LUISS

Dipartimento Di Giurisprudenza

Cattedra Di Diritto Penale 2

Cybersecurity: Criptovalute e responsabilità dei Wallet Provider

Prof. Antonino Gullo

RELATORE

Prof. Maria Lucia Di Bitonto

CORRELATORE

Alessandro Loreti Matr. 150753

CANDIDATO

Anno Accademico 2022/2023

Indice

INTRODUZIONE

La globalizzazione e la rivoluzione digitale hanno favorito la crescita e lo sviluppo di internet e delle innovazioni digitali nonché la creazione e diffusione di nuovi mezzi alternativi di pagamento. Oggi, accanto alla moneta legale si è dapprima affiancata la moneta elettronica, come il bancomat e la carta di credito, e negli ultimi anni, ha preso piede una terza tipologia di moneta: la moneta digitale. Seppure ancora oggi, l'utilizzo della moneta digitale risulti parzialmente limitato a causa di alcune criticità che la affliggono, soprattutto negli ultimi anni si è assistito ad un notevole incremento del suo utilizzo, non solo da parte degli investitori ma anche da parte di alcuni Stati con l'intento di contrastare l'inflazione della moneta avente corso legale.

Il presente lavoro si propone di analizzare dapprima i concetti di moneta elettronica, legale e digitale per poi focalizzarsi sulle caratteristiche e l'evoluzione delle monete digitali, trattando, nello specifico delle implicazioni di natura penale legate all'utilizzo delle criptovalute.

Il primo capitolo del presente elaborato contiene un'introduzione sia del concetto di digitalizzazione sia del termine di moneta digitale, la cui nascita è strettamente collegata all'avvio di un processo di digitalizzazione a livello globale. In particolare, come si vedrà, il processo di digitalizzazione ha favorito l'utilizzo di forme diverse di moneta, le cui caratteristiche saranno oggetto di analisi.

Nella prima parte si evidenzierà come in ambito penale la tecnologia legata alla moneta digitale, ha favorito il proliferare di attività criminose legate al finanziamento delle attività di terrorismo nazionale ed internazionale, nonché, prevalentemente, ai reati di riciclaggio ed autoriciclaggio, oltre al tema del *cyberlaundering*, ossia la ripulitura del denaro "sporco".

Proseguendo, la seconda e terza parte del primo capitolo sono dedicate principalmente alla spiegazione del funzionamento di alcune monete digitali ossia delle criptovalute. Pertanto, essenziale per una visione a tutto tondo del mondo delle

monete digitali, verrà definito il protocollo Blockchain, utilizzato da diverse tipologie di criptovalute, come i Bitcoin, nonché i *crypto-asset* i quali non sono dotati di una definizione univoca. Tuttavia, essi vengono definiti dalla Banca d'Italia come attività registrate realizzate grazie all'utilizzo della crittografia che si distinguono in due tipologie: nativi e non nativi. A questo punto è stato trattato degli *smart contracts* e delle loro implicazioni penali.

La parte conclusiva del primo capitolo, invece, contiene un ulteriore approfondimento delle monete virtuali ossia si tratterà dell'ecosistema delle criptovalute nonché dei soggetti che ne fanno parte: i *Wallet provider.*

Di questi ultimi è stato, sinteticamente, menzionato il tema della responsabilità del *Wallet provider*, che sarà poi ripreso negli altri capitoli dell'elaborato, per evidenziare come il legislatore abbia posto in capo agli stessi obblighi di garanzia e sorveglianza delle operazioni digitali a tutela degli individui coinvolti ed a protezione dei più importanti beni della vita.

Concludendo il capitolo si è deciso di analizzare le implicazioni tecniche legali e sociologiche che potrebbero derivare dall'utilizzo delle valute digitali in totale ovvero parziale sostituzione della moneta avente corso legale.

Tenendo a mente il concetto di criptovalute, ecosistema nonché blockchain, il secondo capitolo sarà dedicato all'analisi della normativa ad oggi vigente relativamente alle monete digitali nonché alle criptovalute. Si mostrerà, dunque, dapprima l'approccio generale adottato dalle autorità pubbliche mondiali, proseguendo con il modello europeo ad oggi vigente. Circa il modello europeo si è ritenuto necessario procedere anche ad un approfondimento, non solo della normativa, ma anche delle autorità che oggi svolgono un ruolo fondamentale di garanzia e controllo delle attività mediante criptovalute.

Il capitolo prosegue con la trattazione della responsabilità del soggetto principale dell'ecosistema delle criptovalute, ossia i *wallet provider*, dei quali saranno oggetto di analisi sia gli obblighi sia le possibili ipotesi di configurazione della responsabilità penale.

Ovviamente dall'intervento del legislatore europeo al quadro normativo attuale sono state realizzate ulteriori integrazioni in materia. In particolare, essendo l'iniziativa *ab origine* di natura europea, è necessario approfondire l'*excursus* del quadro normativo italiano. L'inquadramento giuridico italiano delle criptovalute, si può dire, che abbia predetto quello europeo, introducendo misure atte a contrastare le attività illecite correlate all'utilizzo delle monete digitali successivamente implementate anche a livello europeo.
Nella terza parte del secondo capitolo, quindi, sarà doveroso non solo analizzare l'applicazione della normativa europea da parte del legislatore italiano ma anche analizzare quella che è la giurisprudenza della Corte di Cassazione che ha tentato di interpretare nonché colmare le lacune sia del legislatore italiano sia quelle lasciate dal legislatore europeo, nel rispetto dell'autonomia lasciata ai singoli Stati membri.
In tale contesto, interessante, inoltre, sarà la valutazione della qualificazione fiscale delle criptovalute in Italia nonché la trattazione delle risoluzioni emesse, anche recentemente, dall'Agenzia delle Entrate nel tentativo di creare chiarezza dal punto di vista fiscale ed in generale le possibili conseguenze fiscali ed economiche che sorgono.

Data l'autonomia riconosciuta ai singoli Stati membri, l'ultimo paragrafo del secondo capitolo rappresenta un'analisi comparativa degli approcci adottati da altri Stati membri diversi dall'Italia, tra cui Malta ed Estonia che hanno deciso di adottare un approccio "crypto-friendly" e l'approccio prudente di Francia, Regno Unito e Germania.

Pertanto, analizzato il concetto di criptovalute, blockchain, soggetti dell'ecosistema delle criptovalute e la normativa ad oggi vigente in materia, il terzo capitolo, invece, sarà incentrato sulla sicurezza degli E-Wallet ossia quello strumento che consente di effettuare transazioni digitali. In particolare, saranno oggetto di analisi le possibili minacce informatiche che possono intaccare l'integrità degli E-Wallet, tra cui la memoria e l'archiviazione, i sistemi operativi e i *software* utilizzati, il protocollo Blockchain e ulteriori fattori di rischio. A ciò seguirà una valutazione di come il procedimento penale, volto a perseguire i reati collegati agli E-Wallet, è

mutato nel corso del tempo: dalla tipologia di prove, alle indagini fino ad arrivare alle parti processuali.

Infine, tale capitolo si concluderà con una trattazione di *case study*, in *primis* relativi all'utilizzo delle criptovalute su piattaforme illecite ovvero per la commissione di attività illecite, ed in secondo luogo saranno analizzati una serie di casi in cui il fatto del reato è il furto di criptovalute da parte di ignoti per problematiche relative alla piattaforma dei fornitori di servizi di criptovalute.

L'incertezza relativamente alle criptovalute aleggia a livello globale e non solo europeo. Il quarto ed ultimo capitolo contiene quindi una prima introduzione circa l'evoluzione avvenuta negli ultimi anni relativamente all'utilizzo delle criptovalute e in secondo luogo una trattazione dei rischi e benefici che possono derivare dall'utilizzazione delle monete digitali.

Inoltre, il terzo paragrafo sarà dedicato alle questioni "irrisolte" ossia le criticità e le questioni aperte su cui ancora oggi il dibattito risulta esponenzialmente acceso, sia a livello europeo che mondiale. Tra cui figura anche il possibile esodo dei dati personali degli utenti che utilizzano portafogli di criptovalute. Quindi, sarà necessario analizzare quale sia la giurisprudenza in materia e le criticità che sorgono in materia di protezione dei dati personali.

Infine, per concludere, si è deciso di procedere ad analizzare i futuri possibili eventi che coinvolgeranno il mondo delle criptovalute. In altre parole, si tratterà del futuro delle stesse e dei possibili scenari che si verificheranno nei prossimi anni.

CAPITOLO I

Sommario: 1. La rivoluzione digitale e le criptovalute - 2. Il protocollo Blockchain. Modalità di funzionamento e potenziali utilizzi illeciti - 3. I cripto-asset. Riflessi penali - 4. Ecosistema delle criptovalute, smart contract e loro applicazioni criminali - 4.1 (*Segue*): I *Wallet provider* - 5. Le implicazioni legali e sociologiche della tecnologia blockchain. Cenni al *locus commissi delicti* - 5.1 (*Segue)*: Le implicazioni pratiche della tecnologia blockchain

1. La rivoluzione digitale e le criptovalute

Con la globalizzazione *in primis* e la rivoluzione digitale, in secondo luogo, si è assistito ad un radicale e rapido cambiamento delle abitudini delle persone, sia fisiche che giuridiche. La convergenza delle economie mondiali e l'apertura dei mercati esteri hanno determinato un incremento della necessità di investire sul digitale.[1] Si parla in tal caso di processo di digitalizzazione, processo che ha permesso la crescita e la diffusione di internet e delle innovazioni digitali nonché la creazione e diffusione di nuovi mezzi alternativi di pagamento. Quindi, oggi, si sente parlare spesso di *e-money* ossia moneta elettronica, concetto con il quale si fa riferimento a

> *«qualsiasi valore monetario immagazzinato elettronicamente o magneticamente rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento e accettato da persone fisiche o giuridiche diverse dall'emittente»*.[2]

[1] VALDANI E., BERTOLI G. (2006). *Mercati internazionali e marketing.* 3° edizione, Milano: Egea; pp. 290-292.

[2] Direttiva 2009/110/CE concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la

Si è insediata così una nuova dimensione sempre più virtuale della moneta, la cui diffusione è stata ulteriormente incentivata dal commercio "digitale" sul *web* di beni e servizi, il quale si conclude mediante il pagamento virtuale, ossia senza il trasferimento materiale di risorse finanziarie legate alla consegna del bene/i e/o servizio/i. In altre parole, la circolazione monetaria non viene più regolata dallo scambio materiale del denaro o da titoli di credito ma avviene sulla base di strumenti informatici mediante i quali viene trasferito il denaro da un soggetto all'altro,[3] che costituiscono i punti di forza della moneta elettronica ossia l'immediatezza dei pagamenti, il prelievo di moneta dagli ATM (*Automated Teller Machine*)[4] e la riduzione di costi di transazione favorendone l'utilizzo per pagamenti anche di modesto ammontare.[5]

La moneta elettronica viene definita come la "quarta generazione" dei mezzi di pagamento dopo l'era della moneta legale e di quella bancaria.[6] In un tempo relativamente recente si è assistito ad un'ulteriore svolta: a partire dal 2009, anno in cui è stata creata la criptovaluta denominata Bitcoin, si ebbe un passaggio considerato da molti naturale in un mondo sempre più digitale.[7]

Le criptovalute non rientrano tra le monete elettroniche.[8] Spesso i termini moneta elettronica, moneta digitale, moneta virtuale e criptovaluta vengono usati indifferentemente poiché mezzi di pagamento dematerializzati. Tuttavia, esistono

direttiva 2000/46/CE – Disponibile in oper cource sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32009L0110&from=EL

[3] GATES, M. (2017). *Blockchain: La guida definitiva per conoscere blockchain, bitcoin, criptovalute, contratti smart e il futuro del denaro*. Independently published.

[4] LEMME G. E PELUSO S. (2016). *Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, Rivista di Diritto Bancario, n. 11/2016, p.7 e ss. Disponibile in open source sul sito https://rivista.dirittobancario.it/sites/default/files/pdf_volume/2016_4_.pdf.

[5] GATES, M., *Blockchain: La guida definitiva per conoscere blockchain, bitcoin, criptovalute, contratti smart e il futuro del denaro*. Independently published, cit. 3

[6] LEMME G. E PELUSO S., *Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, cit. 4

[7] TETI A. (2013). *Bitcoin: la criptomoneta del cyberspazio che sfida banche e governi*, Rivista Mondo digitale, n.46, p.3 e ss. Disponibile in open source sul sito https://mondodigitale.aicanet.net/2013-2/articoli/03_Teti.pdf.

[8] COMELLINI S. (2018). *Ecco perchè i Bitcoin e le Criptovalute non sono Moneta Elettronica*. Disponibile in open source sul sito https://www.diritto.it/ecco-perche-i-bitcoin-e-le-criptovalute-non-sono-moneta-elettronica/#:~:text=Inoltre%20i%20soggetti%20che%20emettono,bis%2C%20Testo%20Unico%20Bancario).

significative differenze: se la **moneta elettronica** è una rappresentazione digitalizzata della moneta legale che circola o mediante lo scambio fisico di monete e banconote o mediante trasferimenti elettronici come bonifici, pagamenti bancomat e altre diverse tipologie, la **moneta legale** è la valuta riconosciuta dall'ordinamento giuridico ed emessa e gestita dalla banca centrale nazionale competente (in Italia la Banca d'Italia che si coordina con la Banca Centrale Europea) che regola l'offerta della stessa, monitora il suo andamento nonché quello dell'economia.[9] Invece, la **moneta digitale** è uno strumento di scambio utilizzato in sostituzione di banconote e monete al fine di concludere transazioni sul *web*.[10] Proprio in quest'ultima categoria rientrano le valute virtuali e le criptovalute.[11]

Nel 2012, la BCE (Banca Centrale Europea) ha definito la moneta virtuale come una tipologia di moneta digitale, non regolamentata da alcuna giurisdizione,[12] la quale viene emessa e gestita nonché controllata direttamente dai suoi creatori.[13] Invece, l'EBA (*European Banking Authority*)[14] definisce le monete virtuali come una rappresentazione digitale di valore utilizzata come mezzo di scambio o mezzo di investimento che possono essere trasferite[15] e negoziate in modo elettronico.[16]

---

[9] MORONI P. (2021). *L'inquadramento normativo della moneta virtuale*. Disponibile in open source sul sito https://www.fintastico.com/it/blog/inquadramento-normativo-moneta-virtuale/#:~:text=La%20moneta%20legale%20%C3%A8%20la,come%20tale%20dall'ordinamento%20giuridico.

[10] MANCINI M. (2015). *Valute virtuali e Bitcoin*. Analisi Giuridica dell'Economia, Fascicolo 1, p. 122 e ss. Risorsa digitale disponibile al sito https://www.rivisteweb.it/doi/10.1433/80273. Accesso avvenuto in data 23 marzo 2023.

[11] CAPACCIOLI S. (2020). *Come si pagano le tasse per le criptovalute in Italia*. Cryptpnomist.ch. Disponibile in open source sul sito https://cryptonomist.ch/2020/06/29/come-si-pagano-tasse-criptovalute-italia/.

[12] European Central Bank (2012). *Virtual Currency scheme*. P. 13 e ss.

[13] STEFANI A. (2022). *Euro digitale: presentazione, tempi e prospettive dell'opera della BCE. Pagamenti digitali*. Disponibile in open source sul sito https://www.pagamentidigitali.it/esperti-e-analisti/euro-digitale-presentazione-tempi-e-prospettive-dellopera-della-bce/.

[14] European Banking Authority (2014) EBA Opinion on 'virtual currencies. P. 11 e ss.

[15] Decreto Legislativo 25 maggio 2017, n. 90. Disponibile in open source sul sito https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2017;090

[16] LICATA P. (2019). *L'Autorità bancaria europea chiede di valutare costi e benefici della finanza digitale: potrebbero rendersi necessarie norme a tutela dei consumatori e per scongiurare attività illecite e concorrenza sleale*. Corriere comunicazioni. Disponibile in open source sul sito https://www.corrierecomunicazioni.it/digital-economy/monete-virtuali-leba-apre-alla-regulation-troppi-rischi-per-gli-investitori/.

Con riferimento invece alle criptovalute, uno dei primi utilizzi di tale concetto risale al 1982, con la pubblicazione di un articolo di David Chaum, intitolato "*Blind Signature for Untraceable Payments*"[17], nel quale viene introdotto un nuovo concetto, il concetto di "*firme cieche*", ovvero le "*blind signatures*", una sorta di firma digitalizzata che viene apposta sul messaggio in un momento precedente alla sua apertura e lettura e che può essere applicato per far funzionare un sistema di pagamento anonimo usando la crittografia.[18] Si tratta, quindi, di una modalità facilmente utilizzabile anche nel settore dei pagamenti per garantirne la celerità e soprattutto la sicurezza. Tuttavia, la società fondata dallo stesso David Chaum nel 1990, portatrice delle proprie ideologie in grado di proporre un sistema di pagamenti elettronici per garantire le transizioni economiche veloci, sicure e anonime, fallì poco tempo dopo, nel 1998 a causa di una serie di accordi con banche e società non andati a buon fine.[19]

È evidente che, a partire dagli anni Novanta del Novecento, vi era già un certo interesse in tema di criptovalute. Difatti, tali anni sono stati cruciali per creare le condizioni necessarie per favorire il *boom* delle criptovalute avvenuto a partire dal 2009 con la nascita dei Bitcoin.[20] Più precisamente, il termine blockchain (originariamente *block chain*) fu per la prima volta utilizzato da Satoshi Nakamoto in una stringa di testo nel codice sorgente originale di Bitcoin.[21]

Nakamoto ha spiegato così la sua idea di una moneta virtuale, il Bitcoin, che opera in una rete peer-to-peer in assenza di un'autorità centrale e senza l'emissione di

---

[17] CHAUM D. (1982). *Blind Signature for Untraceable Payments*. Department of Computer Science, University of California. Disponibile in open source sul sito https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF.

[18] COSTANTINO M. (2020). *La storia delle criptovalute dal 1983 al 2007, dai Cypherpunks alle istituzioni*. Disponibile in open source sul sito https://ilcibernetico.it/la-storia-delle-criptovalute-dal-1983-al-2007-dai-cypherpunks-alle-istituzioni/.

[19] HALABURDA H. AND SALVARY M. (2016). *Beyond Bitcoin*, The Economics of Digital currencies, New York. P.111 e ss.

[20] HALABURDA H. AND SALVARY M. (2016). *Beyond Bitcoin*, cit. 20

[21] *I nodi raccolgono le nuove transazioni in un blocco, le inseriscono in un albero di hash e scansionano i valori nonche per fare in modo che l'hash del blocco soddisfi i requisiti di proof-of-work. Quando risolvono il proof-of-work, trasmettono il blocco a tutti e il blocco viene aggiunto alla catena dei blocchi* – Vedi NAKAMOTO S. (1991). *The original Bitcoin source code*. Disponibile in open source sul sito https://github.com/Maguines/Bitcoin-v0.1

monete fisiche (i proprietari hanno solo bisogno di chiavi per dimostrare il possesso).[22] Il 3 gennaio 2009, Nakamoto ha rilasciato il primo software Bitcoin e ha creato il primo blocco della blockchain Bitcoin, noto come "blocco Genesis".

Ad oggi, Bitcoin rimane la prima (e più riuscita) applicazione della tecnologia blockchain. Tuttavia, Bitcoin è stata solo la scintilla che ha innescato la rivoluzione blockchain.

Tra le caratteristiche principali ed innovative che hanno consentito lo sviluppo e la diffusione delle criptovalute ed in primo luogo dei Bitcoin, vi è la decentralizzazione in quanto la creazione dei Bitcoin nonché il suo controllo, a differenza della moneta legale, non avviene da parte di alcuna banca centrale. Il controllo sulle transazioni è eseguito sulla rete da soggetti indipendenti in modo decentralizzato e dislocato; pertanto, non è necessaria la presenza di istituti di credito e/o ente centrale o autorità regolamentari.[23] Da ciò ne consegue che il valore del Bitcoin non verrà influenzato da avvenimenti come crisi politiche e/o economiche, guerre o manovre monetarie in quanto l'elemento determinante è dato dall'incontro della domanda e dell'offerta. La domanda è, naturalmente, oscillante e rispecchia l'interesse dei consumatori e l'offerta, a differenza delle monete legale, viene fissata fin dal principio in quanto non esiste un'autorità o ente centrale che curi l'emissione di tale valuta.[24]

Inoltre, le criptovalute non hanno corso legale in quanto non sono accettati da tutti ma la loro accettazione avviene su base volontaria; ciò significa che a differenza della moneta legale, in caso di rifiuto del creditore l'obbligazione non si potrà considerare estinta.[25]

---

[22] A. M. ANTONOPOULOS (2017). *Mastering Bitcoin – Programming the Open Blockchain*, O'Reilly 1.

[23] CAVICCHIOLI M. (2018). *La decentralizzazione, questa sconosciuta*, www.IlBitcoin.it. Disponibile in open source sul sito https://www.ilbitcoin.news/la-decentralizzazione-questa-sconosciuta/.

[24] CHAN CHU, NADARAJAH E OSTERRIEDER (2017). *A statistical analysis of cryptocurrencies*. In Journal of Risk and Financial Management 10.2, p. 12.

[25] AYOUBI M. (2018). *Dalle radici di Bitcoin alla sua nascita*, www.StayUpgrated.it. Disponibile in open source sul sito https://stayupgrated.wordpress.com/2018/01/16/dalle-radici-di-bitcoin-alla-sua-nascita/.

Le criptovalute garantiscono uno pseudo anonimato. In altre parole, gli istituti di credito oggi procedono all'attività di profilazione dei propri clienti conoscendone la storia del credito, l'indirizzo di residenza o domicilio, il numero di telefono nonché ogni operazione bancaria effettuata. Realtà completamente diversa dalle criptovalute, dove non vi è un'attività di monitoraggio delle finanze dei clienti. Si parla, quindi, di pseudo anonimato poiché le transazioni vengono registrate mediante indirizzi con i quali è estremamente complesso ovvero quasi impossibile risalire all'identità della persona fisica e/o giuridica che ha effettuato l'operazione.[26]

Tra le caratteristiche che hanno garantito la diffusione su larga scala delle criptovalute vi rientrano anche i bassi costi di transazione e la trasparenza delle transazioni stesse. Nonostante le transazioni non avvengano sulla base di commissioni prestabilite, in quanto anche il valore delle transazioni varia in base a determinati fattori (spazio utilizzato dalla transazione, numero di transazioni sulla rete e valore della valuta), con la tecnologia Bitcoin, non essendoci un istituto centrale controllore, le transazioni possono avvenire in tutto il mondo a costi estremamente più bassi rispetto ai comuni circuiti di pagamento.[27] Inoltre, gli scambi vengono annotati in un registro pubblico, la Blockchain, consultabile da tutti; pertanto, viene garantita la trasparenza delle transazioni In tale registro vengono registrati il numero delle transazioni e i saldi associati a ciascun indirizzo, in modo da garantire la trasparenza, la neutralità e la prevedibilità. Inoltre, l'anonimato permane fino al momento in cui non si sceglie di utilizzare un *Exchange* ovvero un servizio soggetto agli obblighi di tipo "*Know Your Customer"*.

A seguito dell'emanazione della quarta Direttiva dell'UE n. 2015/849 relativa alla "*prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento*

[26] LEMME G. E PELUSO S., *Criptomoneta e distacco dalla moneta legale: il caso bitcoin,* cit. 4
[27] PELLIZZARI T. E MORINI M. (2017). *Il boom di Bitcoin non è per tutti.* Il Sole24Ore. Disponibile in open source sul sito https://www.ilsole24ore.com/art/il-boom-bitcoin-non-e-tutti-AEdjw2ID..

europeo e del Consiglio e la direttiva 2006/70/CE della Commissione"[28] del 20 maggio 2015, si prevede che chi offre servizi di compravendita di criptovalute, soggiace all'obbligo di ottenere dai clienti i loro documenti identificativi.

Infine, le transazioni che avvengono mediante i Bitcoin richiedono generalmente pochi minuti, a differenza per esempio dei normali bonifici bancari che possono richiedere anche diversi giorni (cd. giorni di valuta) e le criptovalute non sono duplicabili o falsificabili grazie all'utilizzo di blocchi concatenati tra di loro mediante chiavi crittografiche immodificabili. Ciò garantisce la sicurezza di ciascuna transazione nonché la celerità della stessa.[29]

Per la prima volta nella storia, tutti possono ora effettuare transazioni a livello globale attraverso procedure peer-to-peer crittografate senza l'intermediazione di terzi.[30] Prima dell'avvento della blockchain, era impossibile per un gruppo di individui non correlati in un sistema informatico distribuito confermare, senza affidarsi a un'autorità centrale, che nessuno abbia manomesso i dati.

Quindi, la moneta virtuale paragonata alla moneta legale differisce per una serie di fattori, tra cui il riconoscimento del diritto all'emittente ossia, mentre l'offerta di moneta virtuale è privata e decentralizzata senza la possibilità di modificarne la quantità, le monete legali sono emesse in modo flessibile da istituzioni finanziarie pubbliche. A ciò si aggiunga le variazioni della quantità di unità in circolazione, in quanto la quantità di monete virtuali non può essere cambiata attraverso la politica monetaria da parte delle banche centrali. L'iperinflazione per eccesso di offerta può essere negata per le monete virtuali a causa dell'offerta digressiva del mining.

---

[28] Direttiva UE n.2015/849 relativa alla "*prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione* - Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015L0849&from=IT

[29] LICATA P. (2019). *L'Autorità bancaria europea chiede di valutare costi e benefici della finanza digitale: potrebbero rendersi necessarie norme a tutela dei consumatori e per scongiurare attività illecite e concorrenza sleale*. Corriere comunicazioni. Disponibile in open source sul sito https://www.corrierecomunicazioni.it/digital-economy/monete-virtuali-leba-apre-alla-regulation-troppi-rischi-per-gli-investitori/.

[30] ATZORI M. (2015). *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* Disponibile in open source sul sito http://dx.doi.org/10.2139/ssrn.2709713.

Invece, le monete con corso legale corrono un rischio ridotto di iperinflazione solo in caso di una significativa cattiva gestione politica, e l'iperdeflazione a lungo termine è molto improbabile.[31]

2. Il protocollo Blockchain. Modalità di funzionamento e potenziali utilizzi illeciti.

Il sistema Bitcoin oltre che rappresentare un'innovazione senza precedenti, si fonda su un importante elemento rivoluzionario mai utilizzato in precedenza, ossia l'utilizzo della tecnologia Blockchain. Tale tecnica è stata per la prima volta ideata e descritta nel 1991 da un gruppo di ricercatori al fine di contrassegnare i documenti digitali in modo che non fosse possibile retrodatare o violare i documenti stessi.[32] Tuttavia tale tecnologia è rimasta inutilizzata fino a quando non è stata implementata e quindi riscoperta per la creazione dei Bitcoin, che rappresenta il più noto utilizzo del sistema Blockchain ma ovviamente non l'unico.[33]

Il sistema Blockchain consente la creazione di un grande database decentralizzato, strutturato sulla base di una catena di blocchi tra loro collegati in rete contenenti più transazioni. In altre parole è un libro mastro pubblico, facilmente consultabile sul sito blockchain.info[34], nonché su molti altri, dove è possibile analizzare qualunque aspetto, come ad esempio gli ultimi blocchi aggiunti alla catena, le transazioni in

[31] HE, D. et al. (2018). *Virtual Currencies and Beyond : Initial Considerations* - IMF Staff Discussion Notes 16/3. Disponibile in open source sul sito https://www.imf.org/en/Publications/Staff-DiscussionNotes/Issues/2016/12/31/Virtual-Currencies-and-Beyond-Initial-Considerations-43618

[32] LEWENBERG Y., BACHRACH Y. & SOMPOLINSKY (2015). *Bitcoin Mining Pools: A Cooperative Game Theoretic Analysis*. p. 919 e ss. Disponibile in open source sul sito https://www.avivz.net/pubs/15/fp245-lewenbergA.pdf.

[33] ZAMBON A. (2021). *Blockchain: introduzione e casi d'uso.* Disponibile in open source sul sito https://medium.com/catobistrategy/blockchain-introduzione-e-casi-duso-f88e075c6c50..

[34] Sito ufficiale disponibile su: https://www.blockchain.com/explorer

ciascun blocco e gli indirizzi coinvolti.[35] Essa, inoltre, può rientrare all'interno della categoria delle tecnologie *Distributed Ledger*, DLT, le quali sono definibili come un complesso di sistemi che fanno riferimento a un registro pubblico sui quali è possibile apportare modifiche da parte di più nodi di rete.[36]

Tale sistema, pubblico, trasparente, sicuro, inviolabile, consente di garantire la validità e la certificazione dalla rete di ogni transazione effettuata. Il vero cambiamento si ritrova nel fatto che la Blockchain non è contenuta e quindi, installata in un unico computer ma è distribuita in migliaia di computer sparsi per tutto il globo, i quali contengono tutti lo stesso sistema Blockchain garantendo la stabilità e combattendo ogni tentativo di violazione.

Prima di esaminare la struttura di una transazione su blockchain, è opportuno citare la classificazione comunemente utilizzata dei sistemi blockchain in tre sottocategorie: *i)* blockchain pubblica, chiamata anche blockchain "*permission-less*", in quanto non ci sono restrizioni alla partecipazione. Qualsiasi utente è libero di aderire ed eseguire transazioni sulla blockchain, e il consenso decentralizzato è raggiunto attraverso meccanismi come il mining e il proof-of-work; *ii)* blockchain privata chiamata anche blockchain "*permissioned*", in quanto l'accesso alla rete è controllato e limitato ai membri di una singola organizzazione (o di più organizzazioni sotto lo stesso controllo). L'adesione avviene solo su invito ed è soggetta a un insieme di regole. La differenza con la blockchain pubblica è il grado di decentralizzazione (più centralizzato nelle blockchain private) e l'anonimato; [37] *iii)* la blockchain consortile è un ibrido tra blockchain private e pubbliche. Infatti, non si tratta di una singola organizzazione (come nelle blockchain private), ma di un consorzio di nodi responsabile della convalida dei blocchi. Questi nodi decidono

[35] BELLINI M. (2022). *Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia.* Disponibile in open source sul sito https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/.
[36] GENNAI A. (2018). Investire sulla Blockchain, Sole 24 ore – Plus 24.
[37] PILKINGTON M. (2015). *Blockchain Technology: Principles and Applications*), in Research Handbook on Digital Transformations,, Edward Elgar Publishing

chi può far parte della rete e chi può svolgere attività di mining; soprattutto, un blocco può essere convalidato solo dal consorzio di nodi.[38]

Dal punto di vista pratico la blockchain è semplicemente un database distribuito che registra pezzi di informazioni che sono raggruppate in blocchi e che sono collegate attraverso una procedura crittografica in una catena in continua espansione. In altre parole, la Blockchain si compone di una molteplicità di blocchi di informazioni, i quali sono legati insieme da un sistema crittografico.[39] Le informazioni contenute in ciascun blocco non sono altro che l'insieme delle migliaia di transazioni avvenute negli ultimi dieci minuti. Ogni blocco è preso in carico da un *miner* il quale, mediante l'applicazione di calcoli matematici, consente la validazione della transazione e permette di aggiungere un nuovo blocco alla catena. Tale processo genera un determinato ammontare di Bitcoin che si aggiungeranno all'ammontare mondiale e rappresenteranno la ricompensa del *miner*.

Il mining di Blockchain è per lo più impossibile con un normale desktop e richiede un hardware speciale con una maggiore velocità di calcolo. L'estrazione avviene in due modi. Il primo è il cd. *Mining* individuale in cui ogni minatore imposta l'hardware e si registra per il mining. Quando avvengono nuove transazioni, tutti i minatori della rete Blockchain ricevono un problema matematico. L'hardware dei minatori inizia a lavorare per trovare la soluzione. Il primo minatore che trova la soluzione informa tutti gli altri minatori di averla trovata. Gli altri minatori la verificano per evitare una falsa convalida del blocco. Una volta verificata la soluzione del minatore, questi riceve la ricompensa e le transazioni vengono aggiunte alla Blockchain. Il secondo metodo è il cd. Pool di minatori. A volte, un singolo minatore non dispone di risorse sufficienti per effettuare il mining della Blockchain. In questi casi, un gruppo di minatori si riunisce per formare un *Mining*

[38] PUTHAL D., MALIK N., MOHANTY S., KOUGIANOS E., DAS G. (2018). *Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems*, in IEEE Consumer Electronics Magazine, Vol. 7, Issue 4.

[39] Bitcoin, utilizza l'algoritmo SHA=25626. L'acronimo sta per Secure Hash Algotithm e indica un insieme di cinque diverse funzioni crittografiche di hash sviluppate a partire dal 1993 dalla National Security Agency (NSA).

Pool. [40] Questi minatori uniscono le loro risorse per estrarre la *blockchain* più velocemente. Come nel caso del mining individuale, il pool di minatori riceve il problema e, una volta risolto con successo, ottiene la ricompensa. Questa ricompensa viene divisa tra i minatori a seconda della quantità di risorse che hanno.[41]

Ogni blocco deve contenere una serie di informazioni come i dati contenuti in ciascun blocco, i quali dipendono dalla tipologia di blockchain. Ad esempio, quella utilizzata dai Bitcoin memorizza tutti gli elementi di una transazione quali mittente, destinatario e la quantità dei Bitcoin scambiati. Ciò significa che i dati contenuti e memorizzati all'interno di un blocco dipendono dal tipo di blockchain utilizzata.[42] Oltre ai dati i blocchi contengono un Hash function[43] ossia un'impronta digitale, una rappresentazione di informazioni contenute in un blocco crittografato. Oltre all'Hash function vi è l'Hash del blocco precedente costituente, sostanzialmente, l'elemento che crea la catena tra il blocco precedente e quello successivo. Difatti, tutti i blocchi della catena sono concatenati tra loro mediante un meccanismo di condivisione dell'hash. Per creare un nuovo hash si ha bisogno dei dati della transazione precedente, dell'hash del blocco precedente e di un *nouce* (*number once used*) ossia un numero generato in modo casuale.[44] Se l'hash generato risulterà valido verrà quindi approvato il blocco nella sua interezza, in caso contrario si dovrà generare un nuovo *nonce*. In altre parole, per modificare la Blockchain sarà

[40] BELLINI M. (2018). *Smart Contracts: che cosa sono, come funzionano quali sono gli ambiti applicativi*, www.Blockchain4innovation.it. Disponibile in open source sul sito https://www.blockchain4innovation.it/mercati/legal/smart-contract/blockchain-smart-contracts-cosa-funzionano-quali-gli-ambiti-applicativi/.

[41] HIREMATH O.S. (2023). *Blockchain Mining- All you need to know*, in Edureka. Disponibile in open source sul sito https://www.edureka.co/blog/blockchain-mining/

[42] BELLINI M. (2018). *Osservatorio Blockchain 2018: crescono del 73% i progetti e si afferma un nuovo rapporto con le cryptocurrency*, www.Blockchain 4innovation.it. Disponibile in open source sul sito https://www.blockchain4innovation.it/eventi-e-convegni/osservatorio-blockchain-2018-crescono-del-73-i-progetti-e-si-afferma-un-nuovo-rapporto-con-le-cryptocurrency/.

[43] Funzione matematica dotata delle seguenti qualità: (1) può assumere un input di ogni dimensione; (2) produce un output con dimensioni fisse; (3) irreversibile ossia dall'output non si potrà arrivare all'input quanto l'informazione è già stata criptata. (4) modifiche all'input determinano cambiamenti drastici nell'output.

[44] FLYIP. (2019). *Blockchain: cos'è l'hash function nel protocollo Bitcoin*. Disponibile in open source sul sito https://www.flyip.it/blockchain-cose-hash-function-nel-protocollo-bitcoin/.

necessario modificare nonché procedere al ricalcolo di tutti gli hash che compongono la Blockchain. [45]

Per garantire un elevato livello di sicurezza, la Blockchain utilizza la tecnica chiamata *proof-of-work* (prova di lavoro). La Proof of Work[46], è un protocollo utilizzato da diverse criptovalute - come Bitcoin, Ethereum, Litecoin - al fine di ottenere un'accettazione decentralizzata tra i diversi nodi nel processo di aggiunta di un blocco alla catena.[47] Non è un'attività semplice da svolgere poiché la *proof-of-work* limita la generazione di nuovi blocchi ad uno ogni dieci minuti in media.[48] Riassumendo, la Blockchain è una sistema composto da dati che, in caso di modifica di un blocco precedente della catena, richiede la modifica di tutti i blocchi successivi.

La Blockchain per il suo funzionamento e per garantire l'esistenza dei propri elementi caratteristici necessita di un asset digitale nativo, in quanto senza le rendite di signoraggio associate al suo asset nativo, la Blockchain avrebbe bisogno designare delle figure che si occupino della sua manutenzione, ricadendo così in un paradigma centralizzato e perdendo di conseguenza il suo significato.[49]

Infine, da notare che per effettuare qualsiasi transazione sulla blockchain, gli utenti devono essere in possesso di un portafoglio digitale (paragonabile a un conto corrente bancario) a cui si può accedere solo attraverso un processo crittografico basato su chiavi asimmetriche: una chiave privata, personale per ogni utente e tenuta segreta come una password, e una chiave pubblica, condivisa con tutti gli altri utenti. Per effettuare una transazione, l'acquirente (ovvero il futuro proprietario

[45] BELLINI M. *Smart Contracts: che cosa sono, come funzionano quali sono gli ambiti applicativi*, cit. 40

[46] CAVALLI S. (2018). *Proof of Work vs Proof of Stake*,. Disponibile in open source sul sito https://cryptonomist.ch/2019/10/05/proof-of-work-pow-vs-proof-of-stake-pos-la-guida/.

[47] BANCA D'ITALIA (2019) *Quaderni di Ricerca Giuridica Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale* a cura di Fabrizio Maimeri e Marco Mancini numero 87 della Consulenza Legale. Disponibile in open source sul sito https://www.bancaditalia.it/pubblicazioni/quaderni-giuridici/2019-0087/qrg-87.pdf.

[48] ARCIERI F. (2021). *Che Cos'è Un Algoritmo Di Consenso (Spiegato Facile).* Disponibile in open source sul sito https://checkpointbitcoin.it/algoritmo-di-consenso/.

[49] REDAZIONE (2021). *Asset nativi digitali e soluzioni FinTech*. IVG.it. Disponibile in open source sul sito https://www.ivg.it/2021/11/asset-nativi-digitali-e-soluzioni-fintech/.

dei cripto-asset) invia la sua chiave pubblica al venditore (cioè il proprietario originale dei cripto-asset). Le chiavi private sono invece tenute segrete e utilizzate per firmare digitalmente le transazioni.[50] Quindi, entrambe la chiavi garantiscono la sicurezza della blockchain e significa che se un utente perde la sua chiave privata, perde l'accesso alla sua criptovaluta. Per semplificare il processo, gli utenti spesso utilizzano i portafogli digitali per memorizzare la chiave privata e semplificare le transazioni.

Ad oggi, la tecnologia *blockchain* su cui si basano le criptovalute rappresenta uno strumento importante utilizzato non solo per facilitare lo scambio di monete, ma anche in molti settori, tra cui la sanità e l'istruzione. Tuttavia, come tutte le tecnologie, la *blockchain* è uno strumento e può essere abusato da attori malintenzionati. Difatti, la *blockchain* costituisce una tecnologia imperfetta principalmente per due aspetti: *i)* la giovane età della tecnologia stessa e *ii*) le implicazioni giuridiche che possono derivare dall'utilizzo della stessa. In particolare, si parla di conseguenze che ricadono essenzialmente nell'ambito penale. Come si vedrà anche nel proseguo del presente elaborato, le sfide monetarie, finanziarie ed economiche della *blockchain* sono spesso portate alla ribalta, grazie al notevole successo delle criptovalute; ciò ha determinato, da un lato, il sorgere di nuove "sfaccettature" dei reati di finanziamento del terrorismo e soprattutto del riciclaggio e dall'altro, l'amplificazione di condotte illecite commesse online, come la creazione e l'utilizzo del *dark web.* In altre parole, sebbene la tecnologia *blockchain* prevenga i comportamenti fraudolenti, non è in grado di individuare le frodi da sola[51] in quanto, come analizzato precedentemente, la *blockchain* è una tecnologia che si fonda sulla creazione di blocchi da parte dei *miner* i quali non sono a conoscenza che il denaro, trasferito da un soggetto ad un altro, è frutto di un'attività illecita.

[50] POLCI M. (2013). *Cos'è il bitcoin –seconda parte*, rischiocalcolato.it. Disponibile in open source sul sito http://www.rischiocalcolato.it/2013/12/cose-il-bitcoin-seconda-parte.html.

[51] ACCINNI G. P. (2020). *Cybersecurity e criptovalute. Profili di rilevanza penale dopo la quinta direttiva*. Disponibile in open source sul sito https://www.sistemapenale.it/pdf_contenuti/1589481049_accinni-2020a-cybersecurity-criptovalute-quinta-direttiva-2018-843.pdf

Per questo si è pensato di riconoscere una responsabilità penale nei confronti dei *provider* ossia coloro che gestiscono ovvero utilizzano la struttura decentralizzata di tale tecnologia, i quali prima dei recenti interventi del legislatore europeo nonché italiano, godevano di una certa "immunità" e quindi, erano privi di ogni onere di garanzia e controllo. Come premesso, la tecnologia *blockchain* presenta un altro lato della medaglia ossia l'utilizzo della stessa per indagare sui crimini commessi, sugli schemi di riciclaggio di denaro, raccogliere informazioni e congelare e confiscare beni illeciti. Nonostante si parli di "minacce", gli asset e i servizi crittografici non rappresentano una minaccia intrinseca maggiore rispetto al denaro contante, alle aziende, alle proprietà o persino al sistema commerciale globale, ossia tutti elementi che hanno ancora molte più probabilità di essere utilizzati per riciclare fondi illeciti.

Ciò che la *blockchain* offre sono promettenti opportunità per indagare e smantellare le reti della criminalità organizzata e di recuperare i beni illeciti. Con gli strumenti, le tecniche e i dati adeguati, le forze dell'ordine possono (e lo fanno in molti Paesi) "seguire" i beni illeciti mentre si spostano su una o più *blockchain*. Quindi, la tecnologia *blockchain*, per esempio, presenta l'opportunità di identificare gli individui che si celano dietro lo schema di riciclaggio, spesso perché i criminali stessi commettono errori che rivelano la loro identità; di ampliare le indagini ad altri individui o aziende, potenzialmente rilevanti per scoprire nuove piste e reti di criminalità organizzata; di raccogliere prove di attività illecite da utilizzare in tribunale che, grazie alla natura della *blockchain*, spesso non possono essere distrutte e possono essere conservate, ovvero di confiscare i beni illeciti, anche se i colpevoli non possono essere identificati o si nascondono in una giurisdizione da cui non possono essere estradati.

3. I cripto-asset. Riflessi penali

Come già accennato, la prima applicazione della tecnologia blockchain è stata la pubblicazione di Bitcoin da parte di Satoshi Nakamoto nel 2009.[52] Da allora, decine di criptovalute diverse sono cresciute rapidamente in termini di prezzo e popolarità. Ad oggi, esistono circa 5.392 criptovalute scambiate, con il Bitcoin che rappresenta circa la metà della capitalizzazione di mercato totale.

Le criptovalute sono interamente virtuali, non sono associate ad alcun governo o banca e garantiscono l'anonimato delle parti attraverso procedure di crittografia.

Nonostante non esista una definizione univoca di crypto-asset, esso può essere definito come:

> "*un nuovo tipo di attività registrata in forma digitale e resa possibile dall'uso della crittografia che non è e non intende rappresentare un credito o un debito finanziario di un'entità identificabile. L'emergere dei crypto-asset è stato facilitato dalle tecnologie a registro distribuito (DLT). Una caratteristica distintiva è la mancanza di un credito o debito sottostante, cosa che rende estremamente volatili e speculativi questi asset"*.[53]

Tale definizione di crypto-asset è stata dettata dalla Banca Centrale Europea nel 2019, quando i crypto-asset erano identificati essenzialmente nei Bitcoin. Oggi, i crypto-asset possono essere distinti in due macrocategorie: nativi (esempio le criptovalute) [54] e non nativi (come i token che comprendono però anche le criptovalute)

Entrambi i *crypto-asset* rappresentano codici digitali creati tramite *smart contract* ai quali possono corrispondere diritti o beni esterni alla DLT, quali promesse di

[52] NAKAMOTO S. (2008). *Bitcoin: a peer-to-peer electronic cash system*. Disponibile in open source sul sito https://bitcoin.org/bitcoin.pdf, 2008.
[53] (2020). *Cosa sono i Crypto Asset?* The Liquid Journal. Disponibile in open source sul sito..
[54] UBS (2022). *Che cosa sono gli asset digitali?* inUBS.com. Disponibile in open source sul sito https://www.ubs.com/ch/it/wealth-management/womens-wealth/academy/2022/digital-assets.html#:~:text=Gli%20asset%20digitali%20non%20nativi,all'interno%20della%20blockchain%20stessa.

rendimento o di servizi, monete elettroniche, panieri di beni o, addirittura, opere d'arte.[55] A loro volta i *crypto-asset* sono suddivisibili in quattro tipi[56]: in security (strumenti derivati); ownership (azioni, beni fisici, beni digitali); utility (servizi, voto, community); money (pagamenti, *stablecoin*, CDBC).[57]

Negli ultimi tempi si è assistito ad un incremento dell'interesse nei crypto-asset i quali possono essere utilizzati anche per motivi del tutto speculativi. Alla luce di ciò è sorta la necessità di procedere ad una regolamentazione sul mercato dei crypto-assets mediante l'adozione di un apposito regolamento ossia il MiCAR.[58] Il regolamento MiCA, di cui si parlerà più nello specifico nei successivi capitoli, è diretto a creare una tutela efficace per i consumatori contro i rischi derivanti da investimenti in crypto-attività.[59] Si tratta di un intervento necessario, in quanto ad oggi i consumatori godono di diritti estremamente limitati in materia di protezione o risarcimento.[60]

Le criptovalute hanno scosso l'economia mondiale fin dal loro lancio, in quanto sistema di pagamento sicuro, economico e veloce; le commissioni per il trasferimento di valute virtuali sono infatti molto più basse di quelle imposte dagli operatori di trasferimento di denaro per inviare e ricevere denaro reale.[61]

---

[55] TAGLIAMONTE I. (2021). *Tecnologia blockchain e mercati dei crypto-asset: le opportunità.* L'Eurispes.it. Disponibile in open source sul sito https://www.leurispes.it/tecnologia-blockchain-e-mercati-dei-crypto-asset-le-opportunita/. Accesso avvenuto in data 26 marzo 2023.

[56] POLITECNICO MILANO1863, SCHOOL OF MANAGEMENT IN COLLABORAZIONE CON OSSERVATORI.NET, *Crypto Asset Digital finance, cybersecurity e crypto assets: strategia, normative e evoluzioni dello scenario*, cit. 53

[57] BORSA ITALIANA. GLOSSARIO FINANZIARIO - Crypto-Asset - Disponibile in open source sul sito https://www.borsaitaliana.it/borsa/glossario/crypto-asset.html

[58] PAGLIARI E. (2018). *10 anni di Bitcoin: le principali tappe della storia del re delle criptovalute*, informazione.it. Disponibile in open source sul sito https://www.informazione.it/a/38D70148-2A2E-4248-B1F2-58CBA196FBBD/amp/10-anni-di-Bitcoin-le-principali-tappe-della-storia-del-re-delle-criptovalute

[59] BIENNA M. (2016). *Bitcoin e attacchi hacker: problemi di sicurezza irrisolvibili?* www.money.it.

[60] Comunicato stampa del 30 giugno 2022. Finanza digitale: raggiunto l'accordo sul regolamento europeo sulle cripto-attività (MiCA). Disponibile in open source sul sito https://www.consilium.europa.eu/it/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/.

[61] CHAN C. (2015). *Bitcoin vs Western Union: How Low Fees Are Disrupting the Remittance Industry* Disponibile in open source sul sito https://www.coingecko.com/buzz/bitcoin-vswestern-union-low-fees?locale=it.

I cripto asset sono sempre più utilizzati dai criminali per spostare e riciclare i profitti di vari reati, tra cui droga, frode e riciclaggio di denaro. C'è anche un rischio crescente che i cripto asset vengano sfruttati per raccogliere e spostare fondi per attività terroristiche. I gruppi criminali organizzati possono sfruttare l'intrinseco pseudonimo e la natura decentralizzata delle criptovalute per condurre il riciclaggio di denaro e altri reati legati alla corruzione. I criminali possono, altresì, utilizzare le criptovalute al posto del sistema bancario formale per spostare grandi somme di denaro, il che comporta un rischio potenzialmente minore di essere individuati dalle forze dell'ordine o dalle istituzioni finanziarie tradizionali, che sono tenute a presentare segnalazioni di transazioni sospette. Inoltre, le criptovalute non sono limitate alla criminalità informatica, ma vengono utilizzate per tutti i tipi di reati che comportano la trasmissione di valore monetario. Ciò include il riciclaggio di denaro, l'elusione di sanzioni finanziarie e altri reati legati alla corruzione, come la concussione e l'appropriazione indebita. In particolare, i criminali informatici si stanno rivolgendo sempre più alle criptovalute come forma di valuta preferita, in quanto consentono un movimento istantaneo, liquido e senza confini di fondi utilizzati per acquistare strumenti di hacking, estorcere pagamenti alle organizzazioni e per altri scopi. I crimini informatici si presentano in molte forme, che rispecchiano la diversità dei crimini che si verificano nel mondo reale e non cibernetico. I reati del mondo reale, come il furto, lo stalking, le molestie, lo spionaggio, il traffico di stupefacenti e altri ancora, hanno una loro natura. Gli stessi reati hanno degli equivalenti informatici. Altri crimini informatici sono unici dell'era digitale e del mondo virtuale, come l'inserimento di una linea di codice dannosa o di un virus di rete per consentire il furto di documenti o di denaro, ad esempio. Il desiderio di chiarire che cosa sia o non sia il crimine informatico ha portato diversi ricercatori a proporre diverse tassonomie dei tipi di crimine informatico. Tuttavia, nel contesto delle criptovalute esse possono costituire lo strumento del reato informatico, il prezzo, il prodotto o profitto dello stesso. In particolare, le criptovalute costituiscono lo strumento di attività di *cyber self-laundering*, riconducibili alla fattispecie di cui all’art. 648-ter.1 c.p. (autoriciclaggio), volta a smaterializzare i proventi di un reato. Le criptovalute nei *cybercrime* possono essere anche il prezzo derivante dalla commissione di

un’attività illecita, come la vendita di un bene illecito, oppure il prodotto o il profitto nel caso in cui per la commissione di un’attività criminale l’attore venga ripagato mediante criptovalute oppure il profitto dell’attore a seguito della commissione di un reato sono per esempio le criptovalute depositate su un dato portafoglio.

Oltre al *cyberlaundering* di cui parleremo in seguito, anche l’estorsione tramite *ransomware* (art. 629 c.p.) rappresenta un reato informatico in cui avviene lo scambio tra ciò che è stato “preso in ostaggio” dall’attore e un ammontare di criptovalute che la vittima dovrà pagare.

L’evoluzione normativa può svolgere un ruolo importante nel mitigare i rischi associati all'uso criminale delle criptovalute. Le azioni pertinenti comprendono il coordinamento dello sviluppo e dell'attuazione di quadri normativi e legislativi, l'educazione del pubblico sui rischi dell'uso delle criptovalute e il rafforzamento della capacità delle forze dell'ordine di smantellare le reti criminali. Tuttavia, le risorse spese per arginare la corruzione legata alle criptovalute comportano un esame costo-opportunità. I legislatori dovranno stabilire se le stesse risorse sarebbero meglio impiegate per migliorare le tradizionali pratiche di applicazione della legge o per altre priorità di sviluppo. Si tratta di una considerazione pertinente, dato che, sebbene l'uso delle criptovalute nelle attività criminali sia in aumento, le transazioni in criptovaluta legate alle attività criminali rappresentano solo una quota limitata dell'economia criminale rispetto al denaro contante.

4. Ecosistema delle criptovalute, smart contract e loro applicazioni criminali

L’anno 2008 ha introdotto un intervento importante e rivoluzionario nel mondo della tecnologia con la blockchain. Satoshi Nakamoto ha gettato le basi di un sistema di denaro elettronico *peer-to-peer*, aprendo così la strada a molte applicazioni rivoluzionarie della blockchain in diversi settori. Mentre nei primi anni l’attenzione della blockchain si concentrava in gran parte sulle applicazioni di criptovaluta, si è lentamente evoluta verso catene programmabili che possono

essere adattate a vari casi d'uso.[62] Di conseguenza, negli ultimi anni abbiamo assistito a una crescita esponenziale dell'ecosistema blockchain. Tuttavia, è importante comprendere l'ecosistema e il valore che offre alla blockchain come nuova tecnologia emergente. Quanto discusso qui di seguito aiuta a scoprire l'importanza dell'ecosistema blockchain e contiene una breve panoramica dei componenti significativi dell'ecosistema.[63]

Le criptovalute fanno parte di un ecosistema più ampio, il quale comprende non solo le valute digitali stesse ma anche le *blockchain* su cui le stesse valute digitali sono costruite e tutte le infrastrutture necessarie per favorire l'attività di *mining* e la conservazione.[64]In altre parole, l'ecosistema crittografico si riferisce a una rete di processi e funzioni legati alla crittografia. Gli sviluppatori di blockchain, i minatori e gli *stacker*, gli scambi di criptovalute e gli investitori istituzionali e al dettaglio costituiscono l'ecosistema cripto.[65]

In aggiunta a quanto sopra esposto, l'ecosistema comprende ulteriori elementi, come gli *exchange* in cui vengono scambiate le criptovalute; gli strumenti/applicazioni costituiti sulle *blockchain*; una moltitudine di strumenti di conformità, gestione del rischio e sicurezza progettati per aumentare i livelli di affidabilità nel mercato delle criptovalute, che ha una regolamentazione scarsa o inesistente e gli investitori di venture capital nonchè le offerte iniziali di valute che finanziano gran parte di questo universo. [66]

---

[62] UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II ET AL. (2020). *Reasearch project – L'ecosistema italiano della blockchain.* Disponibile in open source sul sito https://d110erj175o600.cloudfront.net/wp-content/uploads/2020/09/Report.-LEcosistema-Italiano-della-Blockchain.-Drivers-use-cases-e-implicazioni.pdf

[63] NAZIONALE (2022). *L'ecosistema delle criptovalute può trarre vantaggio dagli interessi di Wall Street?* Altarimini.it. Disponibile in open source sul sito https://www.altarimini.it/News156915-lecosistema-delle-criptovalute-puo-trarre-vantaggio-dagli-interessi-di-wall-street.php

[64] PGIM (2022). *L'investimento in criptovalute*. Disponibile in open source sul sito https://insights.pgim.com/pdf/PGIM-Megatrends-Cryptocurrency-Investing-Whitepaper-Italian-0622.pdf

[65] NARULA, N. (2016). *Il futuro del denaro,* Paper presentato alla conferenza internazionale TEDx di Parigi. Disponibile in open source sul sito https://www.ted.com/talks/neha_narula_the_future_of_money?language=it .

[66] SOLDAVINI, P. (2016). *Il futuro della finanza in una BlockChain* in Il sole 24 ore. Disponibile in open source sul sito http://nova.ilsole24ore.com/frontiere/il-futuro-della-finanzain-una-blockchain/ .

Spesso, gli investitori potrebbero trovare proprio all'interno dell'ecosistema maggiori e migliori opportunità piuttosto che nelle criptovalute stesse. Infatti, sebbene gli elementi dell'ecosistema sopra descritti siano fondamentali ne costituiscono solo una parte. Non meno rilevanti sono gli *smart contract*, i quali consistono, essenzialmente, in un accordo la cui esecuzione è automatizzata, ossia vi sono programmi informatici che eseguono automaticamente i termini concordati nel contratto, il quale si perfeziona quando vengono soddisfatte determinate condizioni.[67] Questo programma controlla gli oggetti fisici o digitali necessari per l'esecuzione. Con l'uso dei contratti intelligenti lo scambio di informazioni è rapido e può anche eliminare le intermediazioni in un processo che allungherebbe i tempi di esecuzione di un compito in un processo più ampio. Registra le transazioni in ordine lineare e cronologico e crea un insieme immutabile di registrazioni a prova di manomissione.[68] Ciò che differenzia gli *smart contract* dai contratti tradizionali è il fatto che l'intervento umano nella fase di esecuzione è minimo o nullo, in quanto il processo è gestito automaticamente da un algoritmo come programmi informatici piuttosto che come contratti in senso stretto. I contratti intelligenti operano su una blockchain, garantendo così, come abbiamo già visto, la decentralizzazione.

Gli *smart contract* possono trovare applicazione in tutte le transazioni che hanno per oggetto qualsiasi attivo digitale, compresi i *token* digitali ossia i titoli. Tuttavia, le blockchain e i contratti intelligenti non possono accedere a dati all'esterno della loro rete. Questa mancanza di accesso esterno può sollevare problemi significativi se si considera che, per funzionare correttamente, uno *smart contract* spesso ha bisogno di accesso alle informazioni esterne rilevanti per l'accordo contrattuale.[69] I contratti intelligenti hanno molti usi vantaggiosi, tra cui la realizzazione di una ricca varietà di nuovi strumenti finanziari. Poiché i contratti sono auto-applicativi, essi eliminano la necessità di intermediari fidati o di sistemi di reputazione per ridurre il rischio transazionale. I contratti smart offrono alcuni vantaggi rispetto alle

[67] S. VOSHMGIR, Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy, BlockchainHub Berlin (2019).
[68] GEEKSFORGEEKS (2022). *What is Blockchain Ecosystem?* Disponibile in open source sul sito https://www.geeksforgeeks.org/what-is-blockchain-ecosystem/
[69] VOSHMGIR S. (2019). *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy*, BlockchainHub Berlin.

criptovalute tradizionali come il Bitcoin, in quanto possono consentire uno scambio equo tra parti reciprocamente diffidenti con regole contrattuali ricche ed esprimibili in una logica programmabile. Questa caratteristica impedisce alle parti di modificare o eliminare un protocollo di scambio, ed elimina la necessità di intermediari terzi (potenzialmente truffaldini). Inoltre, gli *smart contract* minimizzano l'interazione tra le parti, riducendo le opportunità di monitoraggio e tracciamento indesiderati. A partire da Ethereum, molte *blockchain* moderne sono state lanciate con la capacità di eseguire contratti intelligenti. I contratti intelligenti ampliano notevolmente le capacità della tecnologia blockchain e introducono un nuovo gruppo in un ecosistema blockchain ossia i progetti costruiti su quella blockchain.[70]

La blockchain Ethereum, rilasciata nel 2015, è stata costruita come la prima piattaforma blockchain in grado di consentire la costituzione degli *smart contract*. Oggi consente inoltre di gestire il finanziamento, il commercio, i servizi di approvvigionamento, di garanzie e non solo.[71] In un sistema completamente distribuito come Ethereum, i contratti intelligenti, quindi, consentono uno scambio equo e generale (scambi atomici) senza l'intervento di una terza parte fidata, e quindi possono garantire efficacemente il pagamento per i dati o i servizi forniti con successo. Data la flessibilità di questi sistemi di contratti intelligenti, è prevedibile che essi stimoleranno non solo nuovi servizi vantaggiosi, ma anche nuove forme di criminalità. Ci riferiamo ai contratti intelligenti che facilitano i crimini nei sistemi di *smart contract* distribuiti come contratti intelligenti criminali (CSC). Un esempio di CSC è uno *smart contract* per il furto di chiavi (private). Pertanto, nonostante i loro vantaggi, hanno un lato oscuro, in quanto sono potenzialmente in grado di facilitare la criminalità, grazie ad un'interazione ridotta al minimo che rende le attività illegali più difficili da monitorare per le forze dell'ordine. In alcuni casi, un criminale può impostare un contratto e, senza ulteriori interazioni, può eseguirlo autonomamente. Le transazioni con uno stato esterno ampliano l'ambito dei

[70] ETHEREUM (2022). *Cos'è un contratto intelligente?* Disponibile in open source sul sito https://ethereum.org/it/developers/docs/smart-contracts/#:~:text=I%20contratti%20intelligenti%20sono%20un,rete%20ed%20eseguiti%20come%20programmato.

[71] PGIM, *L'investimento in criptovalute,* cit. 64

possibili CSC, i quali, ad esempio, possono essere commessi al fine di commettere crimini fisici, ovvero nella realtà (terrorismo, incendio doloso, omicidio, ecc.). Poiché i sistemi decentralizzati di *smart contract* ereditano tipicamente l'anonimato di Bitcoin, offrono una totale segretezza per le attività criminali. In generale, pertanto, c'è il rischio che le capacità abilitate dai sistemi decentralizzati di s*mart contract* permettano di creare nuovi ecosistemi e comunità sotterranee. Quindi, un ecosistema non solo comprende una serie di opportunità ma si riferisce fondamentalmente a una rete di partecipanti con obiettivi, relazioni e processi aziendali condivisi. La rete è in grado di creare e trasferire valore commerciale in modo efficiente. Allo stesso tempo, è importante notare che la blockchain è in realtà un'alleanza complicata che coinvolge diversi attori con obiettivi condivisi. Tuttavia, i diversi attori, di cui parleremo in seguito, hanno prospettive diverse sul raggiungimento degli obiettivi desiderati.[72] I singoli partecipanti all'ecosistema potrebbero avere diversi modelli di business con contributi distinti all'ecosistema. Non è una sorpresa se si scopre che alcuni dei partecipanti all'ecosistema sono concorrenti. Pertanto, la scelta di un modello per i progetti blockchain condivisi dipende da chi deve partecipare alla rete per ottenere la migliore efficacia. D'altra parte, le idee emergenti per l'ecosistema blockchain aiutano anche nell'evoluzione del modello iniziale in altri modelli.[73]

Qui di seguito, alcuni dei principali modelli di collaborazione utilizzati finora per gli ecosistemi blockchain: *i)* **Ecosistema con un solo leader**, in questo caso l'azienda è stata in grado di sviluppare un ecosistema composto da diversi soggetti interessati all'industria della pesca. L'obiettivo principale dell'ecosistema è migliorare la tracciabilità del tonno a pinne gialle dall'oceano alle tavole. I diversi attori dell'ecosistema ittico, tra cui i pescatori, i confezionatori, il personale addetto al trasporto, i distributori e i rivenditori, potrebbero registrare i dettagli sulle reti blockchain. Le informazioni inserite da tutti i partecipanti possono essere disponibili per il cliente con un codice QR. Di conseguenza, può migliorare la

[72] GERONI D. (2021). *Blockchain Ecosystem* Explained. Blockchains.com. Disponibile in open source sul sito https://101blockchains.com/blockchain-ecosystem/

[73] DALY L., *What is a Blockchain Ecosystem? Blockchains are like snowflakes: each one is unique*, cit. 69

fiducia degli acquirenti nel marchio e nel cibo che portano in tavola.;[74]*ii)* **Ecosistemi di joint venture o consorzi** sono esempi di costruzione di ecosistemi con due o più organizzazioni o governi che acquisiscono il controllo. Il modello di consorzio per lo sviluppo di ecosistemi blockchain ha preso il sopravvento sulle joint venture formali. Tuttavia, le imprese devono affrontare un problema notevole quando pensano ad associazioni commerciali strategiche negli ecosistemi blockchain. I partecipanti devono decidere se formare una nuova entità legale per l'associazione o se continuare con accordi contrattuali formali. Alcuni dei fattori importanti che potrebbero definire questa decisione sono i requisiti fiscali, normativi e di finanziamento;[75] *iii)* l'ultima variante di ecosistemi blockchain, i cd. **Ecosistemi blockchain normativi**, si concentrerebbe su progetti condivisi tra agenzie governative che devono auto dichiarare la propria conformità. L'esempio di un progetto condiviso da *Marine Transport International* e dalla *Recycling Association* in Gran Bretagna illustra un ecosistema blockchain normativo. Entrambe le parti mirano a sfruttare uno strumento basato su blockchain per raccogliere dati e soddisfare i requisiti di conformità per la spedizione di rifiuti riciclabili.[76]

Dal punto di vista dei partecipanti e del loro ruolo all'interno dell'ecosistema delle criptovalute, ogni partecipante ha un ruolo specifico nell'ecosistema, con contributi di dati e risorse necessari agli altri partecipanti. Inoltre, l'identificazione dei componenti dell'ecosistema blockchain e dei modi in cui interagiscono tra loro è essenziale per pianificare lo sviluppo dell'ecosistema. Nel documento redatto dalla BCE "*Virtual Currency Scheme - a further analysis*"[77] del 2015 vengono individuati i principali attori e i rispettivi ruoli che essi assumono all'interno

[74] CNBCTV18.com (2022). *Explained | What is a blockchain ecosystem?* Disponibile in open source sul sito https://www.cnbctv18.com/cryptocurrency/explained--what-is-a-blockchain-ecosystem-12587582.htm

[75] CULICCHI R. (2022). *Blockchain e banche d'affari, un rapporto che cresce: ecco i progetti.* Disponibile in open source sul sito https://www.agendadigitale.eu/documenti/blockchain-e-banche-daffari-un-rapporto-che-cresce-ecco-i-progetti/

[76] CNBCTV18.com, *Explained | What is a blockchain ecosystem,* cit. 73

[77] EUROPEAN CENTRAL BANK (2015). *Virtual currency schemes – a further analysis*, Disponibile in open source sul sito https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

dell'ecosistema delle criptovalute. In primo luogo, figurano gli investitori/creatori che sono coloro che generano le valute virtuali e ne sviluppano tecnicamente parte della sua rete. Possono essere persone fisiche o persone giuridiche ed inoltre, possono decidere se essere organizzazioni pubbliche ovvero mantenere la propria identità nascosta. A seguire, vi sono gli emittenti ossia coloro che creano le valute virtuali e ricomprende, a volte, anche coloro che gestiscono il sistema e stabiliscono le regole di utilizzo. Diversamente, nei sistemi decentralizzati, come quello Bitcoin, non vi è tale unica figura ma la creazione delle monete viene realizzata dai *miner* in modo autonomo in base alle loro disponibilità e capacità. In terzo luogo, quali attori all'interno dell'ecosistema delle criptovalute figurano i *miners* i quali, come accennato precedentemente, sono soggetti, spesso facenti parte di un gruppo, che sono necessari per verificare e validare un blocco al fine di aggiungerlo nel registro transazioni avvenute, la *blockchain.* Il loro ruolo è fondamentale nei sistemi decentralizzati in quanto garantiscono la sicurezza delle transazioni. La loro ricompensa avviene mediante la corresponsione di uno specifico ammontare di valute virtuali.[78] Inoltre, nell'ecosistema vi sono i Processing service provider ossia un fornitore di servizi di pagamento (PSP), solitamente una società terza che assiste le imprese nell'accettazione di pagamenti elettronici, come quelli effettuati con carte di credito e carte di debito. I PSP fungono da intermediari tra coloro che effettuano i pagamenti, cioè i consumatori, e coloro che li accettano, cioè i rivenditori. Svolgono un ruolo diretto a facilitare il trasferimento delle valute e spesso tale ruolo viene in parte ricoperto dai *miners*.

Ovviamente, all'interno dell'ecosistema non possono mancare gli utenti ossia coloro che vogliono ottenere un ammontare di valute virtuali al fine di acquisire beni o servizi, per scambiare denaro con altri utenti, o procedere al pagamento di un altro utente per fini di investimento,[79] nonché i *Wallet providers*, di cui

[78] CIRAOLO F. E LA ROSA E. (2022). *Contrasto alle frodi e alle falsificazioni dei mezzi di pagamento diversi dai contanti. Brevi note intorno al d. lgs. n. 184/21 (con focus sulle valute virtuali).* DB non solo diritto bancario. Disponibile in open source sul sito https://www.dirittobancario.it/art/contrasto-alle-frodi-e-alle-falsificazioni-dei-mezzi-di-pagamento-diversi-dai-contanti-brevi-note-intorno-al-d-lgs-n-184-21-con-focus-sulle-valute-virtuali/.

[79] I *digital wallet* sono suddivisi in due macrocategorie: gli *hot wallet*, che possono consentire all'utente di effettuare transazioni semplicemente usando un'applicazione collegata ad internet; i

parleremo meglio nel prossimo paragrafo, che sono coloro che offrono un servizio che prende il nome di *digital wallet*,[80] il quale è fondamentale per mantenere le chiavi delle valute digitali e i codici delle transazioni e consentono di verificare le transazioni effettuate.

Infine, l'ecosistema delle criptovalute viene completato dagli *Exchages*/scambia valute che offrono servizi di *trading* online e conversione delle valute virtuali e dalle piattaforme di trading ossia piattaforme che hanno una funzione di "mercato" che consente a compratori e venditori di acquistare ovvero vendere valute virtuali su una piattaforma che raccoglie domanda e offerta. [81]

Inoltre, l'ecosistema delle criptovalute si compone oltre che dai soggetti sopra descritti anche da elementi logici tra i quali figura per esempio l'applicazione del nodo ossia una particolare applicazione internet che ogni computer connesso deve scaricare per partecipare a un ecosistema blockchain;[82] il libro mastro distribuito secondo componente logico; l'algoritmo di consenso, implementato come parte dell'applicazione del nodo nell'ecosistema blockchain[83] ed infine, costituisce elemento logico, anche la macchina virtuale ossia la rappresentazione dell'ambiente informatico creata da un programma informatico e gestita con istruzioni programmate in un linguaggio. [84] L'implementazione della macchina virtuale avviene insieme all'applicazione del nodo. Ad esempio, nell'ecosistema della blockchain Ethereum, l'EVM risiede all'interno dell'applicazione del nodo. [85]

---

cold wallet, che consentono di conservare le valute digitali in un luogo protetto e non collegato alla rete. – Vedi EUROPEAN CENTRAL BANK, *Virtual currency schemes – a further analysis*, cit. 76

[80] CIRAOLO F. E LA ROSA E., *Contrasto alle frodi e alle falsificazioni dei mezzi di pagamento diversi dai contanti. Brevi note intorno al d. lgs. n. 184/21 (con focus sulle valute virtuali)*, cit. 77

[81] GEEKSFORGEEKS, *What is Blockchain Ecosystem?* Cit. 67

[82] Dopo l'installazione dell'applicazione del nodo, un utente diventa un partecipante alla rete blockchain. Una volta installata l'applicazione del nodo, l'utente può partecipare all'ecosistema.

[83] Essi forniscono le regole del gioco per il modo in cui l'ecosistema arriverà alla visione unica del libro mastro. Ecosistemi diversi hanno modi diversi di ottenere il consenso. Esistono diversi algoritmi di consenso e ogni metodo qualifica i nodi come sicuri a modo loro prima di partecipare al processo di costruzione del consenso.

[84] Cit. 67

[85] GEEKSFORGEEKS, *What is Blockchain Ecosystem?* Cit. 67

4.1. (*Segue*): I *wallet provider*

Come accennato in precedenza, la custodia di attività in criptovalute non garantite avviene tramite portafogli che possono essere diversi per concezione e funzionamento, con implicazioni per la sicurezza e i rischi.

Un portafoglio di criptovalute (*cryptocurrency wallet*) è un software o un hardware che consente agli utenti di conservare e utilizzare le criptovalute. Un portafoglio di criptovalute offre agli utenti un modo per convalidare il saldo del conto e fornire visibilità sulla quantità di criptovalute possedute e consente, altresì, di inviare e ricevere transazioni in criptovalute. Per molti utenti, un portafoglio di criptovalute è il meccanismo principale per gestirne i saldi.[86]

Difatti, i portafogli suddetti svolgono un ruolo fondamentale per consentire agli asset e alle criptovalute di essere funzionalmente utili per gli individui e le organizzazioni, ed in particolare i portafogli di criptovalute sono necessari per diversi aspetti cruciali come per[87]la gestione delle stesse criptovalute in quanto offrono agli utenti la possibilità di monitorare il saldo delle attività svolte in moneta virtuale. In secondo luogo, sono necessari per effettuare transazioni. L'invio e la ricezione di pagamenti in criptovaluta sono una caratteristica importante dei portafogli suddetti. Mediante l'utilizzo dei portafogli digitali viene facilitata non solo la connessione alle app decentralizzate (dApp) ma essi consentono anche di effettuare transazioni con un nome utente che può essere associato a un indirizzo di chiave pubblica su una blockchain. Consentono, altresì, la gestione delle chiavi di

[86] GARAVAGLIA R. (2018). *Valute virtuali, wallet provider, exchange platform: cosa cambia con la quinta direttiva antiriciclaggio e cosa ancora deve cambiare*. Disponibile in open source sul sito https://www.blockchain4innovation.it/criptovalute/valute-virtuali-wallet-provider-exchange-platform-cosa-cambia-con-la-quinta-direttiva-antiriciclaggio-e-cosa-ancora-deve-cambiare/

[87] PAYTM (2023). *Different Types of Digital Wallets – A Comprehensive Guide!* Disponibile in open source sul sito https://paytm.com/blog/payments/mobile-wallet/types-of-digital-wallets/

crittografia private utilizzate per accedere a un determinato indirizzo e consentire una transazione.[88]

La blockchain funziona con un modello di infrastruttura a chiave pubblica per la crittografia.[89] Una chiave pubblica e una chiave privata devono essere conosciute solo dagli utenti che possiedono un determinato asset o criptovaluta. Entrambe le chiavi sono necessarie per accedere e trasferire criptovalute. I portafogli di criptovalute contengono la chiave privata e le informazioni dell'utente, mentre le chiavi pubbliche si trovano sulla blockchain. Grazie alla combinazione di chiavi pubbliche e private, un portafoglio di criptovalute può consentire un'operazione sicura per convalidare un saldo e inviare o ricevere transazioni di criptovalute.[90]

In termini di custodia, un portafoglio può essere gestito direttamente dagli utenti stessi o delegato a un custode terzo (cioè un "fornitore di portafogli"), che spesso è una borsa di cripto valori, ma può anche essere un fornitore di servizi di terze parti non *exchange*.[91] In altre parole, il fornitore di portafogli può essere facilmente definito come qualsiasi persona fisica o giuridica che fornisce servizi di protezione di chiavi crittografiche private per conto dei propri clienti per il possesso, la conservazione e il trasferimento di valute virtuali. [92]

Quando le chiavi private sono ospitate da un fornitore di portafogli di terze parti, viene reintrodotta la centralizzazione e gli utenti non hanno più il controllo dei loro cripto valori e, sebbene i rischi di "perdere" un portafoglio siano ridotti, possono aumentare i rischi di cyberattacchi, di condivisione dei dati e di blocco delle transazioni o dei conti.[93]

---

[88] STEFANI A. (2022). *Wallet digitali per criptovalute: caratteristiche principali, tipi e utilizzo*. Disponibile in open source sul sito https://www.pagamentidigitali.it/blockchain-dlt/wallet-digitali-per-criptovalute-caratteristiche-principali-tipi-e-utilizzo/

[89] STEFANI A., *Wallet digitali per criptovalute: caratteristiche principali, tipi e utilizzo*, cit. 85

[90] PAYTM, *Different Types of Digital Wallets – A Comprehensive Guide!* cit. 84

[91] WORLDLINE (2022). *Cosa sono i wallet e perché entreranno nel tuo portafoglio elettronico*. Disponibile in open source sul sito https://www.worldlineitalia.it/wallet-e-portafoglio-elettronico/

[92] CIRAOLO F. E LA ROSA E., *Contrasto alle frodi e alle falsificazioni dei mezzi di pagamento diversi dai contanti. Brevi note intorno al d. lgs. n. 184/21 (con focus sulle valute virtuali)*, cit. 77

[93] FINTASTICO (2022). *Digital wallet: cosa sono e perché prima o poi ne avrai uno*. Disponibile in open source sul sito https://www.fintastico.com/it/blog/digital-wallet-cosa-sono-e-perche-prima-o-poi-ne-avrai-uno/

Gli utenti dei portafogli di criptovalute possono scegliere non solo il servizio o il fornitore che fornisce un portafoglio di criptovalute, ma anche l'approccio di distribuzione. Esistono due tipi principali di portafogli di criptovalute: i portafogli a caldo, generalmente sempre accesi e connessi a Internet e i portafogli a freddo, tipicamente disconnessi che si collegano online solo quando necessario.[94]

Nella categoria dei portafogli freddi si distinguono due tipi principali[95]: i portafogli hardware e i portafogli di carta.

Con un portafoglio di criptovalute basato su hardware, la chiave privata del saldo di criptovaluta dell'utente è memorizzata su un supporto fisico, in genere un'unità USB. Trattandosi di un dispositivo protetto che non è sempre connesso, il portafoglio hardware garantisce una forma di isolamento quando l'utente estrae la chiave. [96]Invece, il portafoglio cartaceo è una soluzione a bassa tecnologia, in cui l'utente scrive le informazioni sulla chiave pubblica e privata su un pezzo di carta.[97]

All'interno della categoria dei portafogli caldi si trovano tre tipi: *i)* i portafogli online (*web*) che forse rappresentano la forma più comune e diffusa di portafoglio di criptovalute che si trova nei servizi online. Con un portafoglio online, un servizio online come una borsa di criptovalute detiene le chiavi pubbliche e private dell'utente. Gli utenti accedono al portafoglio collegandosi al servizio online; *ii) i p*ortafogli desktop, grazie ai quali le chiavi crittografiche sono memorizzate in un'applicazione sul sistema desktop dell'utente e *iii)* i portafogli mobili che sono un'applicazione mobile la quale può essere utilizzata per memorizzare le chiavi pubbliche e private dell'utente, utili per accedere e utilizzare le criptovalute.[98]

I portafogli desktop sono programmi che vengono installati e utilizzati su un computer, mediante le applicazioni mobili. In particolare, i portafogli desktop sono

[94] TESONE C. (2022). *Wallet digitale per criptovalute* in Fiscomania.com. Disponibile in open source sul sito https://fiscomania.com/wallet-digitale-criptovalute/
[95] BINANCE ACADEMY (2019). *What Is a Crypto Wallet?* Disponibile in open source sul sito https://academy.binance.com/en/articles/crypto-wallet-types-explained
[96] BIT2ME ACADEMY (2019). *Cosa sono i cold wallet*? Disponibile in open source sul sito https://academy.bit2me.com/it/que-son-cold-wallets/
[97] BIT2ME ACADEMY, *Cosa sono i cold wallet*? Cit. 93.
[98] BIT2ME ACADEMY (2020). *Cosa sono gli hot wallet*? Disponibile in open source sul sito https://academy.bit2me.com/it/que-son-hot-wallets/

software che vengono scaricati e installati su un computer.[99] Di solito danno all'utente il controllo completo delle chiavi e dei fondi. Inoltre, i dati sensibili, come le chiavi, sono memorizzati in file locali sul dispositivo e sono in genere crittografati. Pertanto, è fondamentale eseguire il backup dei portafogli in caso di perdita o danneggiamento.[100]

I portafogli mobili sono simili ai portafogli desktop. Vengono installati sotto forma di app su un dispositivo mobile e danno la gestione delle chiavi all'utente. Dal momento che i guasti ai dispositivi mobili, il furto o lo smarrimento e le violazioni della sicurezza sono comuni, è essenziale eseguire regolarmente il backup dell'applicazione. A seconda dell'applicazione utilizzata, il backup viene memorizzato sul dispositivo o trasferito su un server cloud.[101]

I portafogli web sono spesso considerati il tipo di portafoglio meno sicuro poiché sono di proprietà di fornitori terzi, che sono responsabili dell'archiviazione. Tuttavia, un vantaggio per l'utente è rappresentato dal fatto che non richiedono l'installazione e quindi possono essere accessibili da qualsiasi luogo. Inoltre, non possono essere persi e possono essere ripristinati rapidamente.[102]

La differenza tra le tecnologie dei portafogli freddi e caldi è minima. Un portafoglio caldo diventa freddo quando viene disconnesso dalla rete e viceversa. A ciò si aggiunga che l'uso di portafogli caldi e freddi per conservare le chiavi private può comportare una serie di rischi: per esempio i portafogli caldi possono essere soggetti a hacking, in particolare nel caso di portafogli di deposito gestiti da fornitori di servizi terzi. È probabile che questi portafogli conservino le chiavi private di molti clienti e, pertanto, costituiscano un interessante obiettivo per gli hacker. Quindi, i

---

[99] RIZZI F. (2022). *Cosa sono i portafogli di criptovalute: hot wallet vs cold wallet* in Rankia. Disponibile in open source sul sito https://rankia.it/criptovalute/cosa-sono-i-portafogli-di-criptovaluta-caldi-e-freddi-vantaggi-e-svantaggi/

[100] OSSERVATORIO MOBILE PAYMENT & COMMERCE (2014). *Mobile Wallet War: chi vincerà la sfida?* Milano: Osservatori ICT & Management - School of Management del Politecnico di Milano.

[101] SMART CARD ALLIANCE (2007). *Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure*. Disponibile in open source sul sito http://www.smartcardalliance.org/resources/lib/Proximity_Mobile_Payments_20070 9.pdf

[102] CHIAP, R. B. (2019). *Blockchain, tecnolgia e applicazione per il business*. In R. B. Chiap, Blockchain, tecnolgia e applicazione per il business (p. 115). Hoepli.

portafogli caldi potrebbero essere soggetti a maggiori rischi operativi, in quanto il titolare del token si affida ai sistemi e ai controlli di una terza parte.[103] Invece, per i portafogli a freddo, i rischi di perdita o danneggiamento fisico del portafoglio sono maggiori, ma i rischi informatici sono eliminati fino a quando l'utente non ha bisogno di usare il portafoglio e quindi cambia il suo stato da freddo a caldo.[104]

Inoltre, i portafogli possono essere distinti tra portafogli custodiali e non custodiali. La differenza fondamentale tra portafogli custodiali e non custodiali è il controllo. Quando i portafogli con custodia sono portafogli di criptovalute in cui la custodia, ossia il controllo e le operazioni del portafoglio, sono gestite da una terza parte, i portafogli non custodiali sono portafogli di criptovalute in cui la custodia è affidata all'individuo che possiede le chiavi private delle criptovalute sulla blockchain ed è responsabile della loro protezione.[105]

La fornitura di servizi di custodia dei portafogli è una componente critica dell'ecosistema delle criptovalute non garantite e proprio in tale aspetto le risposte normative devono essere adeguatamente robuste.[106] Ad oggi, molte autorità chiedono ai fornitori di *wallet* di considerare la segregazione e custodia dei beni, la resilienza operativa e informatica, la tenuta dei registri dei libri mastri o DLT (Distributed Ledger Technologies) e i requisiti AML/CFT. Come si analizzerà più approfonditamente nel prossimo capitolo relativo alla normativa in materia, a livello nazionale, i *provider* (*wallet provider* ed *exchanger*) ossia coloro che operano con le valute digitali sono tenuti all'osservanza di quanto disposto dal D.lgs 231/2001 in materia di responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica

[103] BINANCE ACADEMY (2022). *Wallet Custodial vs. Non Custodial: qual è la differenza?* Disponibile in open source sul sito https://academy.binance.com/it/articles/custodial-vs-non-custodial-wallets-what-s-the-difference

[104] INVESTGLASS (2023). *Caldo vs. tiepido vs. freddo: Quale portafoglio di criptovalute è adatto a me?*. Disponibile in open source sul sito https://www.investglass.com/it/hot-vs-warm-vs-cold-which-crypto-wallet-is-right-for-me/

[105] MARSALA P. (2020). *Criptovalute: cosa sono i wallet custodial e non-custodial.* Disponibile in open source sul sito https://investire.biz/analisi-previsioni-ricerche/bitcoin-e-criptovalute/criptovalute-wallet-cosa-sono-come-funzionano-differenze-custodial-non-custodial

[106] ARCERI F. (2022). *Wallet Custodial E Non Custodial: Quali Sono E Quando Usarli*. Disponibile in open source sul sito https://checkpointbitcoin.it/wallet-non-custodial-e-custodial-bitcoin-criptovalute/

Tali elementi necessitano di essere considerati in quanto, in alcune giurisdizioni, i *provider* di *wallet* sono tenuti ad assicurare che i fondi o gli asset in criptovaluta detenuti dagli utenti siano tenuti separati dai fondi o dagli asset in criptovaluta dell'entità. Le attività dei clienti dovrebbero essere limitate dal riutilizzo e/o dal prestito senza consenso esplicito da parte degli utenti e senza un'adeguata compensazione. Ciò include la garanzia che gli indirizzi dei portafogli per gli utenti siano diversi dall'indirizzo del *wallet* dell'entità.[107] Inoltre, molte autorità richiedono che i fornitori di *wallet* garantiscano un solido quadro di sicurezza informatica per mantenere al sicuro le attività custodite in criptovaluta. Ci sono state molte occasioni in cui i consumatori non hanno potuto accedere ai loro averi a causa di guasti operativi. Pertanto, è importante che i fornitori di portafogli dispongano di procedure efficaci di gestione di eventi imprevisti ed accidentali, che includano il rilevamento e la classificazione dei principali incidenti operativi e di sicurezza.[108]

La segnalazione di incidenti operativi o informatici deve essere tempestiva e accurata per garantire l'integrità del mercato. Quando i processi informatici o operativi sono delegati a terzi, il fornitore del portafoglio dovrebbe essere responsabile degli incidenti che si verificano presso terzi.

La DLT rientra tra gli elementi da valutare in quanto consente di semplificare l'amministrazione degli asset custoditi mantenendo un registro in tempo reale delle partecipazioni in rete. Molte autorità di regolamentazione richiedono che i fornitori di portafogli garantiscano che tale amministrazione sia sicura, resiliente, tempestiva e accurata. I fornitori di portafogli dovrebbero essere in grado di condividere con l'utente, su richiesta o a intervalli regolari, qualsiasi cambiamento circa quanto in suo possesso. L'affidamento alla DLT per la tenuta dei registri può essere in conflitto con le norme esistenti che richiedono entità centralizzate per la tenuta dei

[107] CUCCHIARATO G. (2019). *Regolamentazione delle ICOs in Italia: pro e contro della proposta Consob*. AgendaDigitale.it. Disponibile in open source sul sito https://www.agendadigitale.eu/documenti/regolamentazione-delle-icos-in-italia-pro-e-contro-della-proposta-consob/

[108] REDAZIONE RHC (2023). *La Blockchain Analysis in chiave cyber-resilienza tra le nuove proposte dell'ACN targata Frattasi*. Disponibile in open source sul sito https://www.redhotcyber.com/post/la-blockchain-analysis-in-chiave-cyber-resilienza-tra-le-nuove-proposte-dellacn-targata-frattasi/?utm_content=cmp-true

registri (ad esempio, il regolamento sui depositi centrali di titoli nell'Unione europea).[109]

Inoltre, in diverse giurisdizioni viene richiesto il rispetto da parte degli operatori delle piattaforme degli standard FATF (ossia Financial Action Task Force quali standard che garantiscono un trattamento equo degli asset virtuali, applicando le stesse tutele del settore finanziario) in materia di prevenzione del riciclaggio e del finanziamento del terrorismo,[110] nonché garanzie adeguate come ad esempio una copertura assicurativa informatica, nel caso di un evento di pirateria informatica, al fine di mitigare i rischi per i consumatori. Tale assicurazione potrebbe coprire una proporzione minima di fondi, determinata dalle autorità.[111] Oltretutto, spesso, quando i fornitori di portafogli fanno parte di un gruppo più ampio, devono assicurare procedure di governance adeguate per garantire l'indipendenza delle decisioni sui servizi di *wallet*[112] e l'assenza di conflitti di interesse con altre attività del gruppo all'interno del gruppo stesso. I servizi di portafoglio devono garantire il miglior interesse degli utenti dei servizi di *wallet*, e questo include requisiti di trasparenza e divulgazione, in cui ogni potenziale conflitto di interesse sia chiaramente comunicato.[113]

Ulteriori requisiti possono essere richiesti in materia di rendicontazione e di regolamentazione prudenziale, ad esempio per quanto riguarda la gestione del rischio (compreso il rischio operativo e informatico), la protezione del patrimonio

[109] ACADEMY (2022). *DLT e Blockchain: storia, differenze e soluzioni.* Disponibile in open source sul sito https://academy.youngplatform.com/blockchain/dlt-blockchain-storia-differenze/

[110] Decreto legislativo 25 maggio 2017, n. 90 - Disponibile in open source sul sito https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2017;090

[111] ZAPPONINI G. (2021). *Cosa sono l'AML e il CFT: le sfide per le aziende dal riciclaggio al terrorismo* in Innolva. Disponibile in open source sul sito https://www.innolva.it/InSight/leggi-riforme/2021-06-AML-CFT

[112] ZAPPONINI G., *Cosa sono l'AML e il CFT: le sfide per le aziende dal riciclaggio al terrorismo*, cit. 108

[113] RIOSA D. (2022). Criptovalute, Mossa sottolinea l'importanza dei wallet. Disponibile in open source sul sito https://www.advisoronline.it/assicurazioni-e-banche/banche/68154-criptovalute-mossa-sottolinea-l-importanza-dei-wallet.action

dei clienti, il capitale minimo e la liquidità (in particolare nei casi in cui il fornitore di servizi wallet riutilizzi le criptovalute del cliente).[114]

Infine, per migliorare il quadro normativo e la sicurezza nell'utilizzo delle criptovalute le autorità potrebbero prendere in considerazione efficaci accordi di liquidazione in caso di fallimento di un portafoglio. Un' adeguata segregazione dei fondi dei clienti può ridurre i danni per i consumatori in caso di fallimento dell'impresa, mentre è importante anche la collaborazione con fornitori terzi e il mantenimento di infrastrutture informatiche critiche.

Inoltre, dal punto di vista penale, in capo ai *provider* risulta facilmente configurabile una specie di funzione di garanzia ai sensi dell'art. 40, comma II, del Codice penale italiano. Gli obblighi imposti negli ultimi anni in capo ai *provider* riflettono chiaramente l'intento del legislatore di prevenire ogni attività illecita da parte di tali soggetti il cui lavoro si caratterizza per lo sfruttamento quotidiano delle valute digitali. L'intento è, quindi, quello di "gravare" la posizione di tali soggetti con l'obbligo di sorveglianza e di segnalazione delle condotte ritenute illecite o comunque sospette, rilevante ai sensi dell'art. 40 comma II del Codice penale. Pertanto, saranno soggetti al dovere di attivarsi ed impedire ovvero prevenire le attività illecite, come il riciclaggio di denaro o il finanziamento del terrorismo. Da ciò ne consegue che in caso di condotta omissiva, i *provider* risponderanno per concorso omissivo al reato commesso dagli utenti, nel caso in cui la condotta sia stata commessa con dolo.

Ciò posto, tuttavia, vi è da notare che l'obbligo di sorveglianza e prevenzione non trova fondamento nella normativa comunitaria. Nonostante le recenti modifiche apportate dal D.lgs. 90/2017, in materia di antiriciclaggio, in recepimento della Direttiva Comunitaria n. 2015/849 del 20 maggio 2015, di cui si parlerà in seguito, le modifiche hanno interessato solo i cambiavalute virtuali. Ciò significa che sarà necessario un ulteriore atto di recepimento interno affinché possa giuridicamente riconoscersi in capo ai *provider* un obbligo impeditivo.

[114] A.G (2018). *Conio. Il wallet bitcoin è un'opportunità per le banche* in aziendabanca.it. Disponibile in open source sul sito https://www.aziendabanca.it/notizie/conio-wallet-bitcoin-banche

5. Le implicazioni legali e sociologiche della tecnologia blockchain. Cenni al *locus commissi delicti*

La rivoluzione della *blockchain* è, prima di tutto, una rivoluzione sociologica. L'idea che la società possa essere gestita attraverso contratti intelligenti individuali senza la necessità di alcuno Stato centrale, insieme a una retorica antigovernativa, ha accompagnato la rivoluzione blockchain fin dal suo inizio. L'obiettivo dei più ferventi sostenitori della blockchain è la definitiva scomparsa degli Stati centralizzati e gerarchici: attraverso contratti intelligenti decentralizzati basati su blockchain, gli individui saranno finalmente in grado di governarsi da soli, senza bisogno di autorità centrali.[115]

Questa idea rivoluzionaria può sembrare familiare: il concetto di membri della società che amministrano lo Stato è infatti alla base della dottrina marxista, secondo la quale lo Stato si farà semplicemente da parte quando i lavoratori avranno raggiunto un livello sufficiente di maturità e di coscienza politica, mettendo così lo Stato "*nel museo delle antichità, accanto all'arcolaio e all'ascia di bronzo*".[116] Esiste tuttavia un'evidente differenza tra i due movimenti. Mentre l'obiettivo del marxismo era la distruzione del capitalismo, per i sostenitori estremi della blockchain il risultato è esattamente l'opposto: la vittoria del libero mercato e degli imprenditori privati sulle istituzioni pubbliche, in un processo definito "anarcocapitalismo".[117]

Mentre l'ala moderata dei sostenitori della blockchain sostiene che la rivoluzione della blockchain creerà una società decentralizzata basata ancora sull'autorità degli Stati, dove "*i quadri giuridici diventeranno più granulari e personalizzati alla situazione*"[118].

[115] CAPACCIOLI S. (2015). *Criptovalute e Bitcoin: un'analisi giuridica*, Milano, pp. 9 ss
[116] ENGELS F. (1884) *Origins of the Family, Private Property and the State*.
[117] ATZORI M. (2015). *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* cit. 30
[118] SWAN M. (2015). *Blockchain. Blueprint for a New Economy*, O'Reilly, 17.

Dal punto di vista invece legale, possiamo facilmente affermare che l'aspetto più delicato della tecnologia blockchain è il suo difficile rapporto con il diritto. Bisogna quindi domandarsi se la *blockchain* risulti compatibile con la legge.

"*Il codice è legge*"[119] è un motto ben noto ai sostenitori della blockchain per affermare la superiorità del codice software rispetto ai sistemi legali. Oggi con l'uso diffuso della tecnologia blockchain è sorto un nuovo insieme di regole auto realizzate da organizzazioni decentralizzate e autonome.[120] Questa rapida e inarrestabile espansione della "legge delle criptovalute" ci riporta alla domanda iniziale:

blockchain e legge sono compatibili?

E, in caso affermativo, abbiamo davvero bisogno di leggi che regolamentino una rete che ha già una sua serie di regole auto applicabili?

Per rispondere alle domande di cui sopra, possiamo partire dal noto approccio della Scuola di Chicago teorizzato dal giurista americano Lawrence Lessig nel suo libro del 1999 "Code and Other Laws of Cyberspace".[121] Secondo Lessig, sono quattro le forze regolatrici solitamente impiegate per limitare le azioni umane: *i)* il mercato (utilizzando incentivi finanziari e disincentivi), *ii)* le norme sociali, *iii)* l'architettura (identificata in un ambiente tecnologico come il codice del software) e *iv)* la legge.[122]

Quando si parla di blockchain, il mercato si identifica con l'interesse personale dei minatori (l'incentivo economico a svolgere attività di mining), le norme sociali con la fiducia e l'architettura con la crittografia; la legge è, invece, esterno alla blockchain, in quanto deriva dalle autorità sovrane. Come possiamo vedere, il codice software è solo un diverso tipo di regolamentazione che coesiste con altri meccanismi come la legge.[123] Tuttavia, mentre il codice software crea regole espresse in termini matematici formali (ad esempio, chiavi asimmetriche, funzioni

[119] LESSIG L. (1999). *Code and Other Laws of Cyberspace*, BasicBooks
[120] ANTONOPOULOS A. M., *Mastering Bitcoin – Programming the Open Blockchain*, cit. 22
[121] LESSIG L. *Code and Other Laws of Cyberspace*, cit. 116
[122] LESSIG L. *Code and Other Laws of Cyberspace*, cit. 116
[123] WERBACH K. (2018), *The Blockchain and the New Architecture of Trust*, MIT Press 154-155.

hash), il diritto usa il linguaggio umano, coprendo quindi tutte quelle aree "umane" che non possono essere descritte con funzioni matematiche (come i diritti individuali, i valori sociali o le strutture di governo e di mercato).

Alla luce di quanto detto, possiamo affermare che la risposta a entrambe le domande è sì. La legge e il codice, infatti, non sono alternative binarie, ma due diverse forze regolatrici che dovrebbero operare in modo sinergico per ottenere i migliori risultati in un ambiente ibrido.[124] Questo non significa che la legge debba rimanere invariata di fronte alla progressiva espansione della tecnologia blockchain; piuttosto, dovrebbe adattarsi per affrontare meglio i problemi posti da questa nuova tecnologia.[125]

Anche se in molti casi la legge e il codice non hanno un contatto diretto, in quanto rappresentano due forze normative diverse, esistono comunque tre potenziali situazioni in cui i codici software basati su blockchain possono interagire con il sistema giuridico:

La prima situazione tipica si verifica quando la blockchain agisce come un'integrazione della legge. Esistono infatti molte situazioni in cui la blockchain può rafforzare il sistema legale, offrendo nuovi modi per raggiungere gli obiettivi definiti dalla legge. Ad esempio, nel caso di un trasferimento di titoli, in diverse giurisdizioni esistono leggi che impongono l'aggiornamento dei registri pubblici per riflettere la nuova partecipazione azionaria della società. La Blockchain può offrire una soluzione diversa: un libro mastro in tempo reale che traccia direttamente la proprietà, evitando così i ritardi o gli inconvenienti che possono verificarsi quando i trasferimenti vengono registrati in un momento diverso.

Un secondo potenziale scenario può verificarsi quando la blockchain funge da complemento alla legge. Potrebbero infatti verificarsi situazioni in cui la legge non riesce a regolamentare adeguatamente alcune aree, di solito perché la fiducia nel sistema legale è insufficiente. In questo caso la blockchain non si limita a fornire

[124] SOLDAVINI, P., (2016). *Il futuro della finanza in una BlockChain* in Il sole 24 ore. Disponibile in open source sul sito http://nova.ilsole24ore.com/frontiere/il-futuro-della-finanzain-una-blockchain/ .
[125] WERBACH K. (2018), *The Blockchain and the New Architecture of Trust,* cit. 120.

una soluzione parallela, ma funge da meccanismo che assicura la conformità alla legge. Un esempio di questa situazione si trova nella legge sul diritto d'autore, in particolare in relazione alle opere di cui non si riesce a trovare il titolare (le cosiddette "opere orfane").[126] A volte, anche se l'opera è di dominio pubblico, i titolari dei diritti possono essere estremamente difficili da individuare, con gravi rischi di violazione del diritto d'autore da parte di potenziali utenti. In questa situazione, un libro mastro basato su blockchain può tenere traccia di tutti gli sforzi compiuti dal potenziale utente per trovare il detentore del diritto, mentre i contratti intelligenti possono garantire il pagamento dei diritti di licenza da parte degli utenti di opere orfane nel caso di rivendicazione della titolarità dei diritti.[127]

La terza e ultima situazione si verifica quando la blockchain agisce come sostituto della legge. In questo caso la blockchain sostituisce completamente la legge e agisce come unico meccanismo di applicazione. Questa situazione può verificarsi in luoghi in cui l'applicazione legale è debole, come le zone di conflitto o alcune aree dei Paesi in via di sviluppo. Ci sono, ad esempio, aree del mondo in cui i registri dei titoli di proprietà terriera sono incompleti o difficili da consultare; questo può essere un ostacolo importante per lo sviluppo economico locale.[128]

Un libro mastro basato su blockchain può costituire in questo caso una valida alternativa ai registri governativi, in quanto gli individui avrebbero un modo più facile, più economico e più efficiente di interagire con i registri dei titoli di proprietà.[129]

Come abbiamo visto, la blockchain è una tecnologia che non è (e non dovrebbe essere) immune da regolamentazioni. Tuttavia, i regolatori dovrebbero valutare attentamente quando e in che misura intervenire, per evitare di soffocare una

[126] SHIN L., (2016). *Republic Of Georgia To Pilot Land Titling On Blockchain With Economist Hernando De Soto*, BitFury, Forbes. Disponibile in open source sul sito: https://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilotland-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/#41908e8744da.
[127] SHIN L., *Republic Of Georgia To Pilot Land Titling On Blockchain With Economist Hernando De Soto,* cit. 123.
[128] WRIGHT A., DE FILIPPI P., (2015). *Decentralized Blockchain Technology and The Rise of Lex Cryptographia.* Disponibile in open source sul sito: http://dx.doi.org/10.2139/ssrn.2580664.
[129] WERBACH K. (2018), *The Blockchain and the New Architecture of Trust,* cit. 120.

tecnologia appena nata e dal potenziale immenso.[130] La prima domanda che i regolatori dovrebbero porsi è:

la tecnologia blockchain ha uno scopo legittimo?

Come sappiamo, alcuni servizi consentono accidentalmente la violazione di obblighi legali, mentre altri sono specificamente mirati a violare le leggi (come i mercati del dark web). Valutare l'intento di un servizio è difficile così come l'entità dell'attività illegale svolta utilizzando tale servizio. A questo proposito, le autorità di regolamentazione dovrebbero condurre un'analisi caso per caso delle applicazioni basate su blockchain al fine di verificare se il singolo servizio persegue uno scopo legittimo. Solo quando la valutazione di cui sopra ha un esito negativo i legislatori dovrebbero prendere in considerazione un intervento normativo, ad esempio il blocco di un servizio o la chiusura di un sito web.

La seconda questione da considerare è se esistano mezzi alternativi alla regolamentazione per raggiungere gli obiettivi sociali. Potrebbero esistere soluzioni di *soft law* che possono raggiungere gli stessi obiettivi politici in modo meno invasivo. Per esempio, le organizzazioni private potrebbero sviluppare una serie di standard e le migliori pratiche attraverso un processo volontario e di autoregolamentazione, senza la necessità di un intervento normativo. Un esempio è la ICO Governance Foundation (IGF),[131] una fondazione globale senza scopo di lucro che ha creato il primo registro ICO, offrendo così uno standard globale per le informazioni sulle ICO e un registro progettato per l'auto registrazione volontaria.[132] Di fatto, questo sistema di autoregolamentazione si è rivelato uno strumento di successo in diverse giurisdizioni. Negli Stati Uniti, per esempio, gli

[130] Le ICO possono essere registrate sul sito web ICODisclosure.com attraverso un processo di deposito volontario e autoregolamentato che aiuta gli investitori nella corretta valutazione dell'offerta prima di investire.*Vedi* CLARK D. (2018). *ICO Governance Foundation Creates First ICO Registry*. Law.com Disponibile in open source sul sito https://www.law.com/corpcounsel/2018/10/10/ico-governance-foundation-createsfirst-ico-registry/?slreturn=20190630111941.

[131] MARTINO P., BELLAVITIS C., DASILVA C. M. (2019). *Blockchain and Initial Coin Offerings (ICOs): a new way of crowdfunding*, SSRN 7 Disponibile in open source sul sito http://dx.doi.org/10.2139/ssrn.3414238.

[132] MARTINO P., BELLAVITIS C., DASILVA C. M., *Blockchain and Initial Coin Offerings (ICOs): a new way of crowdfunding*, cit. 130

standard legali ed etici in alcune aree del diritto dei valori mobiliari sono stabiliti da organizzazioni di autoregolamentazione come la Financial Industry Regulatory Authority (FINRA), per i broker e gli intermediari e la National Futures Association (NFA), per i futuri trader.[133]

La terza e ultima questione da considerare è la valutazione dei costi e dei benefici di un intervento normativo. I regolatori dovrebbero considerare attentamente non solo l'opportunità di intervenire o meno, ma anche in quale misura e attraverso quali meccanismi di applicazione della legge. In un sistema decentralizzato come la blockchain, la questione cruciale è quella di determinare chi è responsabile delle attività illecite svolte sulla blockchain e, quindi, chi dovrebbe essere l'obiettivo di un potenziale intervento normativo. Tuttavia, anche in un ambiente decentralizzato ci saranno sempre potenti intermediari e operatori che gestiscono effettivamente la rete. Pertanto, se minacciati, i regolatori possono adottare una serie di misure contro tali intermediari e operatori al fine di rafforzare lo Stato sulla rete blockchain.[134] I regolatori possono, per esempio, richiedere agli intermediari online di eliminare le applicazioni basate su blockchain dai risultati di ricerca,[135] o di costringere i fornitori di servizi Internet a bloccare il traffico di dati crittografati sui loro siti[136] o addirittura obbligare i produttori di hardware (come Apple) a implementare misure per bloccare o tracciare l'uso di tecniche di crittografia sui loro prodotti.[137]

Tuttavia, gli interventi di cui sopra, senza un attento bilanciamento dei costi e dei benefici, possono risultare un grossolano abuso di potere normativo e, infine,

---

[133] WERBACH K. (2018), *The Blockchain and the New Architecture of Trust,* cit. 120.

[134] WRIGHT A., DE FILIPPI P., *Decentralized Blockchain Technology and The Rise of Lex Cryptographia,* cit. 127

[135] BAUTISTA C (2014). *Google search algorithm changes demote piracy sites from page rankings*, Tech Times, Disponibile in open source sul sito https://www.techtimes.com/articles/18334/20141022/googlesearch-algorithm-changes-demote-piracy-sites-from-page-rankings.htm.

[136] SVENSSON P. (2007). *Comcast Blocks Some Internet Traffic, NBC News* Disponibile in open source sul sito http://www.nbcnews.com/id/21376597/ns/technology_and_science-internet/t/comcast-blocks-some-internet-traffic/#.XUBi7FBS8_U.

[137] BALL J. (2015). *Cameron wants to ban encryption – he can say goodbye to digital Britain*, The Guardian Disponibile in open source sul sito https://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryptiondigital-britain-online-shopping-banking-messaging-terror

possono soffocare i vantaggi economici offerti dalla tecnologia blockchain. Una regolamentazione troppo restrittiva in un determinato Paese spingerà inoltre gli investitori e le attività verso giurisdizioni più permissive, dando origine a pratiche di arbitraggio giurisdizionale. Inoltre, una regolamentazione incontrollata può trasformare la tecnologia blockchain in un potente strumento di sorveglianza di massa nelle mani dei governi, minando così diritti costituzionali fondamentali come la libertà di espressione e la privacy, vanificando l'idea originaria della blockchain come fonte di emancipazione e decentralizzazione.[138]

La sfida per le autorità di regolamentazione è quindi quella di trovare un equilibrio ottimale tra i meccanismi di applicazione volti a bloccare gli usi illegali della blockchain e la crescita economica libera e incondizionata di una nuova tecnologia ispirata a principi democratici e definita in un sistema di governo efficiente decentralizzato. Ciò ovviamente non potrà prescindere dalla responsabilizzazione dei *provider,* al quale il legislatore ha fatto recentemente fronte. Inoltre, dal punto di vista penale, come è noto, per la configurazione del reato è necessario l'elemento soggettivo (dolo o colpa) nonché l'elemento oggettivo (condotta/omissione e nesso causale tra elemento oggettivo e soggettivo ossia l'evento lesivo). La dottrina si è domandata se nei reati commessi nel cyberspazio ed in particolare mediante l'utilizzo delle criptovalute e della tecnologia *blockchain* possano configurarsi tali elementi. Relativamente alla tecnologia *blockchain,* la condotta illecita risulta analoga alle condotte commesse senza l'utilizzo di una tecnologia. Basti pensare a due soggetti che decidono di trasferire un ammontare di valute digitali proveniente da un'attività illecita. In tal caso la condotta verrà definitivamente commessa con la chiusura del blocco della *blockchain* da parte del *miner*. Tuttavia, l'elemento più critico rimane la configurazione dell'evento in quanto lo stesso si verifica in una pluralità di luoghi e per questo risulta difficile l'identificazione del *locus commissi delicti,* ossia il principio secondo cui il luogo di commissione del reato corrisponde al luogo in cui l'autore ha agito o omesso di agire o dove il risultato si è verificato o doveva verificarsi secondo l'intenzione dell'autore. La determinazione del *locus commissi delicti* è cruciale sia per il diritto penale sostanziale che per il diritto

[138] WRIGHT A., DE FILIPPI P., *Decentralized Blockchain Technology and The Rise of Lex Cryptographia,* cit. 125

penale processuale, perché è un criterio importante per stabilire la giurisdizione dello Stato in materia penale e per designare un'autorità competente per condurre le indagini nonché il procedimento penale. Sembra che la prassi del diritto penale dovrà occuparsi sempre più spesso di reati commessi con l'ausilio di Internet e nella rete, a causa della sua sempre maggiore disponibilità e del fatto che i reati sono sempre più diffusi, a causa della sua enorme diffusione e del conseguente crescente ruolo sociale della rete Internet. Ciò significa che la disponibilità universale e territorialmente illimitata di Internet potrebbe rendere irrilevante l'ubicazione dell'attore e del destinatario (o dei destinatari) dell'evento illecito. Tenendo conto della natura specifica dei crimini informatici, si possono distinguere quattro potenziali tipi di comportamento da parte dell'autore del reato: *i) l*'autore del reato si trova al di fuori di un dato Stato A e colpisce un sistema informativo situato al di fuori di un dato Stato A, *ii)* l'autore si trova al di fuori di un dato Stato A e colpisce un sistema informativo situato all'interno dello Stato A, *iii*) l'autore del reato si trova in uno Stato A e colpisce un sistema informativo situato all'esterno dello Stato A, *iv)* l'autore del reato e il sistema di informazioni su cui incide si trovano all'interno dello Stato A.

Nell'esempio utilizzato che integra la fattispecie di riciclaggio (art. 648-bis c.p.) il luogo della commissione del reato potrà essere identificato nel luogo in cui il mittente ha iniziato la transazione, essendo un reato di condotta. Con riferimento, invece ai reati di evento, come la cancellazione dei dati iscritti nei registri pubblici della *blockchain*, utilizzando lo stesso criterio, l'identificazione del luogo in cui viene commesso il reato risulta ancora più difficoltosa.

Tale tema verrà analizzato più approfonditamente nel corso del prossimo capitolo dedicato, nello specifico, all'analisi del quadro normativo europeo e nazionale in materia di valute digitali, in quanto l'identificazione della giurisdizione competente è un problema attuale poichè la legge penale non è adeguata, senza apposita riforma, a regolamentare il locus dei crimini informatici, in tutte quelle situazioni in cui l'autore commette un reato via Internet senza risultato, agendo dall'esterno del paese ma colpendo un sistema informatico situato all'interno del paese stesso.

5.1 (*Segue):* Le implicazioni pratiche della tecnologia blockchain

Dopo aver illustrato le teorie sociologiche e legali che stanno alla base della rivoluzione della blockchain, possiamo ora passare alle implicazioni pratiche di questa tecnologia.

a) Democrazia diretta

La partecipazione diretta dei cittadini alla politica è sempre stata una chimera nei sistemi democratici. Tuttavia, prima dell'avvento della blockchain era quasi impossibile garantire la sicurezza e l'anonimato dei voti online. Al contrario, la tecnologia blockchain può garantire l'identificazione sicura dei votanti attraverso chiavi asimmetriche e l'anonimato dei voti grazie a procedure di crittografia. I cittadini sarebbero quindi in grado di partecipare direttamente alla politica, sia a livello locale che nazionale, votando mediante l'utilizzo dei propri dispositivi attraverso le piattaforme blockchain.

Gli elettori potrebbero, ad esempio, votare sul bilancio proposto per la loro città, o addirittura rimuovere i politici dalle loro cariche se disapprovano le loro decisioni.[139]

Tuttavia, sono state sollevate diverse preoccupazioni sull'affidabilità di un sistema di voto basato su blockchain. In primo luogo, su una *blockchain* completamente decentralizzata potrebbe essere rischioso lasciare l'esito delle elezioni nelle mani di un pool di minatori sconosciuti, in quanto i voti potrebbero essere esposti a un potenziale attacco, oltretutto, non esistendo un controllo diretto sui singoli elettori, sarebbe quasi impossibile controllare (e prevenire) la coercizione o le pratiche di compravendita dei voti,[140] nonostante le piattaforme di voto basate su blockchain stanno guadagnando sempre più credibilità in tutto il mondo.[141]

---

[139] WRIGHT A., DE FILIPPI P., *Decentralized Blockchain Technology and The Rise of Lex Cryptographia,* cit. 127

[140] RYAN P. Y. A. (2019). *Are Blockchain Voting Technologies Safe?* Disponibile in open source sul sito https://www.ispionline.it/it/pubblicazione/are-blockchain-voting-technologies-safe23155.

[141] COLZANI J. (2019). *Blockchain: A Digital Solution for Modern Democracies?* Disponibile in open source sul sito https://www.iai.it/it/pubblicazioni/blockchain-digital-solution-moderndemocracies.

b) La governance algoritmica

Una visione più futuristica e all'avanguardia trova nelle organizzazioni autonome decentralizzate (Decentralized Autonomous Organization) un sostituto dei governi. In questo scenario gli individui sarebbero liberi di creare nazioni senza confini governate da un insieme di regole algoritmiche incluse nei contratti intelligenti.

Di conseguenza, gruppi di cittadini sarebbero in grado di istituire sistemi giuridici personalizzati tramite gli *smart contract*, scegliendo le regole che meglio riflettono le loro preferenze individuali, senza la necessità di un'autorità centrale che faccia rispettare tali regole (dando origine alla cosiddetta "governance algoritmica").[142]

Possiamo immaginare diversi vantaggi derivanti da un uso massiccio della governance algoritmica. Per esempio, il costo di un prodotto può essere calcolato in termini di surplus dal consumatore, le auto a guida autonoma controllate da algoritmi complessi possono ridurre significativamente il numero di incidenti, i dati sanitari raccolti dagli individui (ad esempio, attraverso un orologio intelligente) possono aiutare a identificare malattie o emergenze specifiche e l'algoritmo potrebbe rilevare un attacco di cuore e inviare un'ambulanza esattamente nella posizione in cui si trova la persona.

C'è il rischio, tuttavia, che gli individui rinuncino lentamente (e inconsciamente) al libero arbitrio e lascino tutte le loro decisioni più importanti (ad esempio, per quanto riguarda il lavoro o la famiglia) agli algoritmi. I problemi maggiori sorgono quando ci si rende conto che ci sono molte situazioni in cui gli algoritmi non sempre selezionano la scelta ottimale per tutti gli individui. Uno dei motivi principali è che, anche con le migliori intenzioni, gli algoritmi guidati dai dati possono portare a pratiche e risultati discriminatori, riproducendo gli schemi esistenti di discriminazione e pregiudizio di chi ha preso le decisioni in precedenza. Ciò può

[142] WRIGHT A., DE FILIPPI P., *Decentralized Blockchain Technology and The Rise of Lex Cryptographia*, cit. 127

essere causato, ad esempio, da dati di input mal ponderati[143], o derivare dall'uso di alcuni dati nel contesto sbagliato.[144]

Se consideriamo lo scenario peggiore, in cui i contratti intelligenti vengono automaticamente applicati indipendentemente dalla volontà delle parti, il risultato può essere addirittura un sistema deterministico in cui gli individui sono liberi di scegliere il proprio insieme di regole ma, una volta che la scelta è presa, essi non possono deviare da tali regole, diventando così soggetti a una moderna versione tecnologica dei regimi totalitari[145]

c) Privatizzazione dei servizi pubblici

I sistemi di governance basati sulla blockchain possono offrire una serie di servizi tradizionalmente forniti dai governi.[146] Ad esempio, utilizzando la blockchain come archivio permanente di documenti, sarebbe possibile archiviare documenti governativi come documenti d'identità, passaporti, patenti di guida, atti di proprietà e, infine, "mettere una nazione sulla blockchain"[147] eliminando archivi di Stato, registri fisici e notai.

Utilizzando semplicemente una app, si può ad esempio sposarsi, intestare un terreno, costituire un'azienda, o autenticare un testamento in pochi minuti e per poche monete.[148]

Non possiamo ignorare, ovviamente, gli evidenti vantaggi che possono derivare dalla decentralizzazione dei servizi governativi attraverso una blockchain aperta e

[143] CHRISTIN A., ROSENBLATT A., BOYD D. (2015). *Courts and predictive algorithms*, Data & Civil Rights Primer

[144] LEPRI B. , OLIVER N., LETOUZÉ E., PENTLAND A., VINCK P., (2017). *Fair, transparent and accountable algorithmic decision-making processes. The premise, the proposed solutions, and the open challenges*, in Philosophy & Technology 31(3) 4. Disponibile in open source sul sito http://www.nuriaoliver.com/papers/Philosophy_and_Technology_final.pdf.

[145] WRIGHT A., DE FILIPPI P., *Decentralized Blockchain Technology and The Rise of Lex Cryptographia,* cit. 127

[146] SWAN M. (2015). *Blockchain. Blueprint for a New Economy*, cit. 117.

[147] SWAN M. (2015). *Blockchain. Blueprint for a New Economy*, cit. 117.

[148] VOLLSTÄDT E. (2015). *Totalitarian Cyber State vs Freedom Unbound: Interview with Fabricio & Susanne* Part 2, on Bitnation-blog.com. Disponibile in open source sul sito https://blog.bitnation.co/totalitarian-cyber-state-vs-freedom-unbound-interview-withfabricio-susanne-part-2/.

senza permessi. Per esempio, tutto verrebbe registrato su un libro mastro immutabile e resistente alle manomissioni, facilmente accessibile dai singoli e i tempi e costi si ridurrebbero in modo significativo, poiché i servizi governativi verrebbero forniti attraverso un algoritmo senza alcun intervento umano.[149]

Ci sono tuttavia alcuni aspetti problematici che meritano la giusta attenzione. L'aspetto più significativo da considerare è la natura speculativa della blockchain. Come sappiamo, l'attività di mining implica un enorme investimento in termini di denaro e di energia, in quanto la soluzione dei puzzle matematici per trovare la proof-of-work richiede un'enorme potenza di calcolo. Questo può portare a diverse conseguenze potenziali.

In primo luogo, la centralizzazione della potenza di calcolo nella rete e la dipendenza delle reti da oligarchie private (ad esempio le società di minatori), con l'aumento di poteri di controllo privi di legittimità formale.[150]

In secondo luogo, il predominio della logica di mercato sui servizi pubblici essenziali e sui diritti costituzionali. In effetti, una blockchain pubblica può essere dismessa in qualsiasi momento dalla comunità se considerata non più redditizia, mettendo così a rischio la continuità del servizio e la conservazione dei dati nel lungo periodo (senza alcuna possibilità di individuare un'entità responsabile di tale disservizio).[151] Pertanto, dato il fatto che i servizi governativi richiedono un alto grado di affidabilità, accessibilità e trasparenza, sarebbe consigliabile evitare la decentralizzazione di tali servizi su una blockchain.

d) Diritti e libertà costituzionali

La crittografia altamente affidabile utilizzata dalle blockchain può essere anche uno strumento efficace per proteggere i diritti e le libertà costituzionali degli individui. Diritti individuali come la libertà di parola e la privacy sono sempre stati considerati

[149] SWAN M. (2015). *Blockchain. Blueprint for a New Economy*, cit. 117.
[150] (2022). Blockchain e GDPR: riflessioni su alcuni elementi di contrasto in Iusinitinere.it. Disponibile in open source sul sito https://www.iusinitinere.it/blockchain-e-gdpr-riflessioni-su-alcuni-elementi-di-contrasto-43006
[151] ATZORI M., *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* cit. 30.

come pilastri fondamentali di una società democratica e la crittografia può aiutare i cittadini a proteggere la loro libertà e la loro privacy dai governi e dalle grandi aziende.[152]

Non sorprende quindi che negli ultimi due decenni, si sia assistito a un crescente utilizzo di reti peer-to-peer in grado di proteggere l'anonimato degli utenti e di resistere alla censura e alla sorveglianza di massa da parte dei governi.[153]

e) Protezione dei dati

Infine, vale la pena menzionare l'impatto che la tecnologia blockchain ha sulla protezione dei dati personali, di cui parleremo più approfonditamente nell'ultimo paragrafo del presente elaborato. Con specifico riferimento all'Unione Europea, la questione è diventata particolarmente delicata dopo l'entrata in vigore del Regolamento generale sulla protezione dei dati (GDPR).[154]

A questo proposito, il 24 luglio 2019 il Parlamento europeo ha pubblicato uno studio[155] che esplora la tensione tra la tecnologia blockchain e la conformità al GDPR e come la tecnologia blockchain possa essere utilizzata come strumento di assistenza per la conformità al GDPR,[156] approfondendo sia le incompatibilità tra

[152] ATZORI M., *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* cit. 30.

[153]FARMER J., (2003). *The Spector of Crypto-anarchy: Regulating Anonymity-Protecting Peer-to-Peer Networks*, Fordham Law Review, 72(3).

[154] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) - Disponibile in open source sul sito https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Arricchito+con+riferimenti+ai+Considerando+Aggiornato+alle+rettifiche+pubblicate+sulla+Gazzetta+Ufficiale++dell%27Unione+europea+127+del+23+maggio+2018

[155] EUROPEAN PARLIAMENT (2019). *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?* Disponibile in open source sul sito https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

[156] COOPER D., NASH G. (2019). European Parliament Publishes Study on Blockchain and the GDPR, Covington & Burling. Disponibile in open source sul sito https://www.insideprivacy.com/data-privacy/european-parliament-publishes-studyon-blockchain-and-the-gdpr/

GDPR e tecnologia blockchain sia i benefici che possono derivare dalla loro "collaborazione".

CAPITOLO II

Sommario: 1. L'approccio delle autorità di regolazione - 1.1 *(Segue)*: Il modello europeo - 1.2. *(Segue)*: I cripto-asset come strumenti finanziari 1.3. (*Segue*): Regolamentazione dei cripto-asset che si qualificano come strumenti finanziari – 1.4. (*Segue*): Regolamentazione UE delle valute virtuali - 2. Regolamentazione dei *wallet* provider - 2.1 *(Segue)*: Obblighi per i fornitori di servizi di crypto-asset - 2.2 (*Segue*): Responsabilità penale dei *Wallet provider* – 3. Evoluzione del quadro normativo italiano - 3.1 (*Segue*): La giurisprudenza della Corte di Cassazione in materia di riciclaggio e responsabilità dei *Wallet provider*- 3.2 (*Segue*): 231 e criptovalute: la responsabilità da reato dell'ente nel riciclaggio tramite monete virtuali - 4. Le possibili conseguenze fiscali ed economiche - 4.1 *(Segue)*: La posizione dell'Agenzia delle Entrate - 4.2 (*Segue*): le possibili conseguenze economiche delle criptovalute - 5. I diversi approcci degli Stati membri dell'UE: alcuni esempi - 5.1 (*Segue*): Approccio cripto-friendly: Malta ed Estonia - 5.2 (*Segue*): l'approccio prudente di Regno Unito, Francia e Germania

1. L'approccio delle autorità di regolazione

In un mondo dove sempre più spesso si sente parlare di criptovalute, risulta necessaria l'implementazione di una corretta supervisione del fenomeno da parte di tutti gli stati e delle loro autorità al fine di evitare l'insorgere di una serie di problematiche.[157] In altre parole, nel corso del tempo si è sottolineata l'importanza di istituire regole comuni a livello globale per regolamentare in modo chiaro ed efficace il mondo delle criptovalute.[158] Tuttavia, attualmente, non esiste una vera e propria normativa uniforme né a livello europeo né tanto meno a livello internazionale ma solamente infiniti tentativi isolati di regolarizzare e uniformare la materia. Ciò è determinato anche dall'incertezza giuridica dello status delle

[157] VIGNA P., CASEY J., (2015). *The age of Cryptocurrency: How Bitcoin and digital money are challenging the global economic order*, New York, St. Martin's Press.
[158] CAPACCIOLI S. *Criptovalute e Bitcoin: un'analisi giuridica*, cit. 112

criptovalute a livello legislativo nel contesto mondiale, dalla difficoltà circa l'accertamento della responsabilità penale per le operazioni relative alla circolazione delle criptovalute, nonché da una debole azione di contrasto ai reati penali. La cooperazione internazionale nella lotta contro i reati legati alla circolazione delle criptovalute dovrebbe essere portata avanti sulla base della partecipazione di tutti gli Stati.[159] La cooperazione internazionale dovrebbe essere portata avanti in diversi ambiti e includere la creazione di regolamenti che disciplinano la circolazione delle criptovalute nel mondo, l'elaborazione di raccomandazioni generali per la regolamentazione di questo tema a livello nazionale e l'introduzione di modelli efficaci di cooperazione organizzativa tra gli Stati per combattere i reati penali legati alla circolazione delle criptovalute.

Premesso ciò, i reati penali commessi con l'utilizzo delle criptovalute possono essere divisi in due gruppi.

I reati nei quali le *criptocurrencies* rappresentano il metodo di pagamento più richiesto dai criminali quale contropartita della propria attività illecita; in sostanza, la criptovaluta è utilizzata come mezzo di pagamento. L'altra categoria è costituita dai reati nei quali la criptovaluta è elemento costitutivo del reato in quanto ne rappresenta l'oggetto materiale.

Accanto ai suddetti, ci sono i reati virtuali, che sono reati commessi esclusivamente su *Internet* con l'ausilio di tecnologie informatiche.

Negli ultimi anni si è assistito a una chiara tendenza alla "fusione" tra il mondo criminale reale e il cosiddetto "virtuale", che contribuisce ad aumentare il numero di casi di reati transnazionali. Questa tendenza permette ai gruppi organizzati e alle organizzazioni criminali di implementare schemi criminali più complessi per le loro attività illegali. Di conseguenza, la complessità dell'individuazione e dell'investigazione di tali reati penali aumenta in modo significativo, il che porta a una diminuzione del livello di sicurezza delle persone, della società e dello Stato.[160]

[159] CVETKOVA I. (2018). *Cryptocurrencies legal regulation*. Bricks law journal, 18, pp. 129-153.
[160] CVETKOVA I., *Cryptocurrencies legal regulation*. Bricks law journal, cit. 157

Una delle misure volte a contrastare la criminalità transnazionale è stata l'approvazione della Convenzione contro la criminalità organizzata transnazionale delle Nazioni Unite (ovvero Convenzione di Palermo[161], 2000).[162] I reati previsti dalla Convenzione di Palermo includono il crimine informatico, la corruzione, il terrorismo perpetrato da organizzazioni criminali persistenti e il finanziamento delle loro attività illegali. La comunità internazionale obbliga tutti gli Stati membri a criminalizzare la corruzione, il riciclaggio di denaro, il terrorismo e il suo finanziamento.

Per un certo periodo di tempo, tali misure hanno dato i risultati positivi attesi nella lotta al crimine transnazionale, ma con l'avvento delle criptovalute e della tecnologia Blockchain, l'individuazione e il contrasto dei suddetti crimini è diventato molto più difficile. Questo è dovuto, in primo luogo, all'incertezza giuridica delle criptovalute, in secondo luogo al loro mancato controllo da parte delle agenzie governative e delle autorità finanziarie, dall'anonimato delle operazioni legate alla circolazione delle criptovalute, ed, infine, dall'assenza di restrizioni (ad eccezione del codice) e dalla capacità della rete di effettuare un numero indefinito di transazioni mediante criptovalute.[163]

Pertanto, l'introduzione delle criptovalute ha creato ulteriori minacce alla sicurezza umana, alla società e allo Stato, come vedremo di seguito, il che rende necessario un miglioramento della legislazione e lo sviluppo di nuovi approcci per regolare i rapporti giuridici in questo settore, nonché la lotta contro la criminalità transnazionale.[164]

---

[161] Convenzione di Palermo - Disponibile in open source sul sito https://uif.bancaditalia.it/normativa/norm-antiricic/convenzioni/conv-palermo.pdf

[162] MINISTERO DELL'INTERNO (2020). *Convenzione di Palermo: venti anni di lotta alla criminalità internazionale*. Disponibile in open source sul sito http://www.interno.gov.it/it/notizie/convenzione-palermo-venti-anni-lotta-alla-criminalita-internazionale#:~:text=Era%20il%2015%20novembre%20del,Stati%20dell'Onu%20su%20193.

[163] CAPACCIOLI S. *Criptovalute e Bitcoin: un'analisi giuridica*, cit. 112

[164] BABANINA V., TKACHENKO I., MATIUSHENKOO., e KRUTEVYCH M. (2021). *Cybercrime: History of formation, current state and ways of counteraction*. Amazonia Investiga, 10 (38), pp. 113–122.

Un tipo di criminalità informatica è il funzionamento illegale dei server Internet, dove spesso vengono effettuate le transazioni di criptovalute. I siti Internet più comuni che utilizzano criptovalute in attività criminali illegali sono il Deep web. Il Deep Web è un sito Internet che memorizza dati non disponibili per l'uso pubblico come informazioni riguardanti un segreto di Stato, aziendale o bancario, informazioni sulla vendita di droghe e armi, killer a contratto. Tutte queste informazioni possono essere acquistate in cambio di criptovalute. Esistono altre piattaforme online in cui si vendono droga, armi, pedopornografia e altri beni illeciti venduti principalmente in criptovaluta. Pertanto, le criptovalute sono perlopiù oggetto di reati presupposto, ossia di reati in cui i proventi sono stati ottenuti illegalmente.

Tali reati sono previsti nella maggior parte dei codici penali degli Stati esteri che hanno ratificato la Convenzione del Consiglio d'Europa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi del crimine e sul finanziamento del terrorismo (di seguito "Convenzione").[165]La Convenzione prevede la responsabilità penale di chi, conoscendo l'illecita provenienza dei proventi, commette intenzionalmente: *i)* la conversione o il trasferimento di beni allo scopo di occultare o mascherarne l'origine illecita o di agevolare qualsiasi altra persona coinvolta in un reato presupposto; *ii)* l'occultamento o la dissimulazione della vera natura del provento, della fonte, dell'ubicazione, e di ogni altro movimento di beni e/o valori; *iii)* acquisizione di un bene, possesso o utilizzo dello stesso di provenienza illecita; e *iv)* partecipazione alla commissione, all'associazione o alla cospirazione per commettere tali reati, il favoreggiamento, l'agevolazione e la istigazione nella commissione di uno dei reati di cui all'art. 6 della Convenzione.

Al giorno d'oggi, a causa della diffusione delle criptovalute nel mondo e del loro alto valore, sono state introdotte nuove e fantasiose modalità per commettere i cosiddetti reati informatici. Per questo, nel tempo, sono stati diversi gli atti mediante i quali le autorità globali hanno espresso la necessità di chiarezza in materia di

[165] Convenzione del Consiglio d'Europa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi del crimine e sul finanziamento del terrorismo - Disponibile in open source sul sito https://rm.coe.int/168008371f

criptovalute e la volontà ad una collaborazione internazionale.[166] Ed, in particolare, hanno esternato la necessità di prevenire i reati penali legati alla circolazione delle criptovalute mediante l'adozione delle seguenti misure "preventive", tra cui la determinazione dello status giuridico delle criptovalute, degli scambi di criptovalute, del mining e di altre attività legate alle criptovalute a livello legislativo; la definizione dei diritti e degli obblighi delle persone che effettuano transazioni con le criptovalute e la delimitazione della tutela penale e legale delle relazioni pubbliche nel campo della circolazione delle criptovalute.[167]

Queste misure, una volta adottate, contribuiranno a stabilire un controllo da parte del governo sulla circolazione delle criptovalute e, di conseguenza, garantiranno la sicurezza di tutte le operazioni legate alle criptovalute. Alcuni esempi di tentativi di regolamentazione del passato emergono dal documento emesso nel dicembre 2013, dall'EBA (*European Banking Authority*) avente il titolo "*Warning to consumers on virtual currencies*"[168] con il quale l'EBA ha delineato le caratteristiche principali delle valute virtuali nonché i rischi derivanti dal loro utilizzo. Successivamente, nel giugno 2014, la FAFT (*Financial Action Task Force*)[169] ha emesso un report dal titolo "*Virtual Currencies Key Definitions and Potential AML/CFT Risks*"[170], in cui le monete digitali e i loro potenziali rischi

[166] Vedi Caso Bitzlato: Un'operazione condotta dalle autorità francesi e statunitensi, e fortemente sostenuta da Europol, ha preso di mira la piattaforma di scambio di criptovalute Bitzlato. Lo scambio di criptovalute registrato a Hong Kong e operante a livello globale è sospettato di aver facilitato il riciclaggio di grandi quantità di proventi criminali e di averli convertiti in rubli. L'operazione ha coinvolto anche le forze dell'ordine e le autorità giudiziarie di Belgio, Cipro, Portogallo, Spagna e Paesi Bassi. L'azione coordinata delle autorità giudiziarie e delle forze dell'ordine dei diversi Paesi coinvolti ha portato alla chiusura della piattaforma, al sequestro delle attività finanziarie presenti e a ulteriori analisi tecniche.

[167] BABANINA V., TKACHENKO I., MATIUSHENKOO., e KRUTEVYCH M., *Cybercrime: History of formation, current state and ways of counteractio*, cit 162.

[168] EBA (2013) *Warning to consumers on virtual currencies.* Disponibile in open source sul sito https://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf

[169] Financial Action Task Force (FATF), è un organismo intergovernativo, istituito dal G7 nel luglio 1989 con l'intento di portare avanti strategie per contrastare le attività di riciclaggio di capitali a livello nazionale e internazionale mediante l'adozione di misure adeguate da parte di tutti i paesi membri. Tale organismo emette raccomandazioni che ad oggi costituiscono il pilastro portante delle normative nazionali in materia di antiriciclaggio.

[170] FAFT (*2014*). *Virtual Currencies Key Definitions and Potential AML/CFT Risks*. Disponibile in open source sul sito https://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

vengono analizzati dal punto di vista di riciclaggio del denaro e utilizzo per il finanziamento di attività terroristiche. Proprio in materia di antiriciclaggio si pone maggiormente l'attenzione, in quanto le criptovalute, essendo in grado di celare l'identità dell'utilizzatore, sono diventate gli asset per eccellenza per effettuare operazioni di cd. *cyberlaundering*.[171] In altre parole, le criptovalute sono state adottate come parte di schemi di riciclaggio di denaro e sono particolarmente associate a diversi reati presupposto, tra cui la frode e il traffico di droga. Sono inoltre largamente utilizzate come mezzo di pagamento per beni e servizi illegali offerti online e offline.

Il riciclaggio di denaro è la principale attività criminale associata all'uso illecito delle criptovalute. La crescente popolarità e adozione delle criptovalute hanno portato a un loro crescente utilizzo negli schemi di riciclaggio di denaro. Altre attività criminali che mostrano un uso intensivo delle criptovalute sono legate all'uso delle stesse come metodo di pagamento per beni e servizi illeciti, agli investimenti fraudolenti in criptovalute e alla criminalità informatica. In tutti i casi, i criminali vogliono nascondere la fonte dei beni illeciti con le criptovalute.[172]

Nel prossimo paragrafo saranno oggetto di analisi le iniziative europee adottate al fine di contrastare l'utilizzo di criptovalute per la commissione di reati.

1.1 (*Segue):* Modello europeo

[171] Il *cyberlaundering* è definito come

"*un fenomeno complesso che comprende l'insieme di tutte le attività illecite finalizzate a "ripulire" (letteralmente: "lavare") non solo il "denaro (moneylaundering), 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"*. Vedi PICCOTTI L. (2018). *Profili penali del Cyberlaundering: le nuove tecniche di riciclaggio*, Rivista Trimestrale Diritto Penale Economico, n. 3-4.

[172] EUROPOL SPOTLIGHT (2022). *Cryptocurrencies: tracing the evolution of criminal finances.* Disponibile in open source sul sito https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

Tra gli obiettivi dell'Unione europea, delineati all'interno del Trattato sull'Unione Europea[173], figura la creazione di un mercato finanziario interno unico. Il perseguimento di tale obiettivo ha determinato l'avvio di un processo di armonizzazione europea mediante l'implementazione di standard normativi comuni che hanno parzialmente sostituito e in futuro sostituiranno i regimi nazionali, eliminando così ogni ostacolo all'integrazione.[174] Tale mercato finanziario interno

> "*comprende uno spazio senza frontiere interne nel quale è assicurata la libera circolazione di merci, persone, servizi e dei capitali*".[175]

Al fine di accelerare il processo di armonizzazione, il legislatore europeo, per quanto riguarda le questioni di sua competenza[176], ha spesso utilizzato l'arma più potente ed efficace del suo arsenale: la legislazione vincolante, che può sostanziarsi in un regolamento[177], direttiva[178] o decisioni.[179]

A ciò si aggiunga che l'Unione europea può adottare due diverse strategie quando cerca di armonizzare la legislazione degli Stati membri mediante atti vincolanti. In particolare, da un lato, l'Unione europea può approvare una legislazione che fissi

---

[173] Art. 3(3) Trattato sull'Unione europea: "*L'Unione instaura un mercato interno. Si adopera per lo sviluppo sostenibile dell'Europa, basato su una crescita economica equilibrata e sulla stabilità dei prezzi, su un'economia sociale di mercato fortemente competitiva, che mira alla piena occupazione e al progresso sociale, e su un elevato livello di tutela e di miglioramento della qualità dell'ambiente. Essa promuove il progresso scientifico e tecnologico*." - Disponibile in open source sul sito https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0017.02/DOC_2&format=PDF

[174] MOLONEY N. (2014) *EU Securities and Financial Markets Regulation*, 3rd ed., Oxford European Union Law Library, 8-12.

[175] Art. 26(2) TRATTATO SUL FUNZIONAMENTO DELL'UNIONE EUROPEA.

[176] Artt. 2 al 6, e articolo 352(1), del Trattato sul funzionamento dell'Unione europea definisce i limiti della competenza legislativa dell'UE.

[177] I regolamenti sono le misure più efficaci tra le misure dell'UE, in quanto sono direttamente applicabili in tutti gli Stati membri senza ulteriori azioni a livello nazionale ("*self-executing*").

[178] Le direttive sono vincolanti solo per quanto riguarda il risultato da raggiungere, lasciando quindi agli Stati membri un discreto margine di manovra nella scelta del metodo di attuazione e delle norme da adottare.

[179] Le decisioni si differenziano dagli altri due strumenti vincolanti, in quanto sono indirizzate a specifici Stati membri dell'UE o a singoli Stati membri dell'UE o a singoli individui, e sono vincolanti nella loro interezza per il destinatario – Vedi Art. 288 TRATTATO SUL FUNZIONAMENTO DELL'UNIONE EUROPEA e CRAIG P., DE BÚRCA G. (2011). *EU Law – Text, Cases, and Materials*, 5th ed., Oxford University Press 105-107.

gli standard minimi, lasciando agli Stati membri la libertà di perseguire le loro politiche all'interno dei confini stabiliti dalla legislazione dell'UE; dall'altro lato, l'Unione europea può massimizzare l'armonizzazione fornendo una regolamentazione esaustiva dell'area, prevenendo così il più possibile l'azione nazionale e lasciando agli Stati membri dell'UE un margine di manovra minimo o nullo.[180]

Tuttavia, anche se l'intensa attività legislativa del legislatore europeo assicura un certo livello di armonizzazione dei mercati finanziari tra gli Stati membri dell'UE, ciò non si traduce necessariamente in una regolamentazione completamente uniforme, principalmente a causa dell'interesse degli Stati membri di mantenere il più possibile i propri regimi nazionali (spesso restrittivi).[181] Tale mancanza di uniformità può causare applicazioni diverse, persino opposte, delle norme dell'UE a livello nazionale, in particolare quando si tratta di direttive (data la flessibilità concessa agli Stati membri dell'UE nella loro attuazione).[182]

Il lungo e faticoso processo di armonizzazione della normativa dei mercati finanziari in tutti gli Stati membri ha portato all'adozione di una serie di atti legislativi che coprono un'ampia gamma di questioni, spesso supportati da strumenti di *soft law* come raccomandazioni e linee guida.[183] Il lungo percorso che ha portato alla regolamentazione delle valute virtuali nell'Unione Europea risale al 2012, quando la BCE si è espressa per la prima volta sulle valute virtuali, definendole come

[180] CRAIG P., DE BÚRCA G., *EU Law – Text, Cases, and Materials,*cit. 146. Vedi anche LEMME G.,
PELUSO S. (2016). *Criptomonete e distacco dalla moneta legale: il caso Bitcoin*, in Riv. dir. banc., II, p. 43, p. 5.
[181] BOCCHINI R., (2017). *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in Dir. Inform., I, p. 36.
[182] CAPACCIOLI S. *Criptovalute e Bitcoin: un'analisi giuridica*, cit. 112
[183] GASPARRI G., (2015). *Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?* in Dir. Inform., I, p. 11.

> "*un tipo di moneta digitale non regolamentata che viene emessa e solitamente controllata dai suoi sviluppatori e utilizzata tra i membri di una specifica comunità virtuale*".[184]

La BCE ha inoltre sottolineato che

> "*gli schemi di moneta virtuale si differenziano dai sistemi di moneta elettronica in quanto la moneta viene utilizzata come un'unità di conto che non consta di una parte fisica con corso legale*"

Il rapporto della BCE del 2012 è stato seguito da un parere pubblicato dall'EBA nel luglio 2014[185] indirizzato alle istituzioni dell'UE con il quale sconsigliava vivamente alle istituzioni finanziarie di 'acquistare, vendere o detenere valute virtuali fino all'adozione di una normativa specifica. Il parere suggerisce un approccio normativo a lungo termine, tra cui la creazione di un'entità che risponda all'autorità di regolamentazione delle attività delle valute virtuali, il rispetto dei requisiti di *due diligence* dei clienti per risolvere i problemi di anonimato, la predisposizione di requisiti di abuso di mercato per prevenire l'abuso di informazioni privilegiate e la manipolazione del mercato, la registrazione obbligatoria e la necessaria autorizzazione al fine di fornire servizi di valuta virtuale nonché prove di sistemi informatici sicuri.[186]

Il parere dell'EBA esortava inoltre le istituzioni dell'UE a mettere in atto una risposta normativa immediata nel breve periodo, al fine di prevenire l'aumento del riciclaggio di denaro e di crimini finanziari dovuti all'uso diffuso delle valute virtuali. A questo proposito, l'EBA raccomanda che i legislatori dell'UE prendano in considerazione la possibilità di dichiarare gli scambi di valuta virtuale come

[184] BANCA CENTRALE EUROPEA, (2012), *Virtual Currency Scheme*s Disponibile in open source sul sito https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.
[185] AUTORITA' BANCARIA EUROPEA (2014). *Opinion on 'Virtual Currencies'*, EBA/Op/2014/ Disponibile in open source sul sito https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf.
[186] AUTORITA' BANCARIA EUROPEA, *Opinion on 'Virtual Currencies'*, cit. 153.

"entità obbligate" a rispettare le norme antiriciclaggio e antiterrorismo, come previsto dalla normativa in materia di riciclaggio di denaro.

1.2. (*Segue*): I cripto-asset come strumenti finanziari

Il MiFID II, regolamento di cui parleremo più specificatamente in seguito, definisce gli "strumenti finanziari" come "gli strumenti specificati nella sezione C dell'allegato I".[187] L'elenco della citata sezione C comprende *i*) valori mobiliari, *ii*) strumenti del mercato monetario, *iii*) quote di organismi di investimento collettivo e *iv*) vari strumenti derivati. Per evitare l'esclusione a priori delle criptovalute dalla categoria degli "strumenti finanziari", la Commissione europea ha proposto una modifica della definizione di cui sopra al fine di includere espressamente gli strumenti finanziari basati su *distributed ledger technology* (DLT)[188], insieme a un regime pilota sulle infrastrutture di mercato per tali strumenti.[189] La definizione modificata, una volta approvata, sarà la seguente: "strumento finanziario": "*gli strumenti specificati nella sezione C dell'Allegato I, compresi gli strumenti emessi tramite la tecnologia a libro mastro distribuito*". Inoltre, come vedremo in seguito, la proposta di regolamento MiCA esclude espressamente dal suo ambito di applicazione tutti i cripto-asset che si qualificano come strumenti finanziari, partendo dal presupposto che tali strumenti dovrebbero essere regolamentati ai sensi della vigente normativa finanziaria dell'UE (ad es. MiFID II/MiFIR, MAR).

Pertanto, soprattutto alla luce del crescente interesse del legislatore dell'UE per questo nuovo fenomeno, va da sé che determinare se un cripto-asset si qualifica come "strumento finanziario" ai sensi del MiFID II - e a quale classe di strumenti finanziari appartenga - è della massima importanza. In effetti, sono molte le implicazioni normative che derivano da tale qualificazione tra cui, ad esempio, l'applicabilità dei regimi MiFID II/MiFIR e MAR

[187] Articolo 4(1)(15) MiFID II
[188] Proposta di direttiva del Parlamento europeo e del Consiglio che modifica le direttive 2006/43/CE, 2009/65/CE, 2009/138/UE, 2011/61/UE, UE/2013/36, 2014/65/UE, (UE) 2015/2366 e UE/2016/2341, 2014/65/UE, (UE) 2015/2366 e UE/2016/2341 - COM(2020)596.
[189] Article 6(4) 4(1)(15) MiFID II

Procederemo quindi esaminando brevemente tutte le classi di strumenti finanziari nella sezione C dell'Allegato 1 al MiFID II, al fine di capire quali tipi di cripto-asset possono rientrare in tali categorie per poi proseguire con la normativa finanziaria europea che risulta rilevante ai fini della presente trattazione e per quindi delineare in modo chiaro il quadro normativo in materia di criptovalute.

I "titoli trasferibili" sono la prima categoria di strumenti finanziari elencati nella sezione C dell'allegato I del MiFID II. La definizione di "valori mobiliari" è inclusa nel MiFID II e gran parte degli atti finanziari dell'UE si rifanno a tale definizione. Ad esempio, come vedremo più avanti in dettaglio, il Regolamento 2017/1129 limita il suo ambito di applicazione materiale ai "titoli", identificati come gli strumenti finanziari che rientrano nella definizione di "valori mobiliari" ai sensi del MiFID II (ad eccezione degli strumenti del mercato monetario con scadenza inferiore a 12 mesi).[190] Più precisamente, il MiFID II fornisce innanzitutto una definizione generale di valori mobiliari ("le classi di valori mobiliari che sono negoziabili sul mercato dei capitali") ed esclude esplicitamente gli strumenti di pagamento dalla definizione di valori mobiliari. [191]

Se analizziamo il testo della definizione, noteremo che essa impiega tre criteri formali e due sostanziali per verificare se uno strumento finanziario può essere un valore mobiliare. I criteri formali sono: la trasferibilità[192], la standardizzazione e la negoziabilità. Mentre quelle sostanziali sono la non qualificazione come strumenti

[190] Articolo 2(1)(a) Regolamento (EU) 2017/1129

[191] Secondo la MiFID II, per "valori mobiliari" si intendono "*quelle classi di titoli che sono negoziabili sul mercato dei capitali, con l'eccezione di strumenti di pagamento, quali 1. le azioni di società e altri titoli equivalenti alle azioni di società, società di persone o altre entità, e certificati di deposito di azioni; 2. obbligazioni o altre forme di debito cartolarizzato, comprese le ricevute di deposito relative a tali titoli di credito, comprese le ricevute di deposito relative a tali titoli; 3. qualsiasi altro titolo che dia il diritto di acquisire o vendere uno di tali titoli trasferibili o che diano luogo a un regolamento in contanti determinato con riferimento a valori mobiliari, valute, tassi di interesse o rendimenti, materie prime o altri indici o misure*". - Articolo 4(1)(44) MiFID II.

[192] Trasferibilità significa che i titoli possono essere assegnati a un'altra persona, a prescindere dall'esistenza di certificati che registrano o documentano i titoli.

di pagamento, e la comparabilità del titolo con un elenco non esaustivo di esempi, come azioni e obbligazioni.

Il requisito della trasferibilità delle criptovalute viene rispettato nel momento in cui questo avviene su base contrattuale. Tuttavia, le restrizioni contrattuali se accompagnate da limitazioni tecniche privano le criptovalute della loro trasferibilità e pertanto, non saranno soggette alle leggi dell'Unione europea circa i titoli trasferibili. Pertanto, si sostiene che la normativa dovrebbe considerare fin dall'inizio le criptovalute come trasferibili per evitare una "scappatoia" circa la corretta applicazione della normativa.

In conformità alla definizione di MiFID II, i titoli devono essere "negoziabili su un mercato dei capitali". Mentre la trasferibilità si riferisce al mero fatto di trasmettere la proprietà, la negoziabilità riguarda la facilità con cui la proprietà può essere trasferita (di fatto, la negoziabilità implica la trasferibilità). Per fare chiarezza sul concetto di negoziabilità, la Commissione europea, nel documento Q&A sul MiFID, ha chiarito che se gli strumenti finanziari in questione sono di tipo tale da poter essere negoziati in un mercato regolamentato o in un sistema multilaterale di negoziazione, ciò costituirà un'indicazione conclusiva del fatto che si tratta di titoli trasferibili, anche se i singoli titoli in questione non sono effettivamente negoziati. Al momento i cripto-asset non sono scambiati su mercati regolamentati; sono invece scambiati su borse di criptovalute (come Bittrex, Kraken, o Coinbase). Ciò solleva la questione di dove tracciare la linea di demarcazione tra i mercati dei capitali e gli altri mercati. Gli scambi di criptovalute sembrano rientrare nell'ampia definizione di "mercato dei capitali" fornita dalla Commissione Europea[193], in quanto mettono in contatto interessi di acquisto e di vendita. Pertanto, sembra che i cripto-asset negoziati sulle borse cripto soddisfino il requisito di "negoziabilità" previsto dalla definizione di MiFID II. Se seguiamo l'approccio di cui sopra, i cripto-asset privi di una componente di investimento che comporti un rischio finanziario sotto forma di partecipazione agli utili o di un flusso diretto di pagamenti

[193] EUROPEAN COMMISSION, *Your Questions on MiFID*, Question N. 115, Disponibile in open source al sito https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/mifid-2004-0039-commission-questions-answers_en_0.pdf. – "*il concetto è ampio e intende includere tutti i contesti in cui l'acquisto e la vendita di interessi in titoli si incontrano*".

non possono soddisfare la definizione di "valori mobiliari". Di conseguenza, i token di puro investimento o i token ibridi con qualche componente di investimento sarebbero chiaramente negoziabili sui mercati dei capitali. Al contrario, token di pagamento puro (come il Bitcoin) non sarebbero classificati come valori mobiliari, in quanto la loro struttura è spesso decentralizzata e non esiste una relazione continua tra emittente e investitore.

1.3. (*Segue*): Regolamentazione dei cripto-asset che si qualificano come strumenti finanziari

Come abbiamo visto nel paragrafo precedente esistono alcune classi di cripto-asset che si caratterizzano per una significativa componente di investimento e per la quale possono essere considerati strumenti finanziari ai sensi della definizione di MiFID II e sono pertanto soggetti alla normativa finanziaria dell'UE. In questa sede esamineremo i principali atti legislativi dell'UE che regolano l'offerta e lo scambio di strumenti finanziari e le questioni derivanti dalla loro applicazione alle criptovalute, con particolare attenzione ai crypto-exchange.

Uno dei temi più discussi in merito alla regolamentazione delle criptovalute è il Regolamento (EU) 2017/1129.[194]Lo scopo del Regolamento è quello di armonizzare i requisiti per la redazione, l'approvazione e la distribuzione del prospetto da pubblicare quando gli strumenti finanziari vengono offerti al pubblico o ammessi alla negoziazione in un mercato regolamentato in uno Stato membro dell'UE.[195] Il prospetto deve contenere le informazioni necessarie che sono rilevanti per un investitore al fine di effettuare una valutazione informata degli strumenti finanziari e della situazione finanziaria dell'emittente.[196] Lo scopo principale del

[194] Regolamento (EU) 2017/1129 - Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32017R1129&from=DE. In merito vedi anche BELLINI E. (2019). *Il nuovo Regolamento Prospetto: le opportunità per un più facile ricorso al mercato dei capitali e una più effettiva armonizzazione dei processi a livello comunitario* Disponibile in open source sul sito https://www.rivistadirittosocietario.com/mercato-dei-capitali-processi-a-livello-comunitario

[195] Considerando 2 del Regolamento (EU) 2017/1129

[196] Articolo 6 del Regolamento (EU) 2017/1129

prospetto è quello di garantire un elevato livello di protezione dei consumatori e degli investitori, riducendo le asimmetrie tra emittente e investitori.[197]

Il Regolamento (EU) 2017/1129 è seguito dal MiFID II[198], entrato in vigore il 3 gennaio 2018, ha sostituito la precedente MiFID.[199] Il MiFID, regola i mercati finanziari nell'UE e crea un quadro normativo armonizzato per i mercati finanziari e per i servizi di investimento in tutti gli Stati membri dell'UE. Il MiFID II si concentra principalmente sulle imprese che forniscono servizi ai clienti legati a "strumenti finanziari" (azioni, obbligazioni, quote di organismi di investimento collettivo e derivati), e le imprese che forniscono servizi di investimento collettivo e derivati, e le sedi in cui tali strumenti sono negoziati (mercati regolamentati, sistemi multilaterali di negoziazione (MTF) e sistemi organizzati di negoziazione (OTF)).[200] Lo scopo principale della direttiva è quello di rafforzare la tutela degli investitori attraverso lo sviluppo e l'implementazione di mercati finanziari più efficienti e trasparenti.[201] In altre parole esso ricopre le seguenti aeree: le imprese di investimento, gli operatori del mercato[202], i fornitori di servizi di comunicazione

[197] Considerando 3 e 4 del Regolamento (EU) 2017/1129

[198] Direttiva 2014/65/EU del Parlamento europeo e del consiglio del 15 maggio 2014 relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE. Vedi anche CONSOB (2017). *Recepimento della direttiva 2014/65/UE (MiFID II) e attuazione del regolamento (UE) 600/2014 (MiFIR) modifiche al regolamento mercati*. Disponibile in open source sul sito http://www.assiomforex.it/archivioFiles/consultazione_mercati_20170731%20(1).pdf

[199] Direttiva 2004/39/CE del Parlamento europeo e del consiglio del 21 aprile 2004 relativa ai mercati degli strumenti finanziari, che modifica le direttive 85/611/CEE e 93/6/CEE del Consiglio e la direttiva 2000/12/CE del Parlamento europeo e del Consiglio e che abroga la direttiva 93/22/CEE del Consiglio. Disponibile in open source sul sito https://def.finanze.it/DocTribFrontend/getAttoNormativoDetail.do?ACTION=getSommario&id={2A93CD49-0F64-457C-BF51-B547802136B7}

[200] DÜR A., MARSHALL D., BERNHAGEN P., (2019) *The Political Influence of Business in the European Union*, University of Michigan Press, 92.

[201] QUATTROCCHIO M. L. (2019) *MiFID II e MiFIR. Il quadro europeo di riferimento*. Disponibile in open source sul sito *https*://www.dirittoeconomiaimpresa.it/mifidmifir-il-quadro-europeo-di-riferimento

[202] Per "operatori del mercato" si intende una o più persone che gestiscono e/o operano l'attività di un mercato regolamentato e può essere il mercato regolamentato stesso (articolo 4, paragrafo 1, punto 18, della MiFID II).

dati[203] e le imprese di paesi terzi che forniscono servizi di investimento o svolgono attività di investimento attraverso una filiale localizzata nel territorio nell'UE.

Il MiFID II definisce un'impresa di investimento come qualsiasi persona giuridica la cui occupazione o attività abituale è la prestazione di uno o più servizi di investimento a terzi e/o lo svolgimento di una o più attività di investimento a titolo professionale.[204] L'elemento centrale della definizione è il riferimento alla prestazione di servizi di investimento a terzi e alla prestazione di attività di investimento su base professionale.[205]

Tali servizi e attività di investimento sono elencati nella Sezione A dell'Allegato I alla MiFID II e comprendono, tra l'altro, il ricevimento e la trasmissione di ordini in relazione a uno o più strumenti finanziari, l'esecuzione di ordini per conto dei clienti, la negoziazione per conto proprio, la gestione del portafoglio, la consulenza in materia di investimenti, la sottoscrizione di strumenti finanziari e/o collocamento di strumenti finanziari su base "*firm committed*", il collocamento di strumenti finanziari senza un impegno irrevocabile, la gestione di un sistema multilaterale di negoziazione e la gestione di un sistema organizzato di negoziazione.

Soprattutto, tutti i servizi e le attività elencati devono riguardare uno degli strumenti finanziari inclusi nella sezione C dell'allegato I della MiFID II[206] (ossia valori mobiliari, strumenti del mercato monetario, quote di organismi di investimento collettivo e derivati). Pertanto, l'elenco degli strumenti finanziari e l'elenco dei servizi/attività di investimento sono gli strumenti principali per determinare l'ambito di applicazione della MiFID II e del MiFIR.[207]

---

[203]Per "fornitore di servizi di comunicazione dati" si intende un Approved Publication Arrangement (APA), un Consolidated Tape Provider (CTP) o un Approved Reporting Mechanism (ARM) (articolo 4(1)(63) MiFID II).

[204] Articolo 4(1)(1) MiFID II.

[205] LIEVERSE K. (2016). *The Scope of MiFID II, in Regulation of the EU Financial Markets: MiFID II and MiFIR*, Oxford University Press, 28.

[206] Article 4(1)(2) MiFID II. Financial instruments are defined in Article 4(1)(15) MiFID II as those specified in Section C of Annex I

[207] LIEVERSE K., *The Scope of MiFID II, in Regulation of the EU Financial Markets: MiFID II and MiFIR*, Oxford University Press, cit. 185

Il MiFIR[208] è strettamente correlato alla MiFID II e contiene regole e linee guida direttamente applicabili alle piattaforme di trading e alle imprese di investimento, che definiscono standard armonizzati anche sui requisiti di rendicontazione, trasparenza della sede di negoziazione (pre e post negoziazione) e obblighi di compensazione. In particolare, ai sensi del MiFIDII e MiFIR le imprese di investimento devono rispondere ad una serie di requisiti stabiliti dalla regolamentazione bancaria, con integrazioni specifiche per le caratteristiche peculiari delle attività/servizi di investimento.[209] In particolare, la complessa serie di requisiti di governo societario, che coprono molte aree come la gestione del rischio e le questioni retributive, ha lo scopo di ridurre il rischio sistemico indipendentemente dalla natura dell'attività dell'impresa di investimento.[210]

Il MiFID II dispone una serie di obblighi per le imprese di investimento, come requisiti patrimoniali minimi[211] che variano a seconda del tipo di servizi/attività svolti dall'impresa. Ad esempio, le imprese di investimento che gestiscono un sistema multilaterale di negoziazione o un sistema organizzato di negoziazione, o che negoziano per conto proprio, devono avere un capitale iniziale di almeno 730.000 euro. In aggiunta richiede anche il rispetto di requisiti organizzativi[212] in quanto le imprese di investimento devono disporre di adeguate politiche e procedure per garantire la conformità agli obblighi previsti dalla MiFID II, compresi quelli per la prevenzione dei conflitti di interesse, l'approvazione e la distribuzione di prodotti finanziari ai clienti, continuità operativa, integrità e sicurezza dei dati, tenuta dei registri, controlli interni e gestione del rischio.

---

[208] Regolamento (UE) N. 600/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 15 maggio 2014 sui mercati degli strumenti finanziari e che modifica il regolamento (UE) n. 648/2012 Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32014R0600&from=EN

[209] BINDER J., (2016). *Governance of Investment Firms under MiFID II*, in Regulation of the EU: MiFID II e MiFIR, a cura di D. BUSCH, G. FERRARINI, Oxford, 61.
University Press (2016), 61.

[210] BINDER J., *Governance of Investment Firms under MiFID II,* cit. 189

[211] Articolo 15 MiFID II.

[212] Articolo 16 MiFID II.

Il MiFID II prevede anche obblighi di rispetto dei requisiti di protezione degli investitori.[213] Questi includono disposizioni sia per identificare, prevenire e gestire i conflitti di interesse, sia per agire in modo onesto, equo e professionale in conformità con il miglior interesse dei clienti, per assicurare che tutte le informazioni rivolte agli stessi siano corrette, chiare e non fuorvianti, e eseguire gli ordini alle condizioni più favorevoli per i clienti.

Infine, richiede che le imprese mantengano dei registri delle operazioni[214] , segnalino qualsivoglia transazione sospetta alle autorità nazionali garanti della concorrenza[215] e dispongano che sia gli strumenti azionari che quelli non azionari siano soggetti a regole che disciplinano [216]la trasparenza pre-negoziazione dei prezzi di acquisto e di vendita, le deroghe alla trasparenza pre-negoziazione, le restrizioni a tali deroghe, la trasparenza post-negoziazione e le pubblicazioni differite.[217] I dati pre-negoziazione e post-negoziazione saranno messi a disposizione del pubblico separatamente su una base commerciale ragionevole e garantendo un accesso non discriminatorio; tali informazioni saranno poi rese disponibili gratuitamente quindici minuti dopo la pubblicazione.[218]

Tra le fonti normative di particolare interesse vi è anche il regolamento sugli abusi di mercato (*Market Abuse Regulation*, MAR) [219] il quale stabilisce un quadro normativo comune in materia di abuso di informazioni privilegiate, divulgazione illecita di informazioni privilegiate e manipolazione del mercato (abusi di mercato) nonché le misure di prevenzione degli abusi di mercato per garantire l'integrità dei

[213] Articoli 24-30 MiFID II.
[214] Articolo 25(1) MiFIR.
[215] Articolo 26 MiFIR.
[216] Articolo 18(3) MiFID II
[217] Articoli 3-11 MiFIR
[218] Articoli 12-13 MiFIR
[219] REGOLAMENTO (UE) N. 596/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 16 aprile 2014 relativo agli abusi di mercato (regolamento sugli abusi di mercato) e che abroga la direttiva 2003/6/CE del Parlamento europeo e del Consiglio e le direttive 2003/124/CE, 2003/125/CE e 2004/72/CE della Commissione. Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32014R0596

mercati finanziari nell'Unione europea e per migliorare la protezione degli investitori e la fiducia in tali mercati.[220]

La scelta di un regolamento invece che di una direttiva si basa sull'idea che un regolamento (che è auto esecutivo e direttamente applicabile agli Stati membri dell'UE) è lo strumento più appropriato per definire una materia delicata come gli abusi di mercato nell'UE.[221]

Il regolamento MAR deve essere letto insieme alla direttiva sugli abusi di mercato e sulle sanzioni penali[222], che definisce il quadro generale delle sanzioni penali per le violazioni dei divieti di MAR.[223]

Per quanto riguarda l'ambito di applicazione del regolamento, MAR si applica: *i)* agli strumenti finanziari ammessi alla negoziazione su un sistema multilaterale di negoziazione o per i quali è stata presentata una richiesta di ammissione alla negoziazione su un sistema multilaterale di negoziazione; *ii)* agli strumenti finanziari negoziati su un sistema multilaterale di negoziazione, ammessi alla negoziazione in un sistema multilaterale di negoziazione o per i quali è stata presentata una richiesta di ammissione alla negoziazione in un sistema multilaterale di negoziazione, *iii)* agli strumenti finanziari negoziati su un sistema organizzato di negoziazione; e *iv)* agli strumenti finanziari non coperti dalle lettere a), b) o c), il cui prezzo o valore dipende o ha un effetto sul prezzo o sul valore di uno strumento finanziario di cui ai suddetti punti.[224]

[220] Articolo 1 MAR. Vedi anche DÄSCHLER S. (2022). *Regolamento MAR: Il Regolamento sugli abusi di mercato dell'Unione Europea.* Disponibile in open source sul sito https://www.eqs.com/it/polo-di-conoscenza-compliance/blog/regolamento-mar/

[221] VENTORUZZO M., MOCK S. (2017). *Market Abuse Regulation – Commentary and Annotated Guide*, Oxford University Press, 4

[222] Directive 2014/57/EU DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 16 aprile 2014 relativa alle sanzioni penali in caso di abusi di mercato (direttiva abusi di mercato) - Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32014L0057&from=LT

[223] M. VENTORUZZO, S. MOCK, *Market Abuse Regulation – Commentary and Annotated Guide*, cit. 201

[224] Articolo 2(1) MAR

Le due forme di abuso di mercato descritte da MAR sono l'abuso di informazioni privilegiate e la manipolazione del mercato.

Se i cripto-asset si qualificano come strumenti finanziari, e a condizione che siano negoziati o ammessi alla negoziazione in una sede di negoziazione, si applicherà il MAR. In tal caso, la piattaforma di negoziazione (ossia la borsa delle criptovalute) dovrà disporre di disposizioni, sistemi e procedure efficaci volti a prevenire, individuare e segnalare gli abusi di mercato. Tuttavia, se i cripto-asset non si qualificano come strumenti finanziari, l'attività di negoziazione su di essi non rientrerebbe in teoria nell'ambito di applicazione di MAR. Questa lacuna normativa può comportare rischi rilevanti nelle situazioni in cui il prezzo di uno strumento finanziario (tradizionale) potrebbe essere influenzato da un'attività di trading manipolativa in cripto-asset non qualificabili come strumenti finanziari. Infine, data la novità dei mercati delle criptovalute, potrebbero emergere nuovi comportamenti abusivi che non sono stati presi in considerazione da MAR. Ad esempio, i nuovi partecipanti al mercato, come i minatori e i fornitori di portafogli, potrebbero detenere nuove forme di informazioni interne che potrebbero essere utilizzate per manipolare la negoziazione dei cripto asset.

Tra i diversi regolamenti in materia vi sono anche una serie di direttive relative agli strumenti finanziari tra cui la direttiva sugli organismi d'investimento collettivo in valori mobiliari (OICVM)[225] e la direttiva sui gestori di fondi d'investimento alternativi (AIFMD). [226] La prima crea un regime armonizzato in tutti gli Stati membri dell'UE per la gestione e la vendita di fondi comuni di investimento. A questo proposito, essa prevede le regole di base comuni per l'autorizzazione, la vigilanza, la struttura e le attività degli OICVM stabiliti negli Stati membri

[225] DIRETTIVA 2009/65/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 13 luglio 2009 concernente il coordinamento delle disposizioni legislative, regolamentari e amministrative in materia di taluni organismi d'investimento collettivo in valori mobiliari (OICVM) - Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32009L0065&from=SL

[226] Direttiva 2011/61/UE del parlamento europeo e del consiglio dell'8 giugno 2011
sui gestori di fondi di investimento alternativi, che modifica le direttive 2003/41/CE e 2009/65/CE e i regolamenti (CE) n. 1060/2009 e (UE) n. 1095/2010. Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32011L0061

dell'Unione europea e le informazioni che devono pubblicare.[227] La seconda si applica agli hedge fund, ai fondi di private equity, ai fondi immobiliari e, in generale, a tutti quei fondi che non si qualificano come OICVM.[228] La direttiva AIFMD mira a stabilire requisiti comuni per l'autorizzazione e la vigilanza dei gestori di fondi di investimento alternativi, stabilendo standard per la remunerazione, la responsabilità, raccolta di capitali privati e la rendicontazione dei rischi. Per poter vendere servizi finanziari nel mercato dell'UE, i gestori di fondi di investimento alternativi devono pertanto rispettare tutti i requisiti stabiliti dalla direttiva sui fondi di investimento alternativi. I due scopi principali della direttiva sono proteggere gli investitori attraverso un rigoroso regime di informazione (come la comunicazione dei conflitti di interesse e la valutazione indipendente delle attività) e ridurre il rischio sistemico per l'economia dell'Unione europea regolamentando, tra l'altro, le politiche retributive e la gestione del rischio.[229]

Il Regolamento sulle Infrastrutture dei Mercati Europei (EMIR) [230] stabilisce requisiti di compensazione e di gestione bilaterale del rischio per i contratti derivati over-the-counter (OTC), obblighi di segnalazione per tutti i contratti derivati, e requisiti uniformi per le attività delle controparti centrali (CCP) e dei depositi di dati sulle negoziazioni. L'EMIR mira a migliorare in modo sostanziale l'attenuazione del rischio di credito di controparte e migliorare la trasparenza, l'efficienza e l'integrità delle operazioni.[231] Le finalità sopra menzionate sono perseguite mediante la previsione di l'obbligo di segnalazione per entrambe le controparti, che devono riferire i dettagli di ogni operazione in derivati a uno dei

[227] Considerando 4, DIRETTIVA 2009/65/CE.
[228] Considerando 2 2011/61/UE
[229] STEFANIN G. E ZANIN M. (2013). *La Direttiva 2011/61/UE sui gestori di fondi di investimento alternativi: le discipline dei conflitti di interesse e degli obblighi di trasparenza* in DB non dolo diritto bancario. Disponibile in open source sul sito https://www.dirittobancario.it/art/direttiva-2011-61-ue-discipline-conflitti-di-interesse-obblighi-di-trasparenza/
[230] Regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio, del 4 luglio 2012, sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni - Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:02012R0648-20170103&qid=1491467027228&from=IT
[231] Considerando 9 E - Regolamento (UE) n. 648/2012

repertori di dati sulle negoziazioni;[232] obblighi di compensazione[233], che consistono nell'obbligo di compensare a livello centrale determinate categorie di over-the-counter (OTC)[234] attraverso una CCP, ossia una persona giuridica che si interpone tra le controparti,[235] e tecniche di attenuazione del rischio per i contratti derivati OTC non compensati da CCP, comprese le procedure e gli accordi per misurare, monitorare e mitigare il rischio di credito di controparte.[236]

1.4. (*Segue*): Regolamentazione UE delle valute virtuali

In tempi più recenti, l'Unione Europea ha presentato il cd. *Digital Finance Package*, che ricomprende il Regolamento Markets in Crypto-Assets (di seguito "MiCa"), ossia un testo di regolazione dei crypto-assets, in cui viene fornita una proposta di disciplina delle C.B.D.C. (*Central Bank Digital Currencies*), cioè la regolamentazione delle criptovalute emesse direttamente dalle Banche Centrali, delle *stablecoin* (criptovalute garantite da fondi) e degli utility token. Questo testo è stato recentemente discusso in occasione del G7 di Washington nell'ottobre 2021 durante il quale sono stati fissati tredici principi che le autorità centrali dovranno tenere debitamente in considerazione in caso di emissione di valute digitali a livello centrale.[237] Il testo del Regolamento MiCa, pur non essendo ancora entrato in vigore (presumibilmente entrerà in vigore il mese di luglio 2023), è stato recentemente approvato dal Consiglio europeo. La proposta era stata pubblicata dalla

[232] Articolo 9 E - Regolamento (UE) n. 648/2012

[233] Ai sensi dell'articolo 2, paragrafo 3, dell'EMIR, per "compensazione" si intende "*il processo di definizione delle posizioni, compreso il calcolo delle obbligazioni nette, e la garanzia della disponibilità di strumenti finanziari, di liquidità o di entrambi per assicurare le esposizioni derivanti da tali posizioni*".

[234] Per "derivato OTC" o "contratto derivato OTC" si intende un contratto derivato la cui esecuzione non avviene in un mercato regolamentato o in un mercato di un paese terzo considerato equivalente a un mercato regolamentato ai sensi della normativa UE (cfr. articolo 2, paragrafo 7, dell'EMIR). Vedi anche DI MAIO D. e POMPEI L. (2019). *EMIR refit: cosa cambia per le controparti non finanziarie in Risk & Compliance.* Disponibile in open source sul sito https://www.riskcompliance.it/news/emir-refit-cosa-cambia-per-le-controparti-non-finanziarie/

[235] Articolo 4 EMIR

[236] Articolo 11 EMIR

[237] CRYPTOECONOMY (2022). *Criptovalute: norme attuali e prossimi scenari*. Disponibile in open source sul sito https://www.agendadigitale.eu/cittadinanza-digitale/pagamenti-digitali/criptovalute-cosa-prevede-la-normativa-attuale-e-quali-sono-le-prospettive-future/.

Commissione Europea lo scorso 24 settembre 2020 al fine di rendere l'Europa pronta per l'era digitale e rendere l'economia Europea più all'avanguardia e rivolta al futuro. Le previsioni del regolamento si applicheranno soltanto alle cripto-attività, non qualificabili come strumenti finanziari e, quindi, non assimilabili a strumenti finanziari, depositi o depositi strutturati, cartolarizzazioni e moneta elettronica.[238]

Il MiCA fornisce innanzitutto una definizione generale di cripto-asset come

> "*una rappresentazione digitale di valore o di diritti che possono essere trasferiti e memorizzati elettronicamente, utilizzando la tecnologia del libro mastro distribuito o una tecnologia simile*".[239]

La proposta di regolamento identifica tre classi specifiche di cripto asset: *i)* "asset-referenced token" che si caratterizza per un valore stabile facendo riferimento a valute flat avente corso legale o ad una combinazione di attività;[240] *ii)* "gettone di moneta elettronica" o "token di moneta elettronica", qualificato come un cripto-asset utilizzato come mezzo di pagamento/scambio, il cui valore rimane stabile facendo riferimento ad una moneta legale; [241] *iii)* "utility token", che si propone di favorire l'accesso digitale ad un bene e/o servizio disponibile su DTL.[242]

Non vi sono dubbi sulla valenza che avrà il regolamento MICA sulla legislazione europea in materia, in quanto consentirà di uniformare ed armonizzare tra gli stati membri dell'UE alcune attività legate alle criptovalute che spaziano dall'emissione e negoziazione dei cripto-asset[243], alla vigilanza dei fornitori di servizi nonché alla regolamentazione amministrativa degli stessi, fino a prevedere una serie di norma volte a garantire la salvaguardia dei consumatori e ad evitare abusi di mercato.

---

[238] MATTASSOGLIO F. (2021). *Le proposte europee in tema di crypto-assets e DLT. Prime prove di regolazione del mondo crypto o tentativo di tokenizzazione del mercato finanziario (ignorando bitcoin),* Rivista di Diritto Bancario. Disponibile in open source sul sito https://rivista.dirittobancario.it/le-proposte-europee-tema-di-crypto-assets-e-dlt-prime-prove-di-regolazione-del-mondo-crypto-o

[239] Articolo 3(1)(2) MiCA.

[240] Articolo 3(1)(3) MiCA

[241] Articolo 3(1)(4) MiCA.

[242] Articolo 3(1)(5) MiCA.

[243] CRYPTOECONOMY (2022). *Criptovalute: norme attuali e prossimi scenari*, cit. 190.

Ulteriore passo in avanti compiuto dal MICA è rappresentato dalla circostanza che i fornitori di crypto asset dovranno avere la sede in uno dei paesi della UE per consentirne la supervisione e la vigilanza da parte delle autorità preposte.[244]
Appare opportuno segnalare che la nuova normativa andrà ad influire positivamente nei confronti degli utilizzatori dei crypto-asset in quanto per tutte le operazioni che saranno svolte con la moneta virtuale dovranno informazioni sia sul mittente che sul beneficiario dei trasferimenti per la sicurezza degli scambi. Nel complesso, il nuovo regolamento andrà ad evitare quelle situazioni che hanno comportato il fallimento di alcuni operatori di crypto-asset. Restano espressamente esclusi dall'ambito di applicazione del MiCA i cripto-asset che si qualificano come strumenti finanziari ai sensi della MiFID II. Così come non sono disciplinati i cripto-asset che si qualificano come moneta elettronica ai sensi della EMD2, tranne nel caso in cui si qualifichino come token di moneta elettronica ai sensi del MiCA.

Dal punto di vista soggettivo, saranno coinvolti dalla nuova regolamentazione i soggetti che si occupano dell'emissione di cripto-attività o che forniscono servizi a queste connessi all'interno dell'Unione, con alcune eccezioni per la BCE e le banche centrali nazionali degli Stati membri, in veste di autorità monetaria[245]; la Banca Europea degli Investimenti; il Meccanismo europeo di stabilità e il Fondo europeo di stabilità finanziaria; le organizzazioni internazionali pubbliche.[246] Circa l'applicazione soggettiva del regolamento se ne parlerà più approfonditamente nel successivo paragrafo relativo alla normativa relativa ai *Wallet provider*.

Tra gli atti normativi europei in tema di valute virtuali vi rientra anche la direttiva 110/2009/UE (cd. EMD2) che stabilisce le regole per le pratiche commerciali e la vigilanza degli istituti di moneta elettronica. La direttiva ha inteso gettare le basi per un mercato unico dei servizi di moneta elettronica nell'UE, allineare i requisiti dell'UE per i servizi di moneta elettronica e mettere in atto una serie coerente di

[244] MASI S., *V direttiva antiriciclaggio: obiettivi, ambito di riforma, modifiche*, cit. 188.
[245] BANCA D'ITALIA, *Quaderni di Ricerca Giuridica Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, cit 47.
[246] DB non solo diritto bancario (2022). *Regolamento MiCA sulle criptovalute: il testo approvato dal Consiglio UE*. Dirittobancario.it. Disponibile in open source sul sito https://www.dirittobancario.it/art/regolamento-mica-sulle-criptovalute-il-testo-approvato-dal-consiglio-ue/.

requisiti necessari ad ottenere una licenza come istituto di moneta elettronica. Lo scopo della citata direttiva è stato, inoltre, quello di facilitare l'accesso dei nuovi operatori al mercato della moneta elettronica. Sebbene la stragrande maggioranza delle criptovalute attualmente in uso (tra cui il Bitcoin) sembri essere esclusa dall'ambito di applicazione dell'EMD2, in teoria potrebbero esserci dei casi in cui, in base alle caratteristiche specifiche della criptovaluta in questione, un token di pagamento può qualificarsi come moneta elettronica e rientrare quindi nell'ambito di applicazione dell'EMD2. In tali casi, è necessaria un'autorizzazione come istituto di moneta elettronica per svolgere attività che coinvolgono la stessa.
L'EBA sottolinea che è essenziale effettuare una valutazione caso per caso, tenendo presente che le diverse criptovalute hanno caratteristiche molto diverse le une dalle altre e che si dovrebbe adottare un approccio dove prevale la sostanza sulla forma.

Alla luce di quanto sopra esposto, sembra che una parte significativa di attività che coinvolgono le criptovalute potrebbe non rientrare nell'ambito di applicazione dell'attuale normativa europea sui servizi finanziari. Di conseguenza, le attività che coinvolgono tali criptovalute non sono soggette a uno schema comune di regolamentazione nell'UE. Questo dà origine a potenziali problemi, tra cui quelli riguardanti la tutela dei consumatori e l'integrità del mercato. Inoltre, come sottolinea l'EBA, il fatto che una criptovaluta possa rientrare nell'ambito di applicazione dell'attuale normativa UE sui servizi finanziari, come abbiamo visto, non significa necessariamente che tutti i rischi siano efficacemente mitigati.

2. Regolamentazione dei *wallet provider*

Come abbiamo visto in precedenza, ai cripto-asset come strumenti finanziari o di pagamento e alle imprese che forniscono servizi di investimento si applica una serie dettagliata e completa di norme dell'UE.[247] Tuttavia, considerando che l'attuale quadro giuridico dell'UE non è stato concepito pensando a strumenti come i cripto-

[247] ESMA (2019). *Advice on Initial Coin Offerings and Crypto-Assets*, ESMA50-157- Disponibile in open source sul sito https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.

asset, le autorità nazionali garanti della concorrenza si trovano di fronte a molte sfide nell'interpretare la normativa esistente.[248] Inoltre, come evidenziato nel parere dell'ESMA, le autorità nazionali garanti della concorrenza hanno definito il termine "strumento finanziario" in modo diverso nel recepire la normativa vigente: alcuni hanno optato per un approccio restrittivo alla definizione di strumento finanziario, mentre altre hanno utilizzato un approccio più ampio.[249]

Ovviamente questo crea incertezza sia nella regolamentazione che nella vigilanza dei cripto asset. Un'ulteriore incertezza è generata dal fatto che solo una frazione dell'ampia gamma di cripto-asset attualmente esistenti si qualificherà probabilmente come strumento finanziario ai sensi della MiFID II o come strumenti di pagamento. Ciò significa che tutti i restanti cripto-asset sarebbero al di fuori della regolamentazione dell'UE e saranno quindi regolamentati dalle leggi nazionali, che potrebbero essere significativamente diverse da uno Stato membro dell'UE all'altro. Il risultato è che gli investitori potrebbero non essere in grado di distinguere tra i cripto-asset che rientrano nell'ambito di applicazione della regolamentazione finanziaria dell'UE e quelli che non lo sono.[250]

Considerando l'elevato grado di incertezza normativa, la stragrande maggioranza delle autorità nazionali, interpellate dall'ESMA, ha espresso l'opinione che tutti i crypto-asset dovrebbero essere soggetti a una qualche forma di regolamentazione.

Inoltre, l'incertezza nel mercato interno dell'UE è generata dal fatto che molti Stati membri dell'UE stanno discutendo circa l'introduzione di una normativa specifica per i cripto-asset. Al fine di mitigare tutti i rischi discussi, l'ESMA ha esortato i responsabili politici dell'UE a istituire un regime specifico per i cripto-asset che non si qualificano come strumenti finanziari.[251] La Commissione europea ha accolto con favore il parere dell'ESMA e ha adottato un approccio ampio allo

[248] HACKER P., THOMALE C., (2018). *Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law*, 15 European Company and Financial Law Review 645-696. Disponibile in open source sul sito http://dx.doi.org/10.2139/ssrn.3075820, 8.
[249] ESMA (2019). *Advice on Initial Coin Offerings and Crypto-Assets*, ESMA50-157, cit. 202
[250] ESMA (2019). *Advice on Initial Coin Offerings and Crypto-Assets*, ESMA50-157, cit. 202
[251] ESMA (2019). *Advice on Initial Coin Offerings and Crypto-Assets*, ESMA50-157, cit. 202

sviluppo futuro della finanza digitale[252] adottando il 24 settembre 2020 un nuovo pacchetto.[253]

Forse la parte più interessante e innovativa del pacchetto sulla finanza digitale dell'UE è rappresentata dalla proposta di un nuovo regolamento sui mercati dei cripto-asset (MiCA), già esposto, e una nuova proposta di regolamento su un regolamento pilota per le infrastrutture di mercato basate su *Distributed Ledger Technology* (Regolamento sulle infrastrutture DLT).[254]

Il regolamento sulle infrastrutture DLT si applicherebbe alle imprese che forniscono servizi di negoziazione e regolamento per titoli trasferibili tramite DLT, ed è aperto ai partecipanti al mercato che gestiscono "sistemi multilaterali di negoziazione" o "sistemi di regolamento titoli" che utilizzano la DLT.[255] Tali partecipanti al mercato devono essere autorizzati come imprese di investimento o gestori di mercato ai sensi della MiFID II o come operatori di mercato ai sensi del regolamento 909/2014 (CSDR).[256] Se tali requisiti sono soddisfatti, il partecipante al mercato può richiedere autorizzazione specifica nell'ambito del regime pilota ed essere esentato temporaneamente da alcune regole e obblighi.[257] Tale autorizzazione sarà concessa solo se il richiedente soddisfa una serie di requisiti speciali previsti dal Regime Pilota, tra cui alcune limitazioni sui titoli che saranno negoziati sull'infrastruttura di mercato, nonché alcune limitazioni di carattere

[252] ZETZSCHE D. A., ANNUNZIATA F., ARNER D. W., ROSS R. P., (2020). *The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy, European Banking Institute Working Paper Series No. 2020/77*, University of Luxembourg Law Working Paper Series No. 2020, 2. Disponibile in open source sul sito http://dx.doi.org/10.2139/ssrn.3725395.

[253] FINANCIAL STABILITY, FINANCIAL SERVICES AND CAPITAL MARKETS UNION, EUROPEAN COMMISSION (2020). *Communication on Digital Finance Package.* Disponibile in open source sul sito https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en.

[254] Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo ad un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito, COM(2020) 594 - Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0594&from=EN

[255] RINGE W., ROUF C., (2020) *The DLT Pilot Regime: An EU Sandbox, at Last!*, Oxford Business Law Blog Disponibile in open source sul sito https://www.law.ox.ac.uk/business-lawblog/blog/2020/11/dlt-pilot-regime-eu-sandbox-last.

[256] Regolamento 909/2014 (CSDR) - Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/LSU/?uri=celex:32014R0909

[257] RINGE W., ROUF C., *The DLT Pilot Regime: An EU Sandbox, at Last!*, cit. 210

generale, così come alcuni obblighi generali volti a prevenire i rischi derivanti dall'uso della DLT.[258]

Il MiCA, invece, si occupa di cripto-asset e mira a regolamentare i cripto-asset che sono attualmente al di fuori del campo di applicazione (come le stablecoin, precedentemente definite) e i loro fornitori di servizi nell'UE, a stabilire un regime di licenza unico in tutti gli Stati membri dell'UE e a stabilire regole uniformi per i fornitori di servizi e gli emittenti di cripto-asset a livello UE.

La particolare attenzione alla creazione di un quadro uniforme per i cripto-asset nell'UE è testimoniata anche dal fatto che la stessa ha optato per un regolamento (auto esecutivo e direttamente applicabile) piuttosto che per una direttiva al fine di evitare qualsiasi discrezionalità da parte degli Stati membri dell'UE nell'attuazione delle norme MiCA.[259] In linea con l'attuale regolamento UE sui valori mobiliari, le autorità competenti per lo svolgimento delle funzioni e dei compiti previsti dal regolamento MiCA saranno designate dagli Stati membri dell'UE a livello nazionale.[260] Le autorità nazionali competenti (ANC) cooperano tra loro[261], con l'ESMA e con l'Autorità europea degli strumenti finanziari e dei mercati (AESFEM) per tutti gli scopi del regolamento. Nello svolgimento di queste funzioni, l'ESMA e l'EBA possono avvalersi di un'ampia gamma di poteri che comprendono, tra l'altro, la richiesta di informazioni alle ANC, il coordinamento delle ispezioni e delle indagini transfrontaliere e la risoluzione delle controversie tra le ANC.[262]

Il regolamento MiCA si applica alle:

[258] RINGE W., ROUF C., *The DLT Pilot Regime: An EU Sandbox, at Last!*, cit. 210.
[259] CARRIÈRE P. (2020), *Crypto-assets: le proposte di regolamentazione della Commissione UE. Opportunità e sfide per il mercato italiano*, Diritto Bancario. Disponibile in open source sul sito https://www.dirittobancario.it/art/crypto-assets-le-proposte-diregolamentazione-della-commissione-ue-opportunita-e-sfide-il-mercato-italia/
[260] Articolo 81(1) MiCA.
[261] Articolo 83(1) MiCA.
[262] Articoli 83 e 84 MiCA.

"*persone che sono impegnate nell'emissione di cripto-asset o che forniscono servizi relativi a cripto-asset nell'Unione*".[263]

Tuttavia, alcune categorie di cripto-asset sono espressamente escluse dall'ambito di applicazione di cui sopra, come ad esempio gli strumenti finanziari come definiti ai sensi della direttiva MiFID II e la moneta elettronica come definita dalla EMD2.

Inoltre, la normativa MiCA non si applica ad alcune categorie di enti e persone, quali *i)* la Banca Centrale Europea, le banche centrali nazionali dell'UE e le banche centrali nazionali dell'UE quando agiscono in qualità di autorità monetaria, o altre autorità pubbliche, *ii)* persone che offrono servizi di cripto-asset esclusivamente per le loro società madri, controllate o altre controllate delle loro società madri, e *iii*) organizzazioni pubbliche internazionali.[264]

Gli emittenti di cripto-asset (diversi dai token con riferimento all'attività o dai token di moneta elettronica) devono pubblicare un *white token* ossia un libro bianco per offrire cripto-asset al pubblico o richiedere l'ammissione a una piattaforma di trading per cripto-asset.[265]

La proposta di regolamento prevede esenzioni nel caso in cui i cripto-asset siano[266] offerti gratuitamente, creati automaticamente attraverso l'estrazione mineraria come ricompensa, unici e non fungibili con altri cripto-asset, offerti a un numero di persone fisiche o giuridiche inferiore a 150 per Stato membro dell'UE, nell'arco di un periodo di 12 mesi, offerti al pubblico nell'UE per un corrispettivo totale non superiore a € 1.000.000 (o importo equivalente in un'altra valuta o in criptovaluta), ovvero rivolti esclusivamente a investitori qualificati (e i cripto-asset possono essere detenuti solo da tali investitori qualificati).[267]

[263] Articolo 2(1) MiCA.
[264] Articolo 2(3) MiCA. Vedi anche CARRIÈRE P, *Crypto-assets: le proposte di regolamentazione della Commissione UE. Opportunità e sfide per il mercato italiano*, cit. 215.
[265] Articolo 4(1) MiCA.
[266] MASSIMILIANO N. (2019). *Il regime giuridico delle ICOs. Analisi comparata e prospettive regolatorie italiane*, Diritto Bancario.
[267] Articolo 4(2) MiCA.

L’insieme delle norme previste dal MiCA per gli emittenti della categoria generale di criptovalute riflette sia le prassi consolidate del mercato sia le attuali leggi dell’Unione europea in materia (in particolare il regolamento sui prospetti, la MiFID II/MiFIR e il MAR).[268] In effetti, la previsione di un libro bianco costituiva già una pratica comune tra gli emittenti di token.

Il *white paper* deve contenere una serie di informazioni, tra cui una descrizione dettagliata dell’emittente, del progetto dell’emittente, del tipo e delle ragioni di cripto asset che sarà offerto al pubblico o per il quale si chiede l’ammissione alla negoziazione, dell’uso previsto della valuta fiat o di altri cripto-asset raccolti tramite l’offerta al pubblico, delle caratteristiche dell’offerta al pubblico, dei diritti e degli obblighi connessi ai cripto-asset e dei rischi relativi all’offerta al pubblico di cripto-asset.[269]

Inoltre, laddove l’offerta al pubblico di cripto-asset riguarda token di utilità per un servizio non ancora in funzione, la durata dell’offerta al pubblico descritta nel libro bianco non deve superare i dodici mesi.[270]

Il MiCA regolamenta anche le comunicazioni di marketing relative alle offerte di cripto-asset, che devono essere, tra l’altro, chiaramente identificabili come tali, corrette, chiare e non fuorvianti, coerenti con le informazioni contenute nel libro bianco e indicare chiaramente che è stato pubblicato un libro bianco insieme all’indirizzo del sito web dell’emittente.[271]

Gli emittenti di cripto-asset dovranno notificare il libro bianco, unitamente a comunicazioni di marketing (se presenti), all’autorità nazionale garante della concorrenza del proprio Stato membro d’origine[272] almeno venti giorni lavorativi

---

[268] ANNUNZIATA F. (2020) *Verso una disciplina europea delle cripto-attività. Riflessioni a margine della recente proposta della Commissione UE*, Diritto Bancario. Disponibile in open source sul sito http://www.dirittobancario.it/approfondimenti/fintech/verso-una-disciplinaeuropea-delle-cripto-attivita-riflessioni-margine-recente-proposta-commissione.

[269] Articolo 5(1) MiCA.

[270] Articolo 4(3) MiCA.

[271] Articolo 6 MiCA.

[272] Ai sensi dell'articolo 3, comma 1, punto 22, lett. (a), (b) e (c) MiCA, “Stato membro d'origine” in relazione agli emittenti di cripto-asset diversi dai token con riferimento agli asset o elettronici gettoni monetari significa: (i) dove l'emittente ha la propria sede legale o una succursale nell'UE, lo

prima della pubblicazione del libro bianco;[273] essi dovranno anche spiegare le ragioni per cui tali cripto-asset non rientrano in nessuna delle esenzioni MiCA.[274]

Né il libro bianco né le comunicazioni al mercato sono soggetti ad alcun controllo o approvazione da parte delle NCA.[275] Tuttavia, le autorità nazionali per la concorrenza sono dotate di una serie di poteri di vigilanza e di indagine per adempiere ai loro doveri, tra cui quello di vietare o sospendere un'offerta di cripto-asset al pubblico o un'ammissione alla negoziazione, qualora riscontrino una violazione della normativa MiCA o qualora ci siano ragionevoli motivi per sospettare che sia stata violata.[276]

Sembra che la logica alla base della scelta di escludere qualsiasi controllo *ex ante* sui white paper sia quella di evitare un onere eccessivo per le ANC; tuttavia, un mero potere di intervento *ex post* potrebbe non essere sufficiente a garantire adeguati livelli di integrità e affidabilità dei mercati delle criptovalute.[277]

Gli emittenti di cripto-asset dovranno quindi pubblicare il loro libro bianco e - se del caso - le loro comunicazioni di marketing sul loro sito web (che dovrà essere accessibile al pubblico) entro e non oltre la data di inizio dell'offerta al pubblico di tali cripto-asset o della loro ammissione alla negoziazione.[278] Una volta pubblicato il libro bianco sul sito web dell'emittente, tali cripto-asset possono essere offerti o ammessi alla negoziazione in tutti gli Stati membri dell'UE. Gli emittenti dovranno solo fornire all'autorità nazionale garante della concorrenza dello Stato membro

---

Stato membro dell'UE in cui ha sede legale l'emittente di cripto-asset o a succursale, o (ii) se l'emittente non ha sede legale nell'UE ma ne ha due o più succursali UE, lo Stato membro UE scelto dall'emittente tra quelli membri UE Stati in cui l'emittente ha succursali o (iii) in cui l'emittente è stabilito in un terzo paese e non ha succursale nell'Unione, a scelta di tale emittente, né nell'UE Stato membro in cui le cripto-attività sono destinate ad essere offerte al pubblico per il prima volta o lo Stato membro dell'UE in cui è stata presentata la prima domanda di ammissione alle negoziazioni viene creata una piattaforma di trading per cripto-asset.

[273] Articolo 7(2) MiCA.

[274] Articolo 7(3) MiCA.

[275] Articolo 7(1) MiCA.

[276] Articoli 82(1)(o) e 82(1)(p) MiCA Vedi anche STIEFMUELLER C.M. (2021). *One born every minute: Striking the balance between promoting innovation and protecting citizens. An analysis of the EU Digital Finance Package.*

[277] ANNUNZIATA F., *Verso una disciplina europea delle cripto-attività. Riflessioni a margine della recente proposta della Commissione UE*, cit. 224.

[278] Articolo 8(1) MiCA.

d'origine l'elenco degli Stati membri ospitanti[279]in cui intendono offrire al pubblico i loro cripto-asset o intendono chiedere l'ammissione alla negoziazione.[280]

Gli emittenti di cripto-asset modificheranno il loro white paper di cripto-asset pubblicato e le comunicazioni di marketing (se esistenti) per descrivere qualsiasi cambiamento o nuovo fatto che possa avere un'influenza significativa sulla decisione di acquisto, vendita o scambio di un potenziale investitore.[281] L'emittente informerà immediatamente il pubblico sul proprio sito web della notifica di un white paper modificato con l'autorità nazionale garante della concorrenza e del mercato del suo Stato membro d'origine e fornire una sintesi dei motivi alla base di tale richiesta modifica.[282]

Il regolamento MiCA prevede anche un diritto di recesso obbligatorio che gli emittenti di cripto-asset offriranno a qualsiasi consumatore che acquisti tali cripto-asset direttamente dall'emittente o da un fornitore di servizi di cripto asset che provvede a collocarli per conto di tale emittente; pertanto, il diritto non si applica nel caso in cui i cripto asset siano ammessi alla negoziazione su una piattaforma di negoziazione. I consumatori devono avere un periodo di quattordici giorni di calendario per recedere dal proprio consenso all'acquisto di cripto-asset senza sostenere alcun costo e senza fornire motivazioni.[283]

Gli emittenti sono inoltre soggetti a una serie di obblighi, quali agire onestamente, in modo corretto e professionale, prevenire, identificare, gestire e divulgare eventuali conflitti di interesse, agire nel migliore interesse dei detentori di

[279] Ai sensi dell'articolo 3, paragrafo 1, punto 23, MiCA, per "Stato membro ospitante" si intende lo Stato membro dell'UE Stato in cui un emittente di cripto-asset ha fatto un'offerta al pubblico di cripto-asset o sta cercando l'ammissione al trading su una piattaforma di trading per cripto-asset, o dove a fornitore di servizi di cripto-asset fornisce servizi di cripto-asset, se diverso da Stato membro di origine.
[280] LUCEV R., BONCOMPAGNI F. (2018). *Criptovalute e profili di rischio penale nella attività degli exchanger*, Giurisprudenza Penale, 2018.
[281] Articolo 11(1) MiCA.
[282] Articolo 11(2) MiCA
[283] Articolo 12(1) MiCA.

criptovalute e con parità di trattamento, e restituire i fondi raccolti da acquirenti in caso di annullamento dell'offerta.[284]

Inoltre, l'emittente deve disporre di accordi efficaci per monitorare e salvaguardare i fondi; a tale riguardo, assicura che tutti i fondi e i cripto-asset raccolti durante l'offerta siano tenuti in custodia da un istituto di credito o un cripto-depositario.[285]

Infine, la proposta di regolamento introduce un regime di responsabilità per gli emittenti per le informazioni fornite nel white paper. Infatti, se l'informazione inclusa nel white paper è fuorviante o non è completa, giusta o chiara, il detentore di cripto-asset può chiedere il risarcimento dei danni all'emittente o alla sua direzione per i danni cagionati da detta violazione,[286] fermo restando che la presente disposizione non esclude ulteriori rivendicazioni di responsabilità civile. L'onere della prova ricade sui detentori di cripto-asset, i quali devono dimostrare la violazione dell'articolo 5 del MiCA (che disciplina il contenuto e la forma del libro bianco) e che l'infrazione ha avuto un impatto sulla loro decisione di acquistare, vendere o scambiare le suddette cripto-attività.[287]

2.1 (*Segue):* Obblighi per i fornitori di servizi di crypto-asset

Ai sensi del MiCA, i fornitori di servizi di cripto-asset saranno soggetti a regime di licenza e vigilanza che rispecchia in una certa misura la MiFID II, creando una sorta di "mini-MiFID" per i cripto-asset.[288]

In particolare, il Regolamento MiCA definisce servizi crypto-asset come uno dei seguenti servizi e attività relative a qualsiasi crypto-asset: *i)* la custodia e l'amministrazione di crypto-asset per conto di terzi, *ii)* il funzionamento di una

[284] Articolo 13 MiCA.
[285] Articolo 9(2) MiCA.
[286] Articolo 14(1) MiCA.
[287] Articolo 14(2) MiCA. Vedi anche ANNUNZIATA F., *Verso una disciplina europea delle cripto-attività. Riflessioni a margine della recente proposta della Commissione UE*, cit. 224.
[288] KLINGENBRUNN D., BENZING M., MCQUAID E., (2020) *Observations on the Commission's proposal for a European crypto-assets framework, Lexology*. Disponibile in open source sul sito https://www.lexology.com/library/detail.aspx?g=6a409f79-a121-4acb-a644- b6adc674e605.

piattaforma di trading per crypto-asset, *iii)* lo scambio di crypto-asset per fiat valuta che è legale tender, *iv)* lo scambio di crypto-assets per altri crypto-assets, *v)* l'esecuzione di ordini per criptovalute per conto di terzi, *vi)* collocamento di criptovalute, *vii)* la ricezione e la trasmissione di ordini per criptovalute per conto di terzi parti, e *viii)* fornire consulenza su crypto-assets.[289]

In primo luogo, i servizi di criptovaluta sono forniti solo da persone giuridiche che hanno una sede legale in uno Stato membro dell'UE e sono stati autorizzati come servizio crypto-asset provider.[290] L'autorizzazione per offrire un servizio crypto-asset è valido per l'intera UE e consente di fornire il servizio di crypto-asset in tutti gli Stati membri dell'UE.[291]

La domanda è presentata all'ANC dello Stato membro dell'UE dove il fornitore di servizi di crypto-asset ha il suo ufficio registrato.[292] Entro tre mesi dalla data di ricezione di una domanda completa, l'ANC valuterà se il fornitore di servizi di crypto-asset richiedente soddisfa i requisiti necessari ed emetterà la propria decisione di consenso e diniego.[293]

Le ANC informano l'ESMA di tutte le autorizzazioni concesse a crypto-asset per consentire all'ESMA di esercitare un controllo su tali autorizzazioni in conformità dei suoi compiti di vigilanza. A tale riguardo, l'ESMA può chiedere informazioni per garantire che le ANC concedono autorizzazioni.[294] Inoltre, l'ESMA istituisce un registro di tutti i fornitori di servizi di criptovaluta, che è accessibile al pubblico sul suo sito web e che deve essere aggiornato su base regolare.[295]

---

[289] Articolo 3(1)(9) MiCA. Vedi anche CARRIÈRE P, *Crypto-assets: le proposte di regolamentazione della Commissione UE. Opportunità e sfide per il mercato italiano*, cit. 215.
[290] Articolo 53(1) MiCA.
[291] Articolo 53(4) MiCA.
[292] Articolo 54(1) MiCA.
[293] Articolo 54(5) MiCA.Vedi anche ANNUNZIATA F., ZETZSCHE D. A., ARNER D. W., BUCKLEY R. P., (2020). *The markets in crypto-assets regulation (MICA) and the EU digital finance strategy, European Banking Institute*, Law Working Paper Series, Paper n.018, 2020
[294] Articolo 54(6) MiCA.
[295] Articolo 57(1) MiCA. Vedi anche ANNUNZIATA F., ZETZSCHE D. A., ARNER D. W., BUCKLEY R. P., *The markets in crypto-assets regulation (MICA) and the EU digital finance strategy, European Banking Institute*, cit. 249.

Le ANC revocano l'autorizzazione in una serie di situazioni specifiche come per esempio quando il fornitore di servizi non ha utilizzato la sua autorizzazione entro 18 mesi dalla data in cui è stato concesso, o ha espressamente rinunciato alla sua autorizzazione, ovvero non ha fornito servizi di crypto-asset per nove mesi consecutivi, o ha ottenuto l'autorizzazione con mezzi irregolari, oppure non soddisfa più le condizioni alle quali l'autorizzazione è stata concessa, o ha violato gravemente il regolamento MiCA.[296]

I fornitori di servizi di crypto-asset sono quindi soggetti a una serie di obblighi organizzativi e prudenziali modellati sui requisiti prescritta dalla MiFID II per le imprese di investimento.

In primo luogo, i fornitori di servizi di crypto-asset agiscono in modo onesto, equo e professionalmente in conformità con i migliori interessi dei loro clienti e potenziali clienti, e devono interagire con loro in modo equo, chiaro e non fuorviante.[297] Inoltre, essi devono, in ogni momento, rispettare alcune prescrizioni in termini di requisiti patrimoniali minimi, sotto forma di fondi propri o una polizza assicurativa che copre i territori dell'UE in cui i servizi crypto-asset sono attivamente forniti (o una garanzia paragonabile).[298]

Inoltre, particolare attenzione è rivolta alle misure volte a garantire la continuità e regolarità nelle prestazioni dei servizi di crypto-asset. A tal fine, i fornitori di servizi impiegano risorse adeguate e proporzionate e procedure, compresi sistemi TIC resilienti e sicuri[299], e hanno meccanismi interni di controllo e procedure efficaci per la valutazione dei rischi[300] e atti a monitorare e rilevare abusi di mercato.[301]

I fornitori di servizi crypto-asset devono notificare alle loro autorità competenti le eventuali modifiche occorse al loro organo di gestione e fornire all'autorità

[296] Articolo 56(1) MiCA. Vedi anche ANNUNZIATA F., ZETZSCHE D. A., ARNER D. W., BUCKLEY R. P., *The markets in crypto-assets regulation (mica) and the EU digital finance strategy, European Banking Institute* cit. 249.
[297] Articolo 59 MiCA
[298] Articolo 60 MiCA.
[299] Articolo 61(6) MiCA
[300] Articolo 61(7) MiCA.
[301] Articolo 61(9) MiCA. Vedi anche CARRIÈRE P, *Crypto-assets: le proposte di regolamentazione della Commissione UE. Opportunità e sfide per il mercato italiano*, cit. 215.

competente tutte le informazioni necessarie per valutare il rispetto dei requisiti organizzativi.[302]

Inoltre, i fornitori di servizi di criptovaluta sono soggetti a un numero di altri obblighi prudenziali, tra cui adottare disposizioni adeguate a salvaguardare i diritti di proprietà dei clienti e impedire l'uso da parte un cliente di crypto-asset per conto proprio, tranne con il cliente su espresso consenso,[303] stabilire e mantenere procedure efficaci e trasparenti per trattamento tempestivo, equo e coerente dei reclami ricevuti dai clienti,[304] mantenere e gestire una politica efficace per prevenire, identificare, gestire e rilevare i conflitti di interesse tra loro e i loro azionisti, dirigenti, dipendenti e clienti,[305]e più in generale, adottare tutte le misure ragionevoli per evitare rischio operativo aggiuntivo quando si affidano a terzi per l'esecuzione di funzioni operative (in ogni caso, i fornitori di servizi di crypto-asset rimangono pienamente responsabili per l'esecuzione di tutti i loro obblighi).[306]

2.2 (*Segue*): Responsabilità penale dei *Wallet provider*

Il proliferare delle criptovalute nonché dei gestori e fornitori di tali servizi ha comportato al contempo anche un loro utilizzo al fine di commettere attività criminose rendendo quindi necessario un irrobustimento del presidio penalistico.[307] In particolare, il legislatore europeo è intervenuto al fine di perseguire tutte quelle condotte criminose che constano di un utilizzo indebito e della falsificazione delle criptovalute ovvero, dell'acquisizione illecita e trasferimento fraudolento delle stesse fino ad arrivare a punire anche la detenzione e la diffusione di dispositivi utili a commettere reati nonché l'esercizio abusivo da parte dei prestatori di servizi di

[302] Articolo 62 MiCA.
[303] Articolo 63 MiCA.
[304] Articolo 64 MiCA.
[305] Article 65 MiCA.
[306] Articolo 66 MiCA. Vedi anche CARRIÈRE P, *Crypto-assets: le proposte di regolamentazione della Commissione UE. Opportunità e sfide per il mercato italiano*, cit. 215.
[307] NADDEO M. (2022). *Criptovalute: profili di rilevanza penale* in Penale diritto e procedura. Disponibile in open source sul sito https://www.penaledp.it/criptovalute-profili-di-rilevanza-penale/

crypto asset ai quali oggi possono essere ascritti l'eventuale violazione anche degli obblighi in materia di antiriciclaggio.[308]

Insomma, un pacchetto sanzionatorio complesso e caratterizzato da una tutela preventiva costruita su più livelli.[309]

Per il perseguimento degli illeciti riconducibili alle criptovalute è necessaria la

> "*possibile connessione con fenomeni criminali caratterizzati dall'utilizzo di tecnologie informatiche quali phishing o ransomware, con truffe realizzate attraverso siti Internet o clonazione di carte di credito, ovvero al sospetto di reimpiego di fondi derivanti da attività commerciali non dichiarate, spesso svolte online. Rilevano, altresì, gli acquisti di Virtual asset con fondi che potrebbero derivare da frodi, distrazioni di fondi o schemi piramidali*".[310]

Da un lato, gran parte delle condotte commesse con l'utilizzo delle criptovalute vengono fatte rientrare nelle fattispecie già disciplinate dal Codice Penale (artt. 615-ter (accesso abusivo ad un sistema informatico o telematico[311]), 615-quater (detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici[312]), 617-quinquies (installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche[313]) e 635-bis (danneggiamento di informazioni, dati e programmi informatici)[314]). Dall'altro lato,

---

[308] VADALÀ R. M. (2020). *La disciplina penale degli usi e degli abusi delle valute virtuali*, in *Diritto e internet*, n. 3/2020, pp. 397 ss.

[309] PICOTTI L., (2011). *Sicurezza, informatica e diritto penale*, in M. Donini, M. Pavarini (a cura di), *Sicurezza e diritto penale*, BUP, Bologna, pagg. 217 ss.; SALVADORI I. (2017). *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software"*, in Riv.it. di dir. proc. pen., 2/2017, pagg. 757 ss.

[310] Così, testualmente, la Comunicazione dell'Unità nazionale d'informazione finanziaria UIF del 28 maggio 2019. Disponibile in open source sul sito *https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Comunicazione_VV_2019.pdf*.

[311] Art. 615-ter – Disponibile in open souce sul sito https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-iii/sezione-iv/art615ter.html

[312] Art. 615-quater - Disponibile in open souce sul sito https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-iii/sezione-iv/art615quater.html

[313] Art. 617-quinquies - Disponibile in open souce sul sito https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-iii/sezione-v/art617quinquies.html

[314] Art. 635-bis - Disponibile in open souce https://www.brocardi.it/codice-penale/libro-secondo/titolo-xiii/capo-i/art635bis.html

le condotte dei cybercriminali frequentemente sono caratterizzate da una natura estorsiva (art. 629 c.p.[315]), connesse alla diffusione di malware, che, come vedremo anche nel prossimo capitolo, consentono al reo l'accesso e il furto di dati della vittima, alla quale spesso viene richiesto un riscatto in Bitcoin.[316]

In altre parole, vi sono condotte criminose disciplinate dal Codice penale che non per forza avvengono mediante l'utilizzo di criptovalute ma spesso costituiscono il solo fine del reato.[317]

Tuttavia, con l'entrata in vigore del Decreto legislativo 8 novembre 2021, n. 184[318] sono stati disciplinati reati che vengono commessi mediante strumenti di pagamento diversi dai contanti che vengono puniti in caso di indebito utilizzo e falsificazione (art. 493-ter c.p.)[319] oppure in caso di trasferimento mediante frode informatica (art. 640-ter c.p.).[320]

Ad ogni modo, l'illecito utilizzo delle criptovalute è prevalentemente connesso al reato di riciclaggio. Difatti, dall'analisi delle operazioni ritenute sospette si evidenziano flussi di

> "*un'operatività finanziaria apparentemente connessa all'acquisto di Bitcoin da parte di soggetti indagati per i reati di traffico di stupefacenti, riciclaggio e auto-riciclaggio. L'operatività sui conti loro intestati si caratterizza da un lato per i frequenti e rilevanti versamenti e prelevamenti di contante non giustificati dalle attività da loro svolte e, dall'altro, per i numerosi bonifici da e verso società estere specializzate nella compravendita di criptovalute e conti correnti di cui*

[315] Art. 629 c.p. - Disponibile in open souce sul sito https://www.brocardi.it/codice-penale/libro-secondo/titolo-xiii/capo-i/art629.html

[316] BONCOMPAGNI F. (2021). *Crimini informatici e criptovalute*, in S. Capaccioli (a cura di), *Criptoattività, criptovalute e bitcoin*, Giuffrè, Milano, pagg. 302 ss.

[317] NADDEO M. (2022). *Criptovalute: profili di rilevanza penale,* cit. 293.

[318] Decreto legislativo 8 novembre 2021, n. 184 - Disponibile in open source sul sito https://www.gazzettaufficiale.it/eli/id/2021/11/29/21G00200/sg

[319] Art. 493-ter c.p. - Disponibile in open souce sul sito https://www.brocardi.it/codice-penale/libro-secondo/titolo-vii/capo-iii/art493ter.html

[320] NADDEO M. (2022). *Criptovalute: profili di rilevanza penale,* cit. 263. Vedi art. 640-ter c.p. - Disponibile in open source sul sito https://www.brocardi.it/codice-penale/libro-secondo/titolo-xiii/capo-ii/art640ter.html

sono titolari persone residenti all'estero coinvolte negli stessi procedimenti penali".[321]

Pertanto, il legislatore consapevole di tali problemi è intervenuto da ultimo mediante la Direttiva (UE) 2018/843, c.d. V direttiva antiriciclaggio, precedentemente analizzata, implementando gradualmente la normativa in materia di utilizzo del sistema finanziario a scopo di riciclaggio, aggiungendo nella categoria degli "altri operatori non finanziari" anche "i prestatori di servizi relativi all'utilizzo di valuta virtuale" e "i prestatori di servizi di portafoglio digitale". Tale direttiva è stata implementata in Italia con il D.lgs. 231/2007[322], il quale definisce rispettivamente gli *Exchanger* e i *Wallet provider* come:

"*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*";[323]

"*ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*".[324]

Così facendo, tali figure vengono fatte soggiacere agli obblighi antiriciclaggio *ex* art. 3, comma 5, lettere i) e i-bis) del D.lgs. 231/07, che quindi trova applicazione anche in caso di operazioni mediante valuta virtuale e più precisamente in quanto

[321] Rapporto annuale UIF, Comunicazione cit., pagg. 47 s. – Vedi anche NADDEO M. (2022). *Criptovalute: profili di rilevanza penale,* cit. 293.

[322] D.lgs. 231/2007 - Disponibile in open source sul sito https://www.gazzettaufficiale.it/eli/id/2007/12/14/007X0246/sg

[323] Art. 1, comma 2, lett. ff) del D.lgs. 231/2007

[324] Art. 1, comma 2, lett. ff-bis) del D.lgs. 231/2007

> "*la rappresentazione digitale di valore, non emessa, né garantita 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 o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente*".[325]

L'inserimento dei *Wallet provider* tra i soggetti destinatari della normativa è dovuto al fatto che l'attività illecita mediante criptovalute può facilmente avvenire anche senza il coinvolgimento esteso al *Wallet provider* e quindi anche senza un processo di conversione della stessa valuta.[326] Pertanto, essendo la figura del *Wallet provider* fondamentale nel monitoraggio delle operazioni e preposta a conferire agli utenti i portafogli digitali che favoriscono le operazioni di raccolta e trasferimento delle valute si è ritenuto necessario applicare tale normativa anche a tali categorie di soggetti. Difatti, il legislatore europeo ha affermato che

> "*I prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso legale (vale a dire le monete e le banconote considerate a corso legale e la moneta elettronica di un paese, accettate quale mezzo di scambio nel paese emittente) e i prestatori di servizi di portafoglio digitale non sono soggetti all'obbligo dell'Unione di individuare le attività sospette. Pertanto, i gruppi terroristici possono essere in grado di trasferire denaro verso il sistema finanziario dell'Unione o all'interno delle reti delle valute virtuali dissimulando i trasferimenti o beneficiando di un certo livello di anonimato su queste piattaforme. È, pertanto, di fondamentale importanza ampliare l'ambito di applicazione della direttiva (UE) 2015/849 in modo da includere i prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute legali e i prestatori di servizi di portafoglio digitale. Ai fini dell'antiriciclaggio e del contrasto del finanziamento del terrori-smo (AML/CFT), le autorità competenti dovrebbero essere in*

[325] Art. 1, comma 2lett. qq) del D.lgs. 231/2007
[326] NADDEO M. (2022). *Criptovalute: profili di rilevanza penale,* cit. 263.

> *grado di monitorare, attraverso i soggetti obbligati, l'uso delle valute virtuali. Tale monitoraggio 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*".[327]

Lo schema preventivo disposto dal legislatore opera essenzialmente su due livelli. In primo luogo, vengono "arruolate" le figure come gli *Exchanger* e *Wallet provider* come professionisti coinvolti nelle operazioni che avvengono con valute virtuali[328] e che quindi, sono tenuti a segnalare ogni eventuale operazione sospetta quando

> "*sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa*".[329]

In secondo luogo, sono stati previsti obblighi di iscrizione nella sezione speciale del registro dei cambiavalute tenuto dall'Organismo degli Agenti e dei Mediatori (art. 128-undecies T.U.B.[330]) e di comunicazione al MEF dell'inizio dell'attività con espressa adesione al sistema pubblico antifrode (art. 17-bis, comma 8-bis, D.lgs. 141/10).[331]

Dall'intervento del legislatore europeo al quadro normativo attuale sono state realizzate ulteriori integrazioni in materia. In particolare, essendo l'iniziativa *ab origine* di natura europea è necessario approfondire l'*excursus* del quadro normativo italiano.

---

[327] VIII Considerando della V Direttiva antiriciclaggio

[328] STURZO L. (2018). *Bitcoin e riciclaggio 2.0*, in *Riv. trim. dir. pen. cont.*, n. 5-2018, pag. 29, considera gli *Exchangers* «*custodi del rispetto della normativa antiriciclaggio da parte degli utenti Bitcoin, in quanto unici soggetti in grado di individuare l'identità dell'utente di bitcoin prima che lo stesso sparisca dietro un account composto da numeri e lettere anonime*».

[329] Art. 35, comma 1 del D.lgs. 231/2007

[330] art. 128-undecies T.U.B. - Disponibile in open source sul sito https://www.brocardi.it/testo-unico-bancario/titolo-vi-bis/art128undecies.html

[331] NADDEO M. (2022). *Criptovalute: profili di rilevanza penale,* cit. 293. – Vedi

3. Evoluzione del quadro normativo italiano

Nell'ordinamento nazionale, il legislatore italiano ha introdotto una propria regolamentazione relativamente al fenomeno delle cripto-attività mediante il D.lgs. 90/2017, in materia di antiriciclaggio, in recepimento della Direttiva Comunitaria n. 2015/849 del 20 maggio 2015 (cd. IV Direttiva).[332] Il D.lgs. 90/2017 ha modificato il contenuto del D.lgs. 231/2007 in materia di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio del denaro e di finanziamento del terrorismo[333], introducendo una nuova definizione di valuta virtuale e norme dirette a regolamentare l'attività dei prestatori di servizi connessi alle criptovalute e alcuni obblighi già precedentemente previsti per gli operatori del settore finanziario.[334]

La definizione italiana attribuita al termine di criptovaluta[335], ai sensi dell'articolo 1, comma 2, lettera qq) del D.Lgs 231/2007 come modificato dal D.Lgs 90/2017[336], risulta quindi distante dal concetto di valuta legale in quanto essa può essere utilizzata sia come mezzo di scambio ovvero come strumento di investimento.[337] In aggiunta, il decreto sopra menzionato ha disposto un rafforzamento delle misure in materia di prevenzione dei reati finanziari. L'art. 8-bis estende le disposizioni riguardanti l'antiriciclaggio ai prestatori di servizi relativi all'utilizzo di valuta

---

[332] BANCA D'ITALIA, *Quaderni di Ricerca Giuridica Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, cit 47.

[333] Decreto legislativo 25 maggio 2017, n. 90 - Disponibile in open source sul sito https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2017;090

[334] DEOTTO LOVECCHIO & PARTNERS (2022). *L'inquadramento giuridico delle criptovalute.* Disponibile in open source sul sito https://www.commercialistatelematico.com/articoli/2022/08/inquadramento-giuridico-criptovalute.html.

[335] "*la rappresentazione digitale di valore, non emessa né garantita 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 o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente*" - dell'articolo 1, comma 2, lettera qq) del D.Lgs 231/2007.

[336] Decreto legislativo 25 maggio 2017, n. 90 - Disponibile in open source sul sito https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2017;090

[337] BANCA D'ITALIA, *Quaderni di Ricerca Giuridica Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, cit 47.

virtuale definiti nell'articolo 1, comma 2, lettera ff), del Decreto Legislativo 21 novembre 2007, n. 23, i quali sono altresì tenuti all'iscrizione in una sezione speciale del registro di cui al comma 1.[338]

L'art. 8-*ter* dispone che:

> "*Ai fini dell'efficiente popolamento della sezione speciale di cui al comma 8-bis, con decreto del Ministro dell'Economia e delle Finanze sono stabilite le modalità e la tempistica con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale sono tenuti a comunicare al Ministero dell'Economia e delle Finanze la propria operatività sul territorio nazionale. La comunicazione costituisce condizione essenziale per l'esercizio legale dell'attività da parte dei suddetti prestatori. Con il decreto di cui al presente comma sono stabilite forme di cooperazione tra il Ministero dell'Economia e delle Finanze e le forze di polizia, idonee ad interdire l'erogazione dei servizi relativi all'utilizzo di valuta virtuale da parte dei prestatori che non ottemperino all'obbligo di comunicazione*."[339]

Infine, è da rilevare che il D.lgs. 25 maggio 2017, n. 90 ha modificato l'art. 17 *bis*, del D.lgs. 141/2010, prevedendo l'istituzione ad opera dell'OAM, Organismo degli agenti in attività finanziaria e dei mediatori creditizi, di un Registro dei cambiavalute, il quale si compone oggi di una sezione speciale per il censimento dei prestatori di servizi relativi all'utilizzo di valute virtuali e prestatori di servizi di portafoglio digitale.[340]

---

[338] Decreto legislativo 25 maggio 2017, n. 90 - Disponibile in open source sul sito https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2017;090

[339] Art. 8 *ter* così come modificato, Decreto legislativo 24 febbraio 1998, n. 58 - https://www.consob.it/documents/46180/46181/TUF_agg_dlgs_107_2018.html/72d8db74-31e2-457b-aaa0-7348158bfef3

[340] BANCA D'ITALIA, *Quaderni di Ricerca Giuridica Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, cit 47

Più recentemente, ed in particolare il 14 dicembre 2021 sono entrate in vigore nuove disposizioni di cui al D.lgs. 8 novembre 2021 n. 184[341], in attuazione della direttiva (UE) 2019/713 sulle frodi e falsificazioni di mezzi di pagamento diversi dai contanti. Si introduce una nuova ed ulteriore definizione di valuta virtuale per qualificare giuridicamente le criptovalute in modo più specifico, sostanziandosi nella[342]:

> "*rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è legata necessariamente ad una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettata da persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferita, memorizzata e scambiata elettronicamente*".

Il contenuto di cui all'art. 1 D.lgs. 184/2021 risponde all'esigenza di istituire nuove regole atte a favorire la rapida evoluzione delle tecnologie digitali e dei metodi di pagamento dai quali ne possono conseguire un'evoluzione dei reati di frode e condotte criminali. Pertanto, si tratta di uno sforzo diretto all'inclusione tra le condotte penalmente sanzionate, tutte quelle condotte consistenti in un utilizzo fraudolento di criptovalute, o di valute virtuali.[343]

---

[341] D.lgs. 8 novembre 2021 n. 184 "*Attuazione della direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio*" - Disponibile in open source sul sito https://www.gazzettaufficiale.it/eli/id/2021/11/29/21G00200/sg

[342] CIRAOLO F. E LA ROSA E. (2022). *Contrasto alle frodi e alle falsificazioni dei mezzi di pagamento diversi dai contanti. Brevi note intorno al d. lgs. n. 184/21 (con focus sulle valute virtuali).* DB non solo diritto bancario. Disponibile in open source sul sito https://www.dirittobancario.it/art/contrasto-alle-frodi-e-alle-falsificazioni-dei-mezzi-di-pagamento-diversi-dai-contanti-brevi-note-intorno-al-d-lgs-n-184-21-con-focus-sulle-valute-virtuali/.

[343] REDAZIONE (2021). *Criptovalute, in arrivo in Italia il decreto frodi e falsificazioni di mezzi di pagamento.* Bluerating. Disponibile in open source sul sito https://www.bluerating.com/mercati/746939/criptovalute-in-arrivo-in-italia-il-decreto-frodi-e-falsificazioni-di-mezzi-di-pagamento.

In aggiunta a quanto sopra esposto, recentemente è stato emanato dal Ministero dell'Economia e delle Finanze (MEF) un nuovo decreto, pubblicato nella Gazzetta Ufficiale n. 40 del 17 febbraio 2022 (di seguito il "Decreto"), mediante il quale viene imposto ai provider di servizi di criptovaluta e portafoglio digitale che operano o intendono operare sul territorio italiano l'iscrizione obbligatoria in una sezione speciale del registro tenuta dall'Organismo per gli Agenti e Mediatori, ovvero l'Organismo Agenti e Mediatori di Credito (di seguito "Sezione Speciale"), un requisito ormai obbligatorio per operare in Italia, come precedentemente accennato. Requisito essenziale per l'iscrizione delle imprese è avere un ufficio legale e amministrativo in Italia mentre, per le imprese dell'UE, è sufficiente una filiale in Italia.[344]
Pertanto, gli operatori non italiani non possono più operare in Italia su base transfrontaliera.

Dal punto di vista operativo ai fini dell'iscrizione alla Sezione Speciale del registro OAM, gli operatori che intendono svolgere la propria attività in Italia devono inviare all'OAM una comunicazione elettronica contenente i dati di cui all'articolo 3(4) dello stesso Decreto. Le criptovalute e i fornitori di servizi di portafoglio digitale che già operano in Italia devono inviare la comunicazione di cui sopra entro 60 giorni dall'istituzione della Sezione Speciale e possono continuare ad operare in attesa del processo di registrazione solo se alla data di tale istituzione soddisfano i requisiti di cui all'articolo 17-bis, comma 2 del D.lgs. 141/2010[345] (cioè hanno sede legale o stabile in Italia), pena l'imputazione per l'esercizio illecito di attività sul territorio italiano.[346]
Di conseguenza, le criptovalute estere e i fornitori di servizi di portafoglio digitale già operanti sul territorio italiano, in assenza di una sede legale o di una stabile organizzazione in Italia all'avvio della Sezione Speciale, dovranno sospendere la loro attività in quanto abusiva, fino a quando non avranno provveduto alla

[344] REDAZIONE, *Criptovalute, in arrivo in Italia il decreto frodi e falsificazioni di mezzi di pagamento*, cit. 291
[345] Decreto Legislativo 10 agosto 2010, n. 141 - Disponibile in open source sul sito https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2010-08-13;141
[346] REDAZIONE. *Criptovalute, in arrivo in Italia il decreto frodi e falsificazioni di mezzi di pagamento.* Bluerating, cit. 321.

costituzione di una società o di una controllata e non avranno ottenuto la registrazione. Per gli operatori italiani che già forniscono valute virtuali e servizi di portafoglio digitale, invece, sarà sufficiente inviare la comunicazione entro 60 giorni dalla costituzione della Sezione Speciale del registro.
Dopo aver verificato la correttezza e la completezza delle informazioni inviate, l'OAM entro 15 giorni procederà (o meno) alla registrazione nella Sezione Speciale. Questo termine può essere sospeso una volta per un periodo non superiore a 10 giorni se la documentazione è considerata incompleta e/o sono necessarie integrazioni. Se il fornitore non presenta le integrazioni richieste entro 10 giorni dalla notifica OAM, la comunicazione sarà considerata non ricevuta e l'OAM negherà la registrazione.[347]

L'iscrizione al registro OAM innesca nuovi requisiti di reporting per criptovalute e fornitori di servizi di portafoglio digitale che integrano quelli già richiesti dalla Direttiva V sull'antiriciclaggio. Difatti, l'art. 5 del Decreto prevede che gli operatori crittografici dovranno notificare elettronicamente all'OAM i dati relativi alle operazioni effettuate sul territorio italiano e, in particolare i dati identificativi del cliente di cui all'allegato 1 del decreto, sia in caso di rapporto continuativo sia nel caso in cui si tratti di un rapporto di natura occasionale nel momento in cui vi sia un movimento di valute pari o superiore a € 15.000,00[348] e i dati riepilogativi relativi all'attività per ciascun cliente, come indicati nello stesso allegato 1 del Decreto.[349]

La mancata registrazione nella Sezione Speciale da parte di criptovalute e fornitori di servizi di portafoglio digitale che intendono operare in Italia implica l'esercizio abusivo della loro attività ed è punita, ai sensi dell'art. 17-bis, comma 5, D.lgs. 141/2010, con ammenda amministrativa imposta dal Ministero dell'Economia e

[347] ALBE' G. (2022). *Obbligo di iscrizione al registro OAM per gli operatori cripto: cosa è cambiato e tutte le sanzioni*. Agendadigitale.eu. Disponibile in open source sul sito https://www.agendadigitale.eu/cittadinanza-digitale/pagamenti-digitali/obbligo-di-iscrizione-al-registro-oam-per-gli-operatori-cripto-cosa-e-cambiato-e-tutte-le-sanzioni/
[348] Art. 17 ss del D.lgs. 21 novembre 2007, n. 231.
[349] BONOLIS P., SELVAGGIUOLO E., BACCI F. (2022). Operatori in criptovalute: con l'istituzione del registro...in CSM.LAW.it. Disponibile in open source sul sito https://cms.law/it/ita/publication/operatori-in-criptovalute-con-l-istituzione-del-registro-speciale-dell-oam-scattano-i-requisiti-regolamentari-per-operare-in-italia. Vedi anche art. 31, 32 e 57 del D.lgs. 21 novembre 2007, n. 231

delle Finanze da 2.065 a 10.329 euro. Inoltre, qualora le autorità competenti verifichino che i servizi relativi all'uso di moneta virtuale e/o servizi di portafoglio digitale sono stati effettuati illegalmente in Italia, possono accertare e contestare la violazione in conformità alle disposizioni della legge n. 689/1981[350], che potrebbe portare, tra l'altro, nel caso di attività svolte attraverso siti web, al sequestro dello stesso mediante oscuramento e divieto di accesso agli stessi.[351]

Il nuovo regolamento trova applicazione sia nei confronti dei provider di servizi di criptovaluta ossia persone fisiche e giuridiche che, su base professionale, forniscono a terzi, anche online, servizi relativi all'uso, lo scambio, la conservazione di valute virtuali e il loro scambio da o verso valute a corso legale o in rappresentazioni digitali di valore, comprese quelle convertibili in altre valute virtuali, nonché i servizi di emissione, l'offerta, il trasferimento e la compensazione e qualsiasi altro servizio relativo all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle stesse valute; sia nei confronti dei fornitori di servizi di portafoglio digitale: cioè qualsiasi persona fisica o giuridica che fornisce a terzi, su base professionale, anche online, servizi per la salvaguardia delle chiavi crittografiche private per conto dei propri clienti, per tenere, memorizzare e trasferire valute virtuali.[352]

Il regolamento, pertanto, riguarda tutte le piattaforme utilizzate per offrire a terzi, su base professionale, servizi relativi alle criptovalute, ad eccezione degli emittenti di attività in valuta virtuale che non si qualificano come fornitori di servizi in criptovaluta nella misura in cui tale attività non sia svolta su base professionale e per conto di terzi.[353]

---

[350] ALBE' G., *Obbligo di iscrizione al registro OAM per gli operatori cripto: cosa è cambiato e tutte le sanzioni*, cit. 325.

[351] Legge n. 689/1981 - Disponibile in open source sul sito https://www.gazzettaufficiale.it/eli/id/1981/11/30/081U0689/sg

[352] TUMIETTO D. (2023). *Cripto-attività, ecco il regolamento Mica: le nuove regole da conoscere*, in Agendadigitale.eu. Disponibile in open source sul sito https://www.agendadigitale.eu/documenti/cripto-attivita-ecco-il-regolamento-mica-le-nuove-regole-da-conoscere/

[353] PONTICELLI d. (2023). *Crypto-asset: approvato il Mica. Ecco il nuovo quadro normativo*, in we-wealth.com. Disponibile in open source sul sito https://www.we-wealth.com/news/fintech/blockchain/crypto-asset-approvato-il-mica-ecco-il-nuovo-quadro-normativo

Ai sensi delle disposizioni introdotte dall'articolo 17-bis, comma 8-ter del decreto legislativo 13 agosto n. 141, 2010, il Decreto stabilisce le procedure e i tempi entro i quali i fornitori di servizi di criptovalute e i fornitori di servizi di portafoglio digitale devono comunicare la loro attività sul territorio italiano all'OAM. I requisiti e gli adempimenti previsti dal nuovo Decreto si aggiungono a quelli previsti dal Decreto AML (decreto legislativo n. 231/2007), cui sono già soggetti i suddetti fornitori.[354]

Nonostante il quadro normativo internazionale, europeo ed italiano in materia di criptovalute sia estremamente frammentario ed in continua evoluzione,[355] gli sforzi finora effettuati sono qualificabili come "tasselli" nel percorso progressivo diretto a raggiungere una regolamentazione armoniosa degli asset digitali.[356]

3.1 (*Segue*): La giurisprudenza della Corte di Cassazione in materia di riciclaggio e responsabilità dei *Wallet provider*

In tema di responsabilità dei *Wallet provider* e degli *Exchanger* in caso di utilizzo delle criptovalute come strumento di operazioni di *cyber self-laundering*, ricadenti nella fattispecie di reato di cui all'art. 648-*ter*, comma 1 c.p. (autoriciclaggio), è intervenuta anche la Corte di Cassazione.

Prima di tutto, è necessario ricordare che la fattispecie delittuosa predetta costituisce un reato proprio in quanto può essere commesso solo dall'autore del reato-presupposto, il quale pone in essere attività di impiego, trasferimento o utilizzo di

[354] ALBE' G., *Obbligo di iscrizione al registro OAM per gli operatori cripto: cosa è cambiato e tutte le sanzioni*, cit. 325.
[355] REDAZIONE, *Criptovalute, in arrivo in Italia il decreto frodi e falsificazioni di mezzi di pagamento,* cit. 291
[356] MARINELLO A. (2022). *Un "cripto-condono" e molti nodi irrisolti nel disegno di legge sulla disciplina fiscale delle valute virtuali* in Rivista Telematica di Diritto Tributario. Disponibile in open source sul sito https://www.rivistadirittotributario.it/wp-content/uploads/2022/10/Marinello.pdf

beni o denaro ovvero altre utilità, illecitamente conseguiti, al fine di impedire l'individuazione della loro provenienza delittuosa[357]

Premesso ciò, non può escludersi a priori che la fattispecie in oggetto possa avvenire anche a titolo di concorso.[358] In tale contesto risulta estremamente significativa, la recente pronuncia della Cassazione (Cass. pen., Sez. II, 7 ottobre 2021-25 gennaio 2022, n. 2868)[359] con la quale ha sostenuto che il reato di autoriciclaggio si integri anche nel momento in cui i profitti di un'attività illecita dell'autore del reato vengano convertiti in criptovalute da una società terza. In particolare, i giudici, richiamando l'art. 648 ter c.p. e la sua natura di reato di pericolo hanno sostenuto che tale fattispecie si integri attraverso condotte poste in essere *ex ante* dirette ad ostacolare la natura della provenienza delle utilità derivanti da reato[360], aggiungendo che

> "*le operazioni realizzate attraverso il trasferimento di valuta verso società estere che si interponevano nell'acquisto di criptovalute ed effettuate anche a mezzo di prestanome ponevano un serio ostacolo alla identificazione del ricorrente come beneficiario finale delle transazioni ed effettivo titolare di bitcoin acquistati non da lui ma dalle società estere che fungevano da exchanger di criptovalute[...]. All'attività di cambio della valuta deve essere attribuito carattere finanziario, tanto che in Italia essa è regolamentata dalla legge ed il soggetto che la esercita deve essere iscritto in appositi registri*".[361]

---

[357] LANZI, M. (2018). *Riciclaggio e reati nella gestione dei flussi di denaro sporco*, Giuffrè, Milano, pagg. 339 ss.

[358] STURZO L., *Bitcoin e riciclaggio 2.0*, in *Riv. trim. dir. pen. cont.*, n. 5-2018, cit. 308

[359] Corte di Cassazione, sez. II pen., sentenza 25 gennaio 2022 (ud. 7 ottobre 2021), n. 2868 - Disponibile in open source sul sito https://arsg.it/?p=3648

[360] DE CONNO A. (2022). *Criptovalute, riciclaggio e autoriciclaggio. Cryptocurrency e rischi: la recente pronuncia della Cassazione penale sul punto (sentenza 25 gennaio 2022 n. 2868)*, in Altalex. Disponibile in open source sul sito https://www.altalex.com/documents/news/2022/05/24/criptovalute-riciclaggio-autoriciclaggio

[361] D.lgs. 1 settembre 1993, n. 385, art. 155, comma 5, recante il Testo Unico delle Leggi in materia bancaria e creditizia, stabilisce che i soggetti che esercitano professionalmente l'attività di cambiavalute, sono iscritti in un'apposita sezione dell'Elenco previsto dall'art. 106, comma 1, del T.U.)

Pertanto, la Cassazione sostiene che la fattispecie viene integrata quando

> *"la condotta del ricorrente rientra tra quelle punite dalla norma incriminatrice contestatagli, per avere dato corso al trasferimento del profitto dei reati presupposto in una attività finanziaria costituita dal cambio della valuta posto in essere su suo mandato da società estere. Ciò consente di ritenere del tutto irrilevante verificare quale fosse stato l'utilizzo ancora successivo dei bitcoin infine ottenuti dal ricorrente […]".*

Segue una più recente pronuncia, sempre della Cassazione (Cass. pen., Sez. II, 7 luglio 2022 – 13 luglio 2022, n. 27023)[362] con la quale equipara le valute virtuali ed in particolare il loro acquisto ad attività di natura speculativa in quanto

> "*le valute virtuali possono essere utilizzate per scopi diversi dal pagamento e comprendere prodotti di riserva di valore a fini di risparmio ed investimento*" poiché "*è possibile garantire un alto grado di anonimato (sistema c.d. permissionless), senza previsione di alcun controllo sull'ingresso di nuovi "nodi" e sulla provenienza del denaro convertito (si è anche sottolineato come sia ormai noto il vasto numero di criptovalute utilizzate nel dark web, proprio per le loro peculiari caratteristiche, e che alcune di esse, attraverso l'uso di tecniche crittografiche avanzate, garantiscono un elevato livello di privacy sia in relazione alla persona dell'utente sia in relazione all'oggetto delle compravendite)".*

Pertanto, alla luce delle due pronunce sopra descritte, ad oggi si sostiene che anche i *Wallet provider* ovvero gli *Exchanger* possono integrare la fattispecie di autoriciclaggio nel caso in cui impieghino una valuta derivante da attività illecite in attività di cambio valuta a titolo professionale.[363]

---

[362] Corte di Cassazione, sezione II penale, sentenza 7 luglio 2022 (dep. 13 luglio 2022), n. 27023. Disponibile in open source sul sito https://www.penale.it/page.asp?mode=1&IDPag=1387

[363] NADDEO M. (2016). *Autoriciclaggio: i compromessi di un difficile inquadramento sistematico*, in *Riv. trim. dir. pen. ec*., n. 3-4, pp. 697 ss.

3.2 (*Segue*): 231 e criptovalute: la responsabilità da reato dell'ente nel riciclaggio tramite monete virtuali.

Dal punto di vista dei reati previsti dal D.lgs. 8 giugno 2001, n. 231 inerente alla responsabilità amministrativa delle persone giuridiche, in materia di criptovalute è possibile integrare le ipotesi di reato come: ricettazione (art. 648 c.p.), riciclaggio (art. 648-bis c.p.), autoriciclaggio (art. 648-ter.1 c.p.) e reimpiego (art. 648-ter c.p.). Tali reati possono essere facilmente commessi da un soggetto all'apice dell'azienda ovvero in una posizione subordinata, nell'interesse o a vantaggio dell'ente (es. *Exchanger*) di cui è dipendente. In casi simili si applica quanto disposto dall'art. 25-octies, D.lgs. 231/2001.[364]

Pertanto, dall'analisi della normativa si deduce che gli operatori di criptovalute possono integrare fattispecie criminose previste dal D.lgs. 231/2001 nel momento in cui commettano violazioni di natura dolosa relativamente agli obblighi di segnalazione e realizzando quindi così un'omissione consapevole. In particolare, per quanto riguarda il reato di riciclaggio previsto dall'art. 648 bis del C.P., l'Ente può evitare una condanna solo se dimostra di aver redatto ed applicato appositi strumenti organizzativi, di gestione e di supervisione idonei a prevenire il compimento dell'illecito, come, ad esempio, il controllo circa la provenienza dei fondi, la nomina di un controller interno, l'aggiornamento e la formazione dei dipendenti sulla prevenzione del riciclaggio. Ne consegue, al contrario, che se l'ente non dimostra di aver adottato le citate misure preventive o se tali misure sono state

[364] LUCEV R., BONCOMPAGNI F., *Criptovalute e profili di rischio penale nella attività degli exchanger*, Giurisprudenza Penale, cit. 266. In termini di semplificazione probatoria, MANCINI C. (2012). *Riciclaggio e responsabilità degli enti. I modelli organizzativi*, in E. Cappa, D. Cerqua (a cura di), *Il riciclaggio del denaro. Il fenomeno, il reato, le norme di contrasto*, Giuffrè, Milano, pagg. 104 ss. - art. 25-octies, D.lgs. 231/2001 "*in relazione ai reati di cui agli artt. 648, 648-bis, 648-ter e 648ter del Codice penale, si applica all'ente la sanzione pecuniaria da 200 a 800 quote. Nel caso in cui il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione superiore nel massimo a cinque anni si applica la sanzione pecuniaria da 400 a 1000 quote. Nei casi di condanna per uno dei delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'art. 9, comma 2, per una durata non superiore a due anni […]*."

inefficaci, l'ente può essere condannato per il reato di riciclaggio commesso dai suoi rappresentanti o dipendenti.[365]

Inoltre, recentemente, nell'ambito dell'attività del governo italiano sono stati emanati due nuovi importanti provvedimenti in materia, in attuazione delle due direttive dell'Unione europea: direttiva 2019/713/UE[366] e direttiva 2018/1673/UE.[367] In particolare, i provvedimenti emanati hanno ampliato il novero dei reati di cui al D.lgs 231/2001. Il D.lgs. 184/2021[368] (in recepimento alla direttiva 2019/713/UE) ha introdotto l'art. 25-*octies* che ha inserito tra i reati presupposto della responsabilità amministrativa degli enti i reati di indebito utilizzo e falsificazione di carte di credito e pagamento (art. 493-*ter* c.p.) e detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-*quater* c.p.) nonché il reato di cui all'art. 640-*ter* c.p. nei casi di trasferimento di denaro, valore monetario ossia valuta virtuale, aggravato.[369] Da tale prima novella legislativa ne deriva un ampliamento dell'oggetto del reato che oggi può ricomprendere sia le azioni commesse mediante mezzi di pagamento immateriale ossia digitale sia i mezzi di scambio digitali. Pertanto, il legislatore ha risposto alla necessità di introdurre delle regole adeguate con riferimento all'uso delle criptovalute al quale è stato connesso un aumento delle frodi e dei reati da parte delle persone giuridiche.[370]

---

[365]NADDEO M. (2022). *Criptovalute: profili di rilevanza penale,* cit. 293.

[366] Direttiva 2019/713/UE - Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019L0713&from=IT

[367] Direttiva 2018/1673/UE - Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018L1673&from=de

[368] D.lgs. 184/2021 - Disponibile in open source sul sito https://www.gazzettaufficiale.it/eli/id/2021/11/29/21G00200/sg

[369] ALBERTI M. (2022). *Nuovi reati 231: falsificazioni di pagamenti diversi dal contante, frodi, criptovalute e riciclaggio* in Studio Legale Mascetti. Disponibile in open source sul sito https://www.studiolegalemascetti.it/nuovi-reati-231-falsificazioni-di-pagamenti-diversi-dal-contante-frodi-criptovalute-e-riciclaggio/

[370] ALBERTI M., *Nuovi reati 231: falsificazioni di pagamenti diversi dal contante, frodi, criptovalute e riciclaggio,* cit. 364

Successivamente, il D.lgs. 195/2021[371] (in recepimento alla direttiva 2018/1673/UE) ha invece ampliato il novero dei reati presupposto che ricadono nel reato di riciclaggio, includendo così le contravvenzioni e i delitti colposi che vanno così ad incidere sulla *compliance* ai sensi del d.lgs 231/2001. In altre parole, ricomprendendo anche i delitti colposi vengono ampliate le maglie della responsabilità ai sensi del d.lgs 231/2001 a tutte quelle ipotesi di reato che prima non venivano ricomprese.[372]

Le novità introdotte *in primis* dal legislatore europeo e successivamente dal legislatore italiano hanno determinato la necessità di procedere all'aggiornamento del Modello 231 attribuendo maggiore attenzione ai sistemi informatici, ai reati commessi mediante l'utilizzo di sistemi IT e all'implementazione di misure per la prevenzione dei rischi.[373]

4. Possibili conseguenze fiscali ed economiche

Il presente paragrafo ha ad oggetto l'analisi degli interventi più importanti realizzati dalle autorità nazionali e sovranazionali in materia di regolamentazione del trattamento fiscale delle criptovalute. Come per quanto riguarda il mondo giuridico delle criptovalute, anche la disciplina fiscale delle criptovalute non risulta chiara a causa della natura ibrida di tali strumenti.

L'IRS (*Internal Revenue Service*)[374] ha pubblicato un documento (il *notice* 2014-21)[375] mediante il quale ha previsto una serie di principi fiscali da applicare alle transazioni che avvengono mediante l'utilizzo di valute virtuali. In primo luogo,

[371] D.lgs. 195/2021 - Disponibile in open source sul sito https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2021-12-23;195

[372] BRUNOZZI L. M. e FIORIO C. (2021). *231 e criptovalute. La responsabilità da reato dell'ente nel riciclaggio mediante monete virtuali*. Gaspare Jucan Sicignano.

[373] ALBERTI M., *Nuovi reati 231: falsificazioni di pagamenti diversi dal contante, frodi, criptovalute e riciclaggio,* cit. 364

[374] IRS è l'Agenzia delle entrate del governo federale degli Stati Uniti d'America. I compiti dell'IRS comprendono l'offerta di assistenza fiscale ai contribuenti, il perseguimento e la risoluzione di casi di pratiche fiscali errate o fraudolente.

[375] Sito ufficiale IRS https://www.irs.gov/pub/irs-drop/n-14-21.pdf

l'ente chiarisce che le valute virtuali sono da considerarsi come una forma di proprietà e non una moneta[376] e pertanto, le transazioni avvenute mediante le stesse, per l'acquisto di beni e/o servizi, devono essere incluse nel reddito lordo.[377] Inoltre, sempre nell'ambito fiscale della normativa statunitense, le transazioni mediante le valute virtuali devono essere indicate in dollari, ciò significa che ai contribuenti statunitensi è richiesta la quantificazione del valore delle valute virtuali in dollari.

Sempre l'IRS afferma che i principi contenuti nel documento si devono applicare anche ai *miners*, in quanto la valuta virtuale generata con successo integra il reddito lordo dello stesso ovvero soggiace all'imposta sul lavoro autonomo. L'eventuale violazione di quanto disposto nel *notice* comporta la possibile applicazione di sanzioni nei confronti del contribuente.

Con la sentenza pubblicata il 22 Ottobre 2015 *causa C-264/14*[378] la Corte di Giustizia dell'Unione Europea si è espressa in merito all'applicazione dell'Imposta sul Valore Aggiunto su operazioni di cambio mediante i Bitcoin.[379] L'intervento della Corte di Giustizia europea è stato richiesto da David Hedqvist, il quale offriva un servizio di cambio di Bitcoin in corone svedesi e viceversa.[380] Hedqvist si era preventivamente rivolto alla Commissione Tributaria svedese[381], che ha sostenuto che tali transazioni non sono soggette ad IVA, così come confermato successivamente dalla Corte di Giustizia. Sulla base dell'articolo 2, paragrafo 1,

---

376 BANCA D'ITALIA, *Quaderni di Ricerca Giuridica Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, cit 47

377 SARDAR M. (2017). *Digital Currency: Taxation, Enforcement, and the John Doe Summons*. The Cpa Journal. P. 62 e ss.

378 Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62014CJ0264&from=IT

379 FILODIRITTO.IT (2015). *IVA - Corte di Giustizia: i Bitcoin sono esenti dal pagamento dell'Iva.* Disponibile in open source sul sito https://www.filodiritto.com/iva-corte-di-giustizia-i-bitcoin-sono-esenti-dal-pagamento-delliva.. *Vedi* anche Regolamento (UE) 2017/1001 del Parlamento europeo e del Consiglio del 14 giugno 2017 sul marchio dell'Unione europea - Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32017R1001.

380 BANCA D'ITALIA, *Quaderni di Ricerca Giuridica Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, cit 47

381 FILODIRITTO.IT, *IVA - Corte di Giustizia: i Bitcoin sono esenti dal pagamento dell'Iva*, cit, 347.

della direttiva IVA, Direttiva 2006/112/CE[382] (di seguito "Direttiva IVA) che dispone che le cessioni di beni e prestazioni di servizio a titolo oneroso nel territorio di uno Stato membro da un soggetto passivo che agisca in quanto tale sono assoggettate ad IVA, la Corte ha sostenuto che l'attività di cambio di Bitcoin in valuta legale non può essere qualificata come cessione di bene materiale[383] ai sensi dell'articolo 14 della Direttiva IVA.[384] Pertanto, tali operazioni rientrano nell'applicazione dell'art. 24 della Direttiva IVA, ossia costituiscono prestazioni di servizi. Inoltre, sempre alla luce della Direttiva IVA e dell'art. 135, lettera e), la Corte di Giustizia Europea ha affermato che nel caso concreto i Bitcoin, non avendo altre finalità oltre a quella di mezzo di pagamento, non possono essere qualificati come bene materiale. In altre parole, vengono equiparati alle valute tradizionali e saranno quindi assoggettati alla stessa disciplina delle valute tradizionali, rientrando tra le attività esenti dall'applicazione dell'Iva per le transazioni compiute all'interno del territorio europeo.[385]

Il contribuente detentore di criptovalute, dal punto di vista fiscale, sarà comunque obbligato a dichiarare la detenzione degli asset in oggetto tramite il quadro RW della dichiarazione dei redditi, anche se non vi è mai stata alcuna plusvalenza. L'obiettivo di tale operazione è del tutto informativa e non comporta alcuna tassazione per il contribuente.[386]

[382] Direttiva 2006/112/CE del 28 novembre 2006 relativa al sistema comune d'imposta sul valore aggiunto - Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32006L0112&from=IT

[383] Decreto Legislativo 25 maggio 2017, n. 90 - Disponibile in open source sul sito https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2017;090

[384] CARLINI V. (2022). *Qual è il trattamento fiscale delle criptovalute in Italia?* Sole24Ore Finanza. Disponibile in open source sul sito https://www.ilsole24ore.com/art/qual-e-trattamento-fiscale-criptovalute-italia-AE6kdKOB. Accesso avvenuto in data 29 marzo 2023.

[385] FILODIRITTO.IT, *IVA - Corte di Giustizia: i Bitcoin sono esenti dal pagamento dell'Iva*, cit, 347.

[386] CARLINI V., *Qual è il trattamento fiscale delle criptovalute in Italia?*, cit. 352.

4.1 (*Segue):* La posizione dell'Agenzia delle Entrate

Come già accennato precedentemente, dall'utilizzo sempre più diffuso delle valute digitali è nata l'esigenza anche di regolamentare anche la possibile configurabilità dei reati tributari ex D.lgs. 74/2000.[387]Tuttavia, prima di rispondere a tale esigenza è necessario capire e quindi identificare il regime fiscale delle criptovalute.

Pertanto, innanzitutto è necessario analizzare in primo luogo le pronunce della Corte di Giustizia dell'Unione Europea[388] al fine di analizzare successivamente la pronuncia dall'Agenzia delle Entrate in materia[389], la quale fonda le proprie conclusioni sulla sentenza della Corte di Giustizia dell'Unione Europea da cui prende spunto nelle proprie considerazioni.

La Corte di Giustizia UE, Sez. V, 22 ottobre 2015, Causa C-264/14, Skatteverket c. David Hedqvist ha deciso che le attività di conversione di valuta fiat in valuta virtuale (e viceversa) se

> «*effettuate a fronte del pagamento di una somma corrispondete al margine costituito dalla differenza tra il prezzo di acquisto delle valute e quello di vendita praticato dall'operatore ai propri clienti costituiscono prestazioni di servizi a titolo oneroso,» esse rientrano tra le operazioni* […]»
>
> «*relative a divise, banconote e monete con valore liberatorio di cui all'articolo 135, paragrafo 1, lettera e), della direttiva 2006/112/CE*».

[387] LUCEV R., BONCOMPAGNI F., *Criptovalute e profili di rischio penale nella attività degli exchanger*, Giurisprudenza Penale, cit. 266.

[388] Corte di Giustizia UE, Sez. V, 22 ottobre 2015, Causa C-264/14, Skatteverket c. David Hedqvist, con nota di CAPACCIOLI S. (2015). *Bitcoin: le operazioni di cambio con valuta a corso legale sono prestazioni di servizio esenti*, in Il Fisco.

[389] Risoluzione N. 72/E del 2 settembre 2016 - Disponibile in open source sul sito https://www.agenziaentrate.gov.it/wps/file/nsilib/nsi/normativa+e+prassi/risoluzioni/archivio+risoluzioni/risoluzioni+2016/settembre+2016+risoluzioni/risoluzione+n.+72+del+02+settembre+2016/RISO LUZIONE+N.+72+DEL+02+SETTEMBRE+2016E.pdf

Inoltre, tali operazioni,

> «*pur riguardando operazioni relative a valute non tradizionali (e cioè diverse dalle monete con valore liberatorio in uno o più Paesi), costituiscono operazioni finanziarie in quanto tali valute siano state accettate dalle parti di una transazione quale mezzo di pagamento alternativo ai mezzi di pagamento legali e non abbiano altre finalità oltre a quella di un mezzo di pagamento*».

In altre parole, con tale decisione la Corte di Giustizia ha sancito che le attività sopra descritte sono esenti ai fini IVA poiché rientranti nell'ambito di applicazione dell'art. 135, paragrafo 1, lett. e) della direttiva 2006/112/CE.

Nel contesto nazionale, la Direzione Centrale Normativa dell'Agenzia delle Entrate[390], mediante la pubblicazione della Risoluzione n. 72/E del 2 settembre 2016[391], ha deciso di fornire alcuni chiarimenti circa il trattamento tributario delle valute virtuali.[392] In particolare, l'Agenzia delle Entrate si è pronunciata sulla tassazione sia diretta che indiretta e sul trattamento fiscale delle persone giuridiche e fisiche.

Con riferimento alla tassazione indiretta l'agenzia ha dichiarato che:

> "*in assenza di una specifica normativa applicabile al sistema delle monete virtuali, la predetta sentenza della Corte di Giustizia costituisce*

[390] L'Agenzia delle Entrate è un ente pubblico il cui compito è la riscossione dei tributi e il vigilare sulla corretta applicazione delle leggi in materia tributaria, al fine di garantire l'adempimento degli obblighi fiscali da parte dei contribuenti. - *Vedi* Agenzia delle Entrate, Alternative alle detrazioni. Disponibile in open source sul sito https://www.agenziaentrate.gov.it/portale/alternative-alle-detrazioni.

[391] Risoluzione n. 72/E del 2 settembre 2016 - Disponibile in open source sul sito https://www.agenziaentrate.gov.it/portale/documents/20143/302984/Risoluzione+n.+72+del+02+settembre+2016_RISOLUZIONE+N.+72+DEL+02+SETTEMBRE+2016E.pdf/8e057611-819f-6c8d-e168-a1fb487468d6

[392] CIRAOLO F. E LA ROSA E., *Contrasto alle frodi e alle falsificazioni dei mezzi di pagamento diversi dai contanti. Brevi note intorno al d. lgs. n. 184/21 (con focus sulle valute virtuali)*, cit. 320

necessariamente un punto di riferimento sul piano della disciplina fiscale applicabile alle monete virtuali e, nello specifico ai Bitcoin".[393]

Pertanto, non si può fare a meno di tenere conto di quanto stabilito dalla Corte di Giustizia nella sentenza 22 ottobre 2015 *causa C-264/14*[394], con la conseguenza di ritenere il servizio di intermediazione di valute rientrante nelle prestazioni di servizi esenti da IVA.

Invece per quanto riguarda la tassazione diretta, i ricavi o costi derivanti da attività relative alle valute virtuali da parte di una persona giuridica concorrono nella costituzione del reddito d'esercizio e della base imponibile assoggettata ad imposte come IRES e IRAP.[395] A fine esercizio deve essere calcolato il loro valore di mercato. Per quanto riguarda invece il regime applicabile alle persone fisiche, la risoluzione di cui sopra precisa che

"*le persone fisiche che detengono i bitcoin al di fuori dell'attività d'impresa, si ricorda che le operazioni a pronti (acquisti e vendite) di valuta non generano redditi imponibili mancando la finalità speculativa*".[396]

In altre parole, è stata riconosciuta la possibilità di configurare i reati tributari di cui al D.lgs. 74/2000 per i prestatori di servizi di criptovalute relativamente alle imposte IRES e IRAP (e non all'IVA).

---

[393] Risoluzione n. 72/E del 2 settembre 2016 - Disponibile in open source sul sito https://www.agenziaentrate.gov.it/portale/documents/20143/302984/Risoluzione+n.+72+del+02+settembre+2016_RISOLUZIONE+N.+72+DEL+02+SETTEMBRE+2016E.pdf/8e057611-819f-6c8d-e168-a1fb487468d6

[394] BANCA D'ITALIA, *Quaderni di Ricerca Giuridica Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale* , cit 47

[395] Imposta sul Reddito delle Società (IRES), Imposta Regionale sulle Attività Produttive (IRAP).

[396] Risoluzione n. 72/E del 2 settembre 2016 - Disponibile in open source sul sito https://www.agenziaentrate.gov.it/portale/documents/20143/302984/Risoluzione+n.+72+del+02+settembre+2016_RISOLUZIONE+N.+72+DEL+02+SETTEMBRE+2016E.pdf/8e057611-819f-6c8d-e168-a1fb487468d6

Questa nuova circolare dell'Agenzia delle Entrate ha cercato di mettere chiarezza ad una materia che rimane in continua evoluzione e caratterizzata da una vastità di interpretazioni soggettive di esperti.[397]

Successivamente, l'Agenzia delle Entrate con l'interpello 956-448/2022, ha tentato di chiarire un ulteriore dubbio sorto circa la compilazione del modello RW. Circa gli investimenti all'estero mediante criptovalute, se ciò avviene mediante una piattaforma italiana non è necessario compilare il quadro RW. Il quale sarà da compilare solo al fine di dichiarare i redditi derivanti dalle cessioni di partecipazioni non qualificate, obbligazioni e altri strumenti che generano plusvalenze e ovviamente nel caso in cui la piattaforma si affidi ad una società con sede in un altro Paese. Dalla mancata o irregolare compilazione ne deriva l'applicazione di una sanzione compresa tra il 3% e il 15% del valore di quanto non dichiarato.[398] Pertanto, per il contribuente detentore di valute virtuali sorge l'obbligo di compilazione del quadro RT solo quando vi è una giacenza media di 51.645,69 euro per almeno 7 giorni lavorativi continui e si effettua dal proprio portafoglio elettronico un prelievo di valute virtuali convertite in euro. In tal caso, l'imposta sostitutiva da pagare sarà pari al 26% dell'imponibile, calcolato sull'intero ammontare dell'eventuale plusvalenza.[399] Nei casi di omissione si prevede l'applicazione di una sanzione tra il 3% e il 15% del valore degli importi non dichiarati, come disposto dall'art. 2,[400] comma 5, DL 167/90. Tale sanzione sarà

[397] CONTE D. (2019). *Criptovalute e l'applicazione delle disposizioni tributarie, in Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2 criptovalute e rivoluzione digitale* a cura di Fabrizio Maimeri e Marco Mancini, Quaderni di Ricerca Giuridica della Consulenza Legale. Disponibile in open source sul sito https://www.bancaditalia.it/pubblicazioni/quaderni-giuridici/2019-0087/index.html.

[398] CONZATO A. (2022). *Criptovalute, come dichiararle nei redditi? I chiarimenti dell'Agenzia delle Entrate*. Corriere.it. Disponibile in open source sul sito https://www.corriere.it/economia/finanza/22_settembre_18/criptovalute-come-dichiararle-redditi-chiarimenti-dell-agenzia-entrate-c9b501b2-2216-11ed-bca3-87e269fdfa32.shtml Accesso avvenuto in data 30 marzo 2023.

[399] PESCOSOLIDO J. (2021). *Criptovalute – Tassazione ed obblighi di monitoraggio fiscale (RW)*, Fisco e Tasse. Disponibile in open source sul sito https://www.fiscoetasse.com/approfondimenti/14140-criptovalute-tassazione-ed-obblighi-di-monitoraggio-fiscale-rw.html.

[400] FARINA S. (2022). *Criptovalute da non dichiarare in RW se Piattaforma Italiana* in Blog Fiscale.it. Disponibile in open source sul sito https://www.blogfiscale.it/2022/08/22/criptovalute-non-dichiarare-rw-piattaforma-cripto-italiana-lnterpello-956-448-2022-agenzia-delle-entrate/

raddoppiata nel caso in cui l'investimento è in titolarità presso un paese cd. "paradiso fiscale".

4.2 (*Segue):* le possibili conseguenze economiche delle criptovalute

In primo luogo, la mancanza di accettazione commerciale delle criptovalute e il crollo del mercato delle criptovalute sono il principale rischio economico che può derivare dalla diffusione delle medesime.

Venezuela e Cina sono alcuni degli esempi più eclatanti di accettazione delle criptovalute. Ad esempio, in Venezuela da diversi anni il Petro paga pensioni e stipendi ai dipendenti pubblici. Inoltre, una delle più potenti società petrolifere statali (PDVSA) è già passata completamente ai pagamenti nella criptovaluta nazionale.[401]

La Cina ha lanciato la sua propria piattaforma blockchain nazionale BSN nell'aprile 2020 e il 15 aprile sono iniziati i test della criptovaluta statale DCEP. Nel giugno 2020 è stato pubblicato il Piano di sviluppo dell'innovazione blockchain di Pechino per il periodo 2020-2022 che dovrebbe diventare il più grande hub blockchain del mondo.

A tal fine, nei prossimi due anni è prevista l'integrazione di decine di innovazioni blockchain nell'economia e nelle infrastrutture della città, per poi utilizzarla per la registrazione delle transazioni immobiliari, per scopi fiscali, ecc.

Tuttavia, in alcuni Paesi, ad esempio in Egitto, qualsiasi tipo di cripto-operazione è severamente vietata in quanto contraria ai fondamenti dell'Islam. In generale, nella maggior parte dei Paesi del mondo, il campo di applicazione delle criptovalute è ancora notevolmente limitato: diversi Paesi non le accettano per i pagamenti. Di

[401] MOSAKOVA E.A. (2002). *National cryptocurrency as Venezuela's economic development factor in the 21st century*, Iberoamérica. no. 1. pp. 160-176

conseguenza, la quota delle criptovalute sul totale dei fondi è ancora insignificante e si attesta su un livello inferiore all'1%.[402]

In secondo luogo, l'elevata volatilità del tasso di cambio costituisce la seconda conseguenza economica che può intaccare la diffusione delle monete virtuali. La maggior parte delle criptovalute moderne sono decentralizzate, il che significa che non c'è un unico centro di emissione e quindi non c'è una proprietà di sicurezza per le transazioni. Inoltre, la determinazione del tasso di cambio delle criptovalute viene effettuata solo sulla base dell'interazione di mercato tra domanda e offerta. L'aumento della domanda di criptovalute è dovuto al notevole interesse per il nuovo strumento e, di conseguenza, ha una significativa componente speculativa, che a sua volta crea opportunità per la manipolazione delle criptovalute. Di conseguenza, le transazioni finanziarie con le criptovalute non sono controllate o regolamentate da agenzie governative, per cui rappresentano un rischio finanziario significativo per gli investitori e per l'intero mercato delle criptovalute.

Terzo, il fallimento e/o la chiusura delle borse di criptovalute. Negli ultimi cinque anni, circa la metà delle borse di criptovalute ha chiuso o è fallita. Allo stesso tempo, di norma, gli utenti non hanno avuto il tempo di ritirare il denaro dai loro conti e di conseguenza, le criptovalute sono scomparse. Naturalmente, per mantenere la propria reputazione, molte borse cercano di recuperare le perdite. Un esempio positivo è il fallimento di Bitfinex nel 2018, che è stata in grado di risarcire i propri clienti.

Infine, la possibilità di utilizzare le criptovalute come piramidi finanziarie, che rappresenta una minaccia significativa per l'economia.

5. I diversi approcci degli Stati membri dell'UE: alcuni esempi

Gli approcci alla regolamentazione legale delle criptovalute e gli atteggiamenti nei loro confronti sono diversi nei vari Paesi del mondo. Alcuni esempi. Nella

[402] SHETEWY N., AIT, L. J., e LI, J.-J. (2019). *Challenges of the Bitcoin in the Arabic Countries*

Repubblica di Singapore, la circolazione delle criptovalute e le transazioni relative a questo processo non sono regolate dalla legge. Tuttavia, le attività degli scambi di criptovalute nel territorio di questo Stato sono regolamentate dalle forze dell'ordine sulla sicurezza. A seconda dello Stato americano, una criptovaluta è riconosciuta come una valuta o come una merce di scambio e la sua circolazione è soggetta a licenza, anche se tali transazioni non sono regolamentate a livello federale. Il Giappone regolamenta completamente la circolazione delle criptovalute come asset digitali. A causa dello status legale e finanziario delle criptovalute, le forze dell'ordine giapponesi contrastano adeguatamente le criptovalute illegali e assicurano la sicurezza economica non solo degli individui ma anche delle istituzioni finanziarie pubbliche e private.
In alcuni Paesi le criptovalute sono vietate. Così, le criptovalute sono state vietate in Bolivia, Vietnam, Ecuador, Cina, Thailandia e Turchia. In Ucraina, l'emissione e la circolazione di qualsiasi valuta diversa da quella nazionale e l'uso di surrogati monetari sono vietati.

Dal punto di vista europeo, l'incertezza nel mercato interno dell'UE è generata anche dal fatto che molti Stati membri hanno introdotto o stanno discutendo l'introduzione di una normativa specifica per i cripto-asset. Come vedremo, alcuni Stati membri dell'UE, come Malta e l'Estonia, hanno adottato un approccio progressivo e hanno implementato una normativa nazionale favorevole alle criptovalute al fine di attrarre imprese e investitori stranieri. D'altra parte, alcuni Stati membri dell'UE, come l'Italia che abbiamo analizzato, la Francia, la Germania e il Regno Unito, hanno seguito un approccio più prudenziale nell'implementazione di una regolamentazione interna dei cripto-asset.

5.1 (*Segue):* Approccio cripto-friendly: Malta ed Estonia

Tra gli Stati membri dell'UE che hanno adottato una regolamentazione cripto-friendly di cripto-asset, Malta è stata una delle prime a mostrare un approccio proattivo alla questione. Questo è valso al Paese il soprannome di "*Blockchain*

Island". Infatti, nel luglio 2018, il governo maltese ha approvato il Digital Innovation Framework con l'obiettivo di stabilire un clima normativo favorevole della tecnologia blockchain e cripto-asset. Il quadro, che comprende tre atti (la legge sull'autorità per l'innovazione digitale, la legge sugli accordi e servizi innovativi e la Legge sugli Asset Finanziari Virtuali), richiede alle imprese di ottenere una licenza dalla MFSA (l'autorità nazionale per la concorrenza di Malta) nel caso in cui offrano criptovalute, negozino asset digitali o forniscano portafogli elettronici e attività di intermediazione.[403]

L'Estonia è un altro Stato membro dell'UE che ha introdotto una normativa favorevole alle criptovalute nella prima fase del fenomeno.[404] Infatti, nel 2017 il governo estone ha approvato una serie di nuove leggi volte a sostenere i progetti di criptovaluta introducendo due diverse licenze ossia una per coloro che intendono gestire servizio di scambio di criptovalute e una per coloro che intendono lanciare un'offerta iniziale di monete.[405]

L'Estonia ha anche offerto la possibilità ai cittadini di qualsiasi nazione di ottenere una "residenza digitale" localizzando sé stessi o le proprie aziende in Estonia, ottenendo così le licenze di criptovaluta menzionate, anche se svolgevano la loro attività altrove.[406]

Anche in altri Stati membri dell'UE si possono trovare regimi simili favorevoli alle criptovalute, come la Lituania, Cipro e la Repubblica Ceca.

Ciononostante, negli ultimi due anni, gli Stati membri dell'UE favorevoli alle criptovalute stanno registrando una significativa riduzione del numero di imprese

[403] O'NEAL S. (2020). *As Malta Delays Regulatory Clarity, Fewer Firms Remain on 'Blockchain Island*, Cointelegraph. Disponibile in open source sul sito https://cointelegraph.com/news/asmalta-delays-regulatory-clarity-fewer-firms-remain-on-blockchain-island

[404] ENRIQUES L. (2019). *Welcome to Vilnius: Regulatory Competition in the EU Market for E-Money*, Oxford Business Law Blog. Disponibile in open source sul sito https://www.law.ox.ac.uk/business-law-blog/blog/2019/10/welcome-vilniusregulatory-competition-eu-market-e-money

[405] EVANS C. (2020). *The Great Estonian Exodus — Crypto Firms Are Leaving Estonia*, Cointelegraph Disponibile in open source sul sito https://cointelegraph.com/news/the-greatestonian-exodus-crypto-firms-are-leaving-estonia.

[406] EVANS C., *The Great Estonian Exodus — Crypto Firms Are Leaving Estonia*, Cointelegraph, cit. 372.

che richiedono licenze di criptovaluta o di avviare le loro attività di criptovaluta. La ragione principale è l'attuazione della quinta direttiva antiriciclaggio e antiterrorismo, che deve essere recepita in tutti gli Stati membri dell'UE. Di conseguenza, anche gli Stati membri dell'UE più favorevoli alle criptovalute dovranno ora operare nell'ambito di una normativa ben definita.[407]

5.2 (*Segue):* L'approccio prudente di Regno Unito, Francia e Germania

Dall'altro lato, abbiamo un gruppo di Stati membri dell'UE che, pur mostrando un atteggiamento aperto nei confronti della tecnologia blockchain e delle sue applicazioni, hanno adottato un approccio più prudenziale nella regolamentazione della tecnologia blockchain e delle criptovalute.

a) Regno Unito

Il Regno Unito, ad esempio, regolamenta i cripto-asset solo per il contrasto al riciclaggio e al finanziamento del terrorismo, mentre per altre questioni si affida ancora alla soft law. A questo proposito, la FCA (autorità di regolamentazione finanziaria del Regno Unito) ha pubblicato nel 2019 le sue linee guida sui cripto-asset,[408] con l'obiettivo di fornire agli operatori di mercato e alle parti interessate una chiarezza sulle tipologie di cripto-asset che rientrano nella sfera di competenza della FCA e sugli obblighi normativi che ne derivano per le imprese, insieme alle protezioni normative per i consumatori.[409]

In seguito, il 10 gennaio 2020, la FCA è stata nominata regolatore finanziario e di prevenzione del Regno Unito e supervisore dei cripto-asset nel contesto

[407] O'NEAL S., *As Malta Delays Regulatory Clarity, Fewer Firms Remain on 'Blockchain Island*, Cointelegraph, cit. 370.
[408] FINANCIAL CONDUCT AUTHORITY (FCA) (2019). *Guidance on Cryptoassets*, PS 19/22. Disponibile in open source sul sito https://www.fca.org.uk/publication/policy/ps19-22.pdf.
[409] FINANCIAL CONDUCT AUTHORITY (FCA). *Guidance on Cryptoassets*, PS 19/22, cit. 376

dell'attuazione della Quinta Direttiva Antiriciclaggio. Di conseguenza, le nuove cripto-imprese (che hanno iniziato a operare dopo il 10 gennaio 2020) devono registrarsi presso la FCA prima di iniziare a svolgere la propria attività,

Inoltre, nell'ottobre 2020, la FCA ha pubblicato le regole definitive che vietano la vendita di derivati ed exchange traded notes (ETN) che fanno riferimento ad alcuni tipi di cripto-asset ai consumatori al dettaglio, in quanto la FCA ritiene che questi prodotti non siano adatti ai consumatori al dettaglio a causa dei danni che comportano.[410]

Inoltre, l'ente di riscossione delle imposte del Regno Unito, HMRC (Her Majesty's Revenue and Customs), ha pubblicato nel dicembre 2019 le sue linee guida sulla tassazione dei cripto-asset nel Regno Unito,[411] che coprono attività come il trading di criptovalute, i pagamenti e il mining. Senza entrare nel merito delle questioni fiscali, è interessante menzionare che i cripto-asset (compresi i token di pagamento) non sono considerati moneta o denaro, ma piuttosto beni, in quanto la maggior parte degli individui detiene le criptovalute come investimento personale e, pertanto, pagheranno l'imposta sulle plusvalenze quando ne "disporranno".[412]

b) Francia

La Francia ha regolamentato le offerte iniziali di monete (ICO) e gli intermediari che forniscono servizi di cripto-asset in virtù di una legge del 2019.[413] L'obiettivo era duplice: attirare progetti meritevoli sul suo territorio e, allo stesso tempo, far rientrare questo ecosistema nell'ambito della regolamentazione.[414]

---

[410] Vedi https://www.fca.org.uk/news/press-releases/fca-bans-sale-crypto-derivativesretail-consumers.

[411] Disponibile in open source sul sito https://www.gov.uk/government/publications/tax-oncryptoassets/cryptoassets-for-individuals.

[412] STRICKLAND B. (2019). *Crypto Taxes in the United Kingdom*, TokenTax. Disponibile in open source sul sito https://tokentax.co/guides/crypto-taxes-in-united-kingdom/.

[413] PACTE law n° 2019-486 del 22 maggio 2019.

[414] BARSAN I. (2020)., *France: Regulation of Crypto-assets, Intermediaries and Initial Coin Offerings in France*, Global Compliance News. Disponibile in open source sul sito https://globalcompliancenews.com/france-regulation-of-crypto-assets-intermediariesand-initial-coin-offerings-s-in-france/.

Così, quando la Francia ha recepito la quinta direttiva antiriciclaggio, ha fatto un ulteriore passo in avanti imponendo ulteriori obblighi normativi aggiuntivi per gli intermediari.[415] Ai sensi della normativa vigente, gli emittenti di ICO hanno la possibilità, ma non l'obbligo, di richiedere un "visto" all'autorità francese di regolamentazione dei mercati finanziari (AMF) in cambio del deposito di un documento informativo, fornendo al pubblico comunicazioni chiare, trasparenti e non fuorvianti, e rispettando gli obblighi in materia di antiriciclaggio (AML).[416]
Il visto rimane facoltativo e la raccolta di fondi senza il visto dell'AMF continuerà a essere legale in Francia.

Tuttavia, gli emittenti che non hanno ricevuto il visto AMF non saranno in grado di ricorrere alla sollecitazione generale.[417] Inoltre, se lo desiderano, i fornitori di servizi per gli asset digitali possono ottenere una licenza e sotto la supervisione dell'AMF. Indipendentemente dal fatto che scelgano o meno di ottenere la licenza facoltativa, i fornitori di servizi che desiderano fornire servizi di asset digitali, servizi di custodia a terzi o per l'acquisto/vendita di beni digitali in cambio di moneta legale sono soggetti all'obbligo di registrazione presso l'AMF in conformità alla Quinta Direttiva Antiriciclaggio.
Infine, per quanto riguarda il regime fiscale, secondo le linee guida della Direction Générale des Finances Publiques (DGFP, Direzione Generale delle Finanze Pubbliche), le plusvalenze derivanti dalla vendita di criptovalute sono soggette a tassazione, anche se saranno tassate in modo diverso a seconda che l'acquisizione e la vendita di criptovalute da parte del contribuente sia un'attività occasionale o abituale.

c) Germania

[415] BARSAN I. (2020)., *France: Regulation of Crypto-assets, Intermediaries and Initial Coin Offerings in France*, cit. 382
[416] BARSAN I. (2020)., *France: Regulation of Crypto-assets, Intermediaries and Initial Coin Offerings in France*, cit. 382
[417] Vedi https://www.amf-france.org/en/news-publications/news/towards-new-regimecrypto-assets-france.

La Germania ha adottato un nuovo regime normativo per i cripto-asset in relazione all'attuazione della quinta direttiva antiriciclaggio. In primo luogo, la riforma introduce la nuova categoria di "cripto-asset" nella definizione tedesca di "strumenti finanziari" stabiliti nella legge bancaria tedesca (KWG), che comprende diverse classi di cripto-asset, tra cui i token di pagamento e i token di investimento.[418] Inoltre, la riforma introduce il nuovo servizio finanziario regolamentato ossia l'"attività di custodia di criptovalute", definita come la custodia, amministrazione o custodia di cripto-asset o chiavi crittografiche private utilizzate per detenere, conservare o trasferire cripto-asset come servizio per altri.[419] I fornitori di servizi come i custodi wallet avranno quindi bisogno di una licenza per l'attività di custodia di criptovalute rilasciata dall'autorità di regolamentazione finanziaria tedesca (BaFin).

La BaFin ha pubblicato le sue linee guida sull'interpretazione degli emendamenti al KWG che riguardano l'interpretazione di "attività di custodia di criptovalute" e la domanda di autorizzazione per l'attività di custodia di criptovalute.[420]

Inoltre, la Germania ha approvato una legge, (n. 598/19)[421] che consente alle banche di vendere e archiviare criptovalute e BaFin ha mostrato forte sostegno verso gli investimenti token, mostrando quindi un approccio proattivo.[422] Infine, per quanto riguarda il trattamento fiscale delle criptovalute, anche se non ci sono disposizione giuridiche esplicite, il Ministro delle Finanze tedesco ha pubblicato nel 2018 un

[418] HERKSTRÖTER C., BORN M. (2020). *Crypto Assets: Germany introduces new regulatory regim*e, Norton Rose Fulbright. Disponibile in open source sul sito https://www.regulationtomorrow.com/de/crypto-assets-germany-introduces-newregulatory-regime/.

[419] CHERKSTRÖTER C., BORN M. (2020). *Crypto Assets: Germany introduces new regulatory regim*e, cit. 386.

[420] Federal Financial Supervisory Authority - https://www.bafin.de/EN/Aufsicht/BankenFinanzdienstleister/Zulassung/Krypto verwahrgeschaeft/kryptoverwahrgeschaeft_node_en.html.

[421] Disponibile in open source sul sito https://www.bundesrat.de/SharedDocs/beratungsvorgaenge/2019/0501-0600/0598-19.html

[422] FRIES T. (2020)., *Germany Passes Law Enabling Banks to Store Cryptocurrencies*, The Tokenist. Disponibile in open source sul sito https://tokenist.com/germany-passes-law-enabling-banksto-store-cryptocurrencies/.

documento[423] con cui ha chiarito che la Germania tratterà le criptovalute come le monete aventi corso legale ai fini fiscali quando esse vengono utilizzate per i pagamenti.

Concludendo, i diversi regimi, talvolta incoerenti, presenti nei diversi Stati membri rappresentano un serio rischio per l'armonizzazione della normativa tra i diversi Stati membri nonché per quelle classi di cripto-asset non coperte dal diritto finanziario dell'Unione europea. A ciò si aggiunga che, a livello mondiale, tenendo conto dello sviluppo sempre più attivo delle capacità dei criminali, sia tecniche che intellettuali, è necessario riconoscere le criptovalute come mezzo di pagamento legale. Questo ridurrà il grado di rischiosità dell'utilizzo delle criptovalute nonché consentirà di riconoscere i pagamenti in criptovalute come quelli effettuati in ambito legale.[424]

[423] Disponibile in open source sul sito https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Steuerarten/Umsatzsteuer/Umsatzsteuer-Anwendungserlass/2018-02-27-umsatzsteuerliche-behandlung-von-bitcoin-und-anderen-sog-virtuellen-waehrungen.pdf;jsessionid=50B81F7F4C1885DD69ECE00796509FB1?__blob=publicationFile&v=1.

[424] O'NEAL S., *As Malta Delays Regulatory Clarity, Fewer Firms Remain on 'Blockchain Island*, Cointelegraph, cit. 370.

CAPITOLO III

Sommario: 1. La sicurezza degli E-*Wallet* - 2. Minacce informatiche - 2.1. (*Segue*): Memoria e archiviazione - 2.2. (*Segue*): Sistemi operativi - 2.3. (*Segue*): Software - 2.4. (*Segue*): Protocollo Blockchain - 2.4. (*Segue*): Altri fattori di rischio – 3. Case study e aspetti processuali - 3.1. (*Segue*): Le prove digitali e classificazione giuridica delle prove - 3.2. (*Segue*): le indagini digitali - 3.3. (*Segue*): I soggetti processuali nelle indagini informatiche – 3.4 (*Segue*): il caso Silk Road e Bitgrail - 3.5 (*Segue*): Case study sugli incidenti di sicurezza verificatisi presso i *wallet provider* e analisi delle cause

Il presente capitolo, sarò dedicato all'analisi circa la sicurezza dei portafogli digitali. In particolare, partendo da un'analisi della sicurezza degli *E-Wallet* si provvederà ad illustrare il grado di sicurezza delle diverse tipologie di portafogli digitali fino ad arrivare ad analizzare le diverse minacce informatiche che possono comportare delle problematiche dal punto di vista della sicurezza. Premesso ciò, dato l'elevato numero di reati che avvengono mediante l'attacco a tali tipologie di portafoglio si è deciso di procedere ad un'analisi dei diversi aspetti processuali che ad oggi hanno presentato una necessaria evoluzione per poi concludere con l'analisi di due tipologie di *case study:* la prima tipologia fa riferimento ai casi Silk Road e Bitgrail al fine di evidenziare come la tecnologia *blockchain* e l'utilizzo di tecnologie digitali hanno modificato l'espletamento delle indagini e le prove da ricercare, mentre la seconda tipologia riguarda gli incidenti di sicurezza che interessato diverse società fornitrici di servizi di criptovalute.

1. La sicurezza degli E-*Wallet*

I portafogli elettronici sono un'invenzione abbastanza recente che negli ultimi anni è diventata sempre più rilevante con l'ingresso nell'era della digitalizzazione, in cui si sta verificando una transizione dal denaro fisico al denaro elettronico e alle criptovalute. Essi sono uno strumento digitale che consente a un individuo di memorizzare, inviare e ricevere beni digitali come Bitcoin ed Ethereum. Questi portafogli utilizzano chiavi private o password per accedere alle criptovalute

memorizzate su una blockchain, un registro digitale che registra tutte le transazioni di una specifica attività digitale. I portafogli di criptovalute sono disponibili in varie forme, tra cui applicazioni mobili e dispositivi hardware fisici, e vengono utilizzati per autenticare e completare le transazioni con le criptovalute. È importante notare che un portafoglio di criptovalute non conserva la criptovaluta stessa, ma piuttosto le chiavi private necessarie per accedervi sulla blockchain. Questi portafogli rappresentano una misura di sicurezza fondamentale per la protezione e la gestione dei beni digitali.[425]

I mercati di questi metodi di pagamento elettronici hanno un futuro promettente, ma il loro successo è incerto a causa di potenziali nuove invenzioni tecnologiche nonché a causa delle diverse minacce che i pagamenti elettronici possono presentare.[426]

Un portafoglio elettronico o digitale trasforma il modo in cui le persone acquistano e pagano le cose, cambiando i mezzi di pagamento in app sui telefoni cellulari.[427] Tutte le informazioni memorizzate in un portafoglio sono crittografate attraverso l'uso di coppie di chiavi pubbliche e private, necessarie per garantire che i pagamenti e altri dati siano gestiti in modo sicuro. Come accennato precedentemente, esistono portafogli per le valute convenzionali e per le criptovalute (come il Bitcoin), che richiedono l'utilizzo di chiavi pubbliche e private. [428]

Quindi, i portafogli per le criptovalute sono necessari agli utenti per poter gestire il proprio denaro. Un'applicazione di questo tipo è molto simile a un portafoglio tradizionale. L'utente tiene il proprio denaro in esso fino a quando non si vuole

[425] INTIGROW (2020). *What are the security risks associated with using a cryptocurrency wallet?* Disponibile in open source sul sito https://intigrow.com/what-are-the-security-risks-associated-with-using-a-cryptocurrency-wallet/

[426] DAHLBERG T. et al. (2008). *Past, present and future of mobile payments research: A literature review*. In: Electronic Commerce Research and Applications. Special Section: Research Advances for the Mobile Payments Arena, pp. 165–181.

[427] CHANDLER N. (2012). *How Digital Wallets Work. HowStuffWorks.* Disponibile in open source sul sito https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/digital-wallet.htm

[428] SALAMONE G. (2022). *Wallet e sicurezza informatica* in dgroove.it. Disponibile in open source sul sito https://www.dgroove.it/wallet-e-sicurezza-informatica/9351/

acquistare qualcosa o ottenere il denaro che si desidera, ossia effettuare transazioni. Poiché le criptovalute sono una valuta virtuale, gli utenti devono conservarla su un supporto chiamato portafoglio di criptovalute. Questi portafogli possono esistere in diversi formati che verranno spiegati in seguito.

Il primo passo per un utente è decidere quale tipo di portafoglio utilizzare, ad esempio un'applicazione mobile. Il passo successivo è creare un account. A questo scopo, esistono diversi livelli di anonimato.[429] Alcuni portafogli richiedono il nome e l'indirizzo e-mail, mentre altri non chiedono alcuna informazione personale.

Il portafoglio in sé non conserva alcuna moneta. Tuttavia, memorizza e protegge la chiave privata che è essenziale per eseguire le transazioni e, quindi, per utilizzare le monete. Altre informazioni come l'hash della chiave pubblica che equivale all'indirizzo, la cronologia delle transazioni e la quantità di criptovalute sono memorizzate nella Blockchain. [430]

Un modo per proteggere la chiave privata e gli altri dati sensibili memorizzati nel portafoglio è la crittografia. Questa potrebbe essere combinata con un meccanismo di blocco, un PIN o una password per accedere all'applicazione. Il PIN e altri meccanismi di protezione come le password e l'autenticazione biometrica (ad esempio, le impronte digitali) aiutano a evitare l'accesso di altre persone e quindi le transazioni non autorizzate.

In termini di sicurezza, si possono distinguere tre diversi livelli: i portafogli full-service, i portafogli di sola firma e i portafogli di sola distribuzione.

Il primo tipo, ossia i portafogli full-service, offre tutti i servizi contemporaneamente: può generare chiavi, firmare ed eseguire transazioni. I

[429] SURATKAR S., SHIROLE M. e BHIRUD S. (2020). *Cryptocurrency wallet: A review*. Disponibile in open source sul sito https://www.scopus.com/inward/record.uri? eid=2-s2.0-85100199489&doi=10.1109%5C%2fICCCSP49186.2020.9315193&partnerID=40&md5=ab58c4f8c894676c4662df2e3ac9b7cd.

[430] Disponibile in open source sul sito https://fortgale.com/news/2021/11/15/attacco-html-smuggling-tecnica-sempre-piu-diffusa/

portafogli full-service devono disporre di un accesso a Internet, il che li rende più inclini agli attacchi di rete.

I portafogli di sola firma, invece, rispetto a quelli sopra descritti, cercano di ridurre queste vulnerabilità. Non sono connessi a Internet e quindi non possono eseguire transazioni, il che significa che gli utenti devono combinarli con un portafoglio online.

Infine, l'ultimo tipo è quello dei portafogli di sola distribuzione, che mirano a minimizzare i problemi dei portafogli a servizio completo, essendo organizzati in una rete di portafogli in modo tale che tutti possono calcolare le chiavi pubbliche di ogni portafoglio della rete, ma nessun portafogli esterno può farlo.[431] Per il recupero vengono spesso utilizzate passphrase basate su mnemotecniche. A questo scopo, viene generato un seme di solito composto da 12 - 24 parti, in cui ogni elemento è costituito da una parola diversa, predefinita o auto-selezionata. La chiave viene quindi generata sulla base di queste parole. Gli utenti devono solo ricordare correttamente le parole e la loro sequenza; quindi, possono ricalcolare ripetutamente la chiave e recuperare il portafoglio. Le mnemotecniche sono note per essere più facili da ricordare rispetto alle password convenzionali, che sono generate in modo casuale e hanno una lunghezza di 12-24 parole.

Al fine di garantire la sicurezza dei portafogli digitali vi sono alcune modalità, tra cui la crittografia che viene utilizzata dagli stessi per proteggere le informazioni di pagamento degli utenti da hacker e altri utenti non autorizzati, oppure l'utilizzo di password e PIN per accedere alle informazioni di pagamento. Questo aggiunge un ulteriore grado di sicurezza.

Alcuni portafogli digitali utilizzano l'autenticazione a due fattori, che richiede agli utenti di inserire un codice fornito al telefono o all'e-mail per convalidare la propria identità.

[431] ZAGHLOUL E., LI T., MUTKA M. W. e REN J. (2020). *Bitcoin and blockchain: Security and privacy*, IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10. Disponibile in open source sul sito https://doi.org/10.1109/JIOT.2020.3004273

Nell'era dei pagamenti digitali e delle transazioni online, i portafogli digitali sono diventati un metodo di pagamento sempre più diffuso. Tuttavia, per quanto comodi, i portafogli digitali sono anche vulnerabili alle violazioni della sicurezza e ai tentativi di hacking. Ci sono diversi accorgimenti che gli utenti possono adottare per proteggere il proprio portafoglio di criptovalute e mitigare i rischi di furto o perdita. Una misura importante è quella di scegliere un portafoglio che memorizzi le chiavi private in forma criptata, il che aggiunge un ulteriore livello di sicurezza. Gli utenti dovrebbero anche prendere in considerazione l'aggiunta di ulteriori misure di sicurezza al proprio smartphone, come un autenticatore di impronte digitali, per evitare accessi non autorizzati. Anche password forti e uniche possono aiutare a proteggersi dalle violazioni e molti portafogli offrono ulteriori funzioni di sicurezza, come l'autenticazione a due fattori. È importante disporre di un piano per reagire a qualsiasi attività insolita sul portafoglio o a una potenziale violazione dei dati. Un'altra opzione per aumentare la sicurezza è quella di utilizzare un portafoglio hardware, ovvero un dispositivo fisico che memorizza le chiavi private e richiede un PIN per accedervi. [432]

Questi portafogli, che non sono collegati a Internet e sono spesso definiti portafogli "freddi", possono offrire una maggiore protezione contro gli hacker e altre minacce digitali. È importante che gli utenti dei portafogli di criptovalute prendano provvedimenti per proteggere le loro chiavi private e tutelare i loro beni digitali. Esistono diversi tipi di portafogli tra cui scegliere, tra cui opzioni mobili, desktop, basate sul web e hardware, ognuno con caratteristiche e vantaggi unici. Per ridurre i rischi associati all'uso di un portafoglio digitale, gli utenti dovrebbero considerare l'aggiunta di ulteriori misure di sicurezza, come password forti e autenticazione a due fattori, e scegliere un portafoglio che memorizzi le chiavi private in forma criptata. Adottando queste precauzioni, gli utenti possono assicurarsi che le loro chiavi private rimangano al sicuro e ridurre il rischio di furto o perdita.[433]

[432] REZAEIGHALEH H. (2020). *Improving security of crypto wallets in blockchain technologies.* Disponibile in open source sul sito https://www.cs.ucf.edu/~czou/research/HosseinDissertation-2020.pdf

[433]INTIGROW, *What are the security risks associated with using a cryptocurrency wallet?* cit. 390

Per questo motivo, è importante seguire alcune best practice per mantenere i portafogli digitali al sicuro, come per esempio[434] scegliere un fornitore di portafogli digitali affidabile, controllare la storia del fornitore e le recensioni dei clienti per assicurarsi che abbia una solida reputazione in termini di sicurezza e affidabilità oppure utilizzare password e metodi di autenticazione forti, in quanto, nel concreto, le password forti sono la prima linea di difesa contro l'accesso non autorizzato al portafoglio digitale. Gli utenti dovranno utilizzare password uniche e complesse, difficili da indovinare, e non utilizzare le stesse password su più account, oltre, ad attivare l'autenticazione a due fattori (2FA) per una maggiore sicurezza per accedere al portafoglio digitale effettuando un ulteriore passaggio, come l'impronta digitale o un codice. Altro elemento di sicurezza per l'utente è tenere aggiornato il software del portafoglio digitale oppure utilizzare una rete sicura; ciò significa evitare di utilizzare Wi-Fi pubblici o reti non sicure, perché potrebbero esporre eventuali informazioni sensibili agli hacker. L'utilizzo invece una rete affidabile, come la rete Wi-Fi di casa o una rete mobile dotata di connessione sicura apporterà maggiore sicurezza.

2. Minacce informatiche

Le minacce informatiche possono essere definite come tutte quelle attività di carattere ostile ed aggressivo volte a compromettere la sicurezza di un sistema informatico, di una rete oppure, in molti casi, dei dati in essi contenuti. Questi attacchi possono essere compiuti da individui, gruppi più o meno organizzati o anche da governi stranieri e possono avere diverse finalità quali danneggiare l'integrità dei dati, pregiudicare e/o ritardare il funzionamento di una rete od, anche, richiedere un riscatto per ripristinare il sistema aggredito. Oggi le minacce informatiche si evolvono di pari passo con l'evoluzione dei sistemi informatici e possono assumere diverse forme tra cui, per dirne alcuni, virus, malware, phishing, attacchi ransomware, e tanti altri. Poichè, come detto, esistono diversi modi per accedere alle informazioni sensibili memorizzate nei portafogli, il rischio

[434]SALAMONE G., *Wallet e sicurezza informatica*, cit. 393

maggiore può verificarsi quando alcuni *wallet* memorizzano le chiavi in un formato non appropriato, ad esempio memorizzando le chiavi private in testo in chiaro. In questa sezione, riepiloghiamo i vettori di attacco trovati per applicazioni di portafogli di criptovalute. La struttura di questa sezione si basa sui diversi livelli di vettori di attacco, a partire dagli attacchi/vulnerabilità che utilizzano la memoria del dispositivo, proseguendo con le vulnerabilità a livello di sistema operativo, ad esempio le vulnerabilità basate sul sistema operativo (OS) dei dispositivi Android.[435]

Dopo il sistema operativo, viene analizzato il livello software, per essere più specifici, le vulnerabilità basate sui portafogli di criptovalute. Successivamente, viene preso in considerazione il livello di rete e, ultimo ma non meno importante, i protocolli Blockchain.

2.1 (*Segue):* Memoria e archiviazione

Il livello più basso a cui i portafogli digitali hanno rivelato le vulnerabilità è la memoria.

In questo caso gli attacchi sono di solito utilizzati per raccogliere i dati necessari per individuare la vulnerabilità del portafogli digitale a uno o più livelli. L'analisi portata avanti da Zollner et al. ha dimostrato che a seconda del browser utilizzato, si è in grado di estrarre gli URL di tutti i portafogli utilizzati e artefatti come la passphrase mnemonica e l'ID del portafoglio.[436] Questo è stato possibile con Firefox in modalità di navigazione privata su un computer Windows 7; con il browser Google Chrome in modalità incognito su un computer Windows 7; con l'utilizzo di Internet Explorer in modalità di navigazione privata, è possibile ottenere le stesse informazioni indipendentemente dalla versione di Windows (7 e

[435] FADDA D. (2023). *Il malware BlackGuard si aggiorna e prende di mira i crypto wallet: tutti i dettagli*. Disponibile in open source sul sito https://www.cybersecurity360.it/news/il-malware-blackguard-si-aggiorna-e-prende-di-mira-i-crypto-wallet-tutti-i-dettagli/

[436] ZOLLNER S., CHOO K. K., e LE-KHAC L. L. (2019). A*n automated live forensic and postmortem analysis tool for bitcoin on windows systems*, IEEE Access, vol. 7, pp. 158 250–158 263. Disponibile in open source sul sito https : / / www . scopus . com / inward / record . uri ? eid = 2 - s2 . 0 - 85078049505 & doi = 10 . 1109 % 5C % 2fACCESS . 2019 . 2948774 & partnerID = 40 & md5 = 4ad815a8a0b195da4b292db048801ae5.

10) e con il browser TOR, con il quale però è stato possibile vedere solo l'URL del portafoglio blockchain.info.

Haigh et al. [437] hanno testato sette diverse applicazioni di criptovaluta per Android attraverso una combinazione di analisi dello storage e del codice. L'analisi dello storage o degli artefatti comprende la ricerca sul dispositivo delle chiavi private e dei *seed* (seme) del portafoglio che potrebbero essere utilizzati per accedere al portafoglio stesso ed eseguire transazioni. La cronologia delle transazioni e alcuni dati specifici dell'applicazione, come i PIN, potrebbero essere trovati nella memoria e una volta trovati l'aspetto più critico rilevato è proprio la memorizzazione impropria di informazioni sensibili come chiavi private o semi.[438]

Portafogli basati su Web/browser hanno, quindi, possibilità illimitate di malware. I browser sono tipicamente un bersaglio che possono garantire l'accesso alla memoria agli aggressori. È inoltre frequente assistere a tentativi di phishing che inseriscono una versione dannosa di schermate di transazioni sensibili come "importa conto" o "invia transazione". Anche la sostituzione del contenuto degli appunti con l'indirizzo del portafoglio dell'aggressore è un attacco comune.[439]

2.2. (*Segue*): Sistemi operativi

Quando si parla di vulnerabilità del sistema operativo, la maggior parte dei dati sui portafogli di criptovalute si concentra sulle applicazioni Android. Il modello di attacco presuppone sempre che l'attaccante abbia ottenuto l'accesso al dispositivo, ossia le chiavi e le frasi di accesso a un portafoglio di criptovalute vengono rubate dinamicamente, intercettandole mentre il proprietario del portafoglio digita i

[437] HAIGH T., BREITINGER F. e BAGGILI I. (2018). *If i had a million cryptos: Cryptowallet application analysis and a trojan proof-of-concept*, in International Conference on Digital Forensics and Cyber Crime, Springer, pp. 45–65.

[438]MESSINA A., *Mondo crypto: i principali attacchi e minacce ai conti* in agendadigitale.eu., cit. 403

[439] KP (2023). *An Introduction to Crypto Wallets and How to Keep Them Secure*, in QuickNode. Disponibile in open source sul sito https://www.quicknode.com/guides/web3-fundamentals-security/security/an-introduction-to-crypto-wallets-and-how-to-keep-them-secure/

caratteri della chiave o della frase di accesso nell'applicazione mobile del portafoglio di criptovalute. Per farlo, gli hacker utilizzano in genere uno dei tre metodi seguenti.

Il primo metodo prevede che l'aggressore abbia installato un'applicazione dannosa sul dispositivo della vittima ovvero il cd. *keylogging Malware.* I portafogli che possono essere memorizzati su dispositivi mobili sono soggetti a vulnerabilità mobili.[440] Li et al.[441] spiegano come un'applicazione con funzioni di accessibilità abilitate possa catturare informazioni sensibili se combinata con una tastiera di terzi. La casella di testo della password non può essere osservata facilmente ma l'aggressore potrebbe ascoltare gli eventi di clic attivati dalla tastiera di terze parti. I ricercatori hanno dimostrato che l'attacco descritto sopra è applicabile a Blockchain Wallet e all'applicazione MEWconnect. Inoltre, mediante applicazioni si possono catturare la passphrase e le mnemotecniche utilizzabili nei due portafogli Huobi Wallet e iMToken.[442]

Una volta che l'applicazione dannosa è installata sul dispositivo della vittima, l'aggressore ha ancora più opzioni, tra cui quella di accedere sia alla memoria interna che alla memoria esterna dei dispositivi. In particolare, Android divide tra memoria esterna e interna, che si differenziano principalmente per il livello di sicurezza. Ogni app ha una memoria interna in cui memorizza tutti i dati specifici dell'app e solo l'app stessa o il root possono accedervi. Il permesso di accedere alla memoria esterna, che contiene foto, documenti, video, download e così via, può essere concesso a tutti i membri dell'app, download etc e può essere richiesta da qualsiasi applicazione in fase di esecuzione.[443]

---

[440] KP, *An Introduction to Crypto Wallets and How to Keep Them Secure*, cit. 408

[441] LI C., HE D., Li S., ZHU S., CHAN S. e CHENG Y. (2020). *Android-based cryptocurrency wallets: Attacks and countermeasures*, pp. 9–16. Disponibile in open source sul sito https://www.scopus.com/inward/record.uri?eid=2-s2.0-85099217819&doi=10.1109%5C%2fBlockchain50366.2020.00010&partnerID=40&md5=dd848cd1d86cd627f1114cdfa283cd9a.

[442] LI C., HE D., Li S., ZHU S., CHAN S. e CHENG Y., *Android-based cryptocurrency wallets: Attacks and countermeasures*, cit. 410

[443] MESSINA A., *Mondo crypto: i principali attacchi e minacce ai conti* in agendadigitale.eu., cit. 403

Per costringere l'utente a concedere questa autorizzazione, l'applicazione potrebbe mostrare una finestra pop-up che deve essere accettata per utilizzare l'applicazione. Un'altra opzione potrebbe essere quella di imitare una vecchia versione di Android, dal momento che per queste non è richiesta l'autorizzazione richiesta di routine. Così facendo l'aggressore potrà accedere a informazioni sensibili quali gli ID delle transazioni, la chiave privata e la parola mnemonica.

Il secondo metodo prevede che l'aggressore abbia ottenuto l'accesso utilizzando il debug USB ovvero attacco in sovraimpressione. Nel caso in cui si utilizzi il debug (USB o wireless) come metodo di accesso, esso viene spesso combinato con lo strumento Android Debug Bridge (adb). Supponendo che l'aggressore stesso non abbia accesso diretto al dispositivo può infiltrarsi nel computer a cui il telefono è collegato creando una schermata che può sembrare autentica e che spinge la vittima ad inserire le credenziali.[444] In questo caso l'aggressore potrà eseguire la scansione della memoria del dispositivo mobile e cercare informazioni.[445] Una vulnerabilità, generalmente specifica di Android, che può essere utilizzata come un attacco contro i portafogli di criptovalute.[446]

Il terzo metodo prende il nome di attacco *over-the-shoulder*. Storicamente, questo si riferisce a un hacker che è fisicamente e surrettiziamente abbastanza vicino a un utente da vederlo inserire la frase d'accesso nel *crypto wallet*. Oggi, però, non è necessario essere presenti in quanto, a questo scopo si può abusare di *screenshot* e registrazioni dello schermo. Per difendersi da queste minacce, l'applicazione deve rilevare il *keylogging*, le sovrapposizioni e le registrazioni, in modo da poter intervenire direttamente avvertendo il proprietario del portafoglio o addirittura chiudendo completamente l'applicazione.[447]

---

[444] LI C., HE D., Li S., ZHU S., CHAN S. e CHENG Y., *Android-based cryptocurrency wallets: Attacks and countermeasures*, cit. 410

[445] LI C., HE D., Li S., ZHU S., CHAN S. e CHENG Y., *Android-based cryptocurrency wallets: Attacks and countermeasures*, cit. 410

[446] MELLA L. (2021). *Bitcoin: tre minacce al portafoglio digitale e tre modi per proteggerlo*, in cibersecurity360.it. Disponibile in open source sul sito https://www.cybersecurity360.it/nuove-minacce/bitcoin-tre-minacce-al-portafoglio-digitale-e-tre-modi-per-proteggerlo/

[447] HSU K. (2022). *The Six Most Common Attacks on Crypto Wallets and Why Banks Should Care* in finextra.com. Disponibile in open source sul sito

2.3. (*Segue*): Software

Alcuni problemi non riguardano né la memoria né il sistema operativo, ma il software utilizzato. I portafogli di criptovalute lasciano artefatti sul dispositivo, anche dopo la rimozione del portafoglio.[448] È possibile trovare artefatti nella cronologia del browser, nella memoria temporanea e nei cookie. I file memorizzati del portafoglio possono rivelare informazioni sull'utilizzo oltre ai file temporanei.[449] Alcuni portafogli di criptovalute salvano le loro credenziali in un formato di file inadeguato, ovvero in forma non crittografata; la conservazione delle chiavi private in un formato non crittografato può portare al furto dell'intero contenuto del portafoglio. A ciò si aggiunga che alcuni portafogli hanno mostrato altrettante carenze pur utilizzando una chiave di crittografia codificata o altre informazioni sensibili. Una chiave di crittografia codificata significa che la chiave per crittografare i dati è fornita dagli sviluppatori e non può essere cambiata senza modificare l'applicazione stessa. L'utilizzo di una chiave di crittografia codificata è sconsigliato perché consente a un aggressore di decifrarla con il minimo sforzo. Il processo di generazione della chiave è uno dei passaggi più critici nell'utilizzo delle criptovalute e deve essere eseguito in modo sicuro per proteggere l'utente da perdite o furti. Tuttavia, il codice crittografico può soffrire di difetti di progettazione e di errori di implementazione e richiede un set di competenze di sviluppo molto di nicchia. In genere i problemi di crittografia sono una combinazione di errori di progettazione e di implementazione.[450]

---

https://www.finextra.com/blogposting/22721/the-six-most-common-attacks-on-crypto-wallets-and-why-banks-should-care

[448]ZOLLNER S., CHOO K. K., e LE-KHAC L. L., A*n automated live forensic and postmortem analysis tool for bitcoin on windows systems*, cit. 405.

[449]SAI A. R., BUCKLEY J. e GEAR A. L. (2019). *Privacy and security analysis of cryptocurrency mobile applications*, Fifth Conference on Mobile and Secure Services, pp. 1–6. Disponibile in open source sul sito https://doi. org/10.1109/MOBISECSERV.2019.8686583.

[450] KP, *An Introduction to Crypto Wallets and How to Keep Them Secure*, cit. 408.

2.4. (*Segue*): Protocollo Blockchain

Con l'aumento degli utenti della tecnologia Blockchain, sempre più persone devono gestire le loro chiavi private. Per semplificare l'archiviazione delle chiavi, sono stati introdotti i cosiddetti *brain wallet*.[451] I *brain wallet* sono portafogli Blockchain che derivano da una *passphrase* data dall'utente o generata in modo casuale, per lo più contenente 12 o 24 parole. Questo metodo sostituisce la necessità di avere un dispositivo fisico su cui memorizzare la chiave e rende impossibile per gli aggressori rubarla, poiché non viene salvata in modo permanente (se non nella memoria dell'utente). In altre parole, il *brain wallet* è il più semplice. L'utente sceglie una *passphrase*, e tutte le chiavi segrete e gli indirizzi segreti sono derivati da questa.[452] Quindi, l'utente non ha bisogno di mantenere un portafoglio cartaceo, software o dispositivo come portafoglio. Ogni volta che deve effettuare una transazione, inserisce la passphrase in un programma di portafoglio e costruisce le chiavi segrete. Dopo aver firmato una transazione, il programma rimuove dalla memoria la *passphrase* e tutte le chiavi costruite. [453]

Il *brain wallet* presenta notevoli svantaggi. In primo luogo, se l'utente dimentica la *passphrase*, perde tutti i fondi. In secondo luogo, il malware nel programma del portafoglio può intercettare la *passphrase* e rubare i fondi. Quindi, offrendo l'accesso alla chiave tramite una *passphrase*, l'aggressore può indovinare la password senza alcuna restrizione e, se indovinata, ha il controllo completo del sistema.[454]

---

[451] VAN DER HORST L.,CHOO K.K. e LE-KHAC N.-A. (2017). *Process memory investigation of the bitcoin clients electrum and bitcoin core*, IEEE Access, vol. 5, pp. 22. Disponibile in open source sul sito https : / / www . scopus . com / inward / record . uri ? eid = 2 - s2 . 0 - 85030756556 & doi = 10 . 1109 % 5C % 2fACCESS . 2017 . 2759766 & partnerID = 40 & md5 = cdbed2e307ee201020d2493409748a5d.

[452] PASCUAL J. L. (2021). *Cos'è un BrainWallet?* in academy.bit2me.com. Disponibile in open source sul sito https://academy.bit2me.com/it/que-es-una-brainwallet/

[453] COINSATRA (2022). *What Is A Brain Wallet & How To Create One For Yourself?* Disponibile in open source sul sito https://coinsutra.com/how-to-create-brain-wallet/

[454] SAI A. R., BUCKLEY J. e GEAR A. L. *Privacy and security analysis of cryptocurrency mobile applications*, cit. 418.

2.5. (*Segue*): Altri fattori di rischio

Non solo la sicurezza dei portafogli è essenziale, ma anche quella delle piattaforme di scambio. Le piattaforme di scambio offrono lo scambio tra denaro fiat in criptovalute. Molte piattaforme di scambio offrono la possibilità di utilizzare portafogli online per utilizzare il loro servizio. Per alcune piattaforme, è anche possibile trasferire le monete acquisite in un portafoglio di proprietà.

Poiché queste piattaforme riuniscono un'enorme quantità di criptovalute, vengono prese di mira molto spesso. Una delle rapine più famose e più grandi su una delle borse è stato messo a segno ai danni della società Mt.Gox. 740.000 Bitcoin.[455]

Oltre agli attacchi alle piattaforme, esistono altre attività criminali. Tuttavia, queste attività non attaccano l'aspetto tecnico della Blockchain, ma si riferiscono all'aspetto sociale. Per esempio, le Initial Coin Offerings (ICO) svolgono un ruolo essenziale.[456] Le ICO sono un modo per sostenere gli sviluppatori nella loro fase di avvio per offrire i loro servizi (per lo più in relazione alla Blockchain) fornendo offerte speciali ai potenziali investitori. Tuttavia, a volte le ICO non hanno alcun valore in cambio e servono solo a truffare gli investitori.

Inoltre, sono apparsi degli attacchi in cui l'aggressore ha convinto l'operatore mobile a passare da una SIM all'altra. Applicando questo cosiddetto SIM-swapping, l'aggressore riceve i messaggi originariamente indirizzati all'obiettivo. Inoltre, si è notato che è possibile accedere agli SMS dell'obiettivo grazie a un malware per accedere al portafoglio.[457]

I portafogli di scambio/deposito, a causa della loro natura di depositari e controllati interamente da una terza parte, sono soggetti a una gamma più ampia di minacce.

[455] IlSole24Ore (2018). *Furti di bitcoin / Mt Gox, il furto più grande*. Disponibile in open source sul sito https://www.ilsole24ore.com/art/furti-bitcoin-mt-gox-furto-piu-grande-AEAL57BE?refresh_ce=1

[456] REDAZIONE OSSERVATORI DIGITAL INNOVATION (2020). *Cosa sono le ICO (Initial Coin Offering) e come funzionano realmente* in Osservatori.net digital innovation. Disponibile in open source sul sito https://blog.osservatori.net/it_it/ico-initial-coin-offering-come-funziona

[457] CRYPTOPEDIA STAFF (2021). *What Is a Cell Phone SIM Swap Attack?* in Cryptopedia. Disponibile in open source sul sito https://www.gemini.com/it-it/cryptopedia/sim-swap-attack-preventing-crypto-fraud

Ad esempio, l'intera entità che controlla i fondi deve implementare la sicurezza a livello aziendale, la gestione delle chiavi, la sicurezza delle applicazioni, la sicurezza dei dati, ecc. per proteggere i fondi e le informazioni.[458] Gli utenti si affidano a un'organizzazione per la gestione dei loro portafogli e dei loro dati. Inoltre, gli utenti che utilizzano servizi di custodia sono soggetti a truffe di phishing che possono raccogliere le credenziali di accesso.[459]

A ciò si aggiunga il rischio per la privacy dell'utente. Difatti, una recente dichiarazione di fallimento della piattaforma di prestito di asset digitali Celsius ha rivelato i nomi e la cronologia delle transazioni di quasi mezzo milione di depositanti.[460] Ciò illustra un rischio derivante dalla trasparenza e dalla tracciabilità della blockchain. Lo standard di privacy della maggior parte delle blockchain pubbliche si basa sullo pseudonimo, che può essere facilmente violato per tracciare l'attività e il saldo degli utenti.[461] Di conseguenza, le fughe di dati sui nomi e sugli indirizzi dei portafogli possono danneggiare la privacy degli utenti della blockchain, poiché chiunque abbia una connessione a Internet può facilmente confrontare l'attività sulla catena e gli indirizzi dei portafogli degli utenti Celsius indicati nel documento con le date e gli importi di ogni transazione sul loro portafoglio, esponendo i proprietari dei portafogli al rischio di furto o estorsione. In pratica, tali fughe di dati possono verificarsi anche semplicemente effettuando transazioni con un'altra parte che conosce l'identità altrui.[462]

Per mitigare questo rischio, i detentori di asset digitali impiegano ulteriori tecnologie di miglioramento della privacy per proteggere la riservatezza delle loro

---

[458] BANCA D'ITALIA (2022). *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività*. Disponibile in open source sul sito https://www.bancaditalia.it/media/approfondimenti/2022/cripto/Comunicazioni-della-Banca-d-Italia-DLT-cripto.pdf

[459] KP, *An Introduction to Crypto Wallets and How to Keep Them Secure*, cit. 408.

[460] BELVEDERE A. (2022). *Celsius rilascia dati transazioni propri utenti* in bitconio.net. Disponibile in open source sul sito https://www.bitconio.net/celsius-network-pubblica-14-000-pagine/

[461] BELVEDERE A., *Celsius rilascia dati transazioni propri utenti*, cit. 429.

[462] DAL CO (2022). *Bitcoin e criptovalute, il quadro si complica: rischi e scenari in attesa delle regole* in agendadigitale.eu. Disponibile in open source sul sito https://www.agendadigitale.eu/mercati-digitali/bitcoin-e-criptovalute-il-quadro-si-complica-rischi-e-scenari-in-attesa-delle-regole/

informazioni finanziarie. Il problema è che le attuali tecniche di gestione del rischio di finanza illecita sulle blockchain si basano sulla trasparenza e sulla tracciabilità per valutare l'identità degli utenti. Di conseguenza, gli stessi strumenti utilizzati per proteggere la privacy sulle blockchain pubbliche possono anche vanificare le indagini governative sulle attività illecite.[463]

Un protocollo di privacy molto utilizzato è stato Tornado Cash, che nei mesi scorsi è stato sanzionato dall'*Office of Foreign Assets Control* (OFAC) del Dipartimento del Tesoro degli Stati Uniti[464] con la motivazione che era stato utilizzato in relazione a oltre sette miliardi di dollari di attività finanziarie illecite. Questo mette gli utenti innocenti della blockchain in una situazione difficile: affidarsi alla privacy attraverso lo pseudo-anonimato, che può essere violato, o vedere i propri fondi associati ad attività criminali, aumentando il rischio di incorrere in sanzioni, di vedersi bloccare i fondi o di veder aumentare il proprio profilo di rischio, limitando potenzialmente la propria libertà di transazione.[465]

Nella finanza tradizionale, l'equilibrio tra privacy e legittimi interessi governativi viene raggiunto attraverso gli intermediari finanziari. In Europa e negli Stati Uniti, il diritto civile alla privacy e alla riservatezza finanziaria limita la capacità degli intermediari di utilizzare i dati finanziari e di altro tipo per scopi commerciali, pur prevedendo eccezioni per la condivisione di informazioni richieste dalla legge con le forze dell'ordine e le autorità di regolamentazione.[466] Se l'ipotesi che gli intermediari finanziari siano in grado di proteggere efficacemente le informazioni personali sensibili si è rivelata problematica (come dimostra la frequenza delle

[463] AMATO M. e FANTACCI L. (2016). *Per un pugno di bitcoin: rischi e opportunità delle monete virtuali*. EGEA spa.
[464] Office of Foreign Assets Control (OFAC) - https://ofac.treasury.gov/
[465] MAIMERI F., MANCINI M. (2019). Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale, in Quaderni di Ricerca Giuridica della Consulenza Legale.
[466] AMATO M. e FANTACCI L. (2016). *Per un pugno di bitcoin: rischi e opportunità delle monete virtuali*, cit. 461.

violazioni dei dati), è insostenibile nel contesto della tecnologia blockchain e della finanza decentralizzata.[467] Ciò solleva una domanda importante:

"È possibile mitigare i rischi di finanza illecita negli asset virtuali preservando la riservatezza di base di cui i cittadini godono nel sistema finanziario tradizionale?"

L'unica cosa nuova che le blockchain possono fare è applicare automaticamente le regole programmandole in contratti intelligenti, in pratica una dichiarazione digitale "se-quando" tra le parti che effettuano transazioni. In origine, le blockchain implementavano regole che si limitavano a stabilire chi possedeva gli asset virtuali e quando si muovevano, ma ora è possibile aggiungere regole aggiuntive che soddisfino l'esigenza di affrontare la finanza illecita e altri rischi di conformità. Le tecnologie crittografiche possono affrontare i rischi identificati dalle autorità e dai responsabili politici e sono attualmente in fase di sviluppo da parte dei tecnici nello spazio blockchain.[468] Queste tecnologie, che sono state sviluppate in ambito accademico per decenni e sono utilizzate in alcune blockchain esistenti, promettono di conciliare le richieste concorrenti di privacy e conformità in un modo più solido di quanto sia attualmente possibile. Tali soluzioni potrebbero, ad esempio, consentire il blocco delle transazioni illegali, la segnalazione automatica alle agenzie governative e la visibilità selettiva delle informazioni sensibili, con un accesso limitato agli agenti autorizzati che dispongono dei diritti di visualizzazione delle informazioni, mentre le transazioni e i saldi dei portafogli rimangono privati e protetti dagli attori malintenzionati.[469]

[467] BANCA D'ITALIA (2018). Avvertenza per i consumatori sui rischi delle valute virtuali da parte delle Autorità Europee.

[468] AJ FRONTIERE N. (2015). *Criptovalute tra opportunità e voglia di regolamentazione*. Disponibile in open source sul sito http://nova.ilsole 24ore.com/frontiere/criptovalute-tra-opportunita-erichieste-di- regolamentazione/.

[469] VERGINE S., BORTOLOTTI A. (2021). *Bitcoin, il futuro in blocchi*, in Economia Comportamentale.

Grazie a queste tecnologie e con il sostegno delle autorità di regolamentazione, sia la compliance che la privacy finanziaria possono diventare parte integrante dell'ecosistema degli asset virtuali.[470]

3. Case study e aspetti processuali

Il presente paragrafo verrà dedicato in primo luogo ad alcuni aspetti processuali derivanti dall'utilizzo di dispositivi digitali e rete internet che hanno comportato un mutamento circa lo svolgimento delle attività processuali. In secondo luogo, verranno analizzati dei *case study* relativi in *primis* alla modifica del processo penale in caso di presenza di prove elettroniche e successivamente alcuni casi occorsi in tempi recenti relativamente ad incidenti di sicurezza aventi ad oggetto gli *E-Wallet.*

Alla luce dell'importante diffusione di reati di natura penale posti in essere mediante l'utilizzo di strumentazioni digitali, come il computer e mediante l'utilizzo della rete Internet, sono sorte una serie di problematiche rilevanti sia per il diritto penale sostanziale sia per il diritto penale processuale.
Se prima la condotta illecita veniva commessa mediante atti e azioni rilevanti dal punto di vista penale, ora invece vengono spesso commesse nel mondo virtuale[471] privo di una dimensione materiale, ossia in modalità non più *offline* ma *online*.[472]
Seguendo quanto dettato dalla Corte di Cassazione

> «*il concetto di azione penalmente rilevante subisce nella realtà virtuale una accentuata modificazione fino a sfumare in impulsi elettronici; l'input rivolto al computer da un atto umano consapevole*

[470] S., J. e E. (2022). *We can finally reconcile privacy and compliance in crypto. Here are the new technologies that will protect user data and stop illicit transactions* in Future.com. Disponibile in open source sul sito https://fortune.com/2022/10/28/finally-reconcile-privacy-compliance-crypto-new-technology-celsius-user-data-leak-illicit-transactions-crypto-tromer-ramaswamy/
[471] CUOMO L., RAZZANTE R. (2007). *La disciplina dei reati informatici*, Torino, 14 ss.
[472] FLOR R. (2015). *I limiti del principio di territorialità nel "cyberspace". Rilievi critici alla luce del recente orientamento delle sezioni unite*, in Dir. pen. proc., pagg. 1296 ss.

e volontario si traduce in un trasferimento sotto forma di energie o bit della volontà dall'operatore all'elaboratore elettronico, il quale procede automaticamente alle operazioni di codificazione, di decodificazione, di trattamento, di trasmissione o di memorizzazione di informazioni».[473]

Il diritto, quindi, ha sempre analizzato quale oggetto del reato «beni corporali» ed «oggetti tangibili»,[474] presenti nell'ambiente in cui opera l'autore del reato. Tuttavia, l'avanzamento della tecnologia ha comportato una progressiva dematerializzazione dell'oggetto del reato e pertanto, dei beni della vita delle vittime che vengono lesi.[475] Tale mutamento comporta inevitabilmente un'evoluzione delle modalità con cui o mediante cui vengono commessi i reati, i quali sempre più spesso avvengono mediante l'utilizzo di strumenti elettronici ovvero di Internet (quali truffe online, riciclaggio…) in funzione anche del mutare delle abitudini del singolo che diventa sempre più *digital*.[476]
Come già analizzato ampiamente nel corso del presente elaborato, l'uso delle criptovalute sia da parte dei fornitori di tali tipologie di servizi che da parte di individui possano integrare il reato di riciclaggio mediante condotte parzialmente differenti dal riciclaggio "tradizionale" che avviene mediante l'utilizzo di denaro contante.

Premesso ciò, non solo il diritto penale ha dovuto adeguarsi ma anche il diritto processuale penale ha dovuto adattarsi alle nuove modalità di commissione dei reati.[477]

---

[473] Corte di Cassazione, sezioni unite penali, sentenza 26 marzo 2015 (dep. 24 aprile 2015), n. 17325 - Disponibile in open source sul sito https://www.penale.it/page.asp?mode=1&IDPag=1232
[474]CUOMO L., RAZZANTE R., *La disciplina dei reati informatici,* cit. 469
[475] CUOMO L., RAZZANTE R., *La disciplina dei reati informatici,* cit. 469 e ROSATO A. (2021). *Profili penali delle criptovalute* in Quaderni di C.R.S.T., Centro Ricerca Sicurezza e Terrorismo. Disponibile in open source sul sito https://www.dirittopenaleglobalizzazione.it/wp-content/uploads/2021/01/Profili-penali-delle-criptovalute-Rosato-Antonio.pdf
[476]LUPARIA L. (2009), Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (L. 18 marzo 2008, n. 48), Giuffrè, Milano.
[477] «*I computer possono essere gli strumenti necessari per la commissione di reati (soggetto attivo di delitti), possono contenere le prove dei crimini di tipo tradizionale (testimoni di delitti) oppure*

Difatti, le prove processuali hanno in alcuni casi perso anch'esse la loro natura materiale e sono state sostituite da prove aventi natura dematerializzata.[478] Sono quindi limitate le prove documentali in caso di reati commessi mediante criptovalute: nel caso della blockchain oggetto di indagine saranno sicuramente le transazioni iscritte nell'apposito registro ovvero gli *address* di coloro che hanno effettuato le transazioni. Ciò significa che nei processi relativi a reati commessi mediante l'utilizzo di internet o un dispositivo digitale verranno utilizzate le c.d. prove elettroniche. Ovviamente, la questione processuale nei reati di tale tipologia ha fatto sorgere ulteriori problematiche relative alla competenza, alla giurisdizione ovvero di cooperazione a livello internazionale tra le diverse autorità nonché alla classificazione e riconducibilità alla normativa processuale penale.[479]

3.1. (*Segue*): Le prove digitali e classificazione giuridica delle prove

Le cd. prove digitali ossia elettroniche sono dotate di caratteristiche peculiari rispetto alle prove che solitamente vengono analizzate a livello processuale.

Le prove digitali non sono altro che dei dati di natura informatica che mediante un codice binario[480] sono salvati in supporti fisici come i computer ovvero sulla rete internet. [481]Ciò comporta diverse problematiche relativamente alla loro reperibilità, in quanto si possono ritrovare su diversi dispositivi informatici e ciò comporta problematiche dal punto di vista della giurisdizione circa le indagini da espletare.

---

possono essere l'obiettivo di atti criminali (soggetto passivo di delitti)» CUOMO L., RAZZANTE R., *La disciplina dei reati informatici*, cit. 469

[478] LUPARIA L. (2011). *Computer crimes e procedimento penale*, in GARUTI G. (a cura di), *Modelli differenziati di accertamento*, diretto da G. Spangher, Utet, Torino, 4 ss.

[479] SIGNORATO S. (2016). *Types and features of cyber investigations in a globalized world*. Relazione alla Conferenza biennale internazionale e Diritto penale contemporaneo. Disponibile in open source sul sito https://archiviodpc.dirittopenaleuomo.org/d/5146-types-and-features-of-cyber-investigations-in-a-globalized-world

[480] KERR O.(2005). *Digital Evidence and the New Criminal Procedure*, in 105 Colum. L. Rev., 291

[481] DI PAOLO G. (2013). Voce *Prova informatica* (diritto processuale penale), in Enc. dir., Annali, VI, Giuffrè, Milano, p. 738 ss.; DANIELE M., (2011). *La prova digitale nel processo penale, in Riv. dir. proc., p. 283; anche ID.,* RUGGIERI F. e PICOTTI L. (2011), *Caratteristiche della prova digitale, Nuove tendenze della giustizia penale di fronte alla criminalità informatica: aspetti sostanziali e processuali*, Giappichelli, Torino, p. 284

Inoltre, le prove digitali sono intangibili[482] e pertanto, esistono solo con la presenza di un supporto informatico. Senza di esso non sono autonome ed indipendenti. Esse sono fragili[483] in quanto le prove digitali possono essere modificate ed eliminate sia dal soggetto creatore sia da parte di terzi che ne possono avere accesso come investigatori. Dal punto di vista investigativo, è necessario che l'investigatore valuti la cd. "resistenza informatica alle contestazioni"[484] ovvero la garanzia di integrità[485] e autenticità. Infine, le prove digitali sono promiscue ossia sono dotate della capacità di contenere un numero non definito di dati rilevanti o meno dal punto di vista delle indagini.

Detto ciò, non è da dimenticare, come la ricerca delle prove digitali può facilmente incidere sui diritti costituzionali proprio in virtù del fatto che i dispositivi digitali spesso sono dei contenitori di informazioni promiscue e per questo risulta necessario trovare un equilibrio tra la tutela dei diritti e libertà fondamentali e le esigenze di natura processuale.[486] Pertanto, durante l'indagine non è da tralasciare il disposto di cui all'art. 189 c.p.p. il quale richiama espressamente la libertà morale della persona soggetta alle indagini e il giudice dovrà attentamente valutare se ammettere la prova digitale in processo trovando un equilibrio tra il diritto alla riservatezza e il principio di non dispersione della prova.[487]

---

[482] «*Ciò non significa che esse non abbiano una loro fisicità`: concettualmente si tratta di impulsi elettrici che rispondono ad una sequenza numerica prestabilita e che, convogliati in un supporto informatico dotato di una memoria, originano informazioni intellegibili. È però, una fisicità che, in assenza del supporto, non può essere percepita come tale*». DANIELE M., *La prova digitale nel processo penale*, cit. 478

[483] DI PAOLO G., Voce *Prova informatica* (diritto processuale penale), cit. 478

[484] ZICCARDI (2007). *Scienze forensi e tecnologie informatiche*, in LUPÁRIA L.e ZICCARDI G. (2007). *Investigazione penale e tecnologia informatica*, Milano, 11

[485] «la garanzia di aver mantenuto inalterati tutti i dati e lo stato del supporto fisico che li contiene durante le varie fasi del repertamento e dell'analisi» LUPÁRIA L.e ZICCARDI G., *Investigazione penale e tecnologia informatica*, cit 482

[486] DI PAOLO G., Voce *Prova informatica* (diritto processuale penale), cit. 478

[487] DOMINIONI O., (1997). *Un nuovo idolum theatri: il principio di non dispersione probatoria*, in Cass. pen., 768.; PITTIRUTI M., (2017). *Digital evidence e procedimento penale* in Processo penale e politica criminale, a cura di PAOLOZZI G., - MOCCIA S., - MARAFIOTI L., - LUPARIA L., - MARCHETTI P., Torino.

Inoltre, le problematiche relative alle prove digitali non sono limitate alle caratteristiche proprie delle stesse, ma si estendono anche alla loro classificazione e riconducibilità alle norme del codice di procedura penale.

Innanzitutto, dal punto di vista della categoria di appartenenza delle prove digitale, gli studiosi[488] hanno ravvisato che tra le categorie delle prove rappresentative dirette[489] o delle prove critiche indirette[490], esse sono riconducibili ad entrambe le categorie.

Con riferimento, invece, alla riconducibilità alle norme processuali, a seguito delle modifiche relative gli istituti dei mezzi di prova e di ricerca della prova (L. n. 48/2008)[491], le prove digitali risultano riconducibili a questi due istituti.[492]

3.2. (*Segue*): Le indagini digitali

Attualmente a seguito dell'incremento dei dispositivi digitali, delle criptovalute con una conseguente trasformazione immateriale dell'azione di reato, si è registrato un aumento direttamente proporzionale degli attacchi informatici sia verso persone fisiche che giuridiche; perciò, è stato necessario elaborare nuove modalità di indagine specifiche relativamente alla commissione di tali tipologie di reato. In particolare, le attività di indagine che vengono portate a termine con l'aiuto di un sistema digitale e che hanno ad oggetto prove digitali saranno finalizzate principalmente al perseguimento dei seguenti obiettivi: preservazione, analisi e documentazione degli elementi probatori a fondamento della colpevolezza del reo.[493]

---

[488] FERRUA P. (2013). *La prova nel processo penale: profili generali*, in FERRUA P., - MARZADURI E., - SPANGHER G., (a cura di), *La prova penale*, Torino, 11

[489] «*l'equivalente sensibile sulla cui base occorre rievocare il fatto da provare è costituito da un secondo fatto che rappresenta il primo, consistendo in una narrazione di questo in quanto realmente accaduto.*» MOSCARINI P. (2014). *Principi delle prove penal*i, Torino, 8.

[490] MOSCARINI P., *Principi delle prove penali*, cit. 487

[491] L. n. 48/2008 - Legge di "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno" - Disponibile in open source sul sito https://www.gazzettaufficiale.it/eli/id/2008/04/04/008G0070/sg

[492] PITTIRUTI M., *Digital evidence e procedimento penale*, cit. 485

[493] SIGNORATO S., *Types and features of cyber investigations in a globalized world*, cit. 477

Le caratteristiche delle investigazioni digitali sono l'estrema tecnicità[494] e l'ultra territorialità. Ciò significa che le investigazioni digitali devono essere svolte da personale esperto al fine di evitare di alterare ovvero inquinare la prova da assumere rendendola così inutilizzabile a causa della compromissione della sua capacità probatoria[495] e che le indagini digitali spesso non limitano il proprio raggio operativo ad un solo Stato ma spesso comprendono diverse aree del globo. Risulta quindi necessario definire in modo chiaro norme regolatrici della giurisdizione al fine di evitare conflitti di competenza tra più autorità e problematiche relativamente alla circolazione delle prove.[496]

Possono essere distinte tre tipologie di investigazioni digitali: le investigazioni preventive, le investigazioni preliminari e le investigazioni proattive.

Le investigazioni preventive vengono condotte al fine di prevenire la commissione di reati. Pertanto, tali investigazioni vengono svolte e si collocano in un momento antecedente al ricevimento della notizia di reato. In tali casi, sono fondamentali, sia per gli investigatori che per i giudici, le deposizioni preventive.[497] Nella maggior parte dei casi le investigazioni preventive vengono svolte dalle intelligence, nazionali ovvero internazionali. Raramente sono svolte dalle autorità "ordinarie" mediante software di spionaggio, mezzi estremamente lesivi della privacy dei singoli,[498] in quanto con l'utilizzo degli stessi possono essere acquisiti dati memorizzati su un dato dispositivo nonché l'accesso a webcam e microfoni.[499]

Invece, le investigazioni preliminari vengono realizzate a seguito della ricezione della notizia di reato da parte delle autorità competenti. Le indagini verranno svolte secondo la normativa, nel rispetto dei principi di adeguatezza e proporzionalità.[500]

---

[494] ROSATO A., *Profili penali delle criptovalute* in Quaderni di C.R.S.T., cit. 473
[495] SIGNORATO S., *Types and features of cyber investigations in a globalized world*, cit. 477
[496] ROSATO A., *Profili penali delle criptovalute* in Quaderni di C.R.S.T., cit. 473
[497] ROSATO A., *Profili penali delle criptovalute* in Quaderni di C.R.S.T., cit. 473
[498] ANDOLINA E. (2015). *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della "privacy" e onde eversive*, in Archivio penale, 3, 916-938
[499] SIGNORATO S., *Types and features of cyber investigations in a globalized world*, cit. 477
[500] MOSCARINI P., *Principi delle prove penali*, cit. 487; SIGNORATO S., *Types and features of cyber investigations in a globalized world*, cit. 477

Le investigazioni proattive sono una forma ibrida di investigazione che si colloca a metà tra le investigazioni preventive e le investigazioni preliminari.[501] Rispetto alle altre due forme di investigazione, le investigazioni proattive sono una forma ancora poco conosciuta che viene implementata soprattutto per la prevenzione nonché repressione dei reati di natura terroristica e della criminalità organizzata. A ciò si aggiunga che sono spesso utilizzate nelle investigazioni dirette a scovare prove di natura digitale. [502]

Andando più nello specifico rispondendo ai fini della presente trattazione, le indagini digitali spesso, a "causa" del crescente utilizzo delle criptovalute, riguardano anche la tecnologia blockchain. Si è già discusso nel corso del presente elaborato come le valute virtuali siano uno strumento che si presta perfettamente ad essere utilizzato per la commissione di *cybercrimes*.[503] Difatti, abbiamo visto che spesso esse non solo vengono utilizzate per il riciclaggio di denaro, ma vengono spesso richieste, per esempio, come "riscatto" da pagare per ottenere dati rubati da un *device* ovvero come mezzo di pagamento nel *dark web*. Pertanto, è stato necessario adeguare le tecniche investigative e l'attività delle autorità competenti al fine di perseguire i cybercrimes.[504]

Come già ribadito, il registro delle transazioni che avvengono mediante l'utilizzo delle criptovalute è pubblico e ognuno di noi può accedervi facilmente al fine di consultare ed estrarre una copia delle transazioni effettuate. Si tratta di un importante tassello delle attività investigative utile ad individuare le transazioni con valute virtuali anche se effettuate in diverse giurisdizioni.[505] Tuttavia, come è noto, la tecnologia blockchain tutela la privacy dei propri utenti e omette di indicare gli indirizzi dei *wallet* utilizzati ovvero l'importo delle transazioni. Per esempio, alcune criptovalute come Zchash e Bitcoin lasciano la facoltà all'utilizzatore di scegliere

[501] KOSTORIS E. (2007). *Processo penale, delitto politico e "diritto penale del nemico"*, in Rivista di diritto processuale, 4; SIGNORATO S., *Types and features of cyber investigations in a globalized world*, cit. 477.
[502] SIGNORATO S., *Types and features of cyber investigations in a globalized world*, cit. 477
[503] ROSATO A., *Profili penali delle criptovalute* in Quaderni di C.R.S.T., cit. 473
[504] NEILSON D., HARA S., MITCHELL I. (2016). *Bitcoin Forensics: A Tutorial*, in JAHANKHANI H., (2017) in *Global Security, Safety and Sustainability - The Security Challenges of the Connected World*, in Communications in Computer and Information Science, 630, 1.
[505] NEILSON D., - HARA S., - MITCHELL I., *Bitcoin Forensics: A Tutorial*, cit., 502

se rivelare per ogni transazione l'importo e gli indirizzi ovvero solo l'importo o uno dei due indirizzi; questo perché i fornitori soggiacciono a doveri di compliance (antiriciclaggio) o di audit e ciò consente loro di adempiere.[506]

Nonostante ciò, spesso la crittografia viene monopolizzata dai "cyber-criminali" con l'intento di rallentare o addirittura impedire lo svolgimento delle attività investigative.[507] Per far fronte a tale problematica è necessario la cooperazione tra le autorità e i fornitori/produttori di tali servizi e beni,[508] i quali per di più soggiacciono già agli obblighi previsti dalla V Direttiva antiriciclaggio che di fatto impone ai *wallet provider* di implementare misure atte ad indentificare, verificare ed eventualmente segnalare attività sospette. Questo però avviene a livello europeo e non globale.[509]

Quindi, le indagini informatiche relative a criptovalute spesso pongono le autorità davanti a diverse sfide e sono caratterizzate da diverse peculiarità che spesso compromettono l'avanzamento dell'indagine

3.3. (*Segue*): I soggetti processuali nelle indagini informatiche

Dopo un'attenta analisi delle prove digitali e delle indagini informatiche è ulteriormente necessario identificare i soggetti processuali coinvolti nell'espletamento delle indagini informatiche. Si è detto che a causa della natura

[506] KOSTORIS E. (2007). *Processo penale, delitto politico e "diritto penale del nemico"*, in Rivista di diritto processuale, 4; SIGNORATO S., *Types and features of cyber investigations in a globalized world*, cit. 477.

[507] NAQVI S. (2018). *Challenges of Cryptocurrencies Forensics – A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals in ARES, Proceedings of the 13th International Conference on Availability, Reliability and Securit, Hamburg, Germany*, New York, NY, USA, 2

[508] NAQVI S. *Challenges of Cryptocurrencies Forensics – A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals in ARES, Proceedings of the 13th International Conference on Availability, Reliability and Securit, Hamburg, Germany*, cit. 505; PHILIP J., T., e PARBAT K. (2010). *BlackBerry to open code for security check* - Disponibile in open source sul sito https://economictimes.indiatimes.com/tech/hardware/blackberry-to-open-code-for-securitycheck/articleshow/6249666.cms

[509] ROSATO A., *Profili penali delle criptovalute* in Quaderni di C.R.S.T., cit. 473

complessa delle prove digitali è necessario che le indagini informatiche siano svolte da un soggetto dotato di tutte le competenze tecniche necessarie per evitare la compromissione della prova e rendere la prova stessa ammissibile.[510] Pertanto, al fine di identificare la persona più adatta per l'espletamento delle indagini informatiche in quanto maggiormente dotata di tali competenze e istituire organi di indagini specializzati[511], il legislatore italiano è intervenuto introducendo l'art. 11 della legge n.48/2008 il comma 3-quinquies all'art. 52 del codice di procedura penale che amplia la competenza del pubblico ministero distrettuale nelle indagini preliminari e nei procedimenti di primo grado.[512]
Una tale asimmetria tra normativa in materia di competenza territoriale del giudice e criteri di competenza delle funzioni del pubblico ministero è similarmente[513] prevista dagli artt. 51 comma 3- bis e 3- quater c.p.p. per i reati di criminalità organizzata (anche di natura mafiosa), e di terrorismo (nazionale e internazionale).

Tuttavia, nonostante gli obiettivi lampanti della novella del 2008, sono state diverse le critiche mosse nei suoi confronti. Prima di tutto si è obiettato che l'estensione di competenza realizzata a favore del pubblico ministero distrettuale poteva essere estesa non solo nei confronti dei reati indicati precedentemente ma anche ad altre tipologie di reati.[514] In secondo luogo, tale ampliamento di competenza comporta consequenzialmente anche un ampliamento necessario delle conoscenze del pubblico ministero distrettuale, con conseguente rischio di ulteriore rallentamento dell'attività lavorativa.[515]

---

[510] PITTIRUTI M., *Digital evidence e procedimento penale*, cit. 485
[511] CASSIBBA F., (2009). *L'ampliamento delle attribuzioni del pubblico ministero distrettuale*, in LUPARIA (a cura di), *Sistema penale e criminalità informatica*, 113.
[512] CASSIBBA F., (2009). *L'ampliamento delle attribuzioni del pubblico ministero distrettuale*, cit. 509.
[513] DI BITONTO M., L. (2008). *L'accentramento investigativo delle indagini sui reati informatici*, in *La ratifica della Convenzione del consiglio d'Europa sul cybercrime: profili processuali*, in dir. Internet, , 503 e ss.; LUPARIA L., *Computer crimes e procedimento penale*, in GARUTI G. (a cura di), *Modelli differenziati di accertamento*, cit. 476
[514] PITTIRUTI M., *Digital evidence e procedimento penale*, cit. 485; LUPARIA L., I correttivi alle distorsioni sistematiche contenute nella recente legge di ratifica della Convenzione sul Cybercrime, in LORUSSO S., (a cura di), Le nuove norme sulla sicurezza pubblica, Padova, 2008, 66
[515]LUPARIA L., *Computer crimes e procedimento penale*, in GARUTI G. (a cura di), *Modelli differenziati di accertamento*, cit. 476

Successivamente il D.lgs. 23 maggio 2008, n. 92 e la legge di conversione del 24 luglio 2008, n. 125 è stata estesa la competenza del giudice delle indagini preliminari e del giudice dell'udienza preliminare distrettuale anche ai reati ricompresi nell'art. 51 comma 3-*quinquies*, precedentemente non prevista, mediante la modifica all'art 328, comma 1-*quater*.

In aggiunta alla normativa interna in materia di investigazioni in caso di *cybercrime* è utile accennare anche alla Convenzione di Budapest. La Convenzione sulla criminalità informatica del Consiglio d'Europa è stata aperta alla firma a Budapest nel novembre 2001. Quindici anni dopo, rimane l'accordo internazionale più importante in materia di criminalità informatica e prove elettroniche. L'adesione continua a crescere (ad oggi sono sessantasei i Paesi nel mondo che hanno aderito alla convenzione in esame), mentre la qualità dell'attuazione e il livello di cooperazione tra le parti continuano a migliorare e il trattato stesso si evolve per affrontare nuove sfide. Nel 2001, la questione della criminalità organizzata era diventata sufficientemente importante da giustificare un trattato internazionale vincolante. Negoziata dagli Stati membri del Consiglio d'Europa insieme a Canada, Giappone, Sudafrica e Stati Uniti d'America, la Convenzione sulla criminalità informatica è stata aperta alla firma a Budapest, in Ungheria, nel novembre 2001.
La Convenzione di Budapest è un trattato di giustizia penale che fornisce agli Stati sottoscrittori standard comuni consistenti nell'incriminazione di un elenco di attacchi contro e per mezzo di computer, nell'individuazione di strumenti di diritto processuale per rendere le indagini sulla criminalità informatica e la raccolta di prove elettroniche in relazione a qualsiasi reato più efficaci e soggette alle garanzie dello Stato di diritto, nonché per favorire la cooperazione internazionale di polizia giudiziaria sulla criminalità informatica e sulle prove elettroniche.[516]

L'accordo è un importante traguardo raggiunto in quanto consente a ciascuno Stato di adottare previsioni normative per migliorare le indagini in caso di *cybercrimes*,

[516] MANZARI M. (2021). *I reati informatici e la Convenzione di Budapest*, in bptmavvocati.it. Disponibile in open source sul sito https://www.bptmavvocati.it/portfolio/i-reati-informatici-e-la-convenzione-di-budapest/

definendo i principi di esecuzione delle stesse al fine di garantire la tutela nonché l'integrità delle prove raccolte.[517]

3.4. (*Segue*): Il caso Silk Road e Bitgrail

Internet è sempre più considerato come il motore dei mercati contemporanei delle droghe e farmaci grazie alla promozione dello "shopping" nei punti vendita al dettaglio basati sul web e sugli ambienti per la comunicazione di informazioni da parte degli utenti. Il mercato *online* dei farmaci e delle droghe è diventato nel tempo sempre più dinamico e innovativo nella sua capacità di vendere al dettaglio i farmaci, creare nuovi composti e aggirare i controlli legislativi. È sempre più evidente che le versioni esistenti e nuove di droghe illecite vengono scambiate e discusse tra gli utenti del "Deep Web" o "Invisible Web" ovvero *dark web*, che rappresentano contenuti online non ricercabili dai motori di ricerca standard come Google. Le nuove sostanze sono commercializzate come sostituti di qualità legale o etichettati come non destinati al consumo umano di droghe da strada popolari come ecstasy, anfetamine, cannabis e cocaina.[518] Il passaggio a una diffusa disponibilità globale di tutte le droghe è evidente nella recente presenza online di appositi mercati come "Silk Road". Si tratta di uno dei casi più noti che ha attirato l'attenzione dei media ed ha visto coinvolti un sito appartenente al *dark web* "The Silk Road" e l'FBI, ente investigativo degli Stati Uniti d'America. Si tratta della prima volta in cui il governo degli Stati Uniti ha utilizzato l'analisi della blockchain in un'indagine penale che ha contribuito a smascherare il creatore del mercato oscuro Silk Road, e a catturare due agenti federali corrotti che sono stati coinvolti nel sito del mercato nero e hanno lavorato all'indagine originale.[519]

[517] ROSATO A., *Profili penali delle criptovalute* in Quaderni di C.R.S.T., cit. 473

[518] PREVITI L. (2020). *Silk Road: storia del famoso mercato della droga*, in cyberdude.it. Disponibile in open source sul sito https://cyberdude.it/2020/07/27/silk-road-storia-famoso-mercato-della-droga/

[519] Il Post. (2013). *Come è stato preso il capo di Silk Road.* Disponibile in open source sul sito https://www.ilpost.it/2013/10/04/arresto-ross-ulbricht-silk-road/

Tale sito era stato creato nel 2011 come sito e-commerce di stupefacenti, documenti falsi e altra merce di tipo illegale (armi e munizioni erano consentite fino a marzo 2012 e da allora sono state reinserite in un sito gemello chiamato "The Armory"[520]), in cui i pagamenti avvenivano tramite Bitcoin. Il sito era da tempo noto all'FBI, la quale tuttavia non era a conoscenza del gestore nonché proprietario del sito stesso. Anzi tutto che era in possesso dell'FBI era il solo *username* del proprietario DPR, o Dread Pirate Roberts.

Successivamente mediante tecniche di social engineering, creazione di account fasulli da parte dell'FBI e grazie a problematiche di configurazione del browser fu possibile individuare il soggetto nella persona di Ross Ulbricht. A ciò si aggiunga che uno degli agenti che partecipava alla ricerca di Robb era suo complice, anzi, addirittura, i due effettuavano azioni di depistaggio al fine di salvaguardare la propria "ricchezza". Gli investigatori, tracciando oltre 21.000 bitcoin mancanti hanno scoperto che il denaro era destinato a un agente dei servizi segreti che faceva parte della task force di Silk Road.

Al termine del processo, sono stati oltre 144 i Bitcoin sequestrati dall'FBI,[521] ed inoltre, durante il processo il reo è stato accusato di aver sollecitato sei omicidi su commissione in relazione alla gestione del sito, sebbene non vi siano prove che questi omicidi siano stati effettivamente compiuti.

Un caso simile, anche se dal punto civilistico, in cui le autorità hanno provveduto a sequestrare una somma ingente di Bitcoin è il cd. caso "BitGrail" ossia società italiana fondata nel 2017 controllata da due società italiane, la WebCoin Solutions di Francesco Firano e la BG Services S.r.l..[522] Tale società fu coinvolta nella fraudolenta sottrazione di una criptovaluta scambiata sulla piattaforma chiamata "Nano", un ammontare di circa 12 milioni di criptovalute ossia 120 milioni di euro

[520] Il Post, *Come è stato preso il capo di Silk Road*, cit. 518

[521] PREVITI L., *Silk Road: storia del famoso mercato della droga*, cit. 517.

[522] CIVILETTI G. (2019). *BITGRAIL – Procedura fallimentare dell'exchange italiano*, in Crypto avvocato. Disponibile in open source sul sito https://www.cryptoavvocato.it/articoli/diritto-1/bitgrail-procedura-fallimentare/

circa.[523] La denuncia di sottrazione è stata effettuata direttamente da Francesco Firano.

Nonostante l'offerta della società di risarcire i propri clienti, fu richiesto di dichiarare il fallimento della società fiorentina che fu dichiarato dal Tribunale fallimentare di Firenze, il quale ha ritenuto configurabile una responsabilità civilistica e disposto il sequestro di 2.345 bitcoin e 4 milioni di Nano delle società (dal valore di circa 36 milioni di euro) e di 170 bitcoin e oltre 500.000 euro di Francesco Firano.[524]

L'ammontare sequestrato è stato trasferito su wallet appositamente creato per il curatore, le cui chiavi private sono state depositate in un luogo sicuro senza che chi abbia partecipato al processo possa effettivamente accedervi; ciò allo scopo di evitare quanto accaduto in concomitanza con la fase di indagine di Silk Road durante la quale si era scoperto che due agenti si erano impossessati di alcuni Bitcoin sequestrati.

Ad ogni modo, a seguito dell'espletamento di una consulenza tecnica si scoprì che gli ammanchi erano iniziati già a partire dal maggio del 2017, anche se Firano aveva sostenuto che questi fossero stati registrati a partire da febbraio 2018. Al termine delle indagini si scoprì che la società operava come una banca ossia prendeva i depositi effettuati dai clienti e li depositava in un unico *wallet* senza distinzione. [525]

Più precisamente, nella sentenza il Tribunale Fallimentare di Firenze evidenziava come fosse stato l'Exchange BitGrail, a causa di un difetto del software, a richiedere effettivamente al nodo, più volte, di permettere ai fondi di lasciare il portafoglio" e non la rete Nano che ha permesso i prelievi multipli. Inoltre, l'Exchange avrebbe conservato tutte le sue criptovalute Nano in un "*hot wallet*", compromettendone la sicurezza. Il Tribunale osservava che, in tal modo, nel luglio 2017 venivano rubati 2,5 milioni di Nano dall'Exchange, e che Firano ne era a conoscenza. Secondo la sentenza, nell'ottobre dello stesso anno - tre mesi dopo -

[523] ROSATO A., *Profili penali delle criptovalute* in Quaderni di C.R.S.T., cit. 473

[524] CIVILETTI G., *BITGRAIL – Procedura fallimentare dell'exchange italiano*, cit. 521.

[525] CAPACCIOLI S. e SOLDAVINI P. (2019). *Fallisce Bitgrail, la piattaforma italiana per le criptovalute* in Ilsole24Ore. Disponibile in open source sul sito https://www.ilsole24ore.com/art/fallisce-bitgrail-piattaforma-italiana-le-criptovalute-AE9Dg8LH

venivano rubati altri 7,5 milioni di Nano. Nel dicembre 2017 Firano convertiva il portafoglio centrale in un portafoglio freddo e l'attività dell'Exchange è diventata, secondo quanto riferito, intermittente.[526]

Concludendo, questa prima trattazione di casi aventi ad oggetto la tecnologia blockchain per lo svolgimento delle indagini, ci si accorge come ad oggi la sua implementazione costituisca un elemento essenziale nella lotta contro i *cybercrimes*. Di seguito si andranno ad analizzare un'altra tipologia di casi ossia i casi sugli incidenti di sicurezza verificatisi relativamente agli *E-Wallet.*

3.5. (*Segue*): Case study sugli incidenti di sicurezza verificatisi presso i *wallet provider* e analisi delle cause

L'incidente di sicurezza del portafoglio di criptovalute più famoso e d'impatto del 2022 è stato la gestione impropria delle chiavi private da parte del portafoglio Slope. Slope wallet è un portafoglio di criptovalute non custodiale disponibile come applicazione mobile per iOS e Android e come estensione per Chrome. Supporta diverse blockchain, ma è principalmente attivo sulla blockchain Solana. L' 8 febbraio 2022 circa 4,1 milioni di dollari di attività sono scomparsi dagli indirizzi dei portafogli di 9.231 utenti nel corso di circa quattro ore. Durante le prime due ore dell'incidente, quando la causa era sconosciuta, si scatenò il panico e si diffuse la voce che la blockchain Solana fosse stata violata. Poche ore dopo l'*exploit* iniziale, è stato scoperto che il mnemonico dell'utente era stato inviato al server di registrazione Sentry di Slope durante l'importazione di un account del portafoglio. Chiunque abbia accesso al log può rilevare l'account e trasferire tutte le attività dall'indirizzo.[527]

[526] CAPACCIOLI S. e SOLDAVINI P., *Fallisce Bitgrail, la piattaforma italiana per le criptovalute,* cit. 524.

[527] BitcoinEthereumNews.com (2022). *Gli ingegneri trovano un bug del portafoglio Slope dietro un hack da 6 milioni di dollari basato su Solana*. Disponibile in open source sul sito https://it.bitcoinethereumnews.com/technology/engineers-find-slope-wallet-bug-behind-6m-solana-based-hack/

Due settimane dopo l'incidente, Slope Wallet ha pubblicato il "*Forensics and Incident Response Report*". Dal rapporto si apprende che le chiavi private sono state registrate a partire dal 28 luglio 2022. Il problema avrebbe potuto essere facilmente individuato durante una valutazione della sicurezza o addirittura una revisione interna. Il team di Slope Wallet è rimasto completamente in silenzio su tutti i social media dopo la pubblicazione del rapporto.[528]

Il secondo caso oggetto di trattazione è l'incidente avvenuto al portafoglio Bitkeep. Diversi utenti del portafoglio di criptovalute BitKeep hanno riferito che i loro portafogli sono stati svuotati a Natale del 2022 dopo che gli hacker hanno attivato transazioni che non richiedevano una verifica. BitKeep è un portafoglio decentralizzato multi-catena web3 utilizzato da oltre otto milioni di persone in 168 Paesi per la gestione degli asset e delle transazioni.

Secondo un annuncio ufficiale sul canale Telegram di BitKeep, l'incidente sembra aver colpito gli utenti che hanno scaricato una versione non ufficiale dell'app BitKeep. Questo pacchetto APK troianizzato conteneva un malware che ha permesso agli hacker di svuotare i portafogli degli utenti ignari. Tuttavia, alcuni utenti della comunità hanno affermato che i loro portafogli violati erano stati scaricati dal canale ufficiale. Dopo un'indagine, CertiK ha scoperto che l'applicazione BitKeep per Android disponeva di una funzione di aggiornamento in-app che scaricava l'ultima versione dell'APK dal sito Web di BitKeep, che era già stato dirottato. Di conseguenza, anche i portafogli scaricati da Google Play Store sono stati colpiti. Alle vittime dell'hack è stato chiesto di compilare un modulo per il team di supporto di BitKeep, nel tentativo di offrire una soluzione il più rapidamente possibile. La piattaforma non ha ancora determinato l'ammontare del denaro perso nell'hack, ma è stato riferito che finora sono stati rubati beni per un valore di circa otto milioni di dollari.

Vale la pena notare che non è la prima volta che BitKeep subisce una perdita significativa a causa di un hack. Nell'ottobre 2022, la piattaforma ha perso circa 1

[528] SLOPE FINANCE (2022). *Slope Wallet Sentry Vulnerability — Digital Forensics and Incident Response Report*. Disponibile in open source sul sito https://slope-finance.medium.com/slope-wallet-sentry-vulnerability-digital-forensics-and-incident-response-report-d7a5904e5a39

milione di dollari di Bitcoin dopo che un hacker ha sfruttato una vulnerabilità nella funzione Swap del portafoglio di criptovalute BitKeep. In quell'occasione, BitKeep aveva promesso di rimborsare completamente le persone colpite dall'incidente.

Oltre a Slope e BitKeep anche Profanity, strumento di generazione di indirizzi che consente agli utenti di generare indirizzi di account (EOA) e smart contract personalizzati il quale ha una caratteristica comune a quasi tutti i portafogli di criptovalute: la capacità di generare account di portafoglio. È un esempio perfetto delle conseguenze della generazione di account non sicuri.

La vulnerabilità è stata notata per la prima volta dopo che il team ha pubblicato "*A Vulnerability Disclosed in Profanity, an Ethereum Vanity Address Tool*" il 15 settembre 2022, sostenendo che lo strumento "Profanity" utilizza un seed insicuro e che la chiave privata dell'account generato dallo strumento può essere facilmente recuperata. Cinque giorni dopo, il 20 settembre, un conto del portafoglio del team "Wintermute" è stato violato e l'aggressore ha utilizzato il conto per prelevare 162,5 milioni di dollari da uno smart contract (analisi dell'incidente).[529] L'11 ottobre è stato violato l'account dello sviluppatore del ponte Qanx e l'aggressore ha utilizzato l'account per prelevare i token Qanx dal ponte e venderli sul mercato. Più aggressori hanno cercato attivamente conti vulnerabili sulla blockchain e hanno rubato fondi. La causa principale di questo problema è che il numero totale di semi possibili. Il seme insicuro e il processo reversibile di forza bruta rendono possibile il recupero della chiave privata di un account generato con lo strumento. CertiK ha sviluppato con successo un programma proof of concept ed è riuscito a recuperare le chiavi private di entrambi gli account degli sviluppatori Wintermute e Qanx.[530]

Nel 2013 è stata scoperta una vulnerabilità simile nel generatore di numeri casuali del sistema Android, che riguardava la creazione di portafogli Bitcoin. La crittografia è un campo complesso ed è facile commettere errori che possono

[529] LINCH NETWORK (2022). *A vulnerability disclosed in Profanity, an Ethereum vanity address tool*. Disponibile in open source sul sito https://blog.1inch.io/a-vulnerability-disclosed-in-profanity-an-ethereum-vanity-address-tool/

[530] LINCH NETWORK, *A vulnerability disclosed in Profanity, an Ethereum vanity address tool*, cit. 528.

compromettere la sicurezza. Una pratica di sicurezza comune è "non creare le proprie criptovalute".

Nel 2022 anche il popolare portafoglio MetaMask, utilizzato da oltre 30 milioni di persone per memorizzare i propri token e gestire i propri beni digitali, ha avvertito i propri utenti iOS dei potenziali rischi derivanti dalla memorizzazione dei segreti del proprio portafoglio su iCloud di Apple. I segreti del portafoglio, come la frase di seme, sono crittografati quando vengono caricati su iCloud, ma se l'account Apple del proprietario venisse compromesso e si utilizzasse una password debole, i suoi beni digitali potrebbero essere a rischio.[531]

Questo avvertimento è arrivato dopo un costoso attacco di phishing in cui la vittima è stata vittima di un attacco di social engineering da parte di truffatori che si sono finti addetti all'assistenza Apple, i quali hanno ottenuto l'accesso al suo account *iCloud* e hanno utilizzato le credenziali MetaMask memorizzate per svuotare il suo portafoglio.

Le cause contro gli Exchange di criptovalute, i fornitori di portafogli digitali e le società di servizi mobili a seguito di cyber attacchi hanno raggiunto un nuovo picco nel 2022, in quanto le vittime di hacking hanno provato a intraprendere sempre più spesso azioni legali per recuperare le loro perdite di criptovalute. L'aumento delle cause legali è parallelo alla crescente adozione delle criptovalute tra le crescenti minacce alla sicurezza informatica. Tuttavia, il successo di tali cause rimane incerto a causa della mancanza di precedenti di merito, nonché di ostacoli come le clausole arbitrali obbligatorie che possono tenere tali controversie fuori dai tribunali.[532]

La maggior parte delle cause rientrano in due categorie: quelle che prendono di mira le borse di scambio di criptovalute e i fornitori di portafogli virtuali, sostenendo che le misure di sicurezza non sono riuscite a proteggere gli account degli utenti e quelle che accusano i fornitori di cellulari di aver indirettamente permesso agli hacker di

[531] FELICE M. (2023). *Segnalata falla di sicurezza in Metamask: chi sta rischiando di perdere le proprie criptovalute*, in Criptomercato.it. Disponibile in open source sul sito https://www.criptomercato.it/2023/04/14/falla-sicurezza-metamask-criptovalute/

[532] ESET (2021). *I pericoli per i cryptocurrency wallets e come difendersi*. Disponibile in open source sul sito https://www.eset.com/it/info/eset-blog/sicurezza-it-domestica/i-pericoli-per-i-cryptocurrency-wallets-e-come-difendersi/

accedere ai conti di criptovalute. Estremamente complesso per i giudici anche conoscere l'identità degli hacker.[533]

Ad oggi ancora non si conosce l'esito di molte controversie in materia, ed i tentativi quotidiani di appropriazione indebita di *wallet* altrui hanno comportato una proliferazione del numero degli attacchi cibernetici e di, conseguenza, una proliferazione del lavoro dei tribunali.

[533] ESET, *I pericoli per i cryptocurrency wallets e come difendersi*, cit. 531.

CAPITOLO IV

Sommario: 1. L'evoluzione degli ultimi anni - 2. I benefici e i rischi della moneta virtuale - 3. Le criticità e le questioni aperte - 3.1. (*Segue*): Le tensioni tra blockchain e il GDPR - 4. Il futuro delle criptovalute

1. L'evoluzione degli ultimi anni

Dalla nascita delle criptovalute ad oggi si è assistito ad un'importante evoluzione delle stesse nonché alla capitalizzazione[534] del mercato delle criptovalute, nonostante esso abbia subito un duro colpo nel 2014 quando il grande exchange di Bitcoin Mt. Gox è stato vittima di una grave violazione della sicurezza consentendo agli hacker di rubare 850.000 BTC.[535] In tale periodo, la tecnologia dei portafogli era ancora immatura e non esistevano protezioni assicurative o scambi centralizzati di criptovalute (CEX),[536] tanto che, molti utenti colpiti dall'hack di Mt. Gox sono ancora in attesa della restituzione dei fondi perduti. Sebbene Mt. Gox sia stato un disastro per gli investitori di Bitcoin, ha contribuito a spronare i primi sostenitori della criptovaluta a sviluppare una forma di protezione contro i furti e a migliorare la sicurezza. Oggi le principali borse di criptovalute, come Binance e Coinbase, offrono ai clienti una protezione assicurativa e funzioni di sicurezza come l'autenticazione a due fattori.[537] Ciò nonostante, la

[534] "*In finanza, l'operazione con la quale gli interessi maturati su un capitale sono aggiunti al capitale medesimo[...]*" - DIZIONARIO DI ECONOMIA E FINANZA (2012) - Treccani. Disponibile in open source sul sito https://www.treccani.it/enciclopedia/capitalizzazione_%28Dizionario-di-Economia-e-Finanza%29/

[535] CACIOPPOLI V. (2022). *La storia dell'exchange Mt. GoX* in cryptpnomist.ch. Disponibile in open source sul sito https://cryptonomist.ch/2022/08/28/storia-exchange-mt-gox/

[536] CRYPTOTELLING (2022). *Cos'è un exchange di criptovalute? Differenza tra exchange centralizzato e decentralizzato.* Disponibile in open source sul sito https://cryptotelling.it/cos-e-un-exchange-di-criptovalute/

[537] BIAGIO S. (2014). *Bitcoin senza pace: la piattaforma MtGox hackerata ancora. Per Roubini la criptomoneta è uno "schema Ponzi"*, in IlSole24Ore. Disponibile in open source sul sito

capitalizzazione del mercato delle criptovalute ha raggiunto livelli estremamente elevati[538], raggiungendo i 1.700 milioni di dollari nel gennaio 2022.[539]

Le criptovalute sono diventate così il quarto asset finanziario più diffuso tra gli investitori.[540] Se i Bitcoin sono stati essenziali in fase di sviluppo del mercato e oggi rappresentano le criptovalute più "famose" e disponibili, hanno perso terreno a causa delle nuove criptovalute nate negli ultimi anni.[541] Nel 2013, infatti, è avvenuto il lancio di Ethereum i cui progettisti avevano il principale obiettivo di decentralizzare Internet.[542] Gli sviluppatori introdussero concetti come i contratti intelligenti automatizzati, in grado di eseguire comandi esclusivamente tramite codice una volta soddisfatte le condizioni. Ethereum è diventata rapidamente la seconda criptovaluta al mondo. Ben presto, centinaia di progetti hanno iniziato a utilizzare il protocollo Ethereum per creare applicazioni decentralizzate (dApp).[543]

Insieme alla perdita di mercato dei Bitcoin, registrata negli ultimi anni, si è assistito, inoltre, ad una generale volatilità delle stesse.[544] Come noto, a fronte degli ingenti

https://st.ilsole24ore.com/art/finanza-e-mercati/2014-03-10/bitcoin-senza-pace-mtgox-hackerato-ancora-e-roubini-boccia-criptomoneta-e-schema-ponzi-204128.shtml?uuid=ABnxL81

[538] COINKGECKO (2022). *Quaterly report 2022*. Disponibile in open source sul sito https://assets.coingecko.com/reports/2022-Q2-Report/CoinGecko-2022-Q2-Report.pdf.

[539] MORNINGSTAR (2022). *5 grafici sul passato, presente e futuro delle criptovalute*. Disponibile in open source sul sito https://www.morningstar.it/it/news/225275/5-grafici-sul-passato-presente-e-futuro-delle-criptovalute.aspx.

[540] PESCOSOLIDO J. (2021). *Criptovalute – Tassazione ed obblighi di monitoraggio fiscale (RW), Fisco e Tasse*. Disponibile in open source sul sito https://www.fiscoetasse.com/approfondimenti/14140-criptovalute-tassazione-ed-obblighi-di-monitoraggio-fiscale-rw.html. Accesso avvenuto in data 1 aprile 2023.

[541] MORNINGSTAR (2022). *5 grafici sul passato, presente e futuro delle criptovalute*, cit. 535

[542] CRITOVALUTA.IT (2022). *Che cosa sono gli Ethereum?*. Disponibile in open source sul sito https://www.criptovaluta.it/ethereum/cosa-sono

[543] GREEKS ACADEMY (2022). *Piattaforma Ethereum: la storia del genio informatico che a diciannove anni ha capito il potenziale della blockchain*. Disponibile in open source sul sito https://www.geeksacademy.it/articolo-49/l_inventore-della-piattaforma-ethereum-vitalik-buterin/

[544] BANCA D'ITALIA - EUROSISTEMA (2022). *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività*. Disponibile in open source sul sito https://www.bancaditalia.it/media/approfondimenti/2022/cripto/Comunicazioni-della-Banca-d-Italia-DLT-cripto.pdf.

guadagni iniziali dei primi investitori in criptovalute, oggi, dato l'ingente interesse, vi è stato un crollo del valore nominale.[545]

Tale scenario è sorto in mancanza di una regolamentazione adeguata dello strumento delle criptovalute come già visto nei capitoli precedenti, per la quale si avverte una estrema necessità dovuta, principalmente, al crescente utilizzo delle criptovalute, registrato dalla società ChainAnalysis. Mediante l'utilizzo dell'indice combinato elaborato allo scopo, la ChainAnalysis ha registrato un aumento dell'utilizzo delle valute digitali tra la fine del 2019 e la metà del 2021 pari al +2500%, nonchè un ulteriore incremento nei primi mesi del 2021 dove si è registrato un aumento pari ad una volta e mezzo il dato del 2020.[546]

L'elevata diffusione dell'utilizzo delle criptovalute negli ultimi anni deriva, in parte, anche dall'utilizzo delle valute digitali da parte delle economie emergenti o Paesi in via di sviluppo, i quali a causa di una limitata diffusione degli istituti bancari ed infrastrutture finanziarie, utilizzano le valute digitali in sostituzione di un conto di deposito, per trasferire denaro all'estero più facilmente o per proteggere i risparmi dagli elevati tassi di inflazione e svalutazione della moneta legale. Diversamente, nei Paesi più avanzati si assiste ad una rapida, ma frammentaria regolamentazione delle valute digitali, come già analizzato nei capitoli precedenti.[547]

Pertanto, alla luce di quanto sopra esposto, nei paragrafi successivi verranno analizzati più nello specifico i vantaggi delle valute digitali nonché le criticità riscontrate e infine, le questioni che ad oggi rimangono ancora "aperte" che rendono le valute digitali un mondo, da un lato, in rapida espansione e dall'altro un mercato definito come incerto e pericoloso.548

---

[545] MORNINGSTAR (2022). *5 grafici sul passato, presente e futuro delle criptovalute*, cit. 535

[546] MINELLA M. (2021). *Criptovalute: perché il 2022 sarà l'anno dei regulators*. Il sole24ore. Disponibile in open source sul sito https://www.ilsole24ore.com/art/criptovalute-perche-2022-sara-l-anno-regulators-AEN03wo.

[547] MINELLA M., *Criptovalute: perché il 2022 sarà l'anno dei regulators*, cit. 543

[548] ANNUNZIATA F., *Verso una disciplina europea delle cripto-attività. Riflessioni a margine della recente proposta della Commissione UE*, cit. 224.

2. I benefici e i rischi della moneta virtuale

I vantaggi dei Bitcoin e più in generale delle criptovalute, come già delineato nei capitoli precedenti, sono dati da: decentralizzazione, mancanza di corso legale, pseudo anonimato, bassi costi di transazione, trasparenza, velocità e sicurezza delle transazioni.[549]

Da un'attenta analisi a trecentosessanta gradi dei benefici e rischi delle valute virtuali si evidenzia come i benefici e/o i vantaggi delle criptovalute ne costituiscano, al tempo stesso, fattori di rischio[550]

Ciascun metodo di pagamento, proprio in quanto consta di rischi e benefici specifici, comporta da parte dell'utente-utilizzatore una informata valutazione dei vantaggi e svantaggi di un dato metodo di pagamento, mediante ricerche, consulenze e valutazioni personali.[551]

L'accessibilità rientra nella categoria dei vantaggi e dei rischi specifici derivanti dall'utilizzo delle valute virtuali. Il vantaggio è evidente laddove è possibile per tutti i potenziali investitori e/o utilizzatori di criptovaluta accedere al mercato attraverso l'uso di un computer o di uno smartphone con una connessione a Internet. Per aprire un portafoglio di criptovalute non è necessaria alcuna verifica dell'identità, né un controllo del credito o dei precedenti. È molto più veloce e facile rispetto a quanto accade nelle istituzioni finanziarie. Permette inoltre di effettuare transazioni via internet o di inviare fondi a terzi senza alcuno sforzo. Dall'altro lato però l'accessibilità è un rischio sia per l'utente che può essere vittima di illeciti sia

[549] FOCUS (2022). *Criptovalute e Bitcoin: quali sono i vantaggi e gli svantaggi?* Disponibile in open source sul sito https://www.focus.it/tecnologia/digital-life/criptovalute-bitcoin-quali-vantaggi-e-svantaggi#:~:text=Cominciamo%20da%20vantaggi%20delle%20monete,2%20%2D%20Pi%C3%B9%20trasparenti.

[550] HATTON S. (2016). *Why Competition in FinTech is Great for The Marketplace.* Disponibile in open source sul sito http://www.trusek.com/whycompetition-in-fintech-is-great-for-the-marketplace/

[551] IG (2022). *I vantaggi del trading sulle criptovalute*. Disponibile in open source sul sito https://www.ig.com/it/criptovalute/vantaggi-trading-criptovalute.

per le autorità competenti in materia che sempre più spesso devono affrontare problematiche relative all'utilizzo di valute virtuali in attività criminose.

Molti metodi di pagamento disponibili sul mercato vengono utilizzati in combinazione con la tecnologia (es. pagamento mediante *smartphone*). In tal caso, l'utente dovrà essere particolarmente consapevole e, quindi, valutare i benefici e i rischi che possono derivare dall'utilizzo di un metodo di pagamento in combinato con l'utilizzo di una data tecnologia.[552]

Tra i benefici dell'utilizzo delle criptovalute figura la velocità di transazione. Le transazioni, infatti, avvengono in pochi minuti e questo è un aspetto rilevante che può essere utile in qualunque transazione di carattere commerciale. All'interno delle istituzioni finanziarie, come sappiamo, la maggior parte delle transazioni viene regolata in tre-cinque giorni e i bonifici bancari richiedono almeno 24 ore.

Appare evidente che i rischi ed i benefici che possono derivare dall'utilizzo di monete virtuali sono connessi anche all'evoluzione del settore, o meglio sono condizionati dalla velocità con la quale esso si evolve. In particolare, a partire dagli anni 2000 si è assistiti ad una crescente e sempre più veloce evoluzione dei metodi di pagamento. Difatti, oggi, l'utilizzatore può usufruire di una vastità di nuovi metodi di pagamento caratterizzati da elementi differenti.[553] Mentre, a causa dell'inflazione, il valore di molte valute diminuisce, molti vedono nelle criptovalute una protezione contro l'inflazione. Il Bitcoin ha un limite massimo al numero di monete che vengono coniate. Ad esempio, se la crescita dell'offerta di moneta supera la crescita dell'offerta di Bitcoin, il prezzo del Bitcoin aumenterà. Anche molte altre criptovalute utilizzano lo stesso meccanismo per limitare l'offerta e possono fungere da salvaguardia contro l'inflazione. In termini di quantità, infatti, i Bitcoin rilasciati sono solo 21 milioni. Pertanto, a causa dell'aumento della

[552] BBANCA D'ITALIA - EUROSISTEMA, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività*, cit. 540.

[553] ACADEMY (2020). *Storia della moneta prima di Bitcoin.* Disponibile in open source sul sito https://academy.youngplatform.com/criptovalute/storia-della-moneta/.

domanda, il valore aumenterà, e ciò potrebbe generare risvolti positivi per il mercato e prevenire l'inflazione nel lungo periodo.[554]

Quanto sopra descritto rappresenta una panoramica su quelli che sono i vantaggi derivanti dall'uso delle monete virtuali e delle innovazioni che esse hanno apportato ai metodi di pagamento, ma non ci si può esimere dal riconoscere le criticità e le questioni aperte che verranno analizzate nel successivo capitolo conclusivo.

3. Le criticità e le questioni aperte

Prima di indicare le criticità è opportuno premettere che, dopo un primo periodo di forte scetticismo verso le criptovalute, ad oggi si è sicuramente registrata una maggiore adesione verso un mondo ancora tutto da esplorare nonché una crescente approvazione. Ciò ha registrato, come già accennato in precedenza, anche un aumento del numero delle criptovalute. L'evoluzione tecnologica dei nuovi sistemi di pagamento ha consentito il venir meno di alcune criticità precedentemente esistenti.

Il primo elemento critico delle criptovalute è dato dalla loro volatilità ossia dalle ingenti oscillazioni che registrano e dagli innumerevoli passaggi tra un investitore all'altro. Ciò può comportare un aumento del rischio di perdita anche a causa dei problemi tecnici della tecnologia crittografica blockchain, ossia la tecnologia utilizzata da gran parte delle criptovalute. La principale causa scatenante della volatilità delle criptovalute è da attribuire alla speculazione che è alla base di ogni oscillazione del mercato.[555]

Tuttavia, per fare fronte alla volatilità delle criptovalute, esiste una particolare classe di criptovalute, nota come "stablecoin", che sta diventando sempre più popolare nei mercati. Le stablecoin sono una forma relativamente nuova di token di pagamento, progettata per ridurre al minimo la volatilità del prezzo delle criptovalute e le

[554] ACADEMY, *Storia della moneta prima di Bitcoin*, cit. 550.
[555] ITALIAOGGI (2022). *Volatilità e cripto, fra vantaggi e rischi per gli investitori.* Disponibile in open source sul sito https://www.italiaoggi.it/news/volatilita-e-cripto-fra-vantaggi-e-rischi-per-gli-investitori-202204290950477339.

speculazioni sulle stesse. Le Stablecoin sono tipicamente garantite o da attività (da garanzie fisiche o da cripto-asset) o nella forma di una stablecoin algoritmica (con gli algoritmi utilizzati come modo per stabilizzare la volatilità del valore del token).[556] Un esempio di stablecoin è Libra, la criptovaluta sviluppata e lanciata da Facebook.

Connessa alla volatilità vi è il rischio di liquidità ossia se da un lato l'offerta di valute digitali negli ultimi anni è riuscita a fare fronte all'ingente quantitativo richiesto dagli utilizzatori, dall'altro lato gli *exchanger* stanno prosciugando le loro riserve comportando la illiquidità del mercato delle criptovalute. In altre parole, tale illiquidità comporta il rischio per gli investitori di rivendere le proprie criptovalute ad un prezzo inferiore rispetto a quello di acquisto.

Pertanto, i rischi finanziari di volatilità e liquidità hanno in comune il costo di acquisto ossia il prezzo che viene determinato dal mercato e quindi, dall'incontro della domanda e dell'offerta.[557]

Strettamente collegato alla volatilità delle criptovalute, come ulteriore criticità attribuibile alle stesse, vi è l'assenza di una tutela dei depositi effettuati dagli utenti. In particolare, gli utilizzatori di criptovalute possono in qualsiasi momento perdere il proprio investimento a causa delle variazioni improvvise del valore delle criptovalute, ovvero a causa di frodi. A ciò si aggiunga che l'irreversibilità delle transazioni mediante valute digitali non consente di definire la responsabilità degli utenti a causa della gestione decentralizzata delle criptovalute.[558]

Per quanto sopra, le asimmetrie informative nel mondo delle criptovalute sono troppo grandi per lasciare i clienti a sé stessi. Ci sono diversi approcci che le autorità dei Paesi emergenti possono prendere in considerazione per affrontare i rischi legati alle criptovalute. Questi non si escludono a vicenda e possono includere il contenimento o la regolamentazione del settore delle criptovalute o, addirittura, il

---

[556] EBA (2019). *Report with advice for the European Commission on crypto-assets*. Disponibile in open source sul sito https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20 crypto%20assets.pdf? retry=1.

[557] RASERA S. (2021). *Stablecoin: percezione, elusione e modellizzazione della volatilità*, per Università Ca' Foscari. Disponibile in open source sul sito http://dspace.unive.it/bitstream/handle/10579/20005/858271-1265955.pdf?sequence=2

[558] MINELLA M., *Criptovalute: perché il 2022 sarà l'anno dei regulators*, cit. 543

divieto assoluto. Pertanto, è fondamentale che le autorità di regolamentazione garantiscano che i consumatori vulnerabili siano protetti dai danni.[559]

Come accennato precedentemente, dalla "nascita" delle criptovalute ad oggi si è registrata una notevole espansione, soprattutto a partire dal 2020, tanto che si è passati da circa 2.400 criptovalute a 10.300 registrate nel 2022. La sicurezza cibernetica rimane uno degli argomenti più critici in tema di criptovalute, in quanto secondo alcune fonti nel periodo da settembre 2020 a maggio 2022, 2 miliardi di dollari sono stati sottratti alla gestione decentralizzata.[560]

Un recente studio di Capterra, azienda operante nel settore IT, ha dimostrato che le criticità principali che trattengono gli italiani dall'utilizzare le criptovalute come mezzo di pagamento sono legate alla sicurezza in primis ed all'incertezza del loro futuro. In particolare, i timori sono legati al possibile sostentamento di attività illegali (il 54% degli italiani intervistati[561]), ai possibili attacchi hacker ossi alla sicurezza delle valute digitali (il 20% degli italiani intervistati) o alla volatilità delle criptovalute (il 37% degli italiani intervistati) nonché alla mancanza di un'autorità preposta alla vigilanza circa l'utilizzo delle valute digitali.[562]

Il rischio sulla sicurezza delle criptovalute e sull'utilizzo delle stesse in attività illegali, come l'hackeraggio, costituisce un tema fondamentale verso cui molti Stati hanno acquisito consapevolezza e sensibilità tanto da spingerli ad intervenire mediante una serie di tentativi di regolamentazione della materia.

---

[559] NEWBURY L. B., KERSE M. (2023). *Crypto Consumer Protection: Why 'Wait and See' Is No Longer an Option* in cgap.org. Disponibile in open source sul sito https://www.cgap.org/blog/crypto-consumer-protection-why-wait-and-see-is-no-longer-option

[560] REDAZIONE ANSA (2022). *Consob, oltre 10.300 criptovalute, criticità sulla sicurezza*. Disponibile in open source sul sito https://www.ansa.it/sito/notizie/economia/criptovalute/2022/07/23/consob-oltre-10.300-criptovalute-criticita-sulla-sicurezza_e7c35848-6262-49c7-a803-09af10d320af.html.

[561] Disponibile in open source sul sito https://www.capterra.it/blog/2313/criptovalute-rischi-studio.

[562] CASSE C. (2021) *I rischi delle criptovalute potrebbero frenare la loro espansione in Italia*. Capterra. Disponibile in open source sul sito https://www.capterra.it/blog/2313/criptovalute-rischi-studio.

Purtroppo, ad oggi, non vi è omogeneità tra le regolamentazioni adottate e, pertanto, la mancanza di chiarezza del quadro normativo odierno viene annoverata tra le maggiori criticità delle monete virtuali.

Infatti l'attuale quadro normativo mondiale risulta molto incerto, con autorità nazionali e sovranazionali che intervengono senza un coordinamento centrale. Tale situazione si può ravvisare negli Stati Uniti d'America come in Europa, in cui si tenta di giungere ad una regolamentazione armoniosa ma non troppo stringente per evitare di minacciare i soggetti utilizzatori di tali monete.[563] Al fine di tutelare la trasparenza dei mercati nonché gli utilizzatori ed investitori il legislatore europeo sta intervenendo da diverso tempo con l'intento di regolamentare qualsiasi aspetto delle criptovalute e più in generale, degli asset crittografici.[564]

Tra i provvedimenti europei di maggiore spessore in ambito di criptovalute, di cui abbiamo già trattato in precedenza, figurano il Market in Crypto Asset Regulation (MiCA), non ancora in vigore e che esclude dalla sua applicazione alcuni asset crittografici, affiancato dal Transfer of Funding Regulation ossia il Regolamento (UE) 2015/847 del 20 maggio 2015[565] riguardante i dati informativi che accompagnano i trasferimenti di fondi mediante il quale si sono estese le misure antiriciclaggio applicate alle transazioni di trasferimento fondi anche ai trasferimenti mediante criptovalute[566] e dalla V Direttiva antiriciclaggio o AML5.

L'introduzione di AML5 si può senz'altro ritenere positiva in quanto costituisce una importante guida normativa all'interno del mondo crypto-asset. Non vi è dubbio che persistono ancora numerose lacune legislative nel diritto dell'UE, soprattutto a causa della rapida evoluzione del mondo crittografico delle valute virtuali.

---

[563] EXEO EDIZIONI (2022). *Normativa internazionale relativa al Bitcoin*. Disponibile in open source sul sito https://www.exeo.it/Articoli/8042/bitcoin-regolamentazione.aspx.

[564] REDAZIONE (2022). *Criptovalute, regolamentazione europea: pregi e criticità*. Blue Rating. Disponibile in open source sul sito

[565] Regolamento (UE) 2015/847 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 (CE) n. 1781/2006 - Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015R0847&from=EN

[566] REDAZIONE, *Criptovalute, regolamentazione europea: pregi e criticità*, cit. 573

Il primo problema riguarda la definizione di valute virtuali come

> "*una rappresentazione digitale di valore [...] accettato da persone fisiche o giuridiche come mezzo di scambio*".

Questa descrizione consente di effettuare una riflessione: se le valute virtuali si considerano mezzi di scambio da un punto di vista economico e, pertanto, svolgono la stessa funzione del denaro, rientrano nella normativa antiriciclaggio sono i cd. token valuta, mentre rimangono fuori i token di investimento e i token utilità.[567]

Seppur l'intento del legislatore UE sia stato certamente quello di coprire tutti i potenziali usi di crypto-asset con la direttiva 843/2018, sono emerse alcune inesattezze in ordine alle definizioni, per cui l'incertezza giuridica potrebbe influire negativamente sull'identificazione degli attori coinvolti, ossia i soggetti obbligati.

Alla luce di queste predette incertezze giuridiche, è emersa l'esigenza da parte degli interpreti di proporre una modifica dell'articolo 3(18) in modo che tutti i tipi di criptovalute possano essere incluse e trattate allo stesso modo.[568]

Un altro divario che dovrebbe essere preso in considerazione è rappresentato dalla classificazione di solo fornitori che scambiano criptovalute in denaro fiat e viceversa. In questo senso, tutti i tipi di valute virtuali negoziabili in moneta fiat sono coinvolti in AMLD 5. In altre parole, solo quei fornitori che convertono crypto in valute fiat sono considerati soggetti obbligati.[569] Di conseguenza, anche i provider crypto-to-crypto sono lasciati al di fuori della categoria degli obbligati,

---

[567] MARTORANA M. e SICHI Z. (2022). *Transazioni in criptovalute: pubblicate le regole antiriciclaggio dell'Ocse* in ALTALEX. Disponibile in open source sul sito https://www.altalex.com/documents/news/2022/11/09/transazioni-criptovalute-pubblicate-regole-antiriciclaggio-ocse

[568] MAINIERI N. e DI GABRIELE N. (2022). *Utilizzi a scopi illeciti delle criptovalute: recenti profili giurisprudenziali e normativi italiani ed internazionali e riferimenti al mercato degli NFT* in Giurisprudenza Penale. Disponibile in open source sul sito https://www.giurisprudenzapenale.com/wp-content/uploads/2022/06/mainieri_digabriele_gp_2022_6.pdf

[569] NIGRO R. (2022). *Criptovalute e antiriciclaggio, vicini ad una svolta?* In ALTALEX. Disponibile in open source sul sito https://www.altalex.com/documents/news/2022/02/10/criptovalute-e-antiriciclaggio-vicini-ad-una-svolta

Questo rappresenta un problema per la legge antiriciclaggio, consentendo agli utenti di scambiare in modo anonimo token crittografici ad altri.

Stante la definizione di fornitori di portafogli, intesi come gli strumenti e/o i supporti informatici necessari per la movimentazione delle criptovalute, non risulterebbero inclusi nella normativa antiriciclaggio- AMLD5, i fornitori di non-wallet. Ciò comporta un vuoto legislativa e lascia ampio margine di azione per i criminali.[570] Di conseguenza, i legislatori dell'Unione Europea dovrebbero prendere in considerazione un'eventuale estensione della direttiva antiriciclaggio, al fine di includere anche i fornitori non di portafoglio.

Nell'ambito dello schema di scambio delle criptovalute, uno dei ruoli più importanti è senza dubbio quello che svolge l'utente. Gli utenti partecipano alla transazione di token e per questo motivo dovrebbero essere inclusi nella normativa più volte citata.[571] Di fatto, la quinta direttiva antiriciclaggio ha proposto un sistema di autodichiarazione che facilita l'identificazione degli utenti alle autorità su base volontaria. Tuttavia, sarebbe opportuno rendere la identificazione obbligatoria per rafforzare questo sistema.

Un altro problema riguarda i fornitori di servizi tumbler ossia i servizi forniti da imprese per mascherare l'origine delle criptovalute simulando un gran numero di codici. Questi soggetti non sono regolati dalla direttiva in quanto sono coperti dall'anonimato e ciò consente al criminale di trarre un indubbio vantaggio. Infatti, se i token passano attraverso un servizio tumbler è impossibile rintracciarli. Secondo il principio "conosci il tuo cliente" di AMLD 5, i soggetti obbligati hanno la necessità di controllare e segnalare informazioni su transazioni sospette.[572] In questo senso, se il vero obiettivo dei legislatori dell'UE è quello di regolamentare

[570] PEZZUTO A. (2022). *Obblighi di comunicazione in capo agli operatori in moneta virtuale* in Diritto bancario Tidona. Disponibile in open source sul sito https://www.tidona.com/obblighi-di-comunicazione-in-capo-agli-operatori-in-moneta-virtuale/

[571] VEDANA F. (2022). *Criptovalute col registro entro il 2 giugno* in ItaliaOggi. Disponibile in open source sul sito https://www.italiaoggi.it/news/criptovalute-col-registro-entro-il-2-giugno-2552466

[572] MAINIERI N. e DI GABRIELE N., *Utilizzi a scopi illeciti delle criptovalute: recenti profili giurisprudenziali e normativi italiani ed internazionali e riferimenti al mercato degli NFT*, cit. 578.

ed evitare il riciclaggio di denaro, l'inclusione di tali provider nella lista di soggetti obbligati è essenziale.

Inoltre, risulta rilevante segnalare il Regolamento (UE) 2022/858 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito, che modifica i regolamenti (UE) n. 600/2014 e (UE) n. 909/2014 e la direttiva 2014/65/UE.[573] Questo regolamento dell'Unione Europea, di cui si è parlato poco dalla sua entrata in vigore, prevede l'introduzione di un regime regolatore delle tecnologie a registro distribuito, categorizzati in: sistemi multilaterali di negoziazione, sistemi di regolamento titoli e sistemi di negoziazione e regolamento.[574]

I legislatori dell'UE hanno votato a favore dell'imposizione di limiti alle transazioni effettuate da utenti di criptovalute anonimi e non verificati, come parte delle nuove misure antiriciclaggio (AML) del blocco. I trasferimenti di cripto-asset dovranno essere tracciati e identificati per impedirne l'uso nel riciclaggio di denaro, nel finanziamento del terrorismo e in altri reati. L'obiettivo è garantire che i cripto-asset possano essere tracciati allo stesso modo dei trasferimenti di denaro tradizionali.[575]

Secondo i nuovi requisiti concordati dagli eurodeputati, tutti i trasferimenti di cripto-asset dovranno includere informazioni sulla fonte dell'asset e sul suo beneficiario, informazioni che dovranno essere messe a disposizione delle autorità competenti. Le norme riguarderanno anche le transazioni effettuate dai cosiddetti portafogli non ospitati (un indirizzo di portafoglio di cripto-asset custodito da un utente privato). Le soluzioni tecnologiche dovrebbero garantire che questi trasferimenti di attività possano essere identificati individualmente.

---

[573] Disponibile in open source sul sito https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015R0847&from=EN

[574] BANCA D'ITALIA, *Quaderni di Ricerca Giuridica Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale* , cit 47

[575] PEPE E. (2023). *Il Governo italiano dà via libera all'emissione di azioni e obbligazioni tokenizzate* in COINTELEGRAPH. Disponibile in open source sul sito https://it.cointelegraph.com/news/il-governo-italiano-da-via-libera-allemissione-di-azioni-e-obbligazioni-tokenizzate

L'obiettivo è garantire che i trasferimenti di criptovalute possano essere tracciati e le transazioni sospette bloccate. In quanto, a causa della loro velocità e della loro natura virtuale, le transazioni di criptovalute eludono facilmente le regole esistenti basate sulle soglie di transazione.[576] I deputati hanno quindi deciso di eliminare le soglie minime e le esenzioni per i trasferimenti di basso valore. Inoltre, le regole troverebbero applicazione con riferimento a tutti quei trasferimenti che avvengono da persona a persona senza un fornitore, come le piattaforme di trading di bitcoin, o tra fornitori che agiscono per proprio conto.

A ciò si aggiunga l'introduzione di una nuova responsabilità per i fornitori di servizi di criptovalute consistente nell'obbligo, prima di mettere i cripto-asset a disposizione dei beneficiari, di verificare che la fonte dell'asset non sia soggetta a misure restrittive e che non vi siano rischi di riciclaggio di denaro o di finanziamento del terrorismo.[577]

A causa della mancanza di norme che consentono la tracciabilità dei trasferimenti di cripto-asset e di fornire informazioni sull'ordinante/beneficiario di tali trasferimenti, le nuove norme che fanno parte di un nuovo pacchetto antiriciclaggio, che stabilisce misure per rafforzare le norme dell'UE sulla lotta al riciclaggio di denaro e al finanziamento del terrorismo, perseguono un secondo obiettivo ossia colmare le carenze del quadro normativo esistente, tra cui l'attuazione inefficace, la scarsa sorveglianza e l'insufficiente individuazione di transazioni sospette.[578]

Il 28 marzo 2023 il Parlamento europeo ha inoltre votato a favore dell'applicazione di limiti di pagamento sui portafogli di criptovalute anonimi. Le misure mirano a impedire che le criptovalute, i token non fungibili (NFT) e il metaverso vengano utilizzati per crimini finanziari. I nuovi limiti vietano ai trader di effettuare o ricevere trasferimenti anonimi di criptovalute superiori a 1.000,00 euro (circa

[576] BRAMBILLA G. (2023). *Tokenizzazione degli asset: via libera alle normative* in The Crypto Gateway. Disponibile in open source sul sito https://thecryptogateway.it/tokenizzazione-asset/

[577] PEPE E., *Il Governo italiano dà via libera all'emissione di azioni e obbligazioni tokenizzate*, cit. 585.

[578] MAINIERI N. e DI GABRIELE N., *Utilizzi a scopi illeciti delle criptovalute: recenti profili giurisprudenziali e normativi italiani ed internazionali e riferimenti al mercato degli NFT*, cit. 578.

879,00 sterline).[579] Le transazioni più grandi sono consentite se l'identità del cliente può essere confermata o se è coinvolto un provider di criptovalute regolamentato.

La proposta considera l'uso di monete per la privacy, come il monero (XMR-USD) e i mixer di criptovalute, che offuscano il mittente e il destinatario delle transazioni di criptovalute, come fattori aggiuntivi nella valutazione dei rischi di riciclaggio di denaro.

La legislazione vieta inoltre ai fornitori di criptovalute dell'UE di intrattenere rapporti di corrispondenza con fornitori di criptovalute stranieri non registrati o privi di licenza. La proposta è stata approvata dopo che 99 legislatori hanno votato a favore, otto hanno votato contro e sei si sono astenuti.

Tale intervento fa parte della legislazione legata alla nuova Agenzia dell'Unione Europea contro il riciclaggio di denaro (AMLA). [580]Affinché le nuove misure diventino legge è necessario l'accordo del Parlamento europeo e del Consiglio europeo.[581] L'ecosistema idealizzato dalla normativa si fonderebbe in particolare su tre specifici elementi: la moneta euro in "forma" digitale; una Central Bank Digital Currency (C.B.D.C.), necessaria per effettuare grandi transazioni da parte delle aziende e token monetari forniti dalle banche.[582]

Come abbiamo visto, blockchain è una tecnologia che non è (e non dovrebbe essere) immune dalla regolamentazione. Tuttavia, i regolatori dovrebbero considerare attentamente quando e in quale misura intervenire, per evitare di soffocare una neotecnologia con un potenziale immenso. La prima domanda che i regolatori dovrebbero porsi è:

---

[579] LYONS C. (2023). *Unione Europea imporrà un tetto di 1.000€ ai trasferimenti anonimi di criptovalute* in COINTELEGRAPH. Disponibile in open source sul sito https://it.cointelegraph.com/news/eu-lawmakers-push-for-stricter-rules-on-anonymous-crypto-transfers

[580] LYONS C., *Unione Europea imporrà un tetto di 1.000€ ai trasferimenti anonimi di criptovalute*, cit. 589.

[581] MCGLEENON B. (2023). *EU votes for payment limits on anonymous crypto wallet transactions*. Disponibile in open source sul sito https://it.finance.yahoo.com/news/eu-votes-payment-limits-anonymous-crypto-wallet-transactions-151425821.html

[582] MAINIERI N. e DI GABRIELE N., *Utilizzi a scopi illeciti delle criptovalute: recenti profili giurisprudenziali e normativi italiani ed internazionali e riferimenti al mercato degli NFT*, cit. 578.

"*la blockchain tecnologia uno scopo legittimo?*"

Come sappiamo, alcuni servizi virtuali consentono accidentalmente la violazione degli obblighi di legge, mentre altri sono specificamente finalizzati alla violazione leggi (come mercati dark web come Silk Road). E', naturalmente, un difficile processo per valutare l'intento di un fornitore di servizi, nonché l'entità dell'attività illecita svolta utilizzando tale servizio. A questo proposito, il legislatore dovrebbe condurre un'analisi caso per caso di applicazioni basate sulla tecnologia blockchain per verificare se il singolo servizio persegue uno scopo legittimo.[583]

Solo quando la valutazione di cui sopra ha un esito negativo, i legislatori dovrebbero prendere in considerazione un intervento interdittivo, ad esempio bloccando un servizio o eliminando un sito web.

La seconda questione da considerare è se vi siano mezzi alternativi per procedere alla regolamentazione della tecnologia blockchain mediante interventi non di tipo normativo. Un esempio sono le soluzioni di *soft law* che possono raggiungere gli stessi obiettivi politici in un modo meno invasivo. Per esempio, le organizzazioni private possono sviluppare una serie di standard e di migliori pratiche attraverso un processo volontario e di autoregolamentazione, senza necessità di un intervento normativo.[584]

Concludendo, il quadro normativo che via via il legislatore europeo si sta impegnando a delineare non è chiaro, anzi rappresenta un insieme di norme non armoniose.[585] Difatti, se da un lato vi è un incremento dei vincoli relativi alle attività che utilizzano le criptovalute o le tecniche crittografiche, dall'altro, dove il quadro normativo potrebbe essere più chiaro e contenere maggiori indicazioni per gli Stati membri, queste indicazioni mancano e attribuiscono alle singole autorità il compito di interpretare ed applicare le disposizioni mediante strumenti non chiari e/o non definiti a livello europeo. In altre parole, finché il legislatore europeo non sarà

[583] WERBACH K. (2018), *The Blockchain and the New Architecture of Trust,* cit. 120.
[584] MCGLEENON B., *EU votes for payment limits on anonymous crypto wallet transactions*, cit. 591.
[585] MCGLEENON B., *EU votes for payment limits on anonymous crypto wallet transactions*, cit. 591.

chiaro non si potrà pretendere chiarezza ed armoniosità della normativa dei singoli stati relativa alle criptovalute.[586]

3.1. (*Segue*): Le tensioni tra blockchain e il GDPR

Negli ultimi anni sono stati individuati diversi punti di tensione tra le tecnologie blockchain e il GDPR. In linea di massima, si può affermare che queste tensioni sono dovute a due fattori generali.

In primo luogo, il GDPR si basa sul presupposto che, in relazione a ciascun dato personale esiste almeno una persona fisica o giuridica - il responsabile del trattamento - a cui gli interessati possono rivolgersi per far valere i propri diritti ai sensi della normativa UE sulla protezione dei dati, mentre le blockchain sono caratterizzate dalla decentralizzazione, sostituendo un attore unitario con molti attori diversi. Un ulteriore fattore di complicazione a questo proposito è che, alla luce dei recenti sviluppi giurisprudenziali, la definizione di quali entità si qualifichino come (co)-controllori responsabili del trattamento può essere di difficile inquadramento giuridico.

In secondo luogo, il GDPR si basa sul presupposto che i dati possano essere modificati o cancellati se necessario per ottemperare a requisiti legali come gli articoli 16 e 17 del GDPR. Le blockchain, al contrario, rendono tali modifiche dei dati volutamente onerose per garantirne l'integrità e aumentare la fiducia nella rete.[587]

Anche in questo caso, le incertezze relative a questo settore della legge sulla protezione dei dati sono accresciute dall'incertezza esistente nella legislazione dell'UE in materia. Attualmente, infatti, non è chiaro come debba essere interpretato il concetto di "cancellazione" di cui all'articolo 17 del GDPR.

---

[586] REDAZIONE,*Criptovalute, regolamentazione europea: pregi e criticità*, cit 574

[587] REDAZIONE (2022). *Blockchain e GDPR: riflessioni su alcuni elementi di contrasto* in Iusinitinere.it. Disponibile in open source sul sito https://www.iusinitinere.it/blockchain-e-gdpr-riflessioni-su-alcuni-elementi-di-contrasto-43006

Queste tensioni si manifestano in molti ambiti. Ad esempio, è in corso un dibattito se i dati tipicamente memorizzati su un libro mastro distribuito, come le chiavi pubbliche e i dati transazionali, si qualifichino come dati personali ai fini del GDPR. Nello specifico, la questione riguarda la qualificazione come dati personali ove siano stati crittografati o sottoposti a hash. La soluzione più probabile è che tali dati si possano qualificare come dati personali ai fini del GDPR e ciò significa che la legge europea possa applicarsi anche quando tali dati vengono elaborati.

Più in generale, questa analisi evidenzia anche la difficoltà di determinare il livello di sufficiente anonimizzazione tale da soddisfare la soglia del GDPR.[588]

Un altro esempio di tensione tra blockchain e GDPR riguarda i principi generali di minimizzazione dei dati e di limitazione delle finalità. Mentre il GDPR richiede che i dati personali trattati siano ridotti al minimo e siano trattati solo per finalità che sono state specificate in anticipo, questi principi possono essere difficili da applicare alle tecnologie blockchain. I libri mastri distribuiti sono database di sole appendici che crescono continuamente con l'aggiunta di nuovi dati che, inoltre, sono replicati su molti computer diversi.[589] Entrambi gli aspetti sono problematici dal punto di vista del principio di minimizzazione dei dati. Inoltre, non è chiaro come la "finalità" del trattamento dei dati personali debba essere applicata nel contesto della blockchain ed in particolare se questo includa solo la transazione iniziale o anche il trattamento continuativo dei dati personali (come la loro memorizzazione e il loro utilizzo per la conservazione) una volta che sono stati inseriti nella catena.[590]

Ma la questione che è stata probabilmente più discussa negli ultimi anni è la tensione tra il diritto alla cancellazione (il "diritto all'oblio") e le blockchain. In

[588] BAIARDI F. e COMELLA C. (2021). *GDPR e blockchain, tutte le sfide di un rapporto complesso* in Agenda Digitale. Disponibile in open source sul sito https://www.agendadigitale.eu/documenti/gdpr-e-blockchain-tutte-le-sfide-di-un-rapporto-complesso/

[589] NAMIRIAL 82021). *Blockchain e GDPR. Tutela dei dati ed opportunità*. Disponibile in open source sul sito https://focus.namirial.it/blockchain-gdpr/

[590] BAIARDI F. e COMELLA C., *GDPR e blockchain, tutte le sfide di un rapporto complesso,* cit. 599.

effetti, le blockchain sono di solito deliberatamente progettate per rendere difficile o impossibile la modifica (unilaterale) dei dati. Questo, ovviamente, è difficile da conciliare con i requisiti del GDPR secondo cui i dati personali devono essere modificati (ai sensi dell'articolo 16 del GDPR) e cancellati (ai sensi dell'articolo 16 del GDPR[591]) in circostanze specifiche.

Da questa analisi si desumono due conclusioni generali. In primo luogo, le specificità tecniche e la progettazione della governance dei casi d'uso della blockchain possono essere difficili da conciliare con il GDPR. Secondo, si sottolinea anche l'attuale mancanza di certezza giuridica su come le blockchain possano essere progettate in modo da essere conformi al regolamento. Piuttosto, l'esame di questa tecnologia attraverso la lente del GDPR evidenzia anche significative incertezze concettuali in relazione al regolamento che hanno una rilevanza che va ben oltre il contesto specifico della blockchain. Infatti, la mancanza di certezza giuridica relativa a numerosi concetti del GDPR rende difficile determinare come quest'ultimo si applichi sia a questa tecnologia sia ad altre.[592]

Mentre gran parte del dibattito si è concentrato sulle tensioni tra le blockchain e la normativa europea in materia di protezione dei dati, le prime possono anche fornire un'opportunità per il trattamento dei dati personali e strumenti per soddisfare gli obiettivi della seconda.

È stato sostenuto che le tecnologie blockchain potrebbero essere uno strumento adatto a raggiungere alcuni degli obiettivi di fondo GDPR in quanto esse sono uno strumento di governance dei dati che potrebbero supportare forme alternative di gestione e distribuzione dei dati e fornire vantaggi rispetto ad altre soluzioni contemporanee.[593] Le blockchain possono essere progettate per consentire la condivisione dei dati senza la necessità di un intermediario centrale fidato, offrono

[591] "Diritto di rettifica": "*L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo*".
[592] NERLI F. (2022). *Sistema Blockchain e G.D.P.R., criticità e possibili soluzioni* in affidaty.io. Disponibile in open source sul sito https://affidaty.io/blog/it/2022/03/blockchain-gdpr-dati/
[593] BOLDRINI N. (2018). *Blockchain e GDPR: le sfide (e le opportunità) per la protezione dei dati* in Blockchain4innovation.it. Disponibile in open source sul sito https://www.blockchain4innovation.it/sicurezza/blockchain-gdpr/

trasparenza su chi ha avuto accesso ai dati e le smart chain basate su blockchain e i contratti intelligenti basati su blockchain possono inoltre automatizzare la condivisione dei dati, riducendo così anche i costi delle transazioni.

Inoltre, le strutture di incentivo cripto-economico delle blockchain potrebbero avere il potenziale per influenzare l'attuale economia della condivisione dei dati. Queste caratteristiche possono portare benefici più ampi all'economia contemporanea.[594]

Queste stesse caratteristiche possono essere utilizzate anche per sostenere alcuni degli obiettivi del GDPR, come ad esempio fornire agli interessati un maggiore controllo sui dati personali che li riguardano direttamente o indirettamente. Questa logica può essere osservata anche sulla base dei diritti dell'interessato, come il diritto di accesso (articolo 15 del GDPR[595]) o il diritto di accesso ai dati personali, che forniscono agli interessati il controllo su ciò che gli altri fanno dei loro dati personali e su ciò che essi stessi possono fare con tali dati.

---

[594]BOLDRINI N., *Blockchain e GDPR: le sfide (e le opportunità) per la protezione dei dati*, cit. 603

[595] Diritto di accesso dell'interessato

"*1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni: a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. 2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento. 3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune. 4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui*."

Inoltre, la DLT potrebbe supportare il controllo sui dati personali consentendo di monitorare il rispetto del principio di limitazione delle finalità. Nello stesso tempo, la tecnologia potrebbe essere utilizzata per contribuire all'individuazione di violazioni dei dati e di frodi.[596]

Un altro punto da trattare relativamente al rapporto tra GDPR e criptovalute è relativo al ruolo dei *miner*. Un *miner*, come già previsto in precedenza, ha un'enorme autonomia nell'eseguire le elaborazioni di blocchi da lui accettati. In tal caso sono stati emessi alcuni pareri, come quello del gruppo di lavoro "Articolo 29" e del report del Parlamento europeo[597], che ritengono che il ruolo svolto dal miner è sufficiente per qualificarlo ai sensi del GDPR come *data controller.* Tuttavia, si tratta di un argomento non che non trova il consenso per esempio della *Commission Nationale Informatique et Libertés* che non riconosce i *miner* come *data controller* poiché la loro funzione si limita ad aggiungere *record* ad una blockchain.[598] Al contrario la *Commission Nationale Informatique et Libertés* qualificherebbe i *miner* come *data processor* (ai sensi dell' Art. 4 GDPR) nel caso in cui operino su una blockchain pubblica con transazioni di tipo commerciale.[599] Tuttavia, ciò non risulta possibile in quanto un *data processor* viene definito tale quando opera su dati su mandato del *data controller.*

Concludendo si è evidenziato che, se da un lato, esiste una tensione significativa tra la natura stessa delle tecnologie blockchain e la struttura generale della legge sulla protezione dei dati,[600] dall'altro questa nuova tecnologia potrebbe offrire vantaggi distinti che potrebbero aiutare a raggiungere alcuni degli obiettivi del GDPR,

[596] BOLDRINI N., *Blockchain e GDPR: le sfide (e le opportunità) per la protezione dei dati*, cit. 603

[597] Committee on International Trade, Report on Blockchain: a Forward-Looking Trade Policy (AB-0407/2018), EU parliament, 27/11/2018 - Disponibile in open source sul sito https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

[598]BAIARDI F. e COMELLA C., *GDPR e blockchain, tutte le sfide di un rapporto complesso,* cit. 599.

[599] Commission Nationale Informatique et Libertés,, Premiers Éléments d'analyse de la CNIL: Blockchain, September 2018

[600] BAIARDI F. e COMELLA C., *GDPR e blockchain, tutte le sfide di un rapporto complesso,* cit. 599.

soprattutto per quanto riguarda il maggiore controllo sui dati personali.[601] Infatti, più le persone interagiscono con dispositivi connessi a Internet che raccolgono e condividono dati personali, più diventa cruciale rafforzare la loro protezione e la loro fiducia.[602] La tecnologia blockchain colma il gap di fiducia attraverso crittografia e gli incentivi economici, e aumenta la protezione dei soggetti interessati garantendo un'identità immutabile e fornendo un'autenticazione sicura e crittografata.[603]

La necessità di innovazione circa la gestione dei dati personali è anche in linea con i principi costituzionali che regolano le politiche strategiche dell'UE. Infatti, se da un lato la protezione delle persone fisiche in relazione al trattamento dei dati personali costituisce un diritto fondamentale ai sensi dell'articolo 8, paragrafo 1, della Carta dei diritti fondamentali e dell'articolo 16, paragrafo 1, del TFUE, dall'altra parte l'innovazione è anche un obiettivo significativo dell'UE[604]. Ai sensi dell'articolo 173 TFUE, l'Unione europea e gli Stati membri devono infatti adoperarsi per migliorare la competitività dell'UE che comprende la promozione dell'innovazione e dello sviluppo tecnologico.[605]

4. Il futuro delle criptovalute

Come già detto, il mercato delle criptovalute è semplicemente troppo giovane per un'analisi di mercato dettagliata e circa il futuro delle monete virtuali si possono

[601] EUROPEAN PARLIAMENT (2019). *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?*. Disponibile in open source sul sito https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

[602] SATER S. (2017). *Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows*, 39. Disponibile in open source sul sito http://dx.doi.org/10.2139/ssrn.3080987

[603] SATER S., *Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows*, cit. 612.

[604] FINCK M. (2017). *Blockchains and Data Protection in the European Union*, Max Planck Institute for Innovation and Competition Research Paper No. 18-01, 29, Disponibile in open source sul sito
http://dx.doi.org/10.2139/ssrn.3080322.

[605] FINCK M., *Blockchains and Data Protection in the European Union,* cit. 614.

trarre solo conclusioni molto generali. Questo problema persisterà fino a quando il mercato non mostri una certa "maturità" o se le valute andranno a raggiungere un valore terminale.

Una delle grandi sfide che restano agli analisti delle criptovalute è quella di trovare un modello di prezzo ragionevole, ma ciò potrebbe essere impossibile se si considera che la maggior parte delle criptovalute, almeno al momento, non ha attività sottostanti con valori intrinseci, in quanto è estremamente difficile stabilire un prezzo equo.[606] Non aiuta il caso degli analisti di mercato il fatto che il mercato delle criptovalute sembra essere in una bolla di prezzo e subisce costantemente crolli, scandali, manipolazioni dei prezzi e investitori truffati da losche start up che promettono enormi guadagni. Anche in questo caso, il mercato delle criptovalute potrebbe trovarsi in una bolla e molte delle monete più grandi non potrebbero sopravvivere. A ciò si aggiunga che il 2022 è stato un anno terribile per le criptovalute. In totale, più di 2.000 miliardi di dollari di valore di mercato, in gran parte speculativo, sono evaporati. Milioni di consumatori e aziende hanno perso denaro e, cosa forse ancora più dannosa per un'industria e una tecnologia nascenti, la fiducia fondamentale nella promessa della cripto-finanza, che avrebbe dovuto essere una correzione a molti degli errori che hanno dato origine alla crisi finanziaria del 2008, sta svanendo.[607]

Nel frattempo, i politici che hanno lanciato l'allarme sui rischi eccessivi delle criptovalute, non riuscendo a creare una regolamentazione sensata, non hanno potuto impedire il verificarsi molteplici fallimenti su larga scala.

Sicuramente nei prossimi anni dal punto di vista normativo, si assisterà ad una ulteriore stratificazione delle disposizioni che potranno portare generalmente a due principali risultati: o maggiore chiarezza del quadro normativo e una necessaria

[606] MORGANTINI F. (2023). *Cosa accadrà alla blockchain: prospettive e osservazioni sul futuro delle criptovalute*, in Forbes. Disponibile in open source sul sito https://forbes.it/2023/03/06/prospettive-osservazioni-futuro-criptovalute/

[607] REDAZIONE CONFINELIVE (2023). *Criptovalute: quale futuro per gli investimenti nelle monete digitali?* in ConfineLive. Disponibile in open source sul sito https://www.confinelive.it/criptovalute-quale-futuro-per-gli-investimenti-nelle-monete-digitali/

azione di unificazione ed armonizzazione del diritto in materia a livello nazionale, europeo nonché mondiale ovvero una maggiore confusione normativa con la conseguente nascita di nuove ed ulteriori problematiche riguardanti il tema delle monete virtuali in generale e della tecnologia blockchain nello specifico.

La tecnologia blockchain è una rivoluzione, ma la sua adozione complessiva può essere limitata a causa di problemi tecnici e interni. Per fornire servizi e informazioni migliori e più sicuri a utenti e consumatori, tutte le parti interessate, dagli enti governativi alle aziende, devono collaborare per migliorare e rafforzare l'attuale tecnologia blockchain.[608]

[608] MORGANTINI F., *Cosa accadrà alla blockchain: prospettive e osservazioni sul futuro delle criptovalute*, cit. 616.

CONCLUSIONI

Il presente elaborato ha analizzato il mondo delle criptovalute nonché il ruolo e le responsabilità dei soggetti che operano all'interno dell'ecosistema di tale tipologia di monete virtuali. La ricerca ha portato alla conclusione che il ruolo ricoperto dai legislatori di ogni singolo stato e la collaborazione fra gli stessi è stata e continua ad essere estremamente importante non solo per la sopravvivenza ed il futuro delle criptovalute ma anche per progredire in termini di innovazione tecnologica e sicurezza.

I risultati ottenuti grazie alla presente disamina e alle fonti utilizzate hanno confermato che il mondo delle criptovalute è ancora parzialmente sconosciuto che si trova in una fase embrionale, sia dal punto di vista tecnologico sia dal punto di vista normativo.

Nel corso del primo capitolo abbiamo notato come l'evoluzione delle criptovalute ha interessato tutta la comunità internazionale, la quale probabilmente non era pronta a comprendere il fenomeno e non ha posto in essere quegli interventi idonei ed armonizzati al fine di evitare distorsioni nell'utilizzo delle criptovalute fino a concretizzare illeciti di natura penale.

Abbiamo visto come la frammentazione della normativa sia a livello internazionale che nazionale non ha consentito di costruire una cornice efficace per individuare e sanzionare le responsabilità dei soggetti fornitori di servizi relativi alle criptovalute, a fronte delle esigenze di sicurezza per gli utenti ed i mercati.

Solo recentemente si è iniziato ad imporre alcuni limiti e regole alla attività dei cd. *wallet provider* per i quali rimane complicato individuare la responsabilità penale, tanto che sono ancora rari i casi di incriminazione.

Nell'ambito della responsabilità dei *wallet provider* è stata menzionata la disciplina contenuta nella direttiva (UE) 2015/849, conosciuta con il termine di Direttiva antiriciclaggio in virtù della quale i fornitori di portafogli virtuali sono considerati soggetti obbligati al rispetto delle norme in materia di antiriciclaggio che impongono agli stessi il monitoraggio delle operazioni sospette.

Si è altresì evidenziato che la normativa nazionale ha imposto ai *provider* che operano sul territorio italiano l'iscrizione obbligatoria in una sezione speciale del registro tenuta dall'Organismo per gli Agenti e Mediatori, ovvero l'Organismo Agenti e Mediatori di Credito, necessaria per lo svolgimento delle attività di portafoglio. Quanto detto può essere considerato un fattore di miglioramento verso una piena ed armonica regolamentazione ed un controllo "istituzionale" del mondo delle criptovalute e dei loro operatori.

Certamente non sono da sottovalutare le problematiche intrinseche collegate alle criptovalute e ai portafogli di criptovalute. Come notato nel terzo capitolo, i portafogli sono ancora oggi "depredati" dagli *hacker* che continuano ad eludere i sistemi di sicurezza. Pertanto, si può sostenere che se da un lato la tecnologia ha fatto passi da gigante, dall'altro presenta ancora diverse problematiche connesse a diversi fattori, tra cui la difficoltà di acquisizione delle prove digitali e di conservazione delle stesse, di svolgimento delle indagini per arrivare ad individuare i colpevoli, il più delle volte coperti dall'anonimato delle operazioni crittografate.

Con il presente elaborato si è quindi inteso portare alla luce quelli che sono i benefici ed i rischi connessi alle criptovalute; abbiamo visto che l'utilizzo di queste ultime ha portato una vera rivoluzione nella vita di tutti noi, laddove ci consentono di effettuare operazioni di mercato e di scambio di beni e servizi solamente mediante l'uso di un computer o di uno *smartphone* con connessione Internet.

Come contropartita a tutto ciò, si è però avuta una proliferazione dei rischi e l'esposizione ad attività criminose cibernetiche che solamente con una normativa armonizzata, sovranazionale, si potranno prevenire.

Oggi, ogni singolo utente che si approccia al mondo delle criptovalute deve essere consapevole e pienamente cosciente non solo dei benefici che possono derivare dal suo investimento ma anche dei rischi che possono verificarsi.

Si è portata, quindi, all'attenzione del lettore la questione relativa al rapporto tra la tecnologia *blockchain* e il GDPR. In particolare, all'esito dell'analisi svolta, si riscontrano due conclusioni: la compatibilità tra GDPR e *blockchain* dal punto di vista tecnico rende difficile determinare come il primo possa trovare applicazione nei confronti di tale tecnologia e come la mancanza di certezza giuridica della *blockchain* possa intaccare la tutela dei dati personali prevista dal GDPR.

Il risultato si potrà ottenere solo con le diverse evoluzioni normative.

Pertanto, al fine di migliorare la qualità degli interventi normativi, i legislatori e le autorità finanziarie dovranno adottare un approccio partecipativo che coinvolga gli utenti e tutti gli operatori di mercato dell'industria delle criptovalute. Al momento si è lontani da questo obiettivo in quanto, i più recenti interventi dei regolatori, primo fra tutti la proposta MiCA nell'Unione Europea, sono per lo più un mero adattamento degli attuali atti legislativi ai nuovi bisogni.

Concludendo, l'approccio più produttivo per le autorità di regolamentazione sarebbe quello di riunirsi con i rappresentanti dell'industria delle criptovalute, come gli sviluppatori di *blockchain* e gli operatori di cripto-scambio, al fine di implementare regolamenti mirati a risolvere le sfide normative più significative discusse in questa tesi, senza vanificare le caratteristiche positive di questo nuovo fenomeno. Altrimenti, la conseguenza immediata sarebbe che la *blockchain*, come tutte le nuove tecnologie, muterà sempre in nuove forme e strutture per sfuggire a regolamentazioni troppo stringenti, e i regolatori dovranno, quindi, inseguirla in una rincorsa senza fine.

BIBLIOGRAFIA

ACADEMY (2020). *Storia della moneta prima di Bitcoin.*

ACADEMY (2022). *DLT e Blockchain: storia, differenze e soluzioni.*

ANDOLINA E. (2015). *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della "privacy" e onde eversive*, in Archivio penale.

A.G (2018). *Conio. Il wallet bitcoin è un'opportunità per le banche* in aziendabanca.it.

Agenzia delle Entrate, Alternative alle detrazioni.

AJ FRONTIERE N. (2015). *Criptovalute tra opportunità e voglia di regolamentazione*.

ALBE' G. (2022). *Obbligo di iscrizione al registro OAM per gli operatori cripto: cosa è cambiato e tutte le sanzioni*. Agendadigitale.eu.

ALBERTI M. (2022). *Nuovi reati 231: falsificazioni di pagamenti diversi dal contante, frodi, criptovalute e riciclaggio* in Studio Legale Mascetti.

AMATO M. e FANTACCI L. (2016). *Per un pugno di bitcoin: rischi e opportunità delle monete virtuali*. EGEA spa.

ANNUNZIATA F. (2020) *Verso una disciplina europea delle cripto-attività. Riflessioni a margine della recente proposta della Commissione UE*, Diritto Bancario.

ANNUNZIATA F., ZETZSCHE D. A., ARNER D. W., BUCKLEY R. P., (2020). *The markets in crypto-assets regulation (MICA) and the EU digital finance strategy, European Banking Institute*, Law Working Paper Series, Paper n.018, 2020

ARCIERI F. (2021). *Che Cos'è Un Algoritmo Di Consenso (Spiegato Facile).*

ARCERI F. (2022). *Wallet Custodial E Non Custodial: Quali Sono E Quando Usarli*.

ATZORI M. (2015). *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*

AUTORITA' BANCARIA EUROPEA (2014). *Opinion on 'Virtual Currencies'*, EBA/Op/2014/

AYOUBI M. (2018). *Dalle radici di Bitcoin alla sua nascita*, www.StayUpgrated.it.

S., J. e E. (2022). *We can finally reconcile privacy and compliance in crypto. Here are the new technologies that will protect user data and stop illicit transactions* in Future.com.

BABANINA V., TKACHENKO I., MATIUSHENKOO., e KRUTEVYCH M. (2021). *Cybercrime: History of formation, current state and ways of counteraction*. Amazonia Investiga, 10

BAIARDI F. e COMELLA C. (2021). *GDPR e blockchain, tutte le sfide di un rapporto complesso* in Agenda Digitale.

BALL J. (2015). *Cameron wants to ban encryption – he can say goodbye to digital Britain*, The Guardian

BANCA D'ITALIA (2018). Avvertenza per i consumatori sui rischi delle valute virtuali da parte delle Autorità Europee

BANCA D'ITALIA (2019) *Quaderni di Ricerca Giuridica Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale* a cura di Fabrizio Maimeri e Marco Mancini numero 87 della Consulenza Legale.

BANCA D'ITALIA (2022). *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività*.

BANCA D'ITALIA - EUROSISTEMA (2022). *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività*.

BARSAN I. (2020)., *France: Regulation of Crypto-assets, Intermediaries and Initial Coin Offerings in France*, Global Compliance News.

BAUTISTA C (2014). *Google search algorithm changes demote piracy sites from page rankings*, Tech Times

BELLINI M. (2018). *Osservatorio Blockchain 2018: crescono del 73% i progetti e si afferma un nuovo rapporto con le cryptocurrency*, www.Blockchain 4innovation.it.

BELLINI M. (2018). *Smart Contracts: che cosa sono, come funzionano quali sono gli ambiti applicativi*, www.Blockchain4innovation.it.

BELLINI E. (2019). *Il nuovo Regolamento Prospetto: le opportunità per un più facile ricorso al mercato dei capitali e una più effettiva armonizzazione dei processi a livello comunitario*

BELLINI M. (2022). *Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia.*

BELVEDERE A. (2022). *Celsius rilascia dati transazioni propri utenti* in bitconio.net.

BIAGIO S. (2014). *Bitcoin senza pace: la piattaforma MtGox hackerata ancora. Per Roubini la criptomoneta è uno "schema Ponzi"*, in IlSole24Ore.

BIENNA M. (2016). *Bitcoin e attacchi hacker: problemi di sicurezza irrisolvibili?* www.money.it.

BINANCE ACADEMY (2019). *What Is a Crypto Wallet?*

BINANCE ACADEMY (2022). *Wallet Custodial vs. Non Custodial: qual è la differenza?*

BINDER J., (2016). *Governance of Investment Firms under MiFID II*

BIT2ME ACADEMY (2019). *Cosa sono i cold wallet*?

BIT2ME ACADEMY (2020). *Cosa sono gli hot wallet*?

BitcoinEthereumNews.com (2022). *Gli ingegneri trovano un bug del portafoglio Slope dietro un hack da 6 milioni di dollari basato su Solana*.

BOCCHINI R., (2017). *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in Dir. Inform., I

BOLDRINI N. (2018). *Blockchain e GDPR: le sfide (e le opportunità) per la protezione dei dati* in Blockchain4innovation.it.

BONCOMPAGNI F. (2021). *Crimini informatici e criptovalute*, in S. Capaccioli (a cura di), *Criptoattività, criptovalute e bitcoin*, Giuffrè, Milano

BONOLIS P., SELVAGGIUOLO E., BACCI F. (2022). Operatori in criptovalute: con l'istituzione del registro...in CSM.LAW.it.

BORSA ITALIANA. GLOSSARIO FINANZIARIO - Crypto-Asset

BRAMBILLA G. (2023). *Tokenizzazione degli asset: via libera alle normative* in The Crypto Gateway.

BRUNOZZI L. M. e FIORIO C. (2021). *231 e criptovalute. La responsabilità da reato dell'ente nel riciclaggio mediante monete virtuali*. Gaspare Jucan Sicignano.

CACIOPPOLI V. (2022). *La storia dell'exchange Mt. GoX* in cryptpnomist.ch.

CAPACCIOLI S. (2015). *Bitcoin: le operazioni di cambio con valuta a corso legale sono prestazioni di servizio esenti*, in Il Fisco.

CAPACCIOLI S. (2015). *Criptovalute e Bitcoin: un'analisi giuridica*, Milano.

CAPACCIOLI S. e SOLDAVINI P. (2019). *Fallisce Bitgrail, la piattaforma italiana per le criptovalute* in Ilsole24Ore.

CAPACCIOLI S. (2020). *Come si pagano le tasse per le criptovalute in Italia*

CARLINI V. (2022). *Qual è il trattamento fiscale delle criptovalute in Italia?* Sole24Ore Finanza.

CARRIÈRE P. (2020), *Crypto-assets: le proposte di regolamentazione della Commissione UE. Opportunità e sfide per il mercato italiano*, Diritto Bancario.

CASSE C. (2021) *I rischi delle criptovalute potrebbero frenare la loro espansione in Italia*. Capterra.

CASSIBBA F., (2009). *L'ampliamento delle attribuzioni del pubblico ministero distrettuale*, in LUPARIA (a cura di), *Sistema penale e criminalità informatica*.

CAVALLI S. (2018). *Proof of Work vs Proof of Stake*,

CAVICCHIOLI M. (2018). *La decentralizzazione, questa sconosciu*ta, www.IlBitcoin.it

CHAN C. (2015). *Bitcoin vs Western Union: How Low Fees Are Disrupting the Remittance Industry*

CHAN C., NADARAJAH E OSTERRIEDER (2017). *A statistical analysis of cryptocurrencies*. In Journal of Risk and Financial Management 10.2

CHANDLER N. (2012). *How Digital Wallets Work. HowStuffWorks.*

CHAUM D. (1982). *Blind Signature for Untraceable Payments*. Department of Computer Science, University of California.

CHIAP, R. B. (2019). *Blockchain, tecnolgia e applicazione per il business*. In R. B. Chiap, Blockchain, tecnolgia e applicazione per il business, Hoepli

CHRISTIN A., ROSENBLATT A., BOYD D. (2015). *Courts and predictive algorithms*, Data & Civil Rights Primer

CIRAOLO F. E LA ROSA E. (2022). *Contrasto alle frodi e alle falsificazioni dei mezzi di pagamento diversi dai contanti. Brevi note intorno al d. lgs. n. 184/21 (con focus sulle valute virtuali).* DB non solo diritto bancario.

CIVILETTI G. (2019). *BITGRAIL – Procedura fallimentare dell'exchange italiano*, in Crypto avvocato.

CLARK D. (2018). *ICO Governance Foundation Creates First ICO Registry*. Law.com

CNBCTV18.com (2022). *Explained | What is a blockchain ecosystem?*

COINKGECKO (2022). *Quaterly report 2022*.

COINSATRA (2022). *What Is A Brain Wallet & How To Create One For Yourself?*

COLZANI J. (2019). *Blockchain: A Digital Solution for Modern Democracies?*

COMELLINI S. (2018). *Ecco perchè i Bitcoin e le Criptovalute non sono Moneta Elettronica*

CONTE D. (2019). *Criptovalute e l'applicazione delle disposizioni tributarie, in Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2 criptovalute e rivoluzione digitale*

Convenzione di Palermo (2000).

Convenzione di Budapest (2001).

Convenzione del Consiglio d'Europa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi del crimine e sul finanziamento del terrorismo (2005).

CONZATO A. (2022). *Criptovalute, come dichiararle nei redditi? I chiarimenti dell'Agenzia delle Entrate*. Corriere.it.

COOPER D., NASH G. (2019). European Parliament Publishes Study on Blockchain and the GDPR, Covington & Burling.

Corte di Cassazione, sezioni unite penali, sentenza 26 marzo 2015 (dep. 24 aprile 2015), n. 17325.

Corte di Cassazione, sez. II pen., sentenza 25 gennaio 2022 (ud. 7 ottobre 2021), n. 2868.

Corte di Cassazione, sezione II penale, sentenza 7 luglio 2022 (dep. 13 luglio 2022), n. 27023.

Corte di Giustizia UE, Sez. V, 22 ottobre 2015, Causa C-264/14, Skatteverket c. David Hedqvist

COSTANTINO M. (2020). *La storia delle criptovalute dal 1983 al 2007, dai Cypherpunks alle istituzioni*.

CRAIG P., DE BÚRCA G. (2011). *EU Law – Text, Cases, and Materials*, 5th ed., Oxford University Press

CRITOVALUTA.IT (2022). *Che cosa sono gli Ethereum?.*

CRYPTOECONOMY (2022). *Criptovalute: norme attuali e prossimi scenari*.

CRYPTOPEDIA STAFF (2021). *What Is a Cell Phone SIM Swap Attack?* in Cryptopedia.

CRYPTOTELLING (2022). *Cos'è un exchange di criptovalute? Differenza tra exchange centralizzato e decentralizzato.*

CUCCHIARATO G. (2019). *Regolamentazione delle ICOs in Italia: pro e contro della proposta Consob*. AgendaDigitale.it.

CULICCHI R. (2022). *Blockchain e banche d'affari, un rapporto che cresce: ecco i progetti.*

CUOMO L., RAZZANTE R. (2007). *La disciplina dei reati informatici*, Torino

CVETKOVA I. (2018). *Cryptocurrencies legal regulation*. Bricks law journal, 18.

DAHLBERG T. et al. (2008). *Past, present and future of mobile payments research: A literature review*. In: Electronic Commerce Research and Applications. Special Section: Research Advances for the Mobile Payments Arena.

DAL CO (2022). *Bitcoin e criptovalute, il quadro si complica: rischi e scenari in attesa delle regole* in agendadigitale.eu.

DALY L. (2022). *What is a Blockchain Ecosystem? Blockchains are like snowflakes: each one is unique*. The Motley Fool.

DANIELE M., (2011). *La prova digitale nel processo penale, in Riv. dir. proc., 2011, p. 283; v. anche ID., Caratteristiche della prova digitale*, in RUGGIERI F. e PICOTTI L. (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica: aspetti sostanziali e processuali*, Giappichelli, Torino.

DÄSCHLER S. (2022). *Regolamento MAR: Il Regolamento sugli abusi di mercato dell'Unione Europea.*

DB non solo diritto bancario (2022). *Regolamento MiCA sulle criptovalute: il testo approvato dal Consiglio UE.* Dirittobancario.it.

DE CONNO A. (2022). *Criptovalute, riciclaggio e autoriciclaggio. Cryptocurrency e rischi: la recente pronuncia della Cassazione penale sul punto (sentenza 25 gennaio 2022 n. 2868),* in Altalex.

Decreto legislativo 1 settembre 1993, n. 385

Decreto legislativo 24 febbraio 1998, n. 58

Decreto Legislativo 21 novembre 2007, n. 231

Decreto Legislativo 10 agosto 2010, n. 141

Decreto Legislativo 25 maggio 2017, n. 90.

Decreto legislativo 8 novembre 2021, n. 184.

Decreto legislativo 8 novembre 2021, n. 195.

DEOTTO LOVECCHIO & PARTNERS (2022). *L'inquadramento giuridico delle criptovalute.*

DI BITONTO M., L. (2008). *L'accentramento investigativo delle indagini sui reati informatici*, in *La ratifica della Convenzione del consiglio d'Europa sul cybercrime: profili processuali*, in dir. Internet.

DI MAIO D. e POMPEI L. (2019). *EMIR refit: cosa cambia per le controparti non finanziarie in Risk & Compliance.*

DI PAOLO G. (2013). Voce *Prova informatica* (diritto processuale penale), in Enc. dir., Annali, VI, Giuffrè, Milano.

Direttiva 2004/39/CE

Direttiva 2006/112/CE

Direttiva 2009/65/CE

Direttiva 2009/110/CE

Direttiva 2011/61/UE

Direttiva 2014/65/UE

Direttiva 2014/57/UE

Direttiva 2015/849/UE

Direttiva 2018/843/UE

Direttiva 2018/1673/UE

Direttiva 2019/713/UE

DIZIONARIO DI ECONOMIA E FINANZA (2012) - Treccani

DOMINIONI O. (1997). *Un nuovo idolum theatri: il principio di non dispersione probatoria*, in Cass. pen.

DÜR A., MARSHALL D., BERNHAGEN P., (2019) *The Political Influence of Business in the European Union*, University of Michigan Press, 92.

EBA (2013) *Warning to consumers on virtual currencies.*

EBA (2019). *Report with advice for the European Commission on crypto-assets*.

ENGELS F. (1884) *Origins of the Family, Private Property and the State*.

ENRIQUES L. (2019). *Welcome to Vilnius: Regulatory Competition in the EU Market for E-Money*, Oxford Business Law Blog

ESET (2021). *I pericoli per i cryptocurrency wallets e come difendersi*.

ESMA (2019). *Advice on Initial Coin Offerings and Crypto-Assets*, ESMA50-157

ETHEREUM (2022). *Cos'è un contratto intelligente?*

EVANS C. (2020). *The Great Estonian Exodus — Crypto Firms Are Leaving Estonia*, Cointelegraph

EUROPEAN CENTRAL BANK (2015). *Virtual currency schemes – a further analysis*

EUROPEAN PARLIAMENT (2019). *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?*

EUROPOL SPOTLIGHT (2022). *Cryptocurrencies: tracing the evolution of criminal finances.*

FADDA D. (2023). *Il malware BlackGuard si aggiorna e prende di mira i crypto wallet: tutti i dettagli*.

FAFT (*2014*). *Virtual Currencies Key Definitions and Potential AML/CFT Risks*

FARINA S. (2022). *Criptovalute da non dichiarare in RW se Piattaforma Italiana* in Blogfiscale.it.

FARMER J., (2003). *The Spector of Crypto-anarchy: Regulating Anonymity-Protecting Peer-to-Peer Networks*, Fordham Law Review, 72(3)

FELICE M. (2023). *Segnalata falla di sicurezza in Metamask: chi sta rischiando di perdere le proprie criptovalute*, in Criptomercato.it

FERRUA P. (2013). *La prova nel processo penale: profili generali*, in FERRUA P., - MARZADURI E., - SPANGHER G., (a cura di), *La prova penale*, Torino.

FILODIRITTO.IT (2015). *IVA - Corte di Giustizia: i Bitcoin sono esenti dal pagamento dell'Iva.*

FINANCIAL CONDUCT AUTHORITY (FCA) (2019). *Guidance on Cryptoassets*, PS 19/22.

FINANCIAL STABILITY, FINANCIAL SERVICES AND CAPITAL MARKETS UNION, EUROPEAN COMMISSION (2020). *Communication on Digital Finance Package*

FINCK M. (2017). *Blockchains and Data Protection in the European Union*, Max Planck Institute for Innovation and Competition Research Paper No. 18-01

FINTASTICO (2022). *Digital wallet: cosa sono e perché prima o poi ne avrai uno*.

FLOR R. (2015). *I limiti del principio di territorialità nel "cyberspace". Rilievi critici alla luce del recente orientamento delle sezioni unite*, in Dir. pen. proc.

FLYIP. (2019). *Blockchain: cos'è l'hash function nel protocollo Bitcoin*.

FOCUS (2022). *Criptovalute e Bitcoin: quali sono i vantaggi e gli svantaggi?*

FRIES T. (2020)., *Germany Passes Law Enabling Banks to Store Cryptocurrencies*, The Tokenist.

FRTG (2021). *Attacco HTML Smuggling: tecnica sempre più diffusa*

GARAVAGLIA R. (2018). *Valute virtuali, wallet provider, exchange platform: cosa cambia con la quinta direttiva antiriciclaggio e cosa ancora deve cambiare*.

GASPARRI G., (2015). *Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?* in Dir. Inform., I

GATES, M. (2017). *Blockchain: La guida definitiva per conoscere blockchain, bitcoin, criptovalute, contratti smart e il futuro del denaro*. Independently published.

GBBC (2021). *Global standards mapping initiative 2.0*.

GEEKSFORGEEKS (2022). *What is Blockchain Ecosystem?*

GENNAI A. (2018). Investire sulla Blockchain, Sole 24 ore – Plus 24.

GERONI D. (2021). *Blockchain Ecosystem* Explained. Blockchains.com.

GREEKS ACADEMY (2022). *Piattaforma Ethereum: la storia del genio informatico che a diciannove anni ha capito il potenziale della blockchain*.

HACKER P., THOMALE C., (2018). *Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law*, 15 European Company and Financial Law Review

HAIGH T., BREITINGER F. e BAGGILI I. (2018). *If i had a million cryptos: Cryptowallet application analysis and a trojan proof-of-concept*, in International Conference on Digital Forensics and Cyber Crime, Springer

HALABURDA H. AND SALVARY M. (2016). *Beyond Bitcoin*, The Economics of Digital currencies, New York.

HATTON S. (2016). *Why Competition in FinTech is Great for The Marketplace.*

HE, D. et al. (2018). *Virtual Currencies and Beyond : Initial Considerations* - IMF Staff Discussion Notes 16/3.

HERKSTRÖTER C., BORN M. (2020). *Crypto Assets: Germany introduces new regulatory regim*e, Norton Rose Fulbright.

HIREMATH O.S. (2023). *Blockchain Mining- All you need to know*, in Edureka.

HSU K. (2022). *The Six Most Common Attacks on Crypto Wallets and Why Banks Should Care* in finextra.com.

IG (2022). *I vantaggi del trading sulle criptovalute*.

Il Post. (2013). *Come è stato preso il capo di Silk Road.*

IlSole24Ore (2018). *Furti di bitcoin / Mt Gox, il furto più grande*.

INTIGROW (2020). *What are the security risks associated with using a cryptocurrency wallet?*

INVESTGLASS (2023). Caldo vs. tiepido vs. freddo: Quale portafoglio di criptovalute è adatto a me?.

ITALIAOGGI (2022). *Volatilità e cripto, fra vantaggi e rischi per gli investitori.*

KERR O.(2005). *Digital Evidence and the New Criminal Procedure*, in 105 Colum. L. Rev., 291

KLINGENBRUNN D., BENZING M., MCQUAID E., (2020) *Observations on the Commission's proposal for a European crypto-assets framework, Lexology*.

KOSTORIS E. (2007). *Processo penale, delitto politico e "diritto penale del nemico"*, in Rivista di diritto processuale.

KP (2023). *An Introduction to Crypto Wallets and How to Keep Them Secure*, in QuickNode.

LANZI, M. (2018). *Riciclaggio e reati nella gestione dei flussi di denaro sporco*, Giuffrè, Milano.

Legge n. 689/1981

Legge n. 48/2008

LEMME G. E PELUSO S. (2016). *Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, Rivista di Diritto Bancario, n. 11/2016

LEPRI B. , OLIVER N., LETOUZÉ E., PENTLAND A., VINCK P., (2017). *Fair, transparent and accountable algorithmic decision-making processes. The premise, the proposed solutions, and the open challenges*, in Philosophy & Technology 31(3) 4.

LESSIG L. (1999). *Code and Other Laws of Cyberspace*, BasicBooks

LEWENBERG Y., BACHRACH Y. & SOMPOLINSKY (2015). *Bitcoin Mining Pools: A Cooperative Game Theoretic Analysis*.

LI C., HE D., Li S., ZHU S., CHAN S. e CHENG Y. (2020). *Android-based cryptocurrency wallets: Attacks and countermeasures*

LICATA P. (2019). *L'Autorità bancaria europea chiede di valutare costi e benefici della finanza digitale: potrebbero rendersi necessarie norme a tutela dei*

consumatori e per scongiurare attività illecite e concorrenza sleale. Corriere comunicazioni

LIEVERSE K. (2016). *The Scope of MiFID II, in Regulation of the EU Financial Markets: MiFID II and MiFIR*, Oxford University Press

LINCH NETWORK (2022). *A vulnerability disclosed in Profanity, an Ethereum vanity address tool*.

Linee guida sulla tassazione dei cripto-asset nel Regno Unito 2019

LUCEV R., BONCOMPAGNI F. (2018). *Criptovalute e profili di rischio penale nella attività degli exchanger*, Giurisprudenza Penale, 2018

LUPÁRIA L.e ZICCARDI G. (2007). *Investigazione penale e tecnologia informatica*, Milano

LUPARIA L. (2009), Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (L. 18 marzo 2008, n. 48), Giuffrè, Milano.

LUPARIA L. (2011). *Computer crimes e procedimento penale*, in GARUTI G. (a cura di), *Modelli differenziati di accertamento*, diretto da G. Spangher, Utet, Torino.

MAIMERI F., MANCINI M. (2019). Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale, in Quaderni di Ricerca Giuridica della Consulenza Legale.

MAINIERI N. e DI GABRIELE N. (2022). *Utilizzi a scopi illeciti delle criptovalute: recenti profili giurisprudenziali e normativi italiani ed internazionali e riferimenti al mercato degli NFT* in Giurisprudenza Penale.

MANCINI C. (2012). *Riciclaggio e responsabilità degli enti. I modelli organizzativi.*

MANCINI M. (2015). *Valute virtuali e Bitcoin*. Analisi Giuridica dell'Economia, Fascicolo 1

MANZARI M. (2021). *I reati informatici e la Convenzione di Budapest*, in bptmavvocati.it

MARINELLO A. (2022). *Un "cripto-condono" e molti nodi irrisolti nel disegno di legge sulla disciplina fiscale delle valute virtuali* in Rivista Telematica di Diritto Tributario.

MARSALA P. (2020). *Criptovalute: cosa sono i wallet custodial e non-custodial.*

MARTINO P., BELLAVITIS C., DASILVA C. M. (2019),, *Blockchain and Initial Coin Offerings (ICOs): a new way of crowdfunding*, SSRN 7

MARTORANA M. e SICHI Z. (2022). *Transazioni in criptovalute: pubblicate le regole antiriciclaggio dell'Ocse* in ALTALEX.

MASI S. (2019). *V direttiva antiriciclaggio: obiettivi, ambito di riforma, modifiche* in Altalex.

MASSIMILIANO N. (2019). *Il regime giuridico delle ICOs. Analisi comparata e prospettive regolatorie italiane*, Diritto Bancario.

MATTASSOGLIO F. (2021). *Le proposte europee in tema di crypto-assets e DLT. Prime prove di regolazione del mondo crypto o tentativo di tokenizzazione del mercato finanziario (ignorando bitcoin)*, Rivista di Diritto Bancario.

MELLA L. (2021). *Bitcoin: tre minacce al portafoglio digitale e tre modi per proteggerlo*, in cibersecurity360.it.

MESSINA A. (2023). *Mondo crypto: i principali attacchi e minacce ai conti* in agendadigitale.eu.

MINELLA M. (2021). *Criptovalute: perché il 2022 sarà l'anno dei regulators*. Il sole24ore.

MINISTERO DELL'INTERNO (2020). *Convenzione di Palermo: venti anni di lotta alla criminalità internazionale*.

MOLONEY N. (2014) *EU Securities and Financial Markets Regulation*, 3rd ed., Oxford European Union Law Library.

MORGANTINI F. (2023). *Cosa accadrà alla blockchain: prospettive e osservazioni sul futuro delle criptovalute*, in Forbes.

MORNINGSTAR (2022). *5 grafici sul passato, presente e futuro delle criptovalute*.

MORONI P. (2021). *L'inquadramento normativo della moneta virtuale*.

MOSAKOVA E.A. (2002). *National cryptocurrency as Venezuela's economic development factor in the 21st century*, Iberoamérica. no. 1.

MOSCARINI P. (2014). *Principi delle prove penal*i, Torino.

NADDEO M. (2016). *Autoriciclaggio: i compromessi di un difficile inquadramento sistematico*, in *Riv. trim. dir. pen. ec*., n. 3-4

NADDEO M. (2022). *Criptovalute: profili di rilevanza penale* in Penale diritto e procedura.

NAKAMOTO S. (1991). *The original Bitcoin source code*.

NAKAMOTO S. (2008). *Bitcoin: a peer-to-peer electronic cash system*.

NAMIRIAL 82021). Blockchain e GDPR. Tutela dei dati ed opportunità.

NAQVI S. (2018). *Challenges of Cryptocurrencies Forensics – A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals in ARES, Proceedings of the 13th International Conference on Availability, Reliability and Securit, Hamburg, Germany*, New York, NY, USA.

NARULA, N. (2016). *Il futuro del denaro*, Paper presentato alla conferenza internazionale TEDx di Parigi.

NAZIONALE (2022). *L'ecosistema delle criptovalute può trarre vantaggio dagli interessi di Wall Street?* Altarimini.it.

NEILSON D., HARA S., MITCHELL I. (2016). Bitcoin Forensics: A Tutorial, in JAHANKHANI H., (2017) in *Global Security, Safety and Sustainability - The Security Challenges of the Connected World*, in Communications in Computer and Information Science.

NERLI F. (2022). *Sistema Blockchain e G.D.P.R., criticità e possibili soluzioni* in affidaty.io.

NEWBURY L. B., KERSE M. (2023). *Crypto Consumer Protection: Why 'Wait and See' Is No Longer an Option* in cgap.org.

NIGRO R. (2022). *Criptovalute e antiriciclaggio, vicini ad una svolta?* In ALTALEX.

O'NEAL S. (2020). *As Malta Delays Regulatory Clarity, Fewer Firms Remain on 'Blockchain Island*, Cointelegraph

OSSERVATORIO MOBILE PAYMENT & COMMERCE (2014). *Mobile Wallet War: chi vincerà la sfida?* Milano: Osservatori ICT & Management - School of Management del Politecnico di Milano.

PACTE law n° 2019-486 del 22 maggio 2019.

PAGLIARI E. (2018). *10 anni di Bitcoin: le principali tappe della storia del re delle criptovalute*, informazione.it.

PASCUAL J. L. (2021). *Cos'è un BrainWallet?* in academy.bit2me.com.

PAYTM (2023). *Different Types of Digital Wallets – A Comprehensive Guide!*

PELLIZZARI T. E MORINI M. (2017). *Il boom di Bitcoin non è per tutti*. Il Sole24Ore.

PEPE E. (2023). *Il Governo italiano dà via libera all'emissione di azioni e obbligazioni tokenizzate* in COINTELEGRAPH.

PESCOSOLIDO J. (2021). *Criptovalute – Tassazione ed obblighi di monitoraggio fiscale (RW)*, Fisco e Tasse.

PGIM (2022). *L'investimento in criptovalute*.

PHILIP J., T., e PARBAT K. (2010). *BlackBerry to open code for security check*

PICOTTI L. (2011). *Sicurezza, informatica e diritto penale*, BUP, Bologna

PICCOTTI L. (2018). *Profili penali del Cyberlaundering: le nuove tecniche di riciclaggio*, Rivista Trimestrale Diritto Penale Economico, n. 3-4.

PILKINGTON M. (2015). *Blockchain Technology: Principles and Applications*), in Research Handbook on Digital Transformations,, Edward Elgar Publishing

PITTIRUTI M., (2017). *Digital evidence e procedimento penale* in Processo penale e politica criminale, a cura di PAOLOZZI G., - MOCCIA S., - MARAFIOTI L., - LUPARIA L., - MARCHETTI P., Torino.

POLCI M. (2013). *Cos'è il bitcoin –seconda parte*, rischiocalcolato.it.

POLITECNICO MILANO1863, SCHOOL OF MANAGEMENT IN COLLABORAZIONE CON OSSERVATORI.NET (2020). *Crypto Asset Digital finance, cybersecurity e crypto assets: strategia, normative e evoluzioni dello scenario*.

PONTICELLI d. (2023). *Crypto-asset: approvato il Mica. Ecco il nuovo quadro normativo*, in we-wealth.com.

PREVITI L. (2020). *Silk Road: storia del famoso mercato della droga*, in cyberdude.it

Proposta di regolamento COM(2020) 594

PUTHAL D., MALIK N., MOHANTY S., KOUGIANOS E., DAS G. (2018). *Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems*, in IEEE Consumer Electronics Magazine, Vol. 7, Issue 4.

QUATTROCCHIO M. L. (2019) *MiFID II e MiFIR. Il quadro europeo di riferimento*.

RASERA S. (2021). *Stablecoin: percezione, elusione e modellizzazione della volatilità*, per Università Ca' Foscari

REDAZIONE (2020). *Cosa sono i Crypto Asset?* The Liquid Journal.

REDAZIONE (2021). *Asset nativi digitali e soluzioni FinTech*. IVG.it.

REDAZIONE (2021). *Criptovalute, in arrivo in Italia il decreto frodi e falsificazioni di mezzi di pagamento.* Bluerating.

REDAZIONE (2022). *Blockchain e GDPR: riflessioni su alcuni elementi di contrasto* in Iusinitinere.it.

REDAZIONE (2022). *Criptovalute, regolamentazione europea: pregi e criticità*. Blue Rating.

REDAZIONE ANSA (2022). *Consob, oltre 10.300 criptovalute, criticità sulla sicurezza*.

REDAZIONE CONFINELIVE (2023). *Criptovalute: quale futuro per gli investimenti nelle monete digitali?* in ConfineLive.

REDAZIONE OSSERVATORI DIGITAL INNOVATION (2020). *Cosa sono le ICO (Initial Coin Offering) e come funzionano realmente* in Osservatori.net digital innovation.

REDAZIONE RHC (2023). *La Blockchain Analysis in chiave cyber-resilienza tra le nuove proposte dell'ACN targata Frattasi*.

Regolamento (UE) 2012/648

Regolamento (UE) 2014/596

Regolamento (UE) 2014/600

Regolamento 2014/909 (CSDR)

Regolamento (UE) 2015/847

Regolamento (UE) 2016/679

Regolamento (UE) 2017/1001

Regolamento (UE) 2017/1129

REZAEIGHALEH H. (2020). *Improving security of crypto wallets in blockchain technologies.*

RINGE W., ROUF C., (2020) *The DLT Pilot Regime: An EU Sandbox, at Last!*, Oxford Business Law Blog

RIOSA D. (2022). Criptovalute, Mossa sottolinea l'importanza dei wallet.

Risoluzione N. 72/E del 2 settembre 2016

RIZZI F. (2022). *Cosa sono i portafogli di criptovalute: hot wallet vs cold wallet* in Rankia.

ROSATO A. (2021). *Profili penali delle criptovalute* in Quaderni di C.R.S.T., Centro Ricerca Sicurezza e Terrorismo.

RUGGIERI F. e PICOTTI L. (2011), *Caratteristiche della prova digitale*, *Nuove tendenze della giustizia penale di fronte alla criminalità informatica: aspetti sostanziali e processuali*, Giappichelli, Torino.

RUSS B. A. (2022). *The Benefits and Risks of a Digital Wallet* in idstrong.com.

RYAN P. Y. A. (2019). *Are Blockchain Voting Technologies Safe?*

SAI A. R., BUCKLEY J. e GEAR A. L. (2019). *Privacy and security analysis of cryptocurrency mobile applications*, Fifth Conference on Mobile and Secure Services.

SALAMONE G. (2022). *Wallet e sicurezza informatica* in dgroove.it.

SALVADORI I. (2017). *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software"*, in Riv.it. di dir. proc. pen., 2/2017

SARDAR M. (2017). *Digital Currency: Taxation, Enforcement, and the John Doe Summons*. The Cpa Journal.

SATER S. (2017). *Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows*

SHETEWY N., AIT, L. J., e LI, J.-J. (2019). *Challenges of the Bitcoin in the Arabic Countries*

SHIN L., (2016). *Republic Of Georgia To Pilot Land Titling On Blockchain With Economist Hernando De Soto*, BitFury, Forbes.

SIGNORATO S. (2016). *Types and features of cyber investigations in a globalized world*. Relazione alla Conferenza biennale internazionale e Diritto penale contemporaneo

SLOPE FINANCE (2022). *Slope Wallet Sentry Vulnerability — Digital Forensics and Incident Response Report*.

SMART CARD ALLIANCE (2007). *Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure*.

SOFTWARE ANTIRICICLAGGIO (2019). *Antiriciclaggio, prestatore di servizi di portafoglio digitale e valuta virtuale*.

SOLDAVINI, P. (2016). *Il futuro della finanza in una BlockChain* in Il sole 24 ore.

STEFANI A. (2022). *Euro digitale: presentazione, tempi e prospettive dell'opera della BCE. Pagamenti digitali*.

STEFANIN G. E ZANIN M. (2013). *La Direttiva 2011/61/UE sui gestori di fondi di investimento alternativi: le discipline dei conflitti di interesse e degli obblighi di trasparenza* in DB non dolo diritto bancario.

STIEFMUELLER C.M. (2021). *One born every minute: Striking the balance between promoting innovation and protecting citizens. An analysis of the EU Digital Finance Package.*

STRICKLAND B. (2019). *Crypto Taxes in the United Kingdom*, TokenTax

STURZO L. (2018). *Bitcoin e riciclaggio 2.0*, in *Riv. trim. dir. pen. cont.*, n. 5-2018

SURATKAR S., SHIROLE M. e BHIRUD S. (2020). *Cryptocurrency wallet: A review*.

SVENSSON P. (2007). *Comcast Blocks Some Internet Traffic, NBC News*

SWAN M. (2015). *Blockchain. Blueprint for a New Economy*, O'Reilly, 17.

TAGLIAMONTE I. (2021). *Tecnologia blockchain e mercati dei crypto-asset: le opportunità.* L'Eurispes.it.

TESONE C. (2022). *Wallet digitale per criptovalute* in Fiscomania.com.

TETI A. (2013). *Bitcoin: la criptomoneta del cyberspazio che sfida banche e governi*, Rivista Mondo digitale, n.46

Trattato sul funzionamento dell'Unione europea (2009).

TUMIETTO D. (2023). *Cripto-attività, ecco il regolamento Mica: le nuove regole da conoscere*, in Agendadigitale.eu.

UBS (2022). *Che cosa sono gli asset digitali?* inUBS.com.

UIF, BANCA D'ITALIA (2021). *Rapporto Annuale 2020 Unità di Informazione Finanziaria per l'Italia.*

UNGARETTI F. (2018). *La V Direttiva Antiriciclaggio* in Giurisprudenza penale Web, 2018, 7-8 – ISSN 2499-846X

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II ET AL. (2020). *Reasearch project – L'ecosistema italiano della blockchain.*

VADALÀ R. M. (2020). *La disciplina penale degli usi e degli abusi delle valute virtuali*, in *Diritto e internet*, n. 3/2020

VEDANA F. (2022). *Criptovalute col registro entro il 2 giugno* in ItaliaOggi.

VALDANI E., BERTOLI G. (2006). *Mercati internazionali e marketing.* 3° edizione, Milano: Egea

VAN DER HORST L.,CHOO K.K. e LE-KHAC N.-A. (2017). *Process memory investigation of the bitcoin clients electrum and bitcoin core*, IEEE Access, vol. 5

VENTORUZZO M., MOCK S. (2017). *Market Abuse Regulation – Commentary and Annotated Guide*, Oxford University Press.

VERGINE S., BORTOLOTTI A. (2021). *Bitcoin, il futuro in blocchi*, in Economia Comportamentale.

VIGNA P., CASEY J., (2015). *The age of Cryptocurrency: How Bitcoin and digital money are challenging the global economic order*, New York, St. Martin's Press.

VOLLSTÄDT E. (2015). *Totalitarian Cyber State vs Freedom Unbound: Interview with Fabricio & Susanne* Part 2, on Bitnation-blog.com.

VOSHMGIR S. (2019). *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy*, BlockchainHub Berlin.

WERBACH K. (2018), *The Blockchain and the New Architecture of Trust*, MIT Press

WORLDLINE (2022). *Cosa sono i wallet e perché entreranno nel tuo portafoglio elettronico*.

WRIGHT A., DE FILIPPI P., (2015). *Decentralized Blockchain Technology and The Rise of Lex Cryptographia.*

ZAMBON A. (2021). *Blockchain: introduzione e casi d'uso.*

ZAGHLOUL E., LI T., MUTKA M. W. e REN J. (2020). *Bitcoin and blockchain: Security and privacy*, IEEE Internet of Things Journal, vol. 7, no. 10

ZAPPONINI G. (2021). *Cosa sono l'AML e il CFT: le sfide per le aziende dal riciclaggio al terrorismo* in Innolva.

ZETZSCHE D. A., ANNUNZIATA F., ARNER D. W., ROSS R. P., (2020). *The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy*,

European Banking Institute Working Paper Series No. 2020/77, University of Luxembourg Law Working Paper Series No. 2020, 2.

ZOLLNER S., CHOO K. K., e LE-KHAC L. L. (2019). A*n automated live forensic and postmortem analysis tool for bitcoin on windows systems*, IEEE Access, vol. 7.