponendo ai *CASP* di rispettare i requisiti *ESG* e di dichiarare all'interno del *White Paper*, tra le altre cose, il proprio consumo energetico. Tuttavia, a opinione di chi scrive, ciò che non convince di questa soluzione è, come avvertito anche in ambito antiriciclaggio, la difficoltà di monitorare il reale dispendio energetico del *provider* al fine di confrontare il reale risultato con quello dichiarato. Inoltre, tale onere potrebbe non essere sufficiente in un'ottica di deterrenza. Pertanto, si potrebbe pensare di aggiungere ulteriori elementi di rafforzamento come l'introduzione di una *carbon tax* specie per quelle attività particolarmente energivore oppure, procedere nel senso opposto, attivando misure premiali per tutti quei *provider* che dimostrano di ridurre la propria *carbon footprint*;

- **Privacy:** in merito all'impianto normativo innestato sul tema, «DORA e GDPR pongono sfide e complessità per le “Financial Entities” e i loro fornitori terzi di servizi ICT, che dovranno adottare (e aggiornare, con riferimento al GDPR) piani di adeguamento che tengano conto delle peculiarità di entrambi i quadri giuridici». In altri termini, sarà fondamentale per il Legislatore operare lungo una traccia di ripensamento delle tutele approntate per il dato personale, che dovrebbero ora procedere in parallelo anche in relazione alle offerte del mercato finanziario digitalizzato.

A ben considerare, inquadrando il fenomeno dei CASP da un'altra angolazione, gli ambiti dapprima menzionati richiamano – in modo nemmeno tanto casuale a parere di chi scrive – gli obiettivi di medio-lungo termine che l'Unione Europea si è prefissata di raggiungere:

- **Strategia europea di antiriciclaggio:** *«per affrontare le carenze attuali in materia di supervisione AML/CFT riscontrate nell'Unione, è stata proposta l'istituzione dell'Autorità antiriciclaggio europea (AMLA). Attualmente, la supervisione AML/CFT è basata sugli Stati membri, ma la sua qualità ed efficacia non sono uniformi, e l'approccio a situazioni transfrontaliere non è coerente. L'Autorità antiriciclaggio europea sarebbe un organismo europeo che garantirebbe un livello uniforme di supervisione AML/CFT in tutta l'UE. Questo sarebbe un passo importante per proteggere l'integrità dell'economia e del sistema finanziario dell'UE e la sicurezza dei suoi cittadini»*⁵⁶⁸.
- **Unione fiscale europea:** si tratta di uno *step* a lungo dichiarato come necessario prima di poter assurgere, secondo le aspettative dei principali esponenti del sogno europeo, a un'unione federale degli Stati europei;
- **Green Deal Europeo:** una serie di iniziative strategiche concordate a Parigi hanno reso giuridicamente mandatorio il raggiungimento della neutralità climatica entro il 2050. Nello specifico, l'UE e i suoi Stati membri si sono impegnati a ridurre le emissioni nette di gas a effetto serra nell'UE di almeno il 55% entro il 2030, rispetto ai livelli del 1990. Si tratta di un obiettivo giuridicamente vincolante, basato su una valutazione d'impatto effettuata dalla Commissione;

⁵⁶⁸ [AA.VV., Autorità antiriciclaggio europea: il regolamento di istituzione approvato dal Parlamento UE, Non solo Diritto Bancario, 2023.](#)

- **Strategia europea per i dati e per la cybersicurezza:** la particolare rilevanza che la protezione dei dati personali ha assunto nella società odierna è ormai pacifico. Ciò si manifesta anche con tentativi di rafforzamento della resilienza digitale in ambito finanziario promossi dal Regolamento *DORA*. Quest'ultimo atto normativo costituisce un piccolo tassello di un mosaico ben più grande. L'obiettivo delle istituzioni unionali nei prossimi anni, invero, è implementare una vera e propria strategia europea di cybersicurezza. Il rapido susseguirsi di una crisi pandemica, prima, e di una vera e propria “stagione” bellica, poi, hanno certamente contribuito all'accrescimento quantitativo degli attacchi *cyber* con un livello di sofisticazione sempre più alto.

Sebbene il percorso verso un'Europa finanziariamente in salute, digitalmente resiliente, sostenibile e fiscalmente unita sia senza dubbio irto di ostacoli, i *Crypto-Asset Service Provider* non solo sembrano sprigionare sfumature variegata e complesse, ma per certi versi la loro trasversalità potrebbe fungere da caleidoscopio per monitorare con attenzione la convergenza normativa (e conseguente intreccio) di tutti questi ambiti suindicati nel contesto unionale.

Accingendosi alla conclusione di questa tesi, il presente elaborato, valorizzato da una congiunta analisi sia giuridica che empirica dei *CASP*, ha inteso condividere una visione ampia, trasversale e aggiornata in merito a questi peculiari intermediari da poco emersi nel panorama finanziario digitale.

FONTI E ULTERIORI RIFERIMENTI

[A16zcrypto, State of Crypto, 2023.](#)

[AA.VV., Autorità antiriciclaggio europea: il regolamento di istituzione approvato dal Parlamento UE, Non solo Diritto Bancario, 2023.](#)

[AA.VV., Chapter 8. Digital Assets: Relearning Economic Principles, Economic report of the President, 2023.](#)

[AA.VV., Cos'è la Blockchain e cosa cambia per i sistemi di pagamento digitale?, Worldline, 2021.](#)

[AA.VV., Criptovalute, crolla anche il colosso Genesis. Peggio di Ftx: buco da 3,4 miliardi, Open, 2023.](#)

AA.VV., *Diritto del Fintech*, a cura di Cian M., Sandei C., Cedam, 2020.

[AA. VV., Financial Data Aggregation e Account Information Services. Questioni regolamentari e profili di business, Quaderni FinTech Consob, 2019.](#)

AA.VV., *FinTech*, a cura di Fimmanò F. e Falcone F., Edizioni Scientifiche Italiane, 2019.

AA.VV., *FinTech*, a cura di Paracampo M.T., Giappichelli Editore, 2021.

AA.VV., *Fintech: diritti, concorrenza, regole*, a cura di Finocchiaro G., Falce V., Zanichelli Editore, 2019.

AA.VV., *Fintech: i confini dell'innovazione nella finanza*, a cura di Natale A., Giuffrè, 2022.

[AA.VV., Is a VASP a CASP?, 21Analytics, 2022.](#)

[AA.VV., Mining criptovalute e bitcoin: cos'è, come farlo \(cloud e non\) e guadagni, Blockchain4innovation, 2022.](#)

[AA.VV., TradFi and DeFi: Key difference, Hedera, 2023.](#)

[Abbà M., Efficienza energetica dei data center: 6 piccoli aggiustamenti di successo, NetworkDigital360, 2023.](#)

Abriani N. e Schneider G., *Diritto delle imprese e intelligenza artificiale. Dalla FinTech alla CorpTech*, Il Mulino, 2021.

[Acierno M., *I diritti dell'investitore nella giurisprudenza di legittimità*, Questione Giustizia n. 3, 2017.](#)

[Adami A., *Bitcoin ed Ethereum classificate come commodity: la sentenza definitiva di un tribunale di New York*, The Cryptonomist, 2023.](#)

[Ahnert T. et al., *ECB Working Paper Series. The digital economy, privacy and CBDC* – N. 2662, maggio 2022.](#)

[Alfonso F., *Intermediari del Credito: dall'Europa la sfida verso il Cambiamento*, Intervento del Presidente dell'OAM al Leadership Forum Summer Roma, 2023.](#)

[Alihyaei M. et al., *Development a policy for the production of Bitcoins with renewable energy sources*, Future Energy Vol.3, pp.16-23, 2023.](#)

[Aliperto D., *Criptomonte, faro delle Autorità di vigilanza Ue: "Subito le regole"*, NetworkDigital 360, 2022.](#)

[Allen W. E. D. e Potts J., *Web3 toolkits: A user innovation theory of crypto development*, in Journal of Open Innovation: Technology, Market, and Complexity, 9, 2023.](#)

[Alsalmi N. et al., *Accounting for digital currencies*, Research in International Business and Finance 64, 2023.](#)

[Amase W., *Household Electricity Costs to Mine 1 Bitcoin at Home, Around the World*, CoinGecko, 2023.](#)

[Amaya T., Vice Minister for International Affairs, Financial Services Agency Japan, *Regulating the crypto assets landscape in Japan*, 2023.](#)

Angelucci P. e Bracchi A., *Tassazione e monitoraggio fiscale delle criptovalute. Analisi dei recenti chiarimenti forniti dall'Agenzia delle Entrate – Direzione Regionale della Lombardia nella risposta (non pubblicata) all'interpello n. 956-39/2018*, 2023.

[Anitec - Assinform, *White Paper Attualità e prospettive della Blockchain per la crescita dell'economia italiana*, 2021.](#)

[Anker-Sørensen L. e Zetzsche D.A., *From Centralized Finance to Decentralized Finance. The issue of "Fake-DeFi"*, SSRN, 2021.](#)

[Anti Money Laundering Centre, *The Bitcoin trader: a facilitating role in the cash out of criminal proceeds*, De Bilt, 2017.](#)

Antonacchio F., *Web3 ed economia decentralizzata nuove sfide fiscali*, Il fisco n. 39, 2022.

[Antonovici A., *TradFi vs CeFi vs DeFi: Here's how they differ*, TastyCrypto, 2023.](#)

[APG, *Typologies Report*, 2022.](#)

[Appendino M. et al., *Crypto Assets and CBDCs in Latina America and the Caribbean. Opportunities and Risks*, IMF Working Papers, 2023.](#)

[Aquilina M. et al., *Addressing the risks in crypto: laying out the options*, BIS Bulletin n. 66, 2023.](#)

[Aramonte et al., *DeFi risks and decentralisation illusion*, BIS Quarterly Review, 2021.](#)

Arginelli P., *La tassazione di bitcoin e crypto-attività e la Costituzione*, Bitcoin e crypto-attività, Il Sole 24 Ore, 2023.

Arlacchi P., *La mafia imprenditrice. L'etica mafiosa e lo spirito del capitalismo*, Il Mulino, 1983.

[Arner D.W. et al., *The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023*, University of Hong Kong Faculty of Law Research Paper n. 19, 2023.](#)

[Arnoldi B., *Bitcoin è un bene rifugio come oro e diamanti? Parlano gli esperti*, Everyeye.it, 2023.](#)

[Associazione fra le società italiane per azioni, *Data Governance Act: le regole per il mercato interno dei dati*, in Approfondimenti, fasc. n. 4, 2022.](#)

[Assogestioni, *Oltre le criptovalute. Tecnologie a registro distribuito a servizio dell'asset management*, 2022.](#)

Astone M.A., *Right to be forgotten e il discutibile ruolo dei gestori online e dei motori di ricerca*, Giornale di diritto amministrativo, 2020.

[Atlantic Council, *Central Bank Digital Currency Tracker*, 2023.](#)

[Auer R. e Böhme R., *Central bank digital currency: the quest for minimally invasive technology*, BIS Working Papers n. 948, 2021.](#)

[Auer R. e Claessens S., *Regulating Cryptocurrencies: Assessing Market Reactions*, 2018.](#)

[Auer et al., *Rise of the Central Bank Digital Currencies*, International Journal of Central Banking, 2023.](#)

[Auer R. et al., *The Technology of Decentralized Finance \(DeFi\)*, BIS Working Papers No 1066, 2023.](#)

[Avan-Nomayo O., *Il governo del Regno Unito crea una task force dedicata alle CBDC*, CoinTelegraph, 2021.](#)

Avella F., *L'Irpef sulle cripto-attività dopo la legge di Bilancio 2023*, in *Bitcoin e cripto-attività*, Il Sole 24 Ore, 2023.

[Azani E. e Liv N., *Jihadists' Use of Virtual Currency*, IDC Herzliya – ICT International Institute for CounterTerrorism, 2018.](#)

[Bains P. et al., *Regulating the Crypto Ecosystem: The Case of Stablecoins and Arrangements*, 2022.](#)

[Bains P. et al., *Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets*, 2022;](#)[Banca d'Italia et al., *Caratteristiche degli Smart Contract*, 2023.](#)

[Banca d'Italia, *Avvertenza per i consumatori sui rischi delle valute virtuali da parte delle Autorità europee*, 2018.](#)

[Banca d'Italia, *Avvertenza sull'utilizzo delle cosiddette "valute virtuali"*, 2015.](#)

[Banca d'Italia, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività*, 2022.](#)

[Banca d'Italia, *Consob e Banca d'Italia mettono in guardia contro i rischi insiti nelle cripto-attività*, 2021.](#)

[Banca d'Italia, *Rapporto Annuale 2018. Unità di Informazione Finanziaria per l'Italia*, 2018.](#)

[Banca d'Italia, *Rapporto Annuale 2022. Unità di Informazione Finanziaria per l'Italia*, 2022.](#)

[Banca d'Italia, *Relazione del Responsabile della Protezione dei Dati. Anno 2022, 2023.*](#)

[Banca di Francia, *"Decentralised" or "disintermediated" finance: what regulatory response?*, Discussion Paper, 2023.](#)

Banca Mondiale, *First World Blockchain Bond Global Price Prices, A\$110 Million*, 2018.

[Banca d'Inghilterra, *Financial Stability in Focus: Cryptoassets and decentralised finance*, 2022.](#)

[Barone D.B., *Criptovalute e Jihad: Propaganda, ideologia e comunicazione*, difesa.it, 2019.](#)

Barone D. B., *Il terrorismo islamico si finanzia con i Bitcoin. Ecco perché è allarmante più per la propaganda che per l'economia*, 2018.

[BCE, ECB Working Paper Series: The digital economy, privacy and CBDC, at a panel on the future of crypto at the 22nd BIS Annual Conference, Basel, 2023.](#)

[BCE, Working Paper: the digital economy, privacy and CBDC – N. 2662, 2022.](#)

[BCE, Report on a digital euro, 2020.](#)

[Bennett Jones LLP - Centre for International Governance Innovation, Digitalization of Payments and Currency. Key takeaway from a third Virtual Workshop with Canadian and International Experts on the Digitalization of Money, Conference Report, 2023.](#)

[Berwick A. e Talley I., Hamas Militants Behind Israel Attack Raised Millions in Crypto, Wall Street Journal, 2023.](#)

[Bevilacqua G., La dimensione territoriale dell'oblio, Federalismi.it, 2019.](#)

[Bistarelli S., Bitcoin forensics: le tecniche labeling, clustering e mixnet recognition, 2018.](#)

[Bizioli G. e Salvatore P., Il titolare effettivo dei trust esteri dopo il recepimento della IV direttiva antiriciclaggio, Boll. Trib. d'Inf., 2020.](#)

[Blandini A., Diritto dell'innovazione, Cedam, 2022.](#)

[Blockchain Revolution, Glossario, BlueChain, 2023.](#)

[Boiardi L., DeFi: tutto sulla finanza decentralizzata, The Crypto Gateway, 2023.](#)

[Borgobello M., Riciclaggio con criptovalute, gli sportelli ATM ultima frontiera: vulnerabilità e tutele, Agenda Digitale, 2021.](#)

[Bradley I., How taxes on cryptocurrencies and digital assets will soon take shape, EY, 2022.](#)

[Bradley I., Why crypto service providers face a step change in tax reporting, EY, 2023.](#)

[BRI, Blueprint for the future monetary system: improving the old, enabling the new, BIS Annual Economic Report, 2023.](#)

[BRI, Central bank digital currencies, 2018.](#)

[BRI, The crypto ecosystem: key elements and risks. Report submitted to the G20 Finance Ministers and Central Bank Governors, 2023.](#)

[Briola A. et al., Anatomy of a Stablecoin's failure: The Terra-Luna case, Finance Research Letters Volume 51, 2023.](#)

Brizzi F. et al., *La reimmersione della liquidità illecita nel circuito economico ed il delitto di reimpiego tra prevenzione patrimoniale e giustizia penale: prospettive di future armonizzazioni*, Archivio Penale, n. 2, 2014.

Buso R., *Criptovalute e blockchain, regolamentazione ed evoluzione*, Luiss, 2021.

Califano L., *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati*, in Califano L., Colapietro C. *Innovazione tecnologica e valore della persona*, 2017.

Camera dei Deputati, *FinTech*, Dossier del Servizio Studi, 2022.

Camera dei Deputati, *Lavori preparatori dei progetti di Legge, Atto Camera: 1342. Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2022-2023" (1342)*, 2023.

Camera dei Deputati, *Pacchetto di finanza digitale*, Ufficio Rapporti con l'Unione Europea, 2021.

Camera dei Deputati, *Proposta di legge d'iniziativa dei Deputati Quintarelli, Mucci, Dambruoso, Galgano, Librandi, Menorello, Monchiero, Vargiu, Catalano, Basso, Carrozza, Dallai e Marzano*, 2016.

Campbell-Verduyn M., *Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance*, Crime, Law and Social Change, 2017.

Cancelli E., *Silergate, Silicon Valley Bank e Signature Bank: che succede a Bitcoin?*, Crypto.it, 2023.

Cancelli L., *The Growing Crypto-assets Threat to Anti-money Laundering: How Institutions Are Coping with This Phenomenon*, Università Ca'Foscari Venezia, 2020.

Cancelliere F. e Tardini A., *Risposta (non pubblica) all'interpello n. 956-39/2018: profili fiscali della detenzione di criptovalute da parte di persone fisiche residenti in Italia*.

Capaccioli S. e Deotto D., *Disciplina tributaria delle crypto-attività: novità in chiaroscuro*, il Fisco, n. 4, 2023.

Capaccioli S. e Giordano M. T., *Crypto-asset: Regolamento MiCA e DLT Pilot Regime. Analisi ragionata su token, stablecoin e CASP*, Giuffrè, 2023.

Capaccioli S., *Bitcoin: le operazioni di cambio con valuta a corso legale sono prestazioni di servizio esenti*, Fisco, 2015.

Capaccioli S., *Criptovalute e Bitcoin: un'analisi giuridica*, Milano, 2015.

[Capaccioli S., *Introduzione alle criptovalute e bitcoin*, Coinlex, 2020.](#)

Capaccioli S., *La tassazione delle attività digitali*, Milano, 2023.

Capaccioli S., *Riciclaggio, antiriciclaggio e Bitcoin*, Il Fisco, 2014.

Capolupo S., Carbone M. e Sturzo G., *Antiriciclaggio: gli obblighi dei professionisti*, IPSOA, 2007.

Capriglione F. (a cura di), *Manuale di diritto bancario e finanziario. Seconda edizione*, 2019.

Caramignoli G. e Di Pietro I., *Il fenomeno Bitcoin: moneta “virtuale” con effetti “reali” sull’economia*, Riv. G.d.F., n. 6, 2013.

Carano A. e Salerno S., *D. Lgs 20 febbraio 2004, n. 56: l’attuazione della seconda Direttiva europea nella strategia antiriciclaggio e le novità procedurali e sanzionatorie*, Il Fisco, 2004.

[Carbone F., *Terra LUNA e UST: tutto sul drammatico crollo dello stablecoin*, Fintastico, 2022.](#)

[Carboni K., *La crisi in Kazakhstan sta influenzando il mercato dei bitcoin*, Wired, 2022;](#)

[Carlini V., *Cripto-crack: intrecci sui titoli e contratti automatici, così dilaga il contagio*, Il Sole 24 Ore, 2023.](#)

[Carrière P., *La “cripto-arte” e i non-fungible tokens \(NFT\): tentativi di inquadramento giuridico*, Diritto Bancario, 2021.](#)

[Carrière P. et al., *Tokenizzazione di azioni e azioni tokens*, Quaderni giuridici Consob, n. 25, 2023.](#)

Carta L. e Altiero N., *L’utilizzo di sistemi telematici a scopo di riciclaggio*, Riv. G.d.F., n. 3, 1999.

Cassese E. e Costanzo P., *Il recepimento della seconda direttiva comunitaria “antiriciclaggio”*, Giornale di Diritto Amministrativo, 2004.

Cassese E. e Costanzo P., *La terza direttiva comunitaria in materia di antiriciclaggio e antiterrorismo*, Giornale di Diritto Amministrativo n.1, 2006.

[Catalano S., *Doppia pregiudizialità una svolta opportuna della Corte costituzionale*, Federalismi.it, 2019.](#)

[Cavicchioli M., *Bitcoin, “the great mining migration” is underway*, The Cryptonomist, 2022.](#)

[Cavicchioli M., *Dove la tassazione crypto è più favorevole?*, The Cryptonomist, 2023.](#)

[Cavicchioli M., *USA: i computer quantistici metteranno a rischio bitcoin*, The Cryptonomist, 2022.](#)

Cenci P., *La nuova normativa antiriciclaggio - Direttive comunitarie e normativa nazionale*, Cedam, 2010.

[Centre for International Governance Innovation, *Digitalization of Payments and Currency. Key Takeaways from a Third Virtual Workshop with Canadian and International Experts on the Digitalization of Money*, Conference Report, 2023.](#)

Cerri A., *Riservatezza (diritto alla)*, in Enc. Giur. XXVII, 1995.

[Cesiano D., *Gli obblighi dell'intermediario finanziario nella prestazione dei servizi di investimento dagli orientamenti della giurisprudenza di merito alle Sezioni Unite*, Rivista di Diritto Societario, fasc. 3/2008.](#)

[Chandra A., *CBDC: Design Principles*, Medium, 2020.](#)

Chiap G. et al., *Blockchain. Tecnologia e applicazioni per il business*, Hoepli, 2021.

[Chicco M., *Le 9 crisi più nere delle criptovalute del 2022*, Wired, 2022.](#)

Chischti S. et al., *Il manuale della PayTech. Guida ai pagamenti digitali per imprenditori, manager e operatori della finanza*, Apogeo, 2021.

Choo K. R., *Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks?*, in Chuen D. L. K., *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, Academic Press, Londra, 2015.

Claps P. e Pignatelli M., *L'acquisto e la vendita per conto terzi di "Bitcoin" non sconta l'IVA ma rileva ai fini IRES ed IRAP*, Corr. trib., 2016.

[Clifford Chance, *Payment trends 2023*, Report, 2023.](#)

[Coinbase, *2023 Crypto Market Outlook*, 2022.](#)

[Coincub, *Crypto Tax Report*, 2023.](#)

[Colapietro C., *Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione*, Federalismi, n. 14, 13 maggio 2020.](#)

Colosimo B. e Corbò A., *DAO: Decentralized Autonomous Organization: cos'è, finalità e prospettive giuridiche*, Agenda Digitale, 2022.

Comella C., *Indice, sommari, ricerche e aspetti tecnici della de-indicizzazione*, Diritto dell'informatica, 2014.

Comitato di Basilea, *Implications of Fintech Developments for Banks and Bank Supervisors, Sound Practices*, 2018.

Comporti V., *La sollecitazione all'investimento*, in Patroni Griffi, Sandulli, Santoro (a cura di), *Intermediari finanziari, mercati di società quotate*, 1999.

Commissione per i problemi economici e monetari, *Relazione sulla tecnologia finanziaria: l'influenza della tecnologia sul futuro del settore finanziario, proposta di risoluzione* (relatore: Cora van Nieuwenhuizen), 2016/2243(INI), 2017.

Commissione Europea, *Commission Expert Group on taxation of the Digital Economy - general issues – working paper*, Bruxelles, 2013.

Commissione Europea, *Conseguenze dei cambiamenti climatici, Climate action*, 2023.

Commissione europea, *Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo*, COM(2018) 109 final, 2018.

Commissione Europea, *Strategia in materia di finanza digitale per l'UE*, COM(2020)591 final, 24 settembre 2020.

Consiglio dell'UE, *Anti-money laundering: Council agrees its position on a strengthened rulebook*, Comunicato stampa, 2022.

Consob, *Il Sistema Finanziario attuale: una stilizzazione*, Educazione Finanziaria, 2023.

Consob, *Le offerte iniziali e gli scambi di crypto-attività, Documento per la Discussione*, 2019.

Consob e Banca d'Italia, *Consob e Banca d'Italia mettono in guardia contro i rischi insiti nelle crypto-attività*, Comunicazione pubblica, 2021.

Corasaniti G., *Il trattamento tributario dei Bitcoin tra obblighi antiriciclaggio e monitoraggio fiscale*, cit.; Ferrari E., *Bitcoin e criptovalute: la moneta virtuale tra Fisco e antiriciclaggio, Il fisco*, 2018.

Cross T. e Andrew M. Bailey, *Carbon-neutral bitcoin for nation states*, Financial Cryptography and Data Security, Springer International Publishing, 2022.

Cucuzza O., *Economia internazionale e criminalità organizzata*, Riv. G.d.F., n. 6, 1996.

[Daga M.C. e Buscema S., *La disciplina dei CASP nel contesto nazionale ed europeo*, Osservatori.net digital innovation, 2023.](#)

[De Conno A., *Criptovalute e impatto ambientale: verso una nuova regolamentazione europea*, Altalex, 2022.](#)

[Deloitte, *DeFi deciphered: Navigating disruption within financial services*, 2023.](#)

[Department of The Treasury, *Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art*, 2022.](#)

[DeRoche M. et al., *The Energy Bomb: How Proof-of-Work Cryptocurrency Mining Worsens the Climate Crisis and Harms Communities Now*, 2022.](#)

[Deutsche Bundesbank, *Crypto tokens and decentralised financial applications*, 2021.](#)

[Deutsche Bundesbank, *Distributed ledger technologies in payments and securities settlement: potential and risks*, 2017.](#)

[Di Noia C., *The new frontiers of digital finance – Decentralised Finance \(DeFi\)*, Conferenza Consob, 2023.](#)

[Donyetta B. et al., *BeFi meets DeFi: A behavioural finance approach to decentralized finance asset pricing*, Research in International Business and Finance 65, 2023.](#)

Durrieu R., *Rethinking money laundering and financing of terrorism in international law*, 2013; Fiocca M. e Cosci S., *La Dimensione Finanziaria del Terrorismo e del Contro-Terrorismo Transnazionale*, Rubbettino, 2004.

[EBA-ESMA-EIOPA, *Crypto-assets: ESAs remind consumer about risks*, 2021.](#)

[EBA-ESMA-EIOPA, *FinTech: Regulatory sandboxes and innovation hubs*, 2018.](#)

[Egmont Group, *FIU – FinTech Cooperation and Associated Cybercrime Typologies and Risks*, 2022.](#)

[Elliptic, *NFTs and Financial Crime*, 2022.](#)

[Elliptic, *Preventing Financial Crime in Crypto-assets*, Elliptic typologies report 2022 edition, 2022.](#)

[Elteste U. e Nietsch T., *Exploring DORA: EU tightens IT Security rules for the financial sector, targeting “critical” third-party providers*, K&L Gates Hub, 2023.](#)

[Erb K. P., *White House Proposes 30% Energy Tax To Address Environmental Crypto Mining Costs*, Forbes, 2023.](#)

[ESMA, *Advice, Initial Coin Offerings and Crypto-Assets*, ESMA50-157-1391, 2019.](#)

[ESMA, *ESMA highlights the risks arising from the provision of unregulated products and/or services by investment firms*, Statement, 2023.](#)

[ESMA, *Markets in Crypto-Assets Regulation \(MiCA\)*, 2023.](#)

[ESRB, *Crypto-assets and decentralised finance*, 2023.](#)

[EUR-Lex. *L'accesso al diritto dell'Unione Europea*, 2023.](#)

[EUROFI, *Decentralized finance \(DeFi\): prospects and policy challenges*, in *EUROFI SEMINAR – Digitalisations and payments*, 2022.](#)

[EUROFI, *The EUROFI Views Magazine*, 2023.](#)

[European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 2020.](#)

[Fanti V., *La trasparenza amministrativa tra principi costituzionali e valori dell'ordinamento europeo: a margine di una recente sentenza della Corte costituzionale \(n. 20/2019\)*, Federalismi.it, 2020.](#)

[Fanusie Y.J. e Robinson T., *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*, Center on Sanctions & Illicit Finance, 2018.](#)

[FASB, *Accounting for and Disclosure of Crypto Assets*, 2023.](#)

[Federal Reserve, *Distributed ledger technology in payments, clearing, and settlement*, 2016.](#)

[Ferrajoli L., *Teoria assiomaticizzata del diritto. Parte generale*, 1970.](#)

[Feyen E. et al., *What does digital money mean for emerging market and developing economies?*, BIS Working Papers no. 973, 2021.](#)

[Filippetta A., *Il rapporto del 13 ottobre 2021 dei Ministeri dell'Economia e delle Banche Centrali dei Paesi G7 "Public Policy Principles for Retail Central Bank Digital Currencies \(CBDCs\)"*, Atlante storico del diritto dei dati. Anni 2020-2022 Raccolta della rubrica Diritto e nuove tecnologie pubblicata sulla rivista Persona e Mercato dall'Osservatorio Giuridico sull'Innovazione Digitale, 2022.](#)

[FINMA, Guida pratica per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle initial coin offerings \(ICOs\), 2018.](#)

[Fior T., Gary Gensler salva solo Bitcoin: tutte le crypto sono security, Cryptofacili, 2023.](#)

Fisicaro E., *Antiriciclaggio e terza direttiva UE. Obblighi a carico dei professionisti intermediari finanziari e operatori non finanziari alla luce del D.lgs. 231/2007*, Giuffrè, 2008.

Flick G. M., *Antiriciclaggio, corruzione e ruolo degli intermediari: un'agenda comune*, in Masciandaro D. (a cura di), *La legalità come valore di mercato*, Bancaria Editrice, 2000.

[Focus Group on Digital Currency including Digital Fiat Currency, Reference Documentation: Governance Aspects of Digital Fiat Currency, 2019.](#)

[Foley S., et al., Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Crypto-currencies?, Review of Financial Studies, Forthcoming, 2018.](#)

[Fondazione Finanza etica, Criptovalute e tecnologia blockchain, Capire la finanza, n.26, 2022.](#)

[Fondo Monetario Internazionale, Elements of effective policies for crypto assets, IMF Policy Paper, 2023.](#)

[Fondo Monetario Internazionale, Global Financial Stability Report. Safeguarding Financial Stability amid High Inflation and Geopolitical Risks, 2023.](#)

[Fondo Monetario Internazionale-FSB, IMF-FSB Synthesis Paper: Policies for Crypto-Assets, 2023.](#)

[Fondo Monetario Internazionale, Regulating the Crypto Ecosystem: The Case of Stablecoins and Arrangements, 2022.](#)

[Fondo Monetario Internazionale, The money Revolution. Crypto, CBDCs and the future of finance, IMF Magazine, 2022.](#)

[Fondo Monetario Internazionale, Virtual Assets and anti-money laundering and combating the financing of terrorism \(1\) – Some legal and practical considerations, 2021.](#)

[Forbes, Il Bitcoin come il petrolio e la carne bovina: tra il 2016 e il 2021 ha provocato danni climatici per 12 miliardi di dollari, 2022.](#)

[Forbes, What Really Happened To LUNA Crypto?, 2023.](#)

[Fracassi J. e Ruggieri M., *Lo scenario internazionale del mondo dei pagamenti: evoluzioni e trend*, Webinar promosso da Osservatori.net del Politecnico di Milano, 2023.](#)

[Frankenfield J., *Bitcoin ATM: definition, fees, and locations*, Investopedia, 2021.](#)

[Frosini T. E., *Il costituzionalismo nella società tecnologica*, Liber Amicorum per Pasquale Costanzo, vol. I, 2020.](#)

[Frosini T. E., *Il diritto costituzionale di accesso a Internet*, Rivista AIC, n. 1/2011, 2010.](#)

[FSB, *Decentralised financial technologies. Report on financial stability, regulatory and governance implications*, 2019.](#)

[FSB, *Global Regulatory Framework for Crypto-Asset Activities. Umbrella public note to accompany final framework*, 2023.](#)

[FSB, *Regulation, supervision and oversight of crypto-asset activities and markets: consultative document*, Consultative document, 2023.](#)

[Furnari S.L. e Schettini D., *Euro digitale: primi commenti alla Proposta di Regolamento. Tra innovazione tecnologia e adozione di massa*, 2023.](#)

[G7, *G7 Public Policy Principles for Retail Central Bank Digital Currencies and G7 Finance Ministers and Central Bank Governors' Statement on Central Bank Digital Currencies and Digital Payments*, Policy paper, 2021.](#)

[Garante per la protezione dei dati personali \(GPDP\), *Il potere dell'innovazione e la solitudine digitale. La protezione dei dati a tutela della persona, Relazione del Presidente Pasquale Stanzone – 2022, 2023.*](#)

[Garante per la protezione dei dati personali, *Provvedimento n. 1715015*, 2010.](#)

[Georgieva K., *The Future of Money: Gearing up for Central Bank Digital Currency*, International Monetary Fund \(IMF\), 2022.](#)

[Giammatteo M., *Cash use and money laundering: An application to Italian data at bank-municipality level*, Quaderni dell'antiriciclaggio, 13, 2019.](#)

[Garavaglia R., *Conoscere la blockchain for dummies*, Hoepli, 2022.](#)

[Garavaglia R., *Cripto-asset: MiCAR approvato dal Parlamento europeo*, 2023.](#)

[Garavaglia R., *PSD3 e Fida, ecco il nuovo corso europeo su pagamenti e finanza digitali*, Agenda Digitale, 2023.](#)

[Garavaglia R., *Regolamento \(UE\) 2023/1113: un'analisi delle disposizioni relative ai trasferimenti di fondi e crypto-attività*, 2023.](#)

[Gensler G., *The SEC Treats Crypto Like the Rest of the Capital Markets*, Wall Street Journal, 2022.](#)

Ghiselli F., *Giù le tasse ma con stile!*, Franco Angeli, 2019.

[Giacometti T. e Formenti O., *La nuova disciplina in materia di prevenzione del riciclaggio e di finanziamento del terrorismo \(d.lgs. 25 maggio 2017, n. 90\)*, Dir. Pen. Cont., 2017.](#)

Global Blockchain Business Council (GBBC), *Stronger together: Rebuilding after the Mealstrom of Markets*, in GBBC 2022 Annual Report, 2022.

[Gola C. et al., *La governance delle blockchain e dei sistemi basati sulla tecnologia dei registri distribuiti*, Banca d'Italia, 2023.](#)

[Goldman Z.K. et al., *Terrorist use of virtual currencies: containing the potential threat*, Center for a New American Security, 2017.](#)

[Gorman B., *What Is a Decentralized Autonomous Organization \(DAO\)?*, Avast, 2023.](#)

Greco D. e Catinari E., *Criptovalute: spunti operativi alla luce della Manovra 2023*, Fiscalità e comm. inter., n. 3, 2023.

[Grillo F., *Proof-of-Work e impatto ambientale: problemi e potenziali soluzioni*, Alma Mater Studiorum – Università di Bologna, 2020.](#)

[Gruppo d'Azione Finanziaria Internazionale, *Financing of recruitment for terrorist purposes*, 2018.](#)

[Gruppo d'Azione Finanziaria Internazionale, *Guidance for a risk-based approach virtual currencies*, 2015.](#)

[Gruppo d'Azione Finanziaria Internazionale, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, 2019.](#)

[Gruppo d'Azione Finanziaria Internazionale, *International standards on combating money laundering and the financing of terrorism & proliferation – FATF Recommendations*, 2023.](#)

[Gruppo d'Azione Finanziaria Internazionale, *Linee guida per un approccio ai virtual asset e ai prestatori di servizi in materia di virtual asset basato sul rischio*, MEF - Dipartimento del Tesoro, 2019.](#)

Gruppo d'Azione Finanziaria Internazionale, *The role of hawala and other similar service providers in money laundering and terrorist financing*, Report, 2013.

Gruppo d'Azione Finanziaria Internazionale, *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, 2014.

Harang J. e Petropoulos G., *Web3: the next internet revolution*, Bruegel, 2023.

Hayes A., *Bank for International Settlements: Overview, History*, 2022.

Hicks C., *Cryptocurrency Regulations around the World*, Forbes Advisor, 2023.

HM Treasury, *Future financial services regulatory regime for cryptoassets: Consultation and call for evidence*, 2023.

Hughes C., *Facebook co-founder: Libra coin would shift power into the wrong hands. Regulators should not underestimate the digital currency's disruptive potential*, Financial Times, 2019.

Indipendent, *Bitcoin price is so high because criminals are using it for illegal trades, research suggests*, 2018.

International Organization of Securities Commissions (OICV-IOSCO), *Policy Recommendations for Crypto and Digital Asset Markets*, Consultation Report, 2023.

Ibiz E. e Kaunert C., *Sharing Economy for Tackling Crypto-Laundering: The Europol Associated "Global Conference on Criminal Finances and Cryptocurrencies", Sustainability*, 2022.

Iyer R. e Popescu A., *New Evidence on Spillovers Between Crypto Assets and Financial Markets*, IMF Working paper, 2023.

ISO, *Overview of an interactions between smart contracts in blockchain and distributed ledger technology systems*, ISO/TR 23455:2019.

ISO, *Standards by ISO/TC 307. Blockchain and distributed ledger technologies*, 2023.

ITU-T, *Focus Group on Application of Distributed Ledger Technology*, 2019.

Kahn C. M. et al., *Should the central bank issue e-money?*, 2018.

Khalili J., *Vi fareste scansionare l'iride in cambio di una criptovaluta?*, Wired, 2023.

Khanna A. et al., *L'età ibrida. Il potere della tecnologia nella competizione globale*, Codice Edizioni, 2013.

[Khiaonarong T. et al., *Operational Resilience in Digital Payments: Experiences and Issues*, IMF eLibrary, 2021.](#)

[Kraken Intelligence, *PoW vs. PoS: Securing the Chain*, Report, 2022.](#)

Krogh M., *Gli obblighi e le nuove sanzioni antiriciclaggio nel D.lgs. 25 maggio 2017, n.90*, Il Notariato, 2017.

[Krungsri Research, *Digital Asset \(Part 1\) “When Thais are drawn towards digital assets”*, 2023.](#)

La Rocca L., *La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*, Analisi Giuridica dell’economia, 2015.

La Sala G.P., *Intermediazione, disintermediazione e nuova intermediazione*, in Cian M., Sandei C., *Il diritto del Fintech*, Cedam 2020.

[Lee S. e Park J., *Environmental Implications of a Central Bank Digital Currency \(CBDC\)*, World Bank Group Korea Office, Innovation and Technology Note Series, July 2022, note series number 8.](#)

Lembo M. e Scialoja A., *Antiriciclaggio*, Apogeo Education, 2012.

[Leonardo C., *La stablecoin Tether verso il mining di Bitcoin sostenibile*, 2023.](#)

[Lops V., *Cripto, cresce la voragine di Ftx. In fumo oltre 30 miliardi di dollari*, Il Sole 24 Ore, 2022.](#)

[Leuprecht C. et al., *Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency*, Journal of Financial Crime Vol. 30 No. 4, 2023, pp. 1036-1054.](#)

[Luca G., *Criptovalute*, La piazza d’Italia, 2023.](#)

Lynn T. (a cura di), *Disrupting Finance: Fintech and Strategy in 21st century*, Palgrave – McMillan, 2018.

Magri P., *Delitti contro il patrimonio mediante frode, usura, appropriazione indebita, ricettazione riciclaggio*, Cedam, 2007.

[Makarov I., Schoar A., *Cryptocurrencies and Decentralized Finance \(DeFi\)*, BIS Working Papers no. 1061 – Monetary and Economic Department, 2022.](#)

Magliocco A., *Bitcoin e tassazione*, in *Strumenti finanziari e fiscalità*, 2016.

Malaguti, M. C., *Fintech e piattaforme digitali nel settore finanziario tra concorrenza e regolazione*, in Salce V. e Finocchiaro G. (a cura di), *Fintech: diritti, concorrenza, regole*, 2019, pag. 55-82.

Manes V., *Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale*, Riv. trim. dir. pen. econ., 2004.

[Marini M., *Oblio, deindicizzazione e processo penale: dal diritto eurounitario alla riforma Cartabia*, Sistema Penale n. 1, 2023.](#)

[Marvulli E., *Ue, il Parlamento estende le travel rules alle crypto-attività*, Fisco Oggi, 2023.](#)

[Masciandaro D., *Il riciclaggio dei capitali illeciti profili di analisi economica*, GNOSIS n. 3, 2007.](#)

McCulley P., *Teton Reflections*, Global Central Bank Focus, Federal Reserve of Kansas City, Jackson Hole Economic Symposium, 2007.

Mezzanotte M., *Il diritto all'oblio. Contributo allo studio della privacy storica*, 2009.

[Meegan X. – Koens T., *Lessons learned from Decentralised Finance, \(DeFi\)*, NewIngwb.com, 2022.](#)

[MEF, *Attività del Gruppo d'azione finanziaria \(GAFI/FATF\)*, Dipartimento del Tesoro, 2022.](#)

Miccoli C., *Bitcoin e crypto-valute. La guida per tutti*, Vallardi, 2022.

[Minenna M., *DeFi: come funziona la finanza prêt-à-porter basata sulla blockchain*, Il Sole 24 Ore, 2022.](#)

Monteverde S., *Attuazione della direttiva CEE in materia di riciclaggio*, *Diritto Penale e Processo*, 1997.

Morelli M., *Oblio (diritto all')*, Enc. Dir., VI, 2002.

[Morini G., *Criptovaluta: digitalizzazione di valore e finanza decentralizzata. Tra regolamentazione ed elusione*, Il caso.it, 2023.](#)

Narayanan A. et al., *Bitcoin and cryptocurrency Technologies: a comprehensive introduction*, Princeton University Press, 2016.

[Nasdaq, *Cryptocurrency Regulation Guide*, 2023.](#)

[Nicotra I., *Privacy vs. trasparenza, il Parlamento tace e il punto di equilibrio lo trova la Corte*, Federalismi.it.](#)

[Niola F., *Worldcoin: le sfide normative su identità biometriche e criptovalute*, Agenda Digitale, 2023.](#)

Nuzzo U. e Morgante A., *La rilevanza fiscale dell'impresa illecita*, Finanza e Fisco, n. 10, 1998.

[Olivi G. e Venditti A., *Tra DORA e GDPR: cybersecurity e privacy nel settore bancario*, Diritto Bancario, 2023.](#)

Licini C., *Normativa antiriciclaggio e antiterrorismo per i professionisti*, Ipsoa, 2009.

[Lio O. et al., *Regolamento DORA: ecco cosa devono fare le aziende del settore finanziario per adeguarsi*, Agenda Digitale, 2023.](#)

[OAM, *Primo flusso informativo trasmesso all'OAM dai prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale*, I° trimestre, 2023.](#)

[Ocampo D.G. et al., *Crypto, Tokens and DeFi: navigating the regulatory landscape*, FSI Insights on policy implementation No 49, 2023.](#)

[OCSE, *Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard*, 2022.](#)

[OCSE, *Institutionalisation of crypto-assets and Defi-TradFi interconnectedness*, OECD Publishing, 2022.](#)

[OCSE, *Lessons from the Crypto Winter. DeFi versus CeFi*, OECD Business and Finance Policy Papers, 2023.](#)

[OCSE, *Regulatory approaches to the Tokenisation of Assets*, OECD Blockchain Policy Series, 2021.](#)

[OCSE, *Taxing Virtual Currencies. An Overview of Tax Treatments and Emerging Tax Policy Issues*, 2020.](#)

[OCSE, *The Tokenisation of Assets and Potential Implications for Financial Markets*, OECD Blockchain Policy Series, 2020.](#)

[OCSE, *Why Decentralised Finance \(DeFi\) matters and the policy implications*, OECD Paris, 2023.](#)

[OCSE–International Financial Consumer Protection Organisation \(FinCoNet\), *Developments in Central Bank Digital Currencies and issues for consumers*, Report – International Seminar, 2023.](#)

[Oropallo D., *In Cina l'energia del mining è riutilizzata per scopi ecosostenibili*, 2021.](#)

[Oropallo, D., *La Cina sostiene la sua criptovaluta, banna le altre e il bitcoin crolla*, 2021.](#)

Pacillo V., *Le valute virtuali alla luce della V Direttiva Antiriciclaggio*, Riv. Trim. Dir. Trib., nn. 3-4, 2018.

Pagano F. e Soldavini P., *Il capitale decentralizzato: Blockchain, NFT, Metaverso*, Il Sole 24 Ore, 2022.

[Paesani P., *Bitcoin di Stato? Il caso della moneta digitale di Banca Centrale*, 2018.](#)

[Paliotta A. P., *Guerra in Ucraina: ecco come criptovalute, NFT e crowdfunding finanziano la resistenza*, 2022.](#)

Palumbo G., *Il trattamento tributario dei «Bitcoin»*, Dir. Prat. Trib., 2016.

[Panetta F., *Paradise lost? How crypto failed to deliver on its promises and what to do about it*, 2023.](#)

[Panetta F., Dombrovskis V., *Perché l'Europa ha bisogno di un euro digitale*, 2023.](#)

[Panetta F., *L'euro digitale e l'evoluzione del sistema finanziario*, Intervento BCE, 2022.](#)

[Pannone A., *Il fallimento di Alameda è un rischio per Tether? Ecco quanto ne sappiamo*, The Cryptonomist, 2023.](#)

[Pantaleo A. e Davico D., *ESMA rilascia il proprio parere sui crypto-assets*, Non Solo Diritto Bancario, 2019.](#)

Pantaleo A., *I prestatori di servizi su crypto-attività*, in Capaccioli S. e Giordano M. T., *Crypto-asset: Regolamento MiCA e DLT Pilot Regime. Analisi ragionata su token, stablecoin e CASP*, Giuffrè, 2023.

[Paracampo M. T., *FinTech, modelli di business innovativi e regimi di autorizzazione: il responso delle Autorità europee*, 2019.](#)

Paracampo M.T., *I prestatori di servizi per le crypto-attività. Tra mifidizzazione della MiCA e tokenizzazione della Mifid*, Giappichelli, 2023.

Pardolesi R., *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e continuità*, in Pardolesi R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, vol. I, 2003.

[Pardolesi R., *L'ombra del tempo e \(il diritto al\)l'oblio*, Quest. Giust., 2017.](#)

[Parlamento europeo, *Impatto delle nuove tecnologie sulla tassazione: cripto-attività e blockchain*, Risoluzione del Parlamento europeo del 4 ottobre 2022 sull'impatto delle nuove tecnologie sulla tassazione: cripto-attività e blockchain \(2021/2201\(INI\)\), 2022.](#)

[Parlamento Europeo, *Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione \(2017/2772\(RSP\)\)*, 2018.](#)

[Parlour C. A., *An introduction to Web3 with implications for financial Services*, Federal Reserve Bank of Atlanta's Policy Hub. Center for Financial Innovation and Stability, no. 3, 2023.](#)

Parola L. et al., *Blockchain e smart contract: questioni giuridiche aperte*, Contratti, 2018.

[Pascale R., *Finanza digitale: prospettive e opportunità per le imprese*, Presentazione Banca d'Italia – Servizio Strumenti e Servizi di pagamento al dettaglio, 2023.](#)

[Passarelli N., *Bitcoin e antiriciclaggio*, Sicurezza Nazionale, 2016.](#)

Pecorella G., *Denaro (sostituzione di)*, in *Dig. disc. pen.*, III, UTET, 1989.

Pedotti P., *Gli aspetti contabili delle criptovalute*, in *Amministrazione e finanza*, n. 5, 2022.

[Pellecchia E., *GDPR e tecnologie blockchain: prospettive di evoluzione di un rapporto complesso*, 2021.](#)

[Perrazzelli A., Vice Direttrice Generale della Banca d'Italia, *Le iniziative regolamentari per il Fintech: a che punto siamo?*, Università degli Studi dell'Insubria. Laboratorio di Finanza Digitale, 2021.](#)

[Peterson K. O., *Decentralized finance research and developments around the world*, J Bank Financ Technol. 2022.](#)

[Pezzuto A., *Cripto-attività: classificazione, caratteristiche e prospettive di regolamentazione*, Magistra banca e Finanza, 2022.](#)

[Pezzuto A., *Negoiazione e regolamento di valute virtuali qualificabili come strumenti finanziari ai fini della MiFID II – Il regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito \(DLT\)*, Magistra Banca e Finanza, 2022.](#)

Piasente M., *Esenzione IVA per i “Bitcoin”: la strada indicata dalla Corte UE interpretando la nozione “divise”*, Corr. Trib., 2016.

Picotti L., *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, Riv. trim. dir. pen. econ., n. 3-4, 2018.

Pitruzzella G., *FinTech e i nuovi scenari competitivi nel settore finanziario-creditizio e assicurativo*, Mensile dell'Associazione Bancaria Italiana, 2018.

Pizzetti F., *Il prisma del diritto all'oblio*, Pizzetti F. (a cura di), *Il caso del diritto all'oblio*, 2003.

[Politecnico di Milano, La blockchain spiegata in maniera semplice: significato e applicazioni, blog.osservatori.net.](#)

Pollari N., *Il controllo internazionale sui paradisi finanziari*, Riv. G.d.F., n. 5, 1997.

Pollari N., *L'impresa criminale ed i suoi effetti sui mercati e sugli aggregati macroeconomici*, Rivista GdF., 3/1999.

Pollari N., *La globalizzazione dell'economia e dei presupposti impositivi*, Riv. G.d.F., n. 1, 2001.

Pollari N. e Dal Cioppo A., *Tecnica delle inchieste patrimoniali per la lotta alla criminalità organizzata*, Laurus Robuffo, 2006.

Pollari N. e Nota S., *Percorsi di fiscalità internazionale*, Aracne, 2019.

[Pollicino O. e Repetto G., Not to be Push Aside: the Italian Constitutional Court and the European Court of Justice, Verfassungsblog, 2019.](#)

Pollicino O. e Resta F., *Visibilità del potere, riservatezza individuale e tecnologia digitale. Il bilanciamento delineato dalla Corte*, Diritto dell'Informazione e dell'Informatica (II) fasc. 1, 2019.

[Porcelli A., Il Presidente Biden nella proposta di bilancio federale propone la tassazione del 30% per il mining di Bitcoin, 2023.](#)

[Porcelli A., L'accordo sul tetto del debito USA blocca la tassa del 30% sul mining di Bitcoin, 2023.](#)

[Portale V., Cos'è il Web3 e come funziona: guida al web 3.0, Osservatori.net digital innovation, 2023.](#)

Prasad. E. A., *The future of money. How the digital revolution is transforming currencies and finance*, Harvard University Press, 2021.

[PWC, *Central Bank Digital Currency*, 2023.](#)

[PWC, *Rebuilding confidence in crypto*, 5th Annual Global Crypto Hedge Fund Report, 2023.](#)

Quattrociochi B., *Norme, regole e prassi nell'economia dell'antiriciclaggio internazionale*, Torino, 2017.

Querqui M. e Verrocchi G., *La delega legislativa per il recepimento della direttiva n. 60/2005/CE in materia di contrasto al riciclaggio ed al finanziamento del terrorismo internazionale*, Il Fisco, 2006.

[Ranocchiari M., *Il consumo di acqua dei data center sta diventando un problema. Anche il Cloud ha sete, ma l'impronta idrica dei data center dipende dalla geografia*, Materia Rinnovabile, 2023.](#)

[Renner K., *The environmental impact of DeFi: a growing concern?*, Medium, 2023.](#)

[Rinaldi G., *Approcci normativi e qualificazione giuridica delle criptomonete*, in *Contratto e impresa*, n. 1, 2019.](#)

Ripple, *Measuring the Environmental Impact of Cryptocurrency*, 2021.

[Rociola A., *Storia del più grande crac della storia delle criptovalute. Cosa è successo a Ftx*, la Repubblica, 2022.](#)

[Rochemont, *\(An addendum to\) A cashless society: benefits, risks, issues – Environmental sustainability of a cashless society*, Institute and Faculty of Actuaries, 2018.](#)

[Rudd, M.A., *Bitcoin is full of surprises*, Challenges 14\(2\) 27, 2023.](#)

[Ruggeri A., *La Consulta rimette a punto i rapporti tra diritto eurounitario e diritto interno con una pronuncia in chiaroscuro \(a prima lettura di Corte cost. n. 20 del 2019\)*, in *Giur. Cost.*, Studi 2019/I, 113.](#)

[Ruggiero N., *Criptovalute, come ridurre l'impatto ambientale: ecco le vie più promettenti*, 2022.](#)

[Ruocco A., *Ma è vero che il bitcoin consuma davvero tanta energia?*, 2022.](#)

[Ruocco T., *NFT, così il terrorismo li usa per finanziarsi*, 2022.](#)

Sarzana di S. Ippolito F. e Nicotra M., *Diritto della blockchain, intelligenza artificiale e IoT*, IPSOA, 2018.

[Sapra N. e Shaikh I., *Impact of Bitcoin mining and crypto market determinants on Bitcoin-based energy consumption*, *Managerial Finance*, 2023.](#)

[Sarkar A., *I consumi di Ethereum sono diminuiti del 99,9% dopo il Merge*, 2022.](#)

[Sartori N., *Le valute virtuali e il trattamento fiscale dei proventi a esse connessi*, *Università degli Studi di Milano-Bicocca*, 2023.](#)

[Sasi-Brodesky A. e Nassr I. K., *DeFi liquidations: volatility and liquidity – OECD Working Papers on Finance, Insurance and Private Pensions* No. 48, 2023.](#)

[Sat D. M. et al., *Investigation of money laundering methods through crypto-currencies*, in *Journal of Theoretical and Applied Information Technology*, Vol. 83, n. 2, 2016.](#)

[Savona P., *Rischi, regolamentazione e stabilità finanziaria: senza una modifica dell'architettura istituzionale continueremo a inseguire l'obiettivo senza evitare che le crisi di singoli operatori si tramutino in rischi sistemici*, 2023.](#)

[Scaccia G., *Corte costituzionale e doppia pregiudizialità: la priorità del giudizio incidentale oltre la Carta dei diritti?*, *Forum di Quaderni Costituzionali*.](#)

[Scaling Parrots, *Cosa sono le commissioni sulle transazioni Blockchain e perché esistono?*, 2023.](#)

Schär F., *Defi's promise and pitfalls. Decentralized finance could support a new financial infrastructure if challenges are overcome*, The Money Revolution, 2022.

[Schena C. et al., *Lo sviluppo del Fintech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, *Quaderni FinTech Consob*, 2018.](#)

[Schnepf N. et al., *Introduzione a Web3: Guida*, Oracle, 2023.](#)

[Schwarz N. et al., *Virtual Assets and Anti-Money Laundering and Combating the financing of terrorism \(I\) – Some legal and practical considerations*, in *International Monetary Fund \(IMF\) papers*, 2021.](#)

[Securities and Markets Stakeholder Group \(MSG\), *Advice to ESMA – Own Initiative Report on Initial Coin Offerings and Crypto-Assets*, 2018.](#)

[Sephton C., *Come le stablecoin rimangono stabili, spiegato semplicemente*, *CoinTelegraph*, 2021.](#)

[Siani G., *La regolamentazione delle nuove tecnologie basate sulla Distributed ledger technology – DLT, tra tutela del mercato e rischi di sistema*, Università Luiss Guido Carli di Roma Guardia di Finanza – Scuola di Polizia Economico-Finanziaria, 2022.](#)

[Sica S. e D'Antonio V., *La procedura di de-indicizzazione*, in Resta G., Zeno-Zencovich V. \(a cura di\), *Il diritto all'oblio dopo la sentenza Google Spain*, 2015.](#)

Sicignano G. J., *Bitcoin e riciclaggio*, Giappichelli, 2019.

[Sideri M., *Bitcoin, Mt. Gox chiede il "Chapter 15"*, Corriere della Sera, 2014.](#)

Simoncini E., *Il cyberlaundering: la nuova frontiera del riciclaggio*, Riv. trim. dir. pen. econ., n. 4, 2015.

[Soro A., *Criptovalute. Con la moneta i big del web diventano Stati-padroni*, Il Mattino, 2019.](#)

Soro A., *Democrazia e potere dei dati. Libertà, algoritmi, umanesimo digitale*, Baldini + Castoldi, 2019.

[Starola L., *Il riciclaggio nel d.lgs. 231/2007. Nozione, ambito operativo e soggetti destinatari*, Il nuovo diritto delle società, ODCEC, 2011.](#)

Stile A., *Riciclaggio e reimpiego di proventi illeciti*, Enciclopedia giuridica Treccani, 2009.

[Stimolo S., *Un NFT su Ethereum consuma energia quanto una Tesla*, The Cryptonomist, 2021.](#)

[Strategy&, *European Crypto Survey*, 2022.](#)

[Sturzo L., *Bitcoin e riciclaggio 2.0*, Diritto Penale Contemporaneo, 2018.](#)

[Talley I., *Islamic State Turns to NFTs to Spread Terror Message*, Wall Street Journal, 2022.](#)

Tanda M. e Schena C., *Fintech, Bigtech and Banks: Digitalisation and Its Impact on Banking Business Model*, Palgrave – McMillan, 2019.

[Tar A., *Proof-of-Work, spiegata semplicemente*, CoinTelegraph Italia, 2018.](#)

[Tavelli A., *Bitcoin e sostenibilità ambientale: amici o nemici?*, IARI – Istituto Analisi Relazioni Internazionali, 2023.](#)

Tedeschi E., *Credit scoring: la valutazione del merito creditizio nell'era dell'IA, degli Alternative Data e dei Digital Footprints*, Vol. 256455, La via europea per l'Intelligenza artificiale. Atti Convegno del progetto Dottorale di Alta Formazione in Scienze Giuridiche – Venezia, 25-26 novembre 2021, 2022.

Tedeschi E., *Criptovalute e blockchain nello scenario internazionale: nuove sfide per i regolatori, discipline a confronto, presidi di salvaguardia e di intelligence economica*, 2020.

[Tedeschi E., *Le criptovalute e i rischi di riciclaggio: lo stato dell'arte a contrasto del fenomeno*, La piazza d'Italia, 2022.](#)

[Tedeschi E., *Le Altcoin quali solide alternative al Bitcoin*, 2022.](#)

Thione M. e Silvari M., *Le nuove frontiere del riciclaggio: analisi del fenomeno, linee evolutive ed elaborazioni statistiche di settore*, Il fisco, n. 23, 2006.

Tramontano G. et al., *La IV direttiva antiriciclaggio e antiterrorismo. I nuovi obblighi per gli intermediari finanziari e i professionisti*, Aracne, 2016.

Travaglini G., *Riciclaggio: storia, comparazione, struttura*, Dir. pen. proc., 1996.

Troiano, V., *I soggetti operanti nel settore finanziario*, Capriglione F. (a cura di), *Manuale di diritto bancario e finanziario. Seconda edizione*, 2019.

[Truchet M., *Decentralized Finance \(DeFi\): opportunities, challenges and policy implications*, in EUROFI Regulatory Update, 2022.](#)

[Tumietto D., *Cripto-attività, ecco il regolamento MICA: le nuove regole da conoscere*, 2023.](#)

[United Nations Human Rights Special Procedures, *International Human Rights Law considerations for counter-terrorism financing regulation of crowdfunding, virtual assets and new payment technologies*, 2023.](#)

[Yousaf I., Goodell J. W., *Reputational contagion and the fall of FTX: Examining the response of tokens to the delegitimization of FTT*, Finance Research Letters 54, 2023.](#)

[U.S. Department of the Treasury, *The Future of Money and Payments. Report pursuant to Section 4 \(b\) of Executive Order 14067*, 2022.](#)

[UNHCR, *Meet the Syrian cartoonist behind UNHCR's first-ever NFT fundraiser*, 2021.](#)

Valente P., *Concorrenza fiscale dannosa e paradisi fiscali - Nuovi scenari e tendenze in atto*, Rass. fis. int., n. 3, 1999.

Valente P. et al., *Riciclaggio e criminalità. Idra per gli Stati, Sisifo per la Società, Nesso per gli Organismi Sovranazionali*, Eurilink, Roma, 2017.

Valitutti A., *Il contratto di intermediazione finanziaria privo di forma scritta: nullità selettiva o abuso del diritto?*, Atti del Convegno “Questioni di diritto civile all’esame delle Sezioni Unite – Nullità selettiva” presso la Corte Suprema di Cassazione, 2019.

[Van der Cruijssen C. et al., *Trust in Financial Institutions: A Survey*, DeNederlandscheBank paper, 2020.](#)

[Van Esterik-Plasmejer P.W.J. e Van Raaij F., *Banking system trust, bank trust and bank loyalty*, *International Journal of Bank marketing* 35\(1\), 2017.](#)

[Vermaak W., *What is Yeld Farming*, CoinMarketCap, 2022.](#)

[Volpicelli G. M., *La crisi in Kazakhstan è un grosso problema per i miner di criptovalute*, *Wired*, 2022.](#)

Von Hayek F. A. *La denazionalizzazione della moneta*, Rubbettino, 2018.

[Wensheng G. et al., *Web 3.0: The Future of Internet*, Companion Proceedings of the ACM Web Conference 2023 \(WWW '23 Companion\), 2023.](#)

[Wong J. e Gilkes K., *Why organizations should prepare for quantum computing cybersecurity now*, EY, 2023.](#)

[Woolard C. et al., *8 areas of change for financial services regulatory policy in 2023*, EY, 2023.](#)

[World Economic Forum, *Central Bank Digital Currency. Global Interoperability Principles*, White Paper, 2023.](#)

[World Economic Forum, *Pathways to the Regulation of Crypto-Assets: A Global Approach*, White Paper, 2023.](#)

[Wright A. e De Filippi P., *Decentralized Blockchain Technology and The Rise of Lex Cryptographia*, Social Science Research Network, 2015.](#)

[Zetsche D.A., *Keynote Speech*, Presentazione Conferenza “The regulation on Markets in Crypto-Assets \(MiCA\). The future of Blockchain Technology in Europe”, Bocconi, 2023.](#)