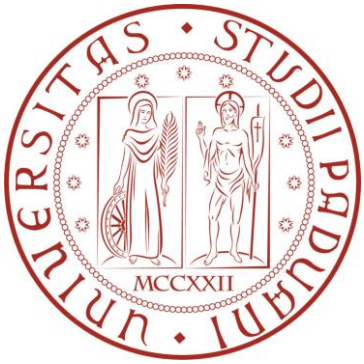

UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea in Diritto e Tecnologia

“Criptovalute e *cybericiclaggio*. Tecniche, normativa e contrasto internazionale”

Relatore:
Chiar.mo prof. Riccardo Borsari

Laureando:
Sebastiano Teani
Matricola 2040119

a.a. 2022/2023

INDICE

INTRODUZIONE

Il presente lavoro intende approfondire la tematica del c.d. *cybericiclaggio*, ossia il fenomeno che ricomprende tutte le pratiche di riciclaggio commesse tramite criptovalute, per giungere, in conclusione, ad un breve accenno alle diverse e complicate problematiche che queste tecniche introducono nel panorama giuridico nazionale ed internazionale. Si mostrerà come le difficoltà che sorgono nell'arginare il fenomeno siano molteplici, da un lato operative, per chi conduce le indagini, dall'altro giuridiche, in cui si imbattono sia gli inquirenti che il legislatore, in quanto devono essere introdotte nell'ordinamento norme *ad hoc* atte a prevenire e perseguire il reato. Il percorso delineato nella stesura dell'elaborato muove dagli elementi tecnici alla base delle criptovalute, dalla *blockchain* ai *wallet*, dal protocollo informatico che ne rappresenta l'architettura al funzionamento delle transazioni in criptovalute, passando per il tema dell'anonimato e dello pseudoanonimato in rete, sino a giungere al quadro normativo attuale per arginare il fenomeno sia a livello nazionale che comunitario ed internazionale.

L'argomento trattato è molto più ampio dello spazio a disposizione in questa sede, tuttavia, la finalità di questo lavoro è quella di introdurre questi argomenti in modo chiaro e comprensibile anche al lettore che non ha familiarità con le terminologie e i concetti trattati. L'obiettivo è affrontare l'argomento con un approccio tecnico e pragmatico, spendibile e utile sia da un punto di vista professionale che civico. Si è consapevoli, come gran parte della dottrina, che le criticità legate al *cybericiclaggio* siano ad oggi sconosciute a molti professionisti, sia giuristi che informatici, i quali ci si auspica che collaborino per adeguare la normativa e le tecniche investigative atte a contrastare queste pratiche.

CAPITOLO I
IL PROTOCOLLO BITCOIN

1. Storia e nascita delle criptovalute

I bitcoin sono stati la prima criptovaluta (dall'inglese *cryptocurrency*) ad essere creata e resa accessibile al grande pubblico. Nati da un misterioso ideatore, tutt'ora anonimo e conosciuto con lo pseudonimo Satoshi Nakamoto, furono annunciati al mondo nel 2008 con la pubblicazione del "*white paper*"[1], vero e proprio manifesto e manuale d'uso con cui avvenne il lancio di questa nuova valuta destinata ad avere enorme successo. A distanza di 15 anni dalla loro introduzione, si può dire che i bitcoin abbiano attraversato diverse fasi: se per i primi anni furono un prodotto di nicchia, successivamente la platea di utilizzatori si ampliò trasformandoli in un fenomeno globale, legato soprattutto ad attività di investimento finanziario[2].

La tecnologia Bitcoin nasce da una serie di precedenti esperimenti volti alla creazione di una moneta digitale anonima, spesso fallimentari, che hanno apportato significativi contributi dal punto di vista tecnico grazie ai quali è stato possibile arrivare alla nascita di Bitcoin[3]. Il processo è frutto dell'impegno collettivo della comunità di attivisti *cypherpunk,* un gruppo eterogeneo e globale di informatici, matematici, appassionati delle nuove

---

[1] Il testo di S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System,Comunemente chiamato White Paper, disponibile al link https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf

[2] Cfr. J.C. Gerlach – G. Demos – D. Sornette, Dissection of Bitcoin's multiscale bubble history from January 2012 to February 2018, The Royal Society Open Science, 2019, disponibile al link: https://royalsocietypublishing.org/doi/abs/10.1098/rsos.180643

[3] G. J. Sicignano, nel suo volume *Bitcoin e riciclaggio*, dedica il primo capitolo a ricostruire la storia dei sistemi precedentemente sviluppati dal movimento *cypherpunk* per implementare e garantire la privacy degli utilizzatori della rete: "Nel corso degli anni nella community dei *cypherpunk* sono stati presentati molti progetti. Alcuni di questi sono alla base di *bitcoin*. Anzi, *bitcoin* rappresenta niente altro che una perfetta combinazione di alcuni di questi lavori. Uno dei primi progetti elaborati dal movimento è l'*"Anonymous remailer*" ovvero un programma che permette di nascondere il nominativo del mittente di una email […]. Un'altra idea elaborata dal movimento è *BlackNet*, ovvero un sistema che permette l'acquisto, la vendita , e la negoziazione di ogni informazione in totale anonimato. Secondo i suoi creatori, *BlackNet* era interessato principalmente a trattare informazioni inerenti i segreti commerciali, le nanotecnologie, la produzione chimica, la droga e i nuovi piani di prodotto […] Secondo il programma originario, i vari acquisti possono essere effettuati con due modalità: o con valuta corrente, e in questo caso *BlackNet* effettua un deposito anonimo sul conto corrente bancario dell'interessato, o mediante "*CryptoCredits*", ovvero la valuta digitale interna di *BlackNet*." (G.J. Sicignano, *Bitcoin e riciclaggio,* Giappichelli Editore, Torino, 2019, pp. 11 e *ss.)*
Dopo questi primissimi esperimenti ad inizio anni '90 ne seguirono diversi che mano a mano introdussero elementi utili alla futura nascita do Bitcoin, come ad esempio la *Proof-of-work* di cui si parlerà nei prossimi paragrafi, attraverso diversi progetti sviluppati ed abbandonati nel corso di pochi anni: *ECash,* Hash*Cash, B-Money, Bit Gold.*

tecnologie, molto spesso provenienti da contesti accademici che sin dagli anni '90 hanno collaborato per realizzare *software open source* con particolare attenzione al rispetto della privacy[4] dell'utente[5]. Nel manifesto del movimento *cypherpunk* firmato da Eric Hughes nel 1993 è possibile rintracciare alcuni dei capisaldi della filosofia del movimento, tra cui spicca la centralità del concetto di privacy:

> *La privacy è necessaria per una società aperta nell'era elettronica. La privacy non è segretezza. Una questione privata è qualcosa che non si vuole che il mondo intero sappia mentre, una questione segreta, è qualcosa che si vuole che nessuno sappia. La privacy è il potere di rivelarsi selettivamente al mondo. […] Dobbiamo difendere la nostra privacy se vogliamo averla. Dobbiamo unirci e creare sistemi che consentano l'esecuzione di transazioni anonime. […] Noi Cypherpunk ci dedichiamo alla costruzione di sistemi anonimi. Difendiamo la nostra privacy con la crittografia, con sistemi di inoltro di posta anonimi, con firme digitali e con moneta elettronica*[6].

Nakamoto, sviluppando la prima criptovaluta, ideò un sistema in cui la tutela della privacy degli utilizzatori era il cardine attorno a cui ruotava

---

[4] "L'odierno utilizzo, nel diritto dell'Unione Europea, del termine privacy nella sua duplice accezione di diritto al rispetto della vita privata e di diritto alla protezione dei dati personali, è frutto di un lungo processo di evoluzione concettuale, che è dipeso in massima parte dall'emersione della società dell'informazione, e che ha avuto origine nell'ordinamento giuridico internazionale. Nello specifico, il termine privacy è stato coniato nel 1890 da due giuristi americani, Warren e Brandeis, che gli hanno dedicato un saggio, intitolato "right to privacy", traducibile con la formula "diritto al rispetto della vita privata" […] Tale diritto è stato inizialmente inteso solo in chiave negativa, cioè come obbligo rivolto alle autorità pubblice di non interferire nella sfera privata dei propri cittadini ("right to be alone", dalla celebre definizione della Corte Suprema degli Stati Uniti d'America […]
L'art.8, par.1 CEDU ("ogni persona ha diritto al rispetto della sua vita provata e familiare, del suo domicilio e della sua corrispndenza", *ndr*) fa della CEDU la prima fonte giuridica a riconoscere il diritto al rispetto della vita privata anche nella sua accezione positiva, che , come precisato dalla giurisprudenza della Corte EDU (C. Eur. Dir. Uomo*, Marckx c. Belgio*, 13 giugno 1979), garantisce al singolo il diritto di formarsi liberamente una propria sfera privata, in cui sviluppare la propria identità. Inoltre, tale disposizione rappresenta la cornice teorica entro cui si è sviluppata un'ulteriore dimensione contenutistica del concetto di privacy. Infatti, in concomitanza con la diffusione di quello che si è indicato come il paradigma tecnologico di fondo della società dell'informazione, ovvero l'elaborazione automatizzata delle informazioni sotto forma di dati, si è riconosciuta la necessità di accordare al singolo una forma di controllo sulla circolazione di quelle informazioni-dati che contribuivano a formare tale sfera privata." F. Rossi Dal Pozzo, *Il mercato unicio digitale europeo e il Regolamento UE sulla privacy* in Il diritto dell'Amministrazione Pubblica digitale, a cura di R. Cavallo Perin e D. Galetta, Giappichelli Editore, Torino, 2020, pp. 49-50

[5] G.J. Sicignano, *Bitcoin e riciclaggio,* Giappichelli Editore, Torino, 2019, pp. 11 e *ss.*

[6] Disponibile in inglese al link https://www.activism.net/cypherpunk/manifesto.html, la citazione in italiano è tratta da https://www.coinpostitalia.it/il-manifesto-cypherpunk/.

l'intero protocollo. Egli ricercò, ed ottenne, all'interno del sistema Bitcoin un sistema fortemente incentrato sull'anonimato dell'utente - o meglio lo pseudoanonimato, come si vedrà in seguito[7] - grazie alla crittografia. La grande rivoluzione apportata da Bitcoin non si limitò tuttavia alla tutela della privacy ma stravolse completamente la concezione di transazione di denaro. Se, fino a quel momento, non era concepibile una movimentazione di moneta elettronica senza l'approvazione di un istituto bancario, dal 2008 si concretizzò la possibilità di inviare e ricevere denaro senza l'autorizzazione di un sistema bancario ufficiale. Grazie alla struttura decentralizzata e distribuita della tecnologia *blockchain*, venne meno la necessità della figura del garante centrale, dotato di poteri speciali in merito alla gestione di tutte le transazioni. Era questo, invero, il ruolo storicamente detenuto dalle banche e dagli enti statali, soggetti accusati dal movimento *cypherpunk* di esercitare la sorveglianza verso i cittadini[8].

Il sistema Bitcoin aspirava a diventare il modello globale per le transazioni ed i pagamenti online di beni e servizi, come auspicato nel White Paper, permettendo così alle persone di compiere pagamenti in modo decentralizzato, anonimo e irreversibile,[9] tuttavia, l'ambizioso obiettivo venne raggiunto solo parzialmente. Infatti, l'esplosione del fenomeno Bitcoin a livello globale fece aumentare progressivamente il valore delle monete virtuali, rendendole appetibili come strumenti finanziari di investimento e, quindi, di speculazione. È proprio questa oggigiorno la funzione maggiormente assolta dalle criptovalute, diffusasi, in particolare, grazie ai vertiginosi guadagni incassati dai primissimi possessori di bitcoin.[10]

Nel giro di pochissimi anni il valore dei *btc* (abbreviazione convenzionalmente accettata di bitcoin) passò da poche decine di euro a molte migliaia, fino ad arrivare nel novembre 2021 al suo picco storico con un

[7] Si veda pag. 5.
[8] Cfr. https://www.activism.net/cypherpunk/manifesto.html, Per approfondire il tema della sorveglianza si rimanda a S. Zuboff, P. Bassotti, *Il capitalismo della sorveglianza : il futuro dell'umanità nell'era dei nuovi poteri.* Luiss University press, 2019.
[9] G.J. Sicignano, Bitcoin e riciclaggio*, op. cit*. pp. 50-51.
[10] Principalmente appartenenti alla comunità *cypherpunk* ma anche investitori entusiasmati dalla novità del momento, cfr. G.J. Sicignano, Bitcoin e riciclaggio*, op. cit*. pp. 23 e *ss*.

valore di € 57.70411[12]. I bitcoin attualmente in circolazione sono più di 19 milioni[13] e di questi non si può sapere con precisione quanti vengano adoperati come strumenti di pagamento e quanti come strumento finanziario. Ad ogni modo, ai soli fini del presente lavoro, verrà analizzata unicamente la loro funzione di moneta in senso stretto, quale mezzo di pagamento e di scambio[14].

2. Il protocollo Bitcoin

Prima di approfondire il funzionamento del protocollo, appare doveroso precisare la differenza che intercorre tra 'Bitcoin' con la B maiuscola e 'bitcoin'. I due termini, infatti, indicano due concetti distinti: il primo rappresenta "un protocollo informatico di comunicazione, ossia l'algoritmo che ne è alla base e il fenomeno mondiale che da esso si è sviluppato. Il secondo […] identifica invece una 'moneta', cioè uno strumento finanziario utilizzato per compiere una serie di particolari forme di transazioni online"[15].

In ambito informatico con il termine protocollo si intende un gruppo di regole, accettate da tutti gli utilizzatori di una certa tecnologia, che consentono la condivisione dei dati all'interno della rete[16]. Nel caso delle criptovalute il protocollo determina la struttura della *blockchain*[17] e di come essa possa essere ampliata, integrata e modificata. Bitcoin, dunque, è un protocollo che regola la *blockchain* e di conseguenza fornisce le informazioni utili alla creazione e al funzionamento delle monete virtuali, nonché delle movimentazioni e del possesso delle stesse.

Le caratteristiche principali[18] della valuta virtuale derivante dal protocollo Bitcoin sono:

---

[12] Fonte: https://coinmarketcap.com/it/currencies/bitcoin/historical-data/.
[13] Corrispondenti al 91% del totale: è stato infatti fissato a 21 milioni il numero massimo di monete che verranno emesse dal sistema, come pronosticato dallo stesso Nakamoto nel White Paper.
[14] Ci si soffermerà sui bitcoin, a discapito di altre monete, in quanto essi rappresentano l'archetipo di tutte le valute digitali in circolazione, il cui numero ad oggi è di 21.502 (Numero aggiornato al 25/10/2022, fonte: https://coinmarketcap.com/it/). Tutte le monete diverse dai bitcoin sono denominate *altcoin*, abbreviazione di *alternative coin.*
[15] F. Pascucci La natura giuridica dei bitcoin, In P. Dal Checco et al., Bitcoin Forensics e Intelligence sulla Blockchain, ed IISFA Educational, Roma, 2019, p. 17.
[16] Cfr. https://it.wikipedia.org/wiki/Protocollo_di_comunicazione.
[17] Si veda par.1.2.2 del presente lavoro, *"L'immutabilità della blockchain"*
[18] Cfr. C. Zeno, *BITCOIN: "La moneta virtuale: il trade off tra mezzo di scambio e asset finanziario",* LUISS, 2018, pp. 4 e *ss.*

- dematerializzazione – i bitcoin, come tutte le criptovalute, esistono solo digitalmente, sotto forma di informazioni condivise tra i computer partecipanti alla rete ed organizzate secondo il protocollo prestabilito da Nakamoto;
- decentralizzazione – è possibile eseguire transazioni in criptovalute senza richiedere l'autorizzazione di alcun istituto bancario, o di altra natura, infatti sono gli utenti stessi della rete che ne accertano la validità;
- trasparenza – tutte le transazioni approvate dalla rete vengono inserite nella *blockchain*, un registro condiviso in cui è tenuta traccia di ogni transazione avvenuta dalla nascita della criptovaluta, una sorta di libro contabile online;
- irreversibilità – una volta che le transazioni vengono inserite nella *blockchain* non c'è possibilità di annullarle grazie ad un sistema basato sulla crittografia che ne presidia l'immutabilità;
- pseudoanonimato – Le transazioni sono operate dagli utenti tramite dei *wallet*, portafogli digitali, associati a dei codici alfanumerici. Pur essendo la *blockchain* completamente trasparente, sul registro non sono riportati i nomi delle persone fisiche che compiono le operazioni ma solo i codici identificativi dei *wallet*;
- economicità e velocità – L'assenza di istituzioni intermediare che validano le transazioni comporta che il loro ruolo venga svolto da particolari utenti attraverso un processo chiamato *mining*[19]. Il *miner*, per il proprio operato, riceve sia un premio in

[19] "Minare" significa creare un blocco, ossia un elenco di transazioni e validarle, affinché possano essere inscritte nella blockchain e riconosciute come valide da tutti i nodi. Il mining si fonda sul meccanismo della *cd. Proof-of-work*, o PoW, un algoritmo di consenso, attraverso il quale la rete richiede un lavoro al nodo che vuole portare a termine l'operazione, la cui corretta realizzazione verrà poi verificata dalla rete. Il lavoro richiesto consiste nell'esecuzione di complesse operazioni di calcolo, definire questo meccanismo è rappresentabile come una sorta di gara a tempo, in cui vince il primo nodo che riesce a generare un output particolare tramite la funzione di Hash, rispondendo alle richieste fornite dal protocollo stesso.
Per vincere la sfida è necessario condividere a tutta la rete la cd. *Proof-of-work*, prova di lavoro, per ottenerla i *miner* si cimentano in una particolare procedura:
Innanzitutto, va formato il blocco, per farlo il *miner* deve raccogliere un numero prestabilito di transazioni inserite nella lista d'attesa della blockchain, verificando che ognuna risponda ai requisiti formali necessari. Dopo aver redatto l'elenco, esso va "impaginato" nel blocco, inserendo nell'intestazione le informazioni richieste dal protocollo (ad es. numero del blocco, data e ora ecc.). Una volta confezionato l'elenco inizia la vera sfida crittografica: il *miner* deve aggiungere a questa stringa di informazioni un elemento casuale

criptovalute[20] dal protocollo stesso che una piccola commissione a carico dall'utente che vuole inviare cripto. Quest'ultima, tuttavia, è molto bassa grazie alla remunerazione da parte del sistema stesso. Inoltre, il tempo medio stimato per ottenere l'approvazione della propria transazione è di dieci minuti, garantendo una riscontrabilità quasi immediata della validazione della transazione;

- informalità – Non essendo riconosciute da quasi nessuno stato[21] le valute virtuali possono essere accettate come forma di pagamento solo su base volontaria, inoltre da ciò deriva che, contrariamente alle valute emessa dalle banche centrali che costituiscono un credito del possessore a fronte di un debito dell'istituto, i bitcoin sono un credito a cui non corrisponde nessun debito. Questa peculiarità le rende simili all'oro, ossia posseggono un valore solo nel momento in cui ci sia qualcuno interessato a comprarle[22];
- Offerta predeterminata – ogni protocollo definisce quale sarà la quantità di criptovaluta emessa, per Bitcoin la cifra è di 21 milioni, uno stratagemma studiato per tutelare le valute virtuali dal fenomeno dell'inflazione.

(detto *nonce*) e ad esso applicare la funzione di Hash. La difficoltà consiste nel cercare di ottenere un valore di Hash tale da soddisfare i requisiti di volta in volta stabiliti dal protocollo.
È la natura stessa della funzione di Hash a stabilire che siano necessari numerosissimi tentativi per ottenere l'output con le caratteristiche desiderate (solitamente la sfida richiede che il valore si apra con un numero n di "0"), e ad ogni tentativo viene modificato il *nonce*.
Ogni utente della rete può provare a minare un blocco tramite appositi software disponibili in rete, tuttavia, nel registro verrà iscritto solo il blocco presentato dal nodo che deposita per primo la "prova di lavoro". Questo nodo, detto *miner*, è l'unico autorizzato ad aggiungere il proprio blocco nella blockchain, al quale verranno immediatamente agganciati i successivi.
Per approfondire si veda la nota 20

[20] Il *miner* che riesce per primo a risolvere la sfida crittografica e dunque a chiudere il blocco, ha diritto ad un premio in bitcoin, come riconoscimento per aver contribuito al funzionamento ed all'immutabilità del registro. L'ammontare del premio è variabile e progressivamente decrescente, secondo uno schema prestabilito da Nakamoto, andandosi a dimezzare ciclicamente finché la somma rilasciata diventerà così piccola che si potrà considerare nulla.
Il sistema è dunque strutturato per emettere in totale 21 milioni di bitcoin, il cui valore è stabilito interamente dal mercato, non essendo associato ad alcun ente statale o governativo.

[21] L'unico stato al mondo ad aver accettato il bitcoin come corso legale è El Salvador, cfr. I. De Cubellis, (A.A. 2021/2022) *Bitcoin come moneta a corso legale: il caso El Salvador.* Tesi di Laurea in Economia dei mercati e degli intermediari finanziari, Luiss, Guido Carli, relatore Francesco Cerri, pp. 43 e *ss*.

[22] Proprio per questa loro caratteristica i Bitcoin vengono definiti "oro digitale", cfr. N. Passarelli, *Bitcoin e antiriciclaggio* in https://www.sicurezzanazionale.gov.it, pag. 2.

Di questi elementi strutturali, ai fini dell'analisi dell'utilizzo illecito delle criptovalute, è utile approfondire come si realizzano decentralizzazione e pseudoanonimato in Bitcoin, rimandando ad altre fonti per una trattazione esaustiva dell'intero argomento[23].

3. La decentralizzazione

La chiave di volta di Bitcoin è la *blockchain,* una particolare struttura dati che prende il nome dalla forma che assume lo schema secondo cui vengono archiviate le informazioni che la compongono, chiamata appunto "catena di blocchi"[24]. Prima di poter definire questa tecnologia è necessario introdurre la distinzione tra sistemi informatici centralizzati e distribuiti. I primi sono definibili tali

> *"quando i dati e le applicazioni risiedono in un unico nodo elaborativo. Viceversa, si parla di sistema informatico distribuito quando almeno una delle seguenti due condizioni è verificata:*
> *• le applicazioni, fra loro cooperanti, risiedono su più nodi elaborativi (elaborazione distribuita);*
> *• il patrimonio informativo, unitario, è ospitato su più nodi elaborativi (base di dati distribuita).*
> *In termini generali, quindi, un sistema distribuito è costituito da un insieme di applicazioni logicamente indipendenti che collaborano per il perseguimento di obiettivi comuni attraverso una infrastruttura di comunicazione hardware e software"*[25].

I sistemi distribuiti si suddividono a loro volta in due modelli, *client-server* e *peer-to-peer,* abbreviato in P2P (letteralmente "da-pari-a-pari"). Il modello *client-server*, tipico della maggior parte delle piattaforme diffuse nel web, è impostato su di una struttura gerarchica in cui gli utenti-client possono solo inoltrare richieste di accedere alle informazioni, detenute e fornite dall'utente-server, previa un'autorizzazione dello stesso. Al contrario, una rete informatica può essere definita P2P quando è caratterizzata da

[23] Per una trattazione approfondita dal punto di vista informatico si rimanda a A.M. Antonopoulos, *Mastering Bitcoin : Programming the Open Blockchain,* Oreilly & Associates Inc, 2017.
[24] Cfr. J.J. Bambara-P.R. Allen, *Blockchain. A Practical Guide to Developing Business, Law, and Technology Solutions*, McGraw-Hill Education, New York, 2018, cap. 1.
[25] C. Batini, B. Pernici, G. Santucci (a cura di), *Sistemi Informativi – Volume 5*. Franco Angeli, 2001, p.1 *e ss.*

un'architettura logica in cui i nodi (termine con cui si indica qualsiasi dispositivo hardware in grado di comunicare con gli altri dispositivi che fanno parte della rete), sono equivalenti, ossia dotati degli stessi poteri.

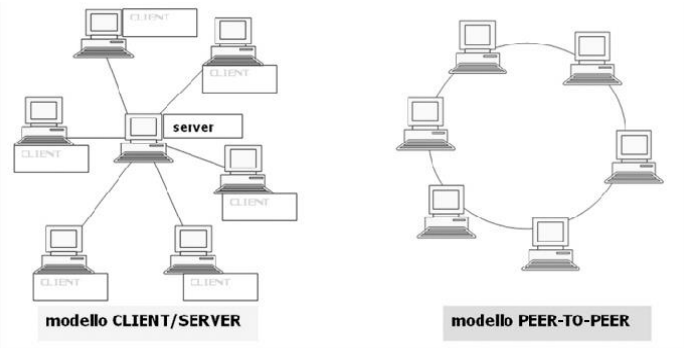

Figura 1: Una rappresentazione schematica dei due diversi modelli di architettura di rete. (fonte: F. Cantone, Shared Technologies in archeologia: nuove prospettive di gestione e condivisione di dati in rete)

La *blockchain* è dunque una tecnologia P2P, progettata come una struttura dati condivisa ed immutabile, consistente in un registro digitale le cui voci anziché essere strutturate all'interno di un unico lungo elenco sono raggruppate in "blocchi", i quali vengono concatenati uno all'altro secondo un ordine cronologico[26]. Questa peculiarità permette di catalogare la *blockchain* come esempio di DLT, *Distributed Ledger Technology,* ossia una tecnologia basata su un registro condiviso fra tutti gli utenti della rete:

> *"Questo registro ha una duplice funzione. Da un lato, esso consente di memorizzare in modo inalterabile le informazioni relative alle transazioni in modo da prevenirne la manipolazione. Dall'altro lato, fornisce il meccanismo che consente l'aggiunta di nuove informazioni anche in assenza di un ente centrale di garanzia: le informazioni non possono essere aggiunte al registro distribuito fino a quando non viene raggiunto, tra i partecipanti al registro stesso, il consenso sulla loro validità; ciò incrementa la resilienza di tali registri rispetto ad eventuali tentativi di contraffazione. Numerosi sono i casi d'uso potenziali della DLT/blockchain, ad esempio nell'ambito dei servizi resi dalla pubblica amministrazione (registri immobiliari, voto, identità digitale ecc.), nel campo della sanità, dei media, dell'energia e altri; al suo utilizzo sono associati rischi di natura sia finanziaria sia non finanziaria"*[27]

26 M.G. Turri, *Le criptovalute. Monete private del capitalismo digitale*, Milano, Meltemi, 2020

[27] Banca d'Italia*, Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività,* Roma, 2022, p.6.

Nel caso del protocollo Bitcoin, infatti, ogni nodo può fungere contemporaneamente sia da client che da server verso gli altri nodi della rete, ossia può al contempo richiedere e fornire le informazioni disponibili nella *blockchain* in base alle richieste avanzate in quel momento[28]. Entrambi questi modelli possono essere applicati nella progettazione delle piattaforme che gestiscono le transazioni di denaro online, generando due scenari molto diversi. Da un lato, con il modello *client-server*, utilizzato ad esempio dalle banche, gli utenti della rete per inviare denaro devono prima trasmettere le informazioni al server centrale, unico autorizzato a validare la transazione e a detenere le relative informazioni. Dall'altro lato, invece, con il modello Bitcoin è stato progettato un sistema in cui sono gli utenti stessi ad autorizzare ed approvare le transazioni all'interno della rete, tramite il *mining*.

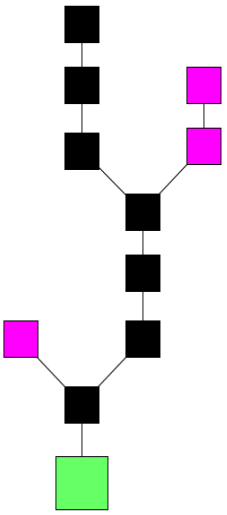

Figura 2: una rappresentazione schematica della blockchain. In verde il primo blocco (genesis block), in nero i successivi blocchi aggiunti al blocco originario e collegati l'un l'altro, in viola i blocchi che non sono stati validati e dunque aggiunti definitivamente. (Fonte: www.wikipedia.com)

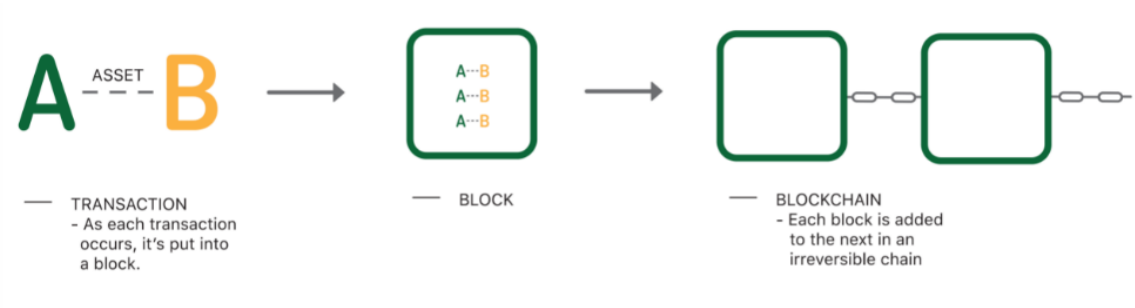

Figura 3: ogni transazione è inserita in un blocco, ogni blocco è concatenato al precedente ed al successivo, andando così a formare la blockchain (fonte: A. Grech-A. Camilleri, Blockchain in Education, Publications Office of the European Union, Luxembourg, 2017)

[28] Cfr. C. Zeno, *BITCOIN: "La moneta virtuale: il trade off tra mezzo di scambio e asset finanziario"*, LUISS, 2018, pp. 15-16

4. L'immutabilità della *blockchain*

L'integrità delle transazioni validate è garantita dall'uso di una funzione matematica che presidia l'immutabilità del registro, detta funzione di hash. Grazie ad essa i blocchi, una volta inscritti nella *blockchain*, non possono più essere modificati senza invalidare l'intero registro. La funzione di hash è un algoritmo[29] che associa ad un *input* uno ed un solo *output* costituito da un codice alfanumerico dalla lunghezza fissa e predefinita, chiamato valore di hash[30]. L'*input* della funzione può essere informazione digitale di qualunque tipo (un testo, un'immagine, una stringa di bit, ecc.) ed è importante sottolineare come, modificandolo anche solo di un singolo bit, la funzione generi un valore totalmente diverso (si veda figura 4).

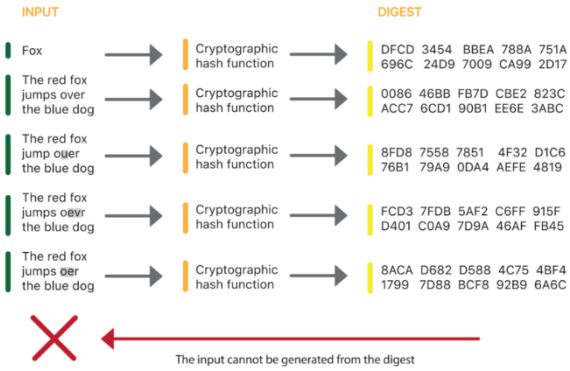

Figura 4: valori di hash *generati da input molto simili (fonte: A. Grech-A. Camilleri, Blockchain in Education, Publications Office of the European Union, Luxembourg, 2017)*

Il valore di hash è univoco e irreversibile, ciò significa che da esso non è possibile risalire all'*input* che lo ha generato[31]. L'utilità della funzione di Hash all'interno delle tecniche di autenticazione digitale è legata al fatto che essa permette di stabilire velocemente e con certezza se l'informazione in esame sia stata manomessa senza bisogno di criptare il messaggio stesso, grazie alla sua lunghezza ridotta e prestabilita. Il valore di hash, infatti, rappresenta una sorta di impronta digitale generata dall'informazione che si vuole condividere, unica e diversa dalle altre, la quale cambia immediatamente al mutare del contenuto che la genera. Perciò, concatenare più funzioni di hash l'una all'altra, come nel caso della *blockchain* permette di verificare che l'intero registro sia integro e uguale per

[29] Con algoritmo si intende un elenco finito di passi che permettono di risolvere un problema o svolgere un'operazione matematica, i quale devono essere finiti e non ambigui.
[30] Esistono numerose funzioni di Hash, il protocollo bitcoin utilizza la funzione SHA-256 (*Secure* Hash *Algoritm)* la quale genera un valore della dimensione di 256 bit.
[31] A.M. Antonopoulos, *Mastering Bitcoin : Programming the Open Blockchain* p. 54 e ss. p.195 e ss.

tutti, semplicemente comparando l'impronta generata dall'ultimo blocco tra più copie dello stesso registro.

Per garantire l'immutabilità delle transazioni in bitcoin, infatti, l'architettura della *blockchain* prevede che esse vengano raccolte in elenchi, detti blocchi, i quali formano una "catena" di informazioni per cui ogni blocco è collegato al successivo tramite la funzione di hash. Essa viene applicata all'insieme delle informazioni contenute nel blocco, per diventare poi parte essenziale del blocco successivo, il quale è composto da un'intestazione (*header*) in cui oltre ad informazioni relative al blocco, è inserito anche l'hash dell'intero blocco precedente. Ne consegue che modificare, anche in maniera minima, le informazioni relative ad una qualsiasi transazione, comporta che l'*header* del blocco successivo diventi completamente diverso e così il successivo, andando ad alterare l'intera catena di valori di Hash, testimoniando così l'avvenuta manomissione.[32]

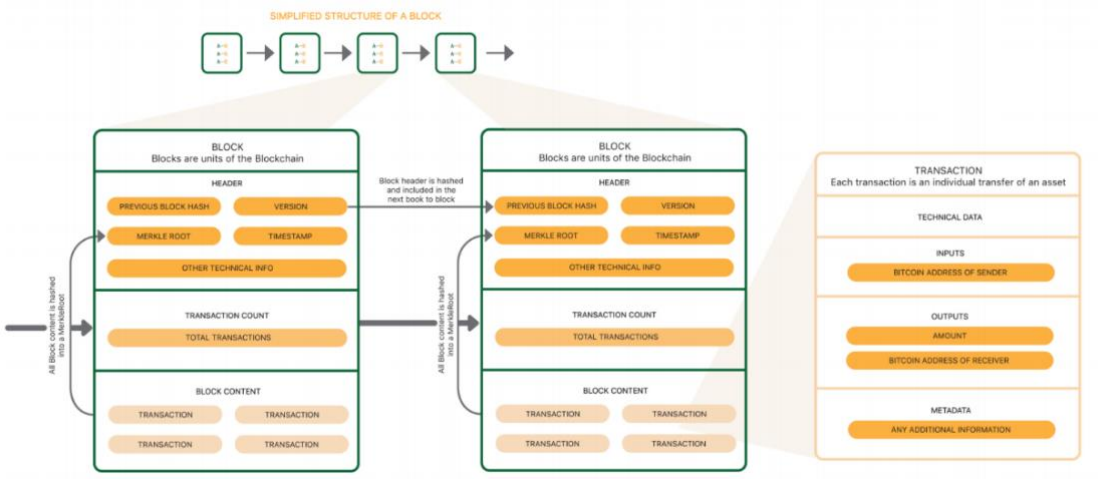

Figura 5: esempio di concatenazione tra i blocchi, in cui il valore di hash *generato da un blocco diviene componente imprescindibile di quello successivo (fonte: A. Grechs-A.Camilleri, Blockchain in Education)*

32 Cfr. consob.it/web/investor-education/criptovalute e M. Bernaschi, E. Mastrastefano, *Una descrizione (quasi) informatica del funzionamento di bitcoin*, EticaEconomia, 2014, https://archivio.eticaeconomia.it/una-descrizione-quasi-informatica-del-funzionamento-di-bitcoin/

Infine, è importante segnalare un elemento rilevante all'interno del funzionamento generale della *blockchain*, ossia il suo consumo energetico. A quindici anni di distanza dalla sua introduzione ed a causa della sempre maggior potenza di calcolo richiesta per minare ogni blocco, l'impronta ecologica generata dall'intero sistema sta assumendo dimensioni notevoli. Considerando che ogni giorno vengono minati circa 140 blocchi e che migliaia di *miners* (spesso formati da più server operanti in rete, detti *mining pool*) lavorano contemporaneamente per validare le stesse transazioni, ne consegue che servono enormi quantità di energia elettrica per alimentare i server che processano continuamente le operazioni di calcolo dedicate al *mining*, un consumo che ha sollevato diverse critiche anche tra i sostenitori stessi della filosofia Bitcoin.[33]

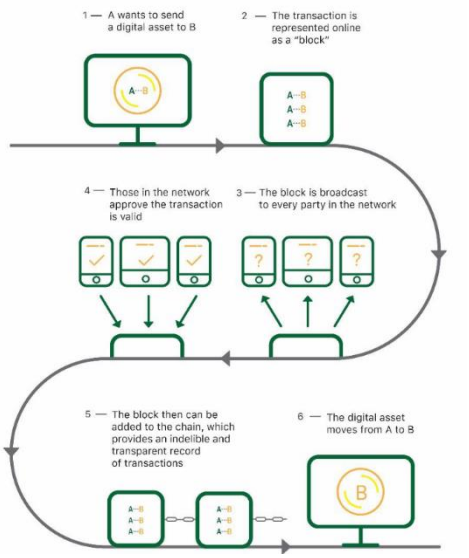

Figura 6: una schematizzazione del processo attraverso il quale le transazioni vengono raggruppate in blocchi ed aggiunte alla blockchain (fonte: A. Grechs-A. Camilleri, Blockchain in Education)

5. Le transazioni in bitcoin

Il protocollo Bitcoin definisce come avvengono le transazioni in bitcoin tra due o più utenti della rete. Il procedimento si compone di una serie di elementi, tra cui i *wallet*, le chiavi crittografiche e gli *addressess*, i *transaction IDs,* gli *UTXO.* Per inviare e ricevere bitcoin è necessario possedere un portafoglio digitale (*e-wallet* o semplicemente *wallet*) al cui interno sono custodite le chiavi crittografiche ed attraverso il quale acquistare, gestire e detenere le proprie

33 Si veda par. 1.4.4 I *limiti*, tratto da L. Saglia, *Soluzioni innovative alle debolezze di Bitcoin,* Politecnico di Torino, Corso di laurea magistrale in Ingegneria Informatica (Computer Engineering), 2022. Inoltre, è importante segnalare che esistono altre tipologie di blockchain in cui è solo un solo server ha minare un blocco, selezionato ad estrazione tra tutti i nodi, secondo il meccanismo della *Proof-of-stake,* Utilizzato da Ethereum, la seconda criptovaluta per capitalizzazione ed importanza, che offre una possibile soluzione funzionale ad abbattere il consumo di energia elettrica.

criptovalute. Nel senso originario e più ampio del termine, *wallet* indica qualunque supporto digitale o fisico nel quale sono archiviate e custodite le chiavi principali (ad esempio i *paper* e gli *hardware wallet*).[34] Tuttavia, con il passare del tempo, si è diffusa la consuetudine di chiamare *wallet* quella che in realtà è una categoria ristretta di portafogli digitali, composta da veri e propri software, i quali non solo custodiscono le chiavi ma svolgono anche il ruolo di interfaccia utente. Tramite questa tipologia di portafogli, come i *desktop*, i *mobile* e gli *online wallet*, il possessore di *btc* può compiere operazioni con le proprie cripto ed inserirle nella *blockchain*. Essi, infatti, consentono all'utente di gestire le proprie monete virtuali, custodendo chiavi e indirizzi, monitorando il saldo nonché creando e firmando transazioni, al pari di un sito di *home banking*.

Ai fini delle tematiche trattate in questo lavoro è utile esporre una breve descrizione delle differenti tipologie di *wallet*:

- *Paper*: veri e propri supporti cartacei su cui sono stampate le chiavi crittografiche che permettono di movimentare i propri bitcoin. Sono i più sicuri dal punto di vista della *cybersecurity* perché tengono le informazioni al riparo da qualsiasi tentativo di attacco informatico, al contempo però espongono le chiavi al rischio di deterioramento o smarrimento;
- *Hardware*: sono il corrispettivo digitale dei *paper wallet*, ossia dispositivi rimovibili e non connessi alla rete sui quali vengono salvati i propri codici. Possono essere chiavette usb o hard disk protetti da password[35];
- *Desktop*: consistono in software scaricabili sul proprio pc che lavorano in locale e si connettono alla rete solamente per effettuare transazioni;
- *Mobile*: sono la versione per smartphone dei desktop wallet, ossia delle app installabili sul proprio cellulare che permettono in modo semplice di inviare e ricevere bitcoin;
- *Online*: portafogli custoditi in remoto dai gestori del server a cui si decide di appoggiarsi per compiere operazioni e

34 A.M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain* p. 93
35 *Ibidem* p. 6 e ss,

conservare le proprie criptovalute. Solitamente è un servizio offerto dalle piattaforme *Exchange*[36][37];

Una volta configurato il proprio *wallet* chiunque è pronto a ricevere ed inviare valuta digitale e le modalità per farlo sono diverse, anche se ad oggi la più diffusa è sicuramente quella legata al mondo degli *Exchange provider*. Un altro metodo, anche se meno comune, sono gli ATM, veri e propri sportelli bancomat attraverso i quali e possibile acquistare e vendere bitcoin in cambio di contanti, ad oggi ne sono presenti in Italia 79.[38] In alternativa, è possibile comprare bitcoin da privati cittadini, contattati tramite internet dove esistono veri e propri siti per mettere in contatto acquirenti e venditori. In questo caso la vendita avviene a fronte di un pagamento in contanti oppure tramite bonifico bancario od altre formule di pagamento digitale, per esempio *Paypal*[39].

7. Le chiavi crittografiche

Alla base di diverse tecnologie, tra cui la *blockchain* e la firma digitale, si trova la crittografia asimmetrica, la quale prevede l'esistenza di due chiavi crittografiche, complementari, tramite cui effettuare la cifratura con una e la decifratura con l'altra. Al contrario, la crittografia simmetrica prevede che esista una sola chiave per entrambe le operazioni.[40] Queste chiavi non sono altro che dei codici alfanumerici[41], grazie ai quali ogni utente può autenticare le informazioni prodotte, criptare quelle

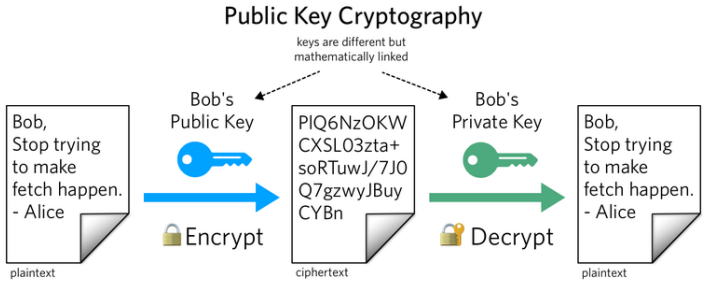

Figura 7: esempio del funzionamento di chiavi crittografiche. Fonte: https://www.twilio.com/blog/what-is-public-key-cryptography

[37] Piattaforme online attraverso le quali si possono facilmente acquistare, vendere e scambiare critpovalute, ad es. Coinbase.com e Binance.com
[38] Fonte: https://coinatmradar.com/countries/
[39] A.M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain* p. 11
[40] Cfr. G. Sartor, L'informatica giuridica e le tecnologie dell'informazione, giappichelli, Torino, 2016, p. 193
[41] Per approfondire il tema della crittografia si veda L. Travaglini, pag. 7 e ss., per un inquadramento generale del rapporto tra crittografia e diritto si consiglia il testo di G. Ziccardi, Crittografia e Diritto, disponibile al link http://ziccardi.org/docs/crittografia.pdf

inviate e decriptare quelle ricevute da un altro utente, a sua volta autenticato. Con le chiavi personali, dunque, è possibile inviare bitcoin, autorizzando l'operazione con la propria chiave privata, indirizzandole all'indirizzo del destinatario, identificato con la sua chiave pubblica, che egli deve aver preventivamente comunicato al mittente. Le chiavi pubbliche, quindi, identificano i *wallet* coinvolti nella transazione: l'indirizzo da cui provengono le transazioni viene detto *input address;* quello verso cui sono indirizzate, *output address*. Ogni transazione operata genera un codice identificativo detto *transaction ID,* il quale, una volta inserito nella *blockchain*, associa la disponibilità dei bitcoin al *wallet* del destinatario del pagamento. Questa disponibilità di bitcoin viene chiamato *UTXO (unspent transaction output)*, ed è una sorta di "credito" di bitcoin associato al wallet del ricevente, il quale a sua volta potrà movimentarli utilizzando la propria chiave privata.[42]

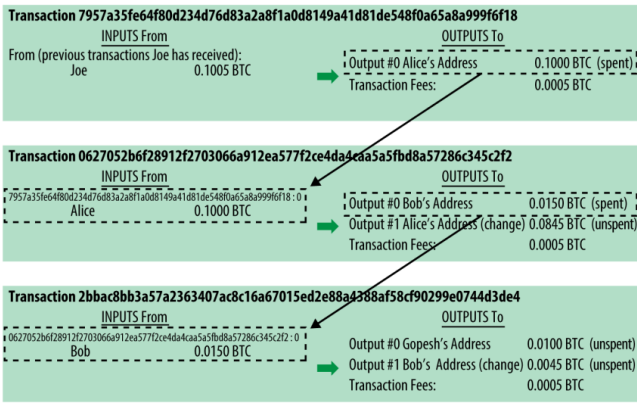

Figura 8: Una catena di transazioni, dove l'output di una transazione diventa l'input della successiva (Fonte: A.M. Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain p. 20)

Come si evince dalla *figura 8*, spesso da un solo indirizzo di input si generano più output, questo per due motivi:

- i bitcoin associati ad una transazione sono indivisibili, dunque, per movimentare una minore quantità di quella connessa ad un transaction ID, il sistema invia al destinatario la frazione prestabilita di bitcoin, mentre la quota rimanente viene reindirizzata in qualità di "resto" al wallet del mittente.
- Una piccola quantità di bitcoin è inviata al miner che validerà la transazione quale ricompensa per il suo lavoro

[42] A.M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain* p. 54 e ss.

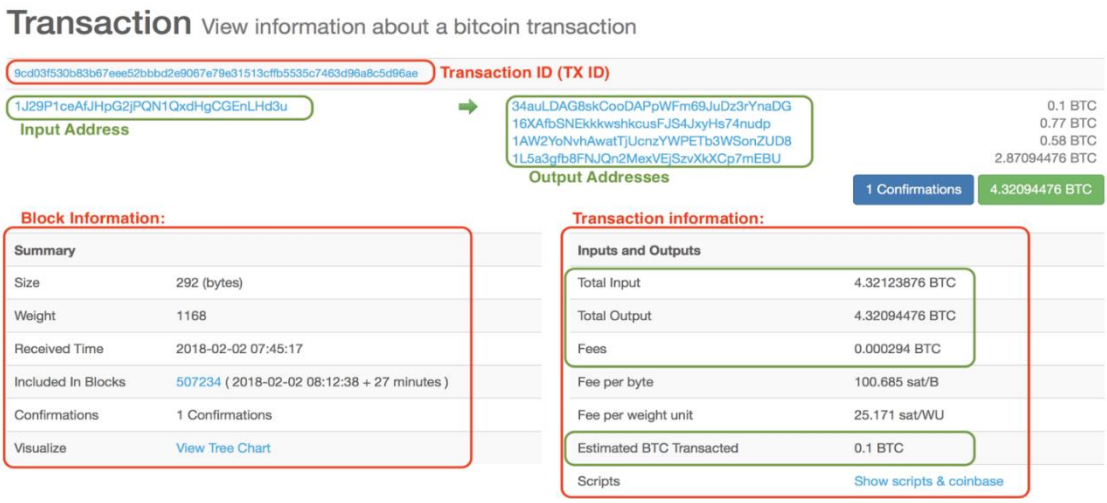

Figura 9: Una rappresentazione grafica delle informazioni relative ad una transazione (Fonte:https://medium.com/coinmonks/bitcoin-transactions-be401b48afe6)

Dopo aver inquadrato il funzionamento di Bitcoin e delle transazioni in criptovalute si andrà ad osservare come queste possano essere utilizzate per operazioni illecite, tra le quali particolare attenzione verrà posta alle innovative tecniche di riciclaggio che sfruttano il funzionamento della *blockchain*, il cosiddetto *cybericiclaggio*. Per affrontare queste tematiche, tuttavia, è necessario prima interrogarsi sul livello di anonimato garantito dal protocollo BTC e dalle implicazioni che ne derivano.

CAPITOLO II

ANONIMATO IN RETE ED OPERAZIONI ILLECITE IN CRIPTOVALUTE

I bitcoin, una volta posseduti, possono essere utilizzati per finalità ed intenti molto diversi fra loro. Come abbiamo visto originariamente sono nati con l'obiettivo di diventare una vera e propria moneta elettronica (status che ad oggi non gli è riconosciuto nel nostro paese e nella maggior parte degli stati), utilizzabile sia per pagare beni e servizi che come mezzo di scambio. Della totalità dei bitcoin in circolazione solo una minima parte assolve a questa funzione, la maggior parte di essi sono utilizzati in altri modi, primo fra tutti quello di strumento di investimento finanziario.

È prassi diffusa quella di acquistare bitcoin nella speranza che il loro valore aumenti generando degli utili a chi li detiene. Oppure ancora, un altro uso finanziario delle criptovalute è il *cd. trading online*, ossia l'attività di compravendita di strumenti finanziari in internet con lo scopo di ottenere un profitto.[43] È possibile, infatti, speculare sui rialzi dei prezzi delle differenti valute ed il ricavato di questa attività può essere venduto in cambio di valute FIAT, termine con cui si indicano le valute correnti riconosciute a livello internazionale, ad es. l'euro, il dollaro, lo yen ecc. Pagare beni e servizi in bitcoin, così come acquistarli o rivenderli secondo l'andamento del mercato, sono attività diffuse e consentite dalla legge per le quali il protocollo garantisce un elevato livello di privacy.

Ci sono tuttavia altre operazioni per le quali sia criminali comuni che pirati informatici sfruttano la *blockchain* per celare la propria identità. Prima di affrontare questo tema è bene chiedersi se Bitcoin sia davvero un sistema anonimo e ad alto livello di sicurezza per la privacy di chi ne fa uso.

1. Anonimato e pseudoanonimato

[43] Fonte : https://it.wikipedia.org/wiki/Trading_online

Riguardo la questione del livello di anonimato garantita dal sistema Bitcoin, è pacifica e condivisa all'interno della comunità scientifica la tesi per cui sia corretto parlare di pseudoanonimato, un termine che sottolinea come sia possibile verificare in ogni momento i movimenti compiuti da qualsiasi utente della rete, per quanto esso sia celato dietro un ID composto da un codice alfanumerico. Il tema su cui si divide la dottrina è piuttosto quanto questo pseudoanonimato sia idoneo a impedire una effettiva tracciabilità delle transazioni e, di conseguenza, come si vedrà nel prossimo capitolo, ad integrare il reato di *cybericiclaggio*.

Emergono su questo punto due posizioni. La prima, che ritroviamo nei testi di Sicignano, sottolinea come la componente di anonimato del protocollo sia secondaria rispetto alla trasparenza sistemica e congenita alla stessa architettura del sistema. È noto, invero, come la *blockchain* assicuri una limpidezza totale riguardo ad ogni transazione compiuta, perché, come abbiamo visto, è la natura stessa delle criptovalute a garantire che il registro delle transazioni sia pubblico ed immutabile. Questa consapevolezza, congiunta all'esistenza di diverse tecniche atte ad identificare i possessori dei wallet, può portarci a definire il Bitcoin come un sistema *pseudo-anonimo* e passibile di controllo da parte di autorità inquirenti esterne. Secondo Sicignano, infatti, celare la propria identità dietro al codice identificativo del portafoglio non è sufficiente per definire il sistema anonimo: venire a conoscenza dell'identità del possessore del *wallet* permetterebbe di ottenere molte più informazioni sullo storico delle transazioni di quante le autorità potrebbero ricavare da un conto in banca.[44]

Di tutt'altro avviso è Sturzo, secondo la quale:

> *L'argomento prontamente proposto dai supporters bitcoin, per cui si tratterebbe in verità di "pseudoanonimato" piuttosto che di anonimato delle transazioni, si rivela essere un puro diversivo. Difatti lo "pseudonimo", ovverosia l'account bitcoin rappresentato da una serie di numeri e lettere, una volta rintracciato dalle forze dell'ordine non permette comunque di risalire oltre, continuando infatti a celare la reale identità fisica del proprietario dell'account individuato. Inoltre, come se non bastasse, un unico soggetto persona fisica può*

[44] Cfr. Cap. 4 G.J. Sicignano, *L'acquisto di bitcoin con denaro di provenienza illecita,* Archivio Penale 2020, n°2, p.12

addirittura divenire contestualmente proprietario di più accounts, operando così più transazioni illecite, ciascuna riconducibile ad un account diverso.[45]

Non è possibile ridurre all'unità queste due posizioni, possiamo però prendere atto del punto in comune ad entrambe le argomentazioni, ossia del fatto che risalire al possessore del *wallet*, impossibile o meno che sia, è un'operazione complicata e che richiede un grande investimento di risorse. Inoltre, come si vedrà nel prossimo paragrafo, esistono delle tecniche atte a rafforzare l'anonimato legato alle proprie operazioni, e queste misure aumentano la difficoltà di rintracciare mittenti e destinatari delle transazioni. Anonimato e pseudo-anonimato sono due visioni diverse di una stessa certezza: non si può affermare che in qualunque caso, dato l'indirizzo di un *wallet*, è possibile risalire al proprietario.

Prendendo le mosse da queste tesi condivise è necessario avere contezza di alcune delle modalità con cui è possibile rafforzare l'anonimato delle operazioni in criptovalute e come esse vengano utilizzate per finalità illecite.

2. Implementare l'anonimato

Le normative attuali impongono alle piattaforme *Exchange* di richiedere alla clientela di identificarsi tramite un documento[46], tuttavia questo non impedisce di comprare bitcoin in maniera anonima e legale. Ecco un esempio di come sia possibile in pochi semplici passaggi, alla luce di quanto visto nel capitolo precedente:

1. aprire un paper *wallet* in pochi secondi tramite siti online che offrono questo servizio senza bisogno di alcun tipo di autenticazione né di fornire un documento di identità al sito;
2. cercare persone interessate a vendere di bitcoin su un forum online o sui social network;
3. pagare il trasferimento e verificare che il pagamento sia stato validato nella *blockchain*.

[45] L. Sturzo, *BITCOIN E RICICLAGGIO 2.0,* p. 31
[46] Si veda cap. 3

In questo modo, con tre operazioni alla portata di qualunque persona dotata di una connessione internet, si dispone di una somma di bitcoin senza che nessuno possa facilmente risalire alla nostra identità, seppur chiunque sia in grado di rintracciare la transazione nel registro. Tuttavia, per far sì che risalire all'autore della transazione sia veramente difficile, occorrono delle precauzioni:

- il pagamento non deve essere tracciato. Può essere fatto in contanti, tramite versamento anonimo oppure provenire da un conto cifrato, ovvero è necessario che i bitcoin siano ceduti a fronte di un pagamento con altre criptovalute, a loro volta non associabili alla persona fisica che esegue l'operazione;
- l'indirizzo IP del dispositivo con cui si è generato il *wallet* non dev'essere rintracciabile né riconducibile all'autore dell'operazione.

Entrambi questi aspetti sono cruciali per ottenere una transazione completamente anonima e generano degli ostacoli di cui bisogna tener conto. A questa complessità, per chi vuole operare in rete celando la propria identità, si aggiunge la consapevolezza per cui le criticità rilevate sono strettamente legate alla giurisdizione in cui si opera: più uno stato è attento a far rispettare le disposizioni circa la trasparenza bancaria oppure limita la libertà di informazione in rete, tanto più è difficile muovere grandi somme di denaro senza lasciare traccia. Per superare il problema del tracciamento del pagamento è ormai dimostrato come le organizzazioni criminali non abbiano difficoltà a muovere grandi quantità di contanti, suddividere i pagamenti affidandosi a dei prestanome, oppure a servirsi di conti cifrati con sede in paradisi fiscali, aumentando così la difficoltà delle autorità nel reperire le informazioni.[47]

Il secondo problema, quello legato all'identificazione tramite indirizzo IP, è facilmente raggirabile con dei semplici escamotage grazie all'uso di tecnologie alla portata di chiunque, tra queste due delle più semplici e diffuse sono TOR e VPN.

[47] Come si evince dagli allarmi delle autorità competenti: si veda cap. 3

TOR, acronimo di *The Onion Router*, è un software libero e gratuitamente disponibile in rete, grazie al quale è possibile utilizzare internet celando il proprio indirizzo IP e raggiungere le pagine web non indicizzate dai principali motori di ricerca, il *cd. Deepweb*.[48] Esso oscura gli indirizzi IP grazie alla c.d. *Multi-layer encription*, tecnica per cui i pacchetti di informazione che costituiscono il flusso della rete vengono occultati da diversi starti di crittografia, in modo che ogni nodo della rete che attraversano è in grado di leggere solo la posizione del nodo precedente (da cui provengono) e di quello successivo (verso cui sono indirizzati), senza poter risalire all'origine né alla destinazione finale del percorso compiuto dai dati.

Il pacchetto IP che viaggia nella rete, dunque, attraversa tre server TOR (come si vede nella figura 10, sono denominati *entry guard, middle relay e exit relay*) selezionati in maniera casuale tra i seimila attualmente sparsi in tutto il globo. Da questo "multistrato" che protegge le informazioni deriva il nome stesso del progetto: *The Onion (cipolla) Router*, a simboleggiare questa stratificazione posta a protezione dei dati dell'utente che viene "sbucciata" progressivamente durante i diversi passaggi che collegano client e server.[49]

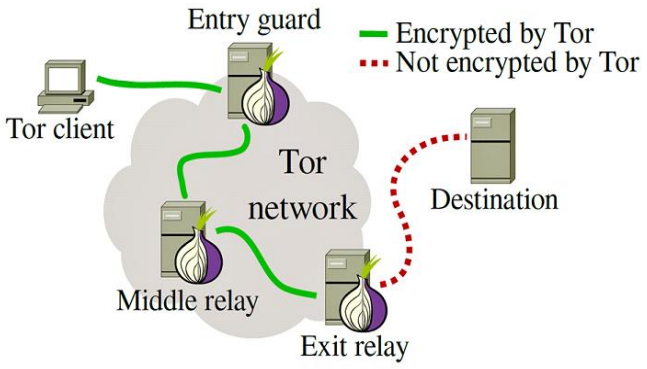

Figura 10: rappresentazione grafica del funzionamento di TOR (fonte: A. Anselmi, Onion routing, cripto-valute e crimine organizzato, Pacini giuridica

VPN, acronimo di Virtual Private Network ossia "rete privata virtuale", è invece una tecnologia che consente ad un utente di creare un canale di comunicazione che rende invisibili le proprie attività in rete, oltre che l'indirizzo IP, grazie a un particolare sistema chiamato *tunneling*. Normalmente, senza utilizzare una VPN l'accesso ad internet è garantito dal proprio *Internet Service Provider*, ossia un fornitore di servizi internet che grazie alla propria infrastruttura permette di

[48] A. Anselmi, *Onion routing, cripto-valute e crimine organizzato*, Pacini giuridica, pp. 13-15
[49] Per una trattazione dettagliata del funzionamento di Tor si rimanda a A. Anselmi, *Onion routing, cripto-valute e crimine organizzato,* Pacini giuridica, Pisa, 2019, pp. 6-13

collegare le diverse reti che compongono internet, garantendo così l'accesso al World Wide Web. Gli ISP però tengono traccia di tutte le attività in rete compiute da un punto di accesso alla rete, identificato con l'indirizzo IP, compromettendo la privacy degli utenti.

Accedendo ad internet attraverso un servizio VPN, invece, tutto il traffico dati viene crittografato e indirizzato ai server del provider della VPN, il quale farà da tramite tra la rete ed il proprio indirizzo IP, oscurando l'attività al proprio ISP, grazie al tunnel criptato,[50] garantendo così anonimato e sicurezza dei dati. Al contrario di TOR, l'efficacia dell'utilizzo di una VPN a tutela della privacy dipende dal provider del servizio stesso, da quali dati conserva nei propri database e con chi esso possa condividerli in futuro, sia volontariamente che involontariamente.

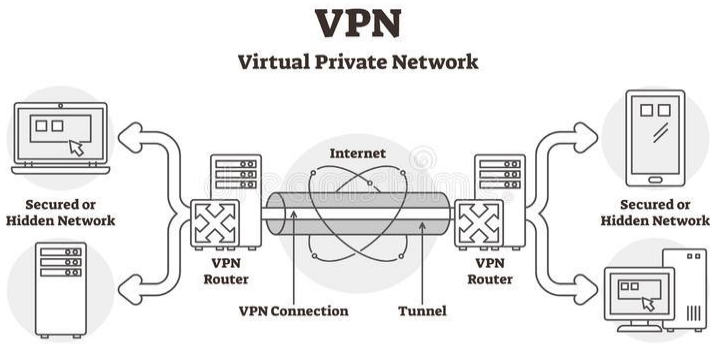

Figura 11: Rappresentazione grafica del funzionamento di una VPN. (Tratto da https://it.dreamstime.com)

Affermare che l'ISP conosce l'indirizzo di accesso alla rete non significa automaticamente che egli violi sistematicamente la privacy dei suoi clienti, né che possa consequenzialmente risalire all'identità del soggetto fisico. Tuttavia, il provider può essere costretto a fornire le informazioni in suo possesso a seguito di una richiesta dell'autorità giudiziaria del proprio paese o di uno stato estero, oppure i suoi database possono essere "bucati" ed i dati in essi contenuti sottratti da dei pirati informatici. Risalire alla persona fisica che opera dietro una connessione internet ad oggi è un'operazione relativamente facile, sia per le autorità inquirenti che per un malintenzionato. Infatti, analizzando le specifiche dell'indirizzo IP (ad esempio la geolocalizzazione) ed incrociandole con i dati contenuti in altri database

[50] Per un approfondimento del tema della VPN e dell'anonimato in rete si consiglia l'articolo di R. Brighi e F. Di Tano, *Identità, anonimato e condotte antisociali in Rete. Riflessioni informatico-giuridiche* in Rivista di filosofia del diritto 1/2022

lascia, sia involontariamente durante la sua navigazione, che volontariamente, ad esempio attraverso i social.

3. Le *alt-coin* completamente anonime

Un'altra modalità di operare transazioni completamente anonime senza bisogno di mascherare il proprio indirizzo IP è costituito dalle criptovalute che assicurano la totale opacità di destinatari e mittenti *by design*, i due casi più illustri sono *Monero* e *Z-Cash*. *Monero* è un progetto lanciato nel 2014 dallo sviluppatore Riccardo Spagni, il cui funzionamento si basa sul protocollo *CryptoNote83*, grazie alle tecnologie cd. *Ring signatures* e *Ring CT:*

> *"Per mascherare gli indirizzi vengono usate firme ad anello o ring signature, dove ogni transizione tra due parti viene inserita e raggruppata ad altre transazioni multiple che si verificano tra diverse parti non correlate. Ciò significa che il trasferimento di moneta da un utente A ad un utente B viene mescolato con le altre transazioni degli utenti Monero e spostato casualmente lungo l'elenco delle transazioni, il che rende esponenzialmente difficile risalire alla fonte o al destinatario.*
> *Agli inizi del 2017 è stato implementato il Ring CT: Ring Confidential Transactions (Ring CT), finalizzato a fornire un miglior anonimato per gli importi delle transazioni. Il sistema gestisce le transazioni dividendo l'importo trasferito in più importi, suddividendoli come fossero transazioni separate. Ad esempio, un utente che trasferisce 100 XMR (unità monetaria di Monero) a un acquirente dovrebbe suddividere l'importo in 22 XMR, 61 XMR e 17 XMR, per un totale di 100 XMR. Ognuno di queste viene trattata separatamente e viene creato un indirizzo univoco per ciascuna delle figure suddivise. Con la firma ad anello, ciascuno di questi importi suddivisi viene combinato con altre transazioni che, ovviamente, sono state divise, rendendo estremamente difficile identificare il mix esatto di 100 XMR che appartiene al destinatario."*[51]

Z-cash invece sfrutta una tecnica diversa per ottenere lo stesso risultato, il suo funzionamento si fonda infatti su di una tecnica crittografico denominata

[51] A. Anselmi*, Onion routing, cripto-valute e crimine organizzato*, pp. 21 e *ss.*

Zero-Knowledge-Proof[52] che permette di trasferire valuta senza che nessuna delle parti coinvolte nella transazione riveli il proprio indirizzo né visualizzi quello delle altre:

> *Questa tecnica rende le transazioni Z-Cash non rintracciabili sulla blockchain offuscando gli indirizzi di entrambe le parti, così come l'ammontare coinvolto in ogni transazione, impedendo la ricostruzione dei passaggi dell'asset. Inoltre, Z-Cash è supportabile dalla maggior parte dei wallet, sia hardware che software, incentivandone l'uso. Essendo in circolazione dalla fine del 2016 ZEC (simbolo di valuta per Z-Cash), è utilizzata in seconda posizione rispetto a Monero, sulla rete da più anni e quindi ritenuta più affidabile, specialmente nelle Darknet. Nonostante questo, a partire dal luglio 2018, la moneta ha avuto un aumento progressivo che continua ancora oggi"*[53].

4. La privacy totale tra usi leciti ed illeciti

TOR e VPN, così come le criptovalute completamente anonime, sono tecnologie dalle enormi potenzialità, sia positive che negative, come spesso capita quando si parla di anonimato. Questo, infatti, può essere vitale per persone che vivono sotto regimi autoritari ai quali è negata ogni forma di libertà di espressione e di informazione. Pensiamo alle migliaia di giornalisti, attivisti e semplici cittadini in tutto il mondo che rischiano la vita per accedere all'informazione indipendente o per pubblicare notizie e inchieste riguardanti i governi dei paesi in cui vivono. Essi, proprio grazie a questi espedienti informatici, riescono a far trapelare all'estero notizie scomode per le autorità e che li potrebbero esporre alla persecuzione governativa.[54]

Dall'altro lato, l'anonimato è il primo indispensabile strumento per operare illegalmente sulla rete. Il progetto Tor negli anni è divenuto un punto di riferimento non solo per attivisti, giornalisti e semplici curiosi ma anche per organizzazioni criminali e terroristiche di tutto il mondo, grazie alla possibilità che esso permette di tutelare la propria identità ed accedere al *dark*

---

[52] Per un approfondimento tecnico del funzionamento della *Zero-Knowledge-Proof* si rimanda a A. Languasco-N. Zaccagnini, Manuale di crittografia. Teoria, algoritmi, protocolli, Ulrico Hoepli editore, Milano, 2015, cap. 8.
[53] *Ibidem.*
[54] Anche se in misura minore, Tor è uno strumento vitale per garantire la libertà d'espressione in alcune parti del mondo, come spiega uno studio riportato dal seguente articolo: https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/.

web, l'insieme di pagine del *deep web* ospitate su server il cui indirizzo IP è a loro volta celato.[55] In questa porzione di *cyberspazio* è possibile accedere a diversi servizi e prestazioni illegali, ad esempio gli utenti possono usare i bitcoin per effettuare acquisti di merce illecita (esistono veri e propri *e-shop* online di droga, armi, banconote false e documenti rubati), la cui consegna a domicilio avviene principalmente tramite corrieri ignari, occultata dentro pacchi comuni. La combinazione dei diversi fattori che ne permettono l'esistenza, quali l'anonimato garantito dal sistema, l'opacità delle transazioni in bitcoin e le tecniche di spedizione, pensate per eludere i controlli, sono gli stessi che rendono molto difficile risalire ai gestori di questi traffici illeciti[56]. Non solo i *dark market*, infatti, sfruttano questi strumenti ma essi sono familiari anche alle più disparate tipologie di reati informatici: da chi divulga materiale pedopornografico ai pirati informatici che, tramite attacchi *ransomware*, accedono abusivamente ai sistemi informatici altrui per "sequestrare" i dati criptandoli e chiedendo successivamente un riscatto (ovviamente in criptovalute) per decriptarli[57].

Il problema legato all'anonimato e all'utilizzo dei bitcoin può essere paragonato a quello dei pagamenti in contanti: non integrano di per sé una fattispecie di reato; tuttavia, potrebbero essere prodromici e funzionali al compimento di attività criminose e di riciclaggio. Non ci si interrogherà in questa sede sulle questioni etiche legate all'anonimato in rete, piuttosto si andrà ad approfondire come i capitali ottenuti illegalmente vengano riciclati e movimentati tramite le criptovalute sfruttando l'anonimato e quali misure di contrasto sono state introdotte dal legislatore e dalla comunità internazionale.

---

[55] *Ibidem* p.39 e ss.

[56] La criticità legata all'utilizzo di Tor a fini criminosi trascende la tematica dei bitcoin, infatti, come osserva Capaccioli "la presenza della rete TOR (The onion router) anonima non è una caratteristica fondante del protocollo Bitcoin e costituisce una problematica non dello strumento ma di ogni reato informatico" S. Capaccioli*, Riciclaggio, antiriciclaggio e bitcoin*, in Il fisco, n. 46/2014, p.4.

[57] Questa tipologia di attacco informatico prende il nome di *Ransomware: "*una classe di malware che rende inaccessibili i dati dei computer infettati e chiede il pagamento di un riscatto, in inglese ransom, per ripristinarli." Fonte: https://www.cybersecurity360.it/nuove-minacce/ransomware/ransomware-cose-come-rimuoverlo-e-come-difendersi/.

CAPITOLO III.
IL CYBERICICLAGGIO

1. Inquadramento giuridico dei bitcoin

I bitcoin, così come le criptovalute in generale, sono valute virtuali definite dal nostro ordinamento come "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"[58]. Nonostante ad oggi il legislatore sia riuscito a darne una definizione condivisa, questa non ha risolto il problema dell'inquadramento giuridico delle criptovalute, un tema ampiamente dibattuto e su cui si sono scontrate diverse opinioni. Le ipotesi prese in considerazione sono state diverse, esse sono stati definite nel tempo in vari modi, tra cui monete elettroniche, monete complementari, strumenti di pagamento o ancora beni immateriali, *commodities*, prodotti finanziari etc.[59].

Ognuna di queste definizioni riesce a inquadrare solo parzialmente gli aspetti tipici delle criptomonete ma, dato che esse hanno introdotto nel panorama monetario classico elementi inediti, difficilmente possono essere etichettate secondo termini consolidati senza commettere errori logico-giuridici o dandone definizioni incomplete. Ad esempio, nonostante i bitcoin siano nati e vengano usati come mezzo di pagamento, essi non si possono considerare denaro secondo la teoria statalista di moneta[60] perché non sono coniati da alcuno Stato e non hanno nessuna efficacia solutoria *ex lege*. Inoltre, la loro creazione non è riferibile ad una autorità centrale e il loro

[58] D. Lgs. 4 ottobre 2019, n. 125 attuativo della Direttiva 2018/843 del Parlamento europeo e del Consiglio del 30 maggio 2018 (cosiddetta V direttiva antiriciclaggio).
[59] Per un'analisi dettagliata di ciascuna di queste ipotesi si veda J.G. Sicignano, *Bitcoin e riciclaggio*, cap. 3.
[60] Secondo la teoria Statalista (o cartalista) della moneta è lo Stato che definisce le caratteristiche fisiche di banconote e moneta. Questo approccio è presente nel nostro ordinamento, trovando riconoscimento nell'art.1277 cc. e viene ribadita, anche se in forma indiretta, nell'art. 47 della Costituzione, il quale rimanda ad una legge ordinaria per la sua disciplina, la legge banc. 141/1938. Cfr. J.G. Sicignano, *Bitcoin e riciclaggio*, pp. 77-79.

scambio può essere riconosciuto come adempimento di obbligazione solo qualora ci sia un accordo tra le parti in questo senso. Infine, nessuno può essere sanzionato amministrativamente se non accetta un pagamento in bitcoin, né la falsificazione degli stessi dà luogo a responsabilità penale[61]. Ne consegue che, di conseguenza, essi non possano essere definiti nemmeno come moneta elettronica, perché privi di riconoscimento da parte della autorità preposte[62]. Altresì, i bitcoin non possono essere ricondotti al concetto penalistico di cosa o di bene senza violare il principio di tassatività e il divieto di analogia previsti dal diritto penale in quanto tecnicamente non sono altro che dati informatici[63]. Sono infatti definibili beni immateriali le opere dell'intelletto, categoria a cui i bitcoin non appartengono in quanto sono un mero elenco di bit generato da un protocollo, ma, soprattutto, un bene immateriale deve essere espressamente definito tale da una legge, in quanto elemento tipico dell'ordinamento, ed al momento nessun testo normativo lo prevede; perciò, anche questa è un'ipotesi da escludere[64].

La soluzione a questo problema è stata indicata nel 2017 dalla giurisprudenza che, con una sentenza decisiva del Tribunale di Verona, ha definito i bitcoin strumenti finanziari[65] . I giudici hanno qualificato in quella sede i bitcoin come "strumento finanziario utilizzato per compiere una serie di particolari forme di transazioni online costituito da una moneta che può essere coniata da qualunque utente ed è sfruttabile per compiere transazioni, possibili grazie ad un *software open source* e ad una rete *peer to peer*[66]." Il problema dell'inquadramento giuridico non è irrilevante, in quanto da esso dipende la configurabilità dei reati che tramite essi possono essere perpetrati. Si andrà ora ad analizzare il caso del riciclaggio a mezzo criptovalute.

[61] J.G. Sicignano, *Bitcoin e riciclaggio,* pp. 78-79.
[62] *Ibidem*
[63] M. Croce, *Cyberlaundering e valute virtuali. la lotta al riciclaggio nell'era della distributed economy*, in Sistema Penale, 4, 2021, p. 138
[64] J.G. Sicignano, *Bitcoin e riciclaggio,* p.90.
[65] Trib- Verona, Sez. II civ., 26 gennaio 2017, n.195 in *Banca, borsa, tit. cred*., n.4,2017, p.471 ss. Con nota di M. Passaretta.
[66] *Ibidem.*

2. Il cybericiclaggio

L'organizzazione criminale che ha accumulato proventi illeciti e vuole ripulire i capitali può servirsi dei bitcoin per attuare tecniche di *cybericiclaggio (cyberlaundering)*, termine che indica una specifica modalità di attuazione del più generico reato di riciclaggio (art. 648 *bis* c.p.). La norma che disciplina quest'ultimo punisce con la reclusione da quattro a dodici anni colui che "sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa"67.

L'articolo citato delinea il riciclaggio come un reato istantaneo di mera condotta e di pericolo concreto, si configura infatti non appena viene messa in atto ogni pratica ad esso riconducibile, aldilà dell'effettivo verificarsi dell'evento desiderato. È un delitto plurioffensivo in quanto danneggia, oltre che l'ambito patrimoniale, anche l'economia ed il mercato andando a falsare la libera concorrenza e a minare la stabilità e l'affidabilità degli intermediari finanziari. L'elemento soggettivo del reato è il dolo generico, infatti, chi commette operazioni atte a riciclare agisce volontariamente e consapevolmente, tuttavia, si ritiene che il reato possa configurarsi anche come dolo eventuale; in tale ipotesi, è sufficiente una consapevolezza generica della provenienza delittuosa dei beni. Il terzo comma del 648 *bis* c.p. prevede che la pena è aumentata qualora i fatti siano commessi nell'esercizio di una professione, come ad esempio l'attività bancaria o finanziaria. Il reato di riciclaggio prevede la commissione di un reato presupposto e, qualora l'autore del suddetto sia lo stesso che si adopera successivamente per ripulire il denaro, si configura il reato di autoriciclaggio introdotto dal legislatore con la legge 186/2014 all'art. 648 *ter* 1.

L'articolo 648 *bis* c.p. è ad oggi il riferimento normativo anche per il cybericiclaggio in quanto non è stato introdotto nel nostro Codice penale un articolo *ad hoc* per il riciclaggio informatico, al contrario di quanto accaduto in altri casi, ad esempio per i reati di frode informatica, falso informatico o di danneggiamento informatico, introdotti ad opera della legge n. 547/1993[68].

[67] art. 648 bis c.p
[68] Si veda V. Plantamura, *Cybericiclaggio* in C. Cadoppi et. al. *Cybercrime*, Utet giuridica, pag. 871.

Da questo vuoto normativo ne è derivata una questione circa l'integrazione del reato di riciclaggio qualora venga commesso a mezzo criptovalute, infatti, perché si configuri il reato è necessario poter affermare che le stesse rientrino in una delle tre categorie tipizzate dalla norma: denaro, beni o altre utilità. La dottrina è tendenzialmente concorde a catalogare le criptovalute nella categoria delle "altre utilità"[69], non potendo essere definite, come si è visto, né beni immateriali né denaro. Pur senza una norma specifica la dottrina è riuscita, in anticipo rispetto al legislatore, a dare al cybericiclaggio "un'accezione criminologica, prima che giuridico-penale, quale 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", resi disponibili dalle ICT"[70]. La struttura del cybericiclaggio delineata sin qui ricalca quella del riciclaggio tradizionale e ne riprende i passaggi tipici, denominati *placement, layering* e *integration*:

1. *Placement*: fase in cui i capitali vengono collocati nell'economia legale: quando il denaro viene convertito in criptovalute e utilizzato per acquistare beni o servizi;
2. *Layering*: fase di dissimulazione dei proventi illeciti attraverso una serie di operazioni finanziare "stratificate" atte ad occultare la reale provenienza del capitale;
3. *Integration*: fase che mira a reintrodurre il capitale, ormai ripulito, nel circuito economico attraverso una rete di complessità al fine di eludere la tracciabilità del provento illecito da parte delle autorità di regolamentazione.[71]

[69] Vanno in questa direzione, tra le altre, le argomentazioni di Sicignano, Brighi, Sammario, Dell'Osso. Si vedano: J.G. Sicignano, *Bitcoin e riciclaggio,* pp. 122-129; R. Brighi – P. Sammario, *Cyberlaundering e Blockchain,* pp.194-197; A.M. Dell'Osso, *Riciclaggio di proventi illeciti e sistema penale*, Giappichelli, Torino, 2017 p.112.
[70] L. Picotti, *Profili penali del Cyberlaundering: le nuove tecniche di riciclaggio* in *Rivista trimestrale di diritto penale dell'economia*, n. 3-4, 2018, p. 593-594.
[71] R. Brighi – P. Sammario, *Cyberlaundering e Blockchain Forensics* In R. Brighi et al. *Nuove questioni di informatica forense*, ed. Aracne, Roma, 2022, pp.192-193.

La differenza sostanziale tra il reato classico e quello "*cyber",* appurato il medesimo intento criminoso, consiste nell'utilizzo delle potenzialità offerte dalla rete e dai sistemi informatici, nello specifico dalle criptovalute. Particolarità da cui discendono due principali conseguenze che contraddistinguono il *cyberlaundering*. Innanzitutto, è fondamentale la distinzione tra riciclaggio integrato e strumentale: con il primo termine si intende il reato ove sono i bitcoin stessi (incassati come mezzo di pagamento per prestazioni illegali) ad essere ripuliti; nel caso del riciclaggio strumentale, invece, è il denaro di provenienza illecita ad essere utilizzato per acquistare criptovaluta e, successivamente, farne perdere le tracce[72]. Un esempio di riciclaggio strumentale può prevedere che i proventi del reato accumulati in valuta corrente siano utilizzati per acquistare criptovaluta (operazione che rappresenta in questo caso la fase del *placement*) le quali possono essere a loro volta scambiate a fronte dell' acquisto di altre valute virtuali oppure di altri tipo di beni (*layering)*, tra cui spesso ritroviamo l'acquisto di moneta legale o di azioni societarie, oppure è prassi molto diffusa l'utilizzo di questi capitali nel gioco d'azzardo *online*, le cui vincite possono essere incassate sottoforma di denaro pulito adoperato spesso per intraprendere attività legali che generano profitti leciti (*integration*)[73].

La seconda differenza rispetto al riciclaggio classico è una conseguenza della natura stesse delle criptomonete, ossia la peculiarità che le tre fasi del reato sopra ricordate risultino meno definite e spesso si intreccino all'interno di una stessa operazione, la quale può racchiudere più passaggi[74]. Ad esempio, un *cyberlaunderer*, con la medesima transazione, può acquistare delle criptovalute (*placement*) utilizzando tecniche particolari o tramite soggetti terzi che ne vanno ad oscurare la tracciabilità (*layering*), grazie ad esempio alle criptovalute completamente anonime oppure attraverso il ricorso ai cd. *mixer,* come si vedrà nel prossimo paragrafo.

[72] J.G. Sicignano, *Bitcoin e riciclaggio,* pp. 138 e *ss.*
[73] Cfr.R. Brighi – P. Sammario, *Cyberlaundering e Blockchain Forensics* In R. Brighi et al. *Nuove questioni di informatica forense*, ed. Aracne, Roma, 2022, pp.192-193.
[74] Per una spiegazione esaustiva dei tre passaggi del riciclaggio e della loro evoluzione grazie alla tecnologia delle criptovalute si veda R. Brighi – P. Sammario, *Cyberlaundering e Blockchain Forensics* In R. Brighi et al. *Nuove questioni di informatica forense,* ed. Aracne, Roma, 2022, pp.192-193

Infine, si parla altresì di (*cyber)*autoriciclaggio, sulla scorta della definizione di prevista dall'articolo art. 648 *ter*.1 c.p.[75], qualora la persona che agisca al fine di far perdere le tracce dei proventi di un precedente reato tramite criptovalute sia la stessa che l'abbia precedentemente commesso. Anche in questo caso non è prevista una norma *ad hoc* ma si tratta di una rilettura del Codice penale alla luce delle nuove tecnologie.[76]

3. Tecniche di *cyberlaundering*

Per poter reimmettere nell'economia legale i proventi criminosi è necessario prima ostacolare ogni possibilità di ricostruire la tracciabilità delle criptovalute, operazione che integra il reato, trattandosi infatti nella pratica di "ostacolare l'identificazione della loro provenienza delittuosa"[77]. Avendo visto nei precedenti capitoli come avvengono a livello tecnico le transazioni in bitcoin, è facile immaginare come lo pseudoanonimato, o peggio le valute completamente anonime, ben si prestano ad essere adoperate per le operazioni di lavaggio del denaro sporco. Questo può avvenire in diversi modi, ad esempio grazie ad una serie di transazioni digitali verso indirizzi a cui non è associato alcun intestatario oppure tramite la frammentazione dei pagamenti in una pluralità di micro-transazioni verso *wallet* anonimi.

Per occultare in maniera più efficace le monete virtuali si fa ampio ricorso ai cosiddetti *mixer*[78]*,* ossia degli intermediari che, dietro il pagamento di una commissione, si prestano a ricevere una quantità di bitcoin da indirizzi il cui anonimato è compromesso, ossia facilmente aggirabile dagli inquirenti, per poi inoltrarli ad indirizzi appositamente creati, da cui i committenti possono successivamente recuperare i propri proventi senza correre rischi. Il *mixer*, infatti, incamerando questi fondi nel suo portafoglio, li mischia con valute di altra provenienza (da qui il termine frullatore) per poi riversarli in

[75] "Si applica la pena della reclusione da due a otto anni e della multa da euro 5.000 a euro 25.000 a chiunque, avendo commesso o concorso a commettere un delitto impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa"

[76] R. Brighi – P. Sammario, *Cyberlaundering e Blockchain Forensics* In R. Brighi et al. *Nuove questioni di informatica forense*, ed. Aracne, Roma, 2022, p.197.

[77] Art. 648 bis, c.p.

[78] R. Brighi – P. Sammario, *Cyberlaundering e Blockchain Forensics* In R. Brighi et al. *Nuove questioni di informatica forense*, ed. Aracne, Roma, 2022, p.193.

wallet creati *ad hoc*, spesso tramite una moltitudine di transazioni, anche in criptovalute diverse. In questo modo risalire al proprietario del *wallet* finale è molto più complicato, se non impossibile.[79]

4. La normativa italiana e gli accordi internazionali

La diffusione dell'uso illecito delle criptovalute pone sfide impellenti al legislatore, in quanto l'orizzonte operativo della criminalità acquisisce nuovi e potenti strumenti per perpetrare reati, i quali possono essere arginati dalla magistratura soltanto attraverso innovative tecniche di indagine e non senza disporre di un'efficace base normativa. La questione pone diverse criticità, infatti, nonostante alcune contromisure siano già state introdotte, il quadro normativo non può ancora dirsi soddisfacente. Rilevante è stato l'intervento del nostro legislatore che, per primo in Europa, con il D.lgs. n.90 del 25 maggio 2017 ha anticipato la V direttiva antiriciclaggio europea del 2018[80]. Il suddetto decreto ridefinisce la precedente normativa (contenuta nel D.lgs. 231/2007) adeguandola agli sviluppi tecnologici e apportando notevoli interventi volti a rendere più trasparente la fornitura di servizi in questo ambito, ad esempio introducendo l'obbligo in capo ai fornitori di *wallet* di verificare adeguatamente l'identità della clientela, al pari degli istituti bancari, nonché l'onere di segnalazione di attività sospette all'UIF[81]. Il legislatore è intervenuto nuovamente nel 2021 con il d.lgs 195/2021, dando attuazione alla direttiva europea 2018/1673 in tema di lotta al riciclaggio[82], il quale però non ha introdotto una molto attesa previsione specifica per l'utilizzo delle criptomonete, privando l'ordinamento di "un'eventuale

[79] *Ibidem*.
[80] Direttiva 843/2018 del Parlamento e del Consiglio Europeo (https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32018L0843).
[81] "L'Unità di Informazione Finanziaria per l'Italia (UIF) è stata istituita presso la Banca d'Italia dal d.lgs. n. 231/2007, in conformità di regole e criteri internazionali che prevedono la presenza in ciascuno Stato di una Financial Intelligence Unit (FIU), dotata di piena autonomia operativa e gestionale, con funzioni di contrasto del riciclaggio e del finanziamento del terrorismo". Tratto dal sito istituzionale visitabile al link: https://uif.bancaditalia.it/
[82] D.lgs. 195/2021, *Attuazione della direttiva (UE) 2018/1673 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla lotta al riciclaggio mediante diritto penale*

esplicitazione [che] avrebbe sicuramente giovato al tasso di chiarezza dei precetti normativi"[83].

Il primo passo compiuto nel 2017 quindi, per quanto lodevole, si rivela tuttavia inefficace e limitato se rimane un intervento isolato ed il legislatore non interviene per aggiornarlo, integrarlo ed ampliarlo. Allo stesso modo la normativa nazionale e comunitaria si rivela insufficiente qualora i rei si affidino a operatori e circuiti internazionali che permettono loro di eludere la normativa europea operando in altre giurisdizioni, dove è possibile utilizzare portafogli digitali completamente anonimi. Oltretutto, per risultare operativi con un indirizzo IP straniero e aggirare l'obbligo di trasparenza, non è necessario cambiare stato fisicamente ma, come si è visto, è sufficiente utilizzare strumenti alla portata di tutti come TOR o VPN[84]. Si pone dunque come fondamentale il raggiungimento di accordi internazionali per arginare o quantomeno ostacolare il fenomeno a livello globale.

Nel corso degli ultimi decenni, grazie alla stipula di diversi trattati internazionali, sono state attuate alcune azioni di contrasto ai reati finanziari e di riciclaggio, si citano di seguito i più importanti:

1) il recepimento dell'accordo statunitense *FATCA* da parte del nostro paese, che nel 2015 sancì un processo di scambio di informazioni antifrode, per quanto limitata ai soli USA;

2) la direttiva europea 2376/2015, approvata nel 2017 con il D.lgs n.32, che impone lo scambio obbligatorio di informazioni nel settore fiscale tra gli stati membri;

3) il *Common Reporting Standard* varato dall'OCSE del 2017, che impone lo scambio obbligatorio di informazioni fiscali tra le amministrazioni finanziare con l'obiettivo di arginare l'evasione fiscale transnazionale[85].

[83] A. Gerbino, C*yberlaundering: una nuova frontiera del riciclaggio nella distributed economy,* in Ius in Itinere – rivista semestrale di diritto, 11/2022
[84] A. Anselmi*, Onion routing, cripto-valute e crimine organizzato,* Pacini giuridica, Pisa, 2019, pp. 6-13
[85] Si veda G. Reccia, *Il mercato delle valute virtuali* In P. Dal Checco et al*., op. cit.,* pp. 66-71 dove, oltre a questi trattati sopracitati sono esposte diverse normative interne di riferimento a livello mondiale

Altresì fondamentale è stata l'istituzione dello *European Cybercrime Centre (EC3)* nel 2013 da parte dell'Europol, un corpo operativo che si occupa di crimine informatico, ambito in cui ha raggiunto importanti risultati[86].

Queste misure sono state importanti ma, malgrado ciò, esse non sono sufficienti per un effettivo contrasto della fattispecie criminosa a livello internazionale, in particolar modo a fronte dell'abilità diffusa tra le organizzazioni criminali di sfruttare le giurisdizioni a esse più favorevoli.

[86] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

CONCLUSIONI

La problematica legata al *cybericiclaggio* non è insuperabile, tuttavia è importante sottolineare come l'attività di contrasto all'uso illecito delle criptovalute comporti inedite complicazioni e sfide, le quali sottopongono il legislatore, i magistrati, la polizia giudiziaria, i professionisti e la società civile ad una continua sollecitazione. Anche se non sono state affrontate in questo elaborato, si presentano molte altre problematiche operative collegate al tema della lotta al *cybericiclaggio*, tra cui le indagini, la *blockchain intelligence*, i sequestri, la gestione delle criptovalute e dei *wallet*[87].

Particolarmente importante, in questo contesto, risulta il ruolo dei professionisti, in quanto una mancanza di consapevolezza riguardo a questi temi e, soprattutto, circa la volatilità dei bitcoin, potrebbe condurre erroneamente a reputare un massiccio investimento in criptovalute al pari di altri investimenti finanziari, quando in realtà dovrebbe essere trattato come un possibile campanello d'allarme di comportamenti illeciti e, in determinate circostanze, andrebbe segnalato alle autorità competenti. Per questo motivo il ruolo di commercialisti, revisori, avvocati, bancari e consulenti finanziari, ossia di tutti coloro i quali hanno a che fare con la contabilità, l'analisi dei bilanci e la gestione degli investimenti, è centrale per arginare il fenomeno alla radice e supportare significativamente gli inquirenti, applicando una condotta deontologica collaborativa, così come già accade in altre circostanze di dubbia regolarità.

Infine, è interessante notare quanto, anche in questo particolare settore investigativo e giudiziario, incidano le stesse difficoltà che accomunano ampi settori dell'attività inquirente *tout court*: la scarsità di fondi, la mancanza di cooperazione internazionale, i vuoti normativi di alcuni Paesi che affossano processi, rogatorie ed estradizioni, la necessità costante di maggiori investimenti per aggiornare e incrementare personale ed attrezzature, l'urgenza di un'azione legislativa veloce ed efficace, la scarsa

[87] Si rimanda per una trattazione di questi temi al volume di P. Dal Checco et al., *Bitcoin Forensics e Intelligence sulla Blockchain*, ed. IISFA Educational, Roma, 2019.

consapevolezza del fenomeno e dei rischi da parte di professionisti e società civile.[88]

Investire nel contrasto al *cybericiclaggio* è dunque uno strumento importante per indebolire il potere economico della criminalità organizzata, che tramite esso riesce a reinvestire grandi capitali illeciti nell'economia legale. È perciò fondamentale che l'azione dello Stato sia repentina, incisiva, organica e che non sottovaluti i rischi arrecati dall'uso criminoso delle nuove tecnologie, le quali, è importante ricordare, non sono intrinsecamente nocive ma, come ogni strumento, si prestano all'uso che si sceglie di farne, qualunque esso sia.

[88] P.L. Toselli, *OSINT, Cryptoforensics e investigazioni nel Dark Web* in *Ciclo di seminari di "Informatica Forense" edizione 2021/22* a cura di R. Brighi et al.

BIBLIOGRAFIA

Accinni G. P., *Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017)*, in Archivio Penale, 2018/1

Anselmi A., *Onion routing, cripto-valute e crimine organizzato*, Pacini giuridica, Pisa, 2019.

Antonopoulos A.M., *Mastering Bitcoin : Programming the Open Blockchain,* Oreilly & Associates Inc, 2017.

Aranguena G., *Bitcoin: una sfida*, in «Diritto mercato tecnologia», gennaio/marzo 2014.

Bambara J.J.- Allen P.R., *Blockchain. A Practical Guide to Developing Business, Law, and Technology Solutions*, McGraw-Hill Education, New York, 2018.

Banca d'Italia*, Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività,* Roma, 2022.

Batini C., Pernici B., Santucci G. (a cura di), *Sistemi Informativi – Volume 5*. Franco Angeli, 2004.

Bernaschi M., Mastrastefano E., *Una descrizione (quasi) informatica del funzionamento di bitcoin*, EticaEconomia, 2014.

Bocchini R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in Diritto dell'Informazione e dell'Informatica (Il), fasc. 1, febbraio 2017.

Brighi R. e F. Di Tano, *Identità, anonimato e condotte antisociali in Rete. Riflessioni informatico-giuridiche* in Rivista di filosofia del diritto 1/2022.

Brighi R.–Sammario P., *Cyberlaundering e Blockchain Forensics* In R. Brighi et al. *Nuove questioni di informatica forense*, ed. Aracne, Roma, 2020.

Capaccioli S*., Riciclaggio, antiriciclaggio e bitcoin*, in Il fisco, n. 46/2014,

Croce M., *Cyberlaundering e valute virtuali. la lotta al riciclaggio nell'era della distributed economy*, in Sistema Penale, 4, 2021.

Dal Checco P. et al., *Bitcoin Forensics e Intelligence sulla Blockchain*, ed. IISFA Educational, Roma, 2019.

De Cubellis I., *Bitcoin come moneta a corso legale: il caso El Salvador.* Tesi di Laurea in Economia dei mercati e degli intermediari finanziari, Luiss, Guido Carli, relatore Francesco Cerri, A.A. 2021/2022.

Dell'Osso A.M., *Riciclaggio di proventi illeciti e sistema penale*, Giappichelli, Torino, 2017.

Di Vizio F., *Lo statuto giuridico delle valute virtuali: le discipline e i controlli, Tra oro digitale ed ircocervo indomito*, 2018.

Gerbino A., C*yberlaundering: una nuova frontiera del riciclaggio nella distributed economy,* in Ius in Itinere – rivista semestrale di diritto, 11/2022.

Gerlach J.C. –Demos G. – Sornette D., *Dissection of Bitcoin's multiscale bubble history from January 2012 to February 2018*, The Royal Society Open Science, 2019.

Languasco A.- Zaccagnini N., *Manuale di crittografia. Teoria, algoritmi, protocolli*, Ulrico Hoepli editore, Milano, 2015.

Leone F.- Parisella S., *La blockchain, il protocllo cryptonote e le criptovalute,* in *Bitcoin e criptovaulte* (a cura di) Razzante Ranieri 2018.

Lucev R. – Boncompagni F., *Criptovaluta e profili di rischio penale nell'attività degli exchanger*, in Giurisprudenza Penale, 2018.

Mancini M*., Valute Virtuali e Bitcoin*, in Analisi Giuridica dell'Economia, 1/2015, 1.

Nakamoto S., Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

Noether S., Mackenzie A., Monero Reserch Lab, *Ring Confidential Transaction*, 2016.

Passarelli N., *Bitcoin e antiriciclaggio*, in www.sicurezzanazionale.gov, 2016

Passaretta M., *Bitcoin: il Leading Case italiano,* in Banca Borsa Titoli di Credito, fasc.4, 2017.

Perri R. - Angela I.S.M., *Anonymity within the Bitcoin system. Tracking digital footprints: anonymity within the bitcoin system,* Research Paper, Emerald Publishing Limited, 2017.

Perugini M.L. – Maioli C., *Bitcoin tra moneta virtuale e commodity finanziaria*, 2014.

Picotti L., *Profili penali del Cyberlaundering: le nuove tecniche di riciclaggio* in *Rivista trimestrale di diritto penale dell'economia*, n. 3-4, 2018.

Plantamura V., *Cybericiclaggio* in C. Cadoppi et. al. *Cybercrime*, Utet giuridica, 2023.

Rapetto U., *Cyberlaundering – Il riciclaggio del terzo millennio, "Cyberlaundering 2000",* Università di Trento 1999.

Rossi Dal Pozzo F., *Il mercato unicio digitale europeo e il Regolamento UE sulla privacy* in Il diritto dell'Amministrazione Pubblica digitale, a cura di R. Cavallo Perin e D. Galetta, Giappichelli Editore, Torino, 2020.

Saglia L., *Soluzioni innovative alle debolezze di Bitcoin,* Politecnico di Torino, Corso di laurea magistrale in Ingegneria Informatica (Computer Engineering), 2022.

Sartor G*., L'informatica giuridica e le tecnologie dell'informazione*, giappichelli, Torino, 2016.

Sicignano G.J., *Bitcoin e riciclaggio,* Giappichelli Editore, Torino, 2019.

Sicignano G.J., *L'acquisto di bitcoin con denaro di provenienza illecita,* Archivio Penale 2020, n°2.

Sturzo L., *BITCOIN E RICICLAGGIO 2.0,* in Dir. pen. cont., fasc. 5/2018.

Toselli P.L., *OSINT, Cryptoforensics e investigazioni nel Dark Web* in *Ciclo di seminari di "Informatica Forense" edizione 2021/22* a cura di R. Brighi et al.

Turri M.G., *Le criptovalute. Monete private del capitalismo digitale*, Milano, Meltemi, 2020.

Vardi N., *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei bitcoin,* in Diritto dell'Informazione e dell'Informatica (Il), fasc. 3, 2015.

Zeno C., *BITCOIN: "La moneta virtuale: il trade off tra mezzo di scambio e asset finanziario",* LUISS, 2018.

Ziccardi G., *Crittografia e Diritto*, Giappichelli, Torino, 2003.

Zuboff S., *Il capitalismo della sorveglianza: il futuro dell'umanità nell'era dei nuovi poteri.* Luiss University press, 2019.