UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M. FANNO"

CORSO DI LAUREA IN ECONOMIA

PROVA FINALE

L'EVOLUZIONE DELLE CRIPTOVALUTE E IL LORO IMPIEGO IN TRANSAZIONI ILLECITE

RELATORE:

CH.MO PROF. ANTONIO PARBONETTI

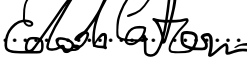
LAUREANDO: EDOARDO COSTENIERO

MATRICOLA N. 2034888

ANNO ACCADEMICO 2023 – 2024

Dichiaro di aver preso visione del "Regolamento antiplagio" approvato dal Consiglio del Dipartimento di Scienze Economiche e Aziendali e, consapevole delle conseguenze derivanti da dichiarazioni mendaci, dichiaro che il presente lavoro non è già stato sottoposto, in tutto o in parte, per il conseguimento di un titolo accademico in altre Università italiane o straniere. Dichiaro inoltre che tutte le fonti utilizzate per la realizzazione del presente lavoro, inclusi i materiali digitali, sono state correttamente citate nel corpo del testo e nella sezione 'Riferimenti bibliografici'.

I hereby declare that I have read and understood the "Anti-plagiarism rules and regulations" approved by the Council of the Department of Economics and Management and I am aware of the consequences of making false statements. I declare that this piece of work has not been previously submitted – either fully or partially – for fulfilling the requirements of an academic degree, whether in Italy or abroad. Furthermore, I declare that the references used for this work – including the digital materials – have been appropriately cited and acknowledged in the text and in the section 'References'.

Firma (signature) ……  ……

INDICE

INTRODUZIONE

La presente tesi ha l'obiettivo di analizzare e descrivere l'evoluzione delle criptovalute, concentrandosi sul loro impiego sia legale che illecito. Nel primo capitolo verranno esplorate le caratteristiche fondamentali delle criptovalute, la tecnologia blockchain su cui si basano e il loro sviluppo storico. Questo capitolo fornirà una panoramica dettagliata della natura decentralizzata delle criptovalute, della sicurezza garantita dalla crittografia, nonché dei vantaggi e delle sfide che queste valute comportano, inclusi i loro usi e impatti socioeconomici.

Il secondo capitolo si focalizza invece sull'utilizzo delle criptovalute in contesti di operazioni anomale e traffici illeciti. Verranno esaminate le normative vigenti a livello nazionale e internazionale per contrastare tali usi, analizzando come la natura delle criptovalute faciliti attività come il riciclaggio di denaro e il finanziamento del terrorismo. Inoltre, si discuteranno le tecniche di tracciamento e monitoraggio adottate per prevenire tali attività illecite, con particolare riferimento al quadro normativo italiano e alle linee guida dell'Unità di Informazione Finanziaria per l'Italia (UIF).

CAPITOLO 1

LE CRIPTOVALUTE

Il presente capitolo funge da base fondamentale fornendo una presentazione delle criptovalute, analizzando le loro caratteristiche principali, il funzionamento e l'evoluzione nel tempo. Viene descritta la *blockchain*, la tecnologia sottostante a queste valute virtuali, evidenziando come questo meccanismo sia estremamente differente dalle valute tradizionali. Inoltre, il capitolo offre una panoramica della storia delle criptovalute, seguendo le varie tappe della loro evoluzione e analizzando l'impatto socioeconomico che hanno avuto, sottolineandone vantaggi e svantaggi.

Le criptovalute sono valute digitali o virtuali utilizzate come mezzo di scambio che utilizzano la crittografia per garantire privacy e sicurezza nelle transazioni, controllare ogni movimentazione, creazione di nuove unità o trasferimento di assets. Il termine è costituito da due parole: cripto e valuta, e ciò rappresenta la loro natura nascosta per cui solo chi conosce un determinato codice informatico può accedere e utilizzarle. Le criptovalute lavorano su reti decentralizzate basate sulla tecnologia *blockchain* a differenza delle valute tradizionali emesse dai governi e dalle banche centrali (come dollaro o euro). Le criptovalute esistono unicamente in formato digitale e vengono scambiate solo per via telematica; non esiste dunque un formato fisico di carta o metallo.

1.1 Caratteristiche principali delle criptovalute

Le caratteristiche distintive delle criptovalute sono principalmente la decentralizzazione, la crittografia, la trasparenza, e l'immutabilità.

1.1.1 Decentralizzazione

La natura decentralizzata delle criptovalute è la caratteristica che le contraddistingue maggiormente dalle monete tradizionali. Esse, infatti, non sono gestite da un'autorità centrale, come un governo o una banca, ma operano su una rete *peer-to-peer*, ovvero tra due dispositivi direttamente senza necessità di intermediari. Questo significa che il controllo e la gestione della

rete sono distribuiti tra molti partecipanti, e nessuna singola entità dispone di un controllo totale. Le transazioni vengono validate dai nodi della rete, che sono computer o dispositivi collegati alla rete stessa, ciascuno dei quali possiede una copia del registro completo delle transazioni e partecipa al processo di verifica e convalida. Questo riduce il rischio di censura, manipolazione e interferenza da parte di entità centralizzate. Distribuendo il controllo tra molti partecipanti, le criptovalute offrono maggiore sicurezza, trasparenza e resilienza, rendendole un'opportunità innovativa e potente per il mondo digitale.

1.1.2 Crittografia

Le criptovalute utilizzano la tecnologia della crittografia per rendere le transazioni anonime e sicure senza il bisogno di un ente intermediario.
Partendo dalla definizione, la crittografia è la disciplina che si occupa della protezione e dello scambio di informazioni attraverso codici e dati cifrati tra due parti, consentendo solo al mittente e al destinatario di vederne il contenuto.
Esistono vari tipi di crittografia; quella impiegata per la sicurezza delle criptovalute è nota come crittografia asimmetrica o a chiave pubblica-privata. Questa tecnologia consente al mittente di criptare i dati tramite la chiave pubblica e al destinatario di decifrarli tramite la chiave privata. Ciascuna coppia di chiavi è unica e legata matematicamente da una funzione; solo chi possiede la chiave privata corrispondente alla chiave pubblica può accedere al messaggio criptato.
Il funzionamento di questo meccanismo prevede che ad ogni singolo utente venga assegnata la cosiddetta chiave privata, una password numerica molto complessa, a partire dalla quale viene generata tramite crittografia la chiave pubblica, più precisamente tramite la cosiddetta "funzione di hash" ossia un metodo di elaborazione di una serie di dati con un complesso algoritmo matematico. La chiave pubblica può essere condivisa con chiunque, invece quella privata deve essere mantenuta segreta.
Quando un utente vuole inviare un messaggio al proprietario delle chiavi, cifra il messaggio utilizzando la chiave pubblica del destinatario, il quale utilizzando la propria chiave privata potrà decrittare il messaggio e sarà l'unico a poterlo fare.

Per capire meglio il funzionamento della crittografia asimmetrica consideriamo il seguente esempio.
Due utenti A e B vogliono scambiarsi dei messaggi criptati. A vuole inviare un documento a B accertandosi che solo B possa leggerlo; A, quindi, cripta il messaggio con la chiave pubblica di B; B riceve il messaggio e riesce a decifrarlo utilizzando la sua chiave privata.

Figura 1.1: Crittografia Asimmetrica 1

[Fonte: Come funziona la crittografia asimmetrica, Criptoinvestire.com]

B dopo aver letto il messaggio vuole rispondere utilizzando lo stesso meccanismo di crittografia così da assicurarsi che solo A possa leggerne il contenuto; B, dunque, cripta il documento con la chiave pubblica di A che a sua volta, dopo aver ricevuto il messaggio, riesce a decifrarlo utilizzando la propria chiave privata.

Figura 1.2: Crittografia Asimmetrica 2

[Fonte: Come funziona la crittografia asimmetrica, Criptoinvestire.com]

1.1.3 Trasparenza

La trasparenza è una caratteristica distintiva, ma al tempo stesso controversa, delle criptovalute. Tutte le attività e le transazioni eseguite su una rete sono registrate in un registro pubblico accessibile a tutti, consentendo di tracciare ogni movimento e garantendo un elevato livello di trasparenza riguardo ai contenuti e agli oggetti delle transazioni, ma meno per quanto riguarda l'identità di chi le effettua. Questo meccanismo permette di verificare in qualsiasi momento l'origine e l'importo di ogni transazione, riducendo il rischio di frodi e creando un sistema economico più sicuro e affidabile, su cui sia le aziende sia i consumatori possono contare. Tuttavia, risulta spesso difficile identificare con precisione l'identità di chi effettua le transazioni, poiché la struttura crittografica delle criptovalute facilita l'anonimato. Pertanto, la trasparenza è un elemento chiave che rende le criptovalute uniche e le distingue dai sistemi finanziari tradizionali, in cui le transazioni avvengono tramite intermediari come banche o altre istituzioni finanziarie. Al contempo, però, è importante evidenziare che la struttura delle criptovalute rende pubblico e registrato quasi tutto, tranne l'informazione più cruciale: la vera identità di chi effettua le transazioni.

1.1.4 Immutabilità

La tecnologia alla base delle criptovalute rende estremamente complessa la modifica dei dati relativi alle transazioni una volta inseriti nella *blockchain*, conferendo così all'immutabilità il ruolo di caratteristica chiave. Infatti, una volta registrata una transazione, è impossibile alterarla o cancellarla dal database, garantendo un elevato livello di sicurezza e fiducia ed eliminando le possibilità di frodi o manipolazione dei dati. Questa peculiarità rende le criptovalute particolarmente efficienti per la registrazione di contratti, transazioni finanziarie delicate e dati sensibili, custodendoli in un ambiente sicuro e resistente.

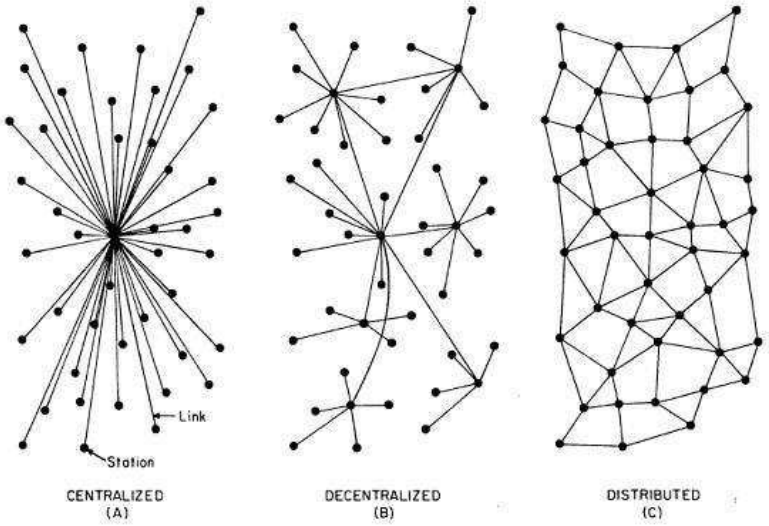
1.2 Blockchain

Alla base della maggior parte delle criptovalute c'è la tecnologia *blockchain*, un registro digitale distribuito in grado di memorizzare transazioni e dati in modo sicuro e permanente.

1.2.1 Cos'è la Blockchain?

La tecnologia *blockchain* rappresenta un sofisticato meccanismo di gestione dei dati che consente una condivisione trasparente delle informazioni tra i partecipanti di una rete. Un database basato su *blockchain* organizza i dati in blocchi concatenati, formando una sequenza ininterrotta e cronologicamente coerente. Questa struttura garantisce che i dati non possano essere eliminati o modificati senza il consenso della rete, assicurando così l'integrità delle informazioni. Pertanto, la *blockchain* può essere utilizzata per stabilire un registro contabile immutabile, ideale per il tracciamento di ordini, pagamenti, conti e altre transazioni. Inoltre, il sistema incorpora meccanismi di sicurezza integrati che impediscono l'inserimento di transazioni non autorizzate, garantendo una coerenza uniforme nella visualizzazione condivisa delle stesse.
Le fondamenta della tecnologia *Blockchain* partono dal concetto di *ledger*, ossia il libro mastro. La forma più semplificata del *ledger* è il *centralised ledger*, un sistema centralizzato dove le operazioni e le transazioni fanno riferimento a un'unica struttura centrale come una banca o un governo centrale che controlla e gestisce il contenuto del libro mastro. La seconda tipologia di organizzazione del *ledger* è il *decentralised ledger*, un sistema decentralizzato che prevede la ripetizione del precedente sistema centralizzato in più strutture di dimensione minore distribuite su tutta la rete. La struttura di *ledger* più evoluta è la *Distributed Legder*, una rete distribuita in cui non esistono più controlli centrali ma è basata sulla fiducia e il controllo dei singoli utenti. La *Blockchain* è basata sull'ultimo modello citato ossia il *Distributed ledger*.

Figura 1.3: Tipologie di *ledger*



[Fonte: Medium, 2017]

1.2.2 Componenti della blockchain

I componenti principali della *blockchain* sono:

- Blocchi: costituiscono l'insieme di una o più transazioni avvenute in un determinato periodo; l'unione di una serie di blocchi collegati in ordine cronologico costituisce la *blockchain.*

- Nodi: sono i dispositivi che partecipano alla rete e contengono una copia del registro; si tratta di nodi completi quando conservano una copia integrale della *blockchain* e nodi leggeri quando ne conservano solo una parte.

- Transazioni: costituiscono un insieme di dati e azioni che vengono registrati e sono gli oggetti di scambio.

- Hash: è un algoritmo matematico generato crittograficamente che funge da identificatore unico del blocco.

- Consenso: è l'algoritmo utilizzato dai diversi nodi per gestire la rete e concordare la creazione e l'aggiunta di nuovi blocchi alla catena; i due principali algoritmi sono il *Proof of Work* (PoW), in cui i partecipanti devono risolvere complessi problemi matematici per validare i nuovi blocchi, e il *Proof of Stake (PoS)*, in cui i coloro che validano l'aggiunta di nuovi blocchi sono scelti in base alla quantità di criptovalute possedute.

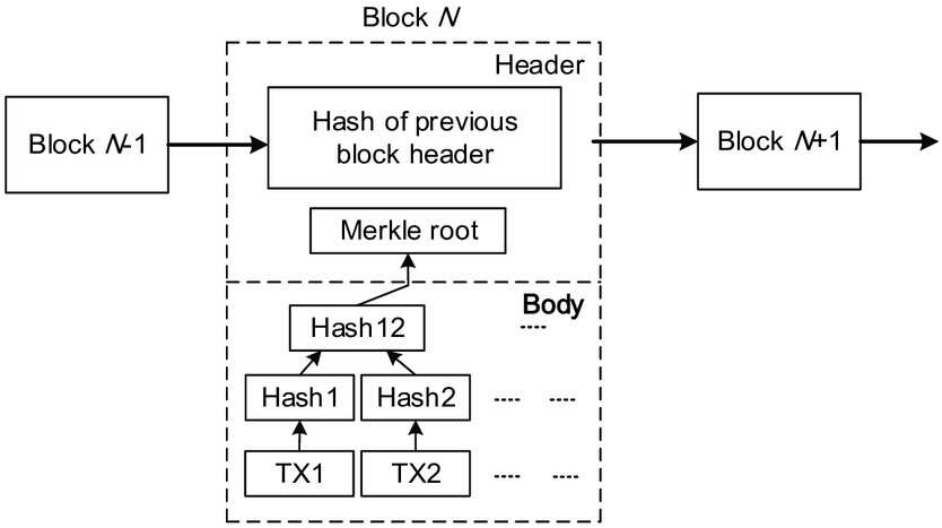
- Miners: sono i nodi che, dopo aver creato un nuovo blocco, gareggiano per cercare la soluzione della *Proof of Work*; in seguito, l'algoritmo del consenso PoW consente ai *miners* di convalidare il nuovo blocco e aggiungerlo alla *blockchain* solo se il resto dei nodi sono in accordo con la soluzione trovata.

L'insieme di tutte queste componenti collabora e lavora insieme per rendere la *blockchain* un sistema decentralizzato, sicuro e trasparente per le transazioni digitali.

1.2.3 Come funziona la Blockchain?

Quando due utenti della rete desiderano effettuare una transazione, si verifica il seguente processo. Tutte le transazioni rimangono in sospeso finché non vengono selezionate dai *miner*s, che le raggruppano e creano un nuovo blocco da aggiungere alla catena. Successivamente, al nuovo blocco deve essere associato il valore di *hash* del blocco precedente, come richiesto dal sistema. Una volta creato il blocco, il *miner* deve eseguire il *Proof of Work* cercando di risolvere un complesso calcolo matematico, la cui soluzione corrisponderà a una lunga stringa di numeri e cifre. Come ricompensa per gli sforzi compiuti per risolvere il problema matematico, il *miner* che giunge alla soluzione riceve delle criptovalute. Ottenuto questo risultato, il *miner* lo condivide con tutti gli altri nodi della rete, che verificano la legittimità della soluzione e la sua conformità ai requisiti del sistema. Quando tutti i partecipanti raggiungono il consenso, il nuovo blocco viene collegato alla catena in modo sicuro e non è più possibile modificarne i contenuti. Ogni nuovo blocco rafforza la verifica e la sicurezza del blocco precedente e dell'intera *blockchain*. Infine, il sistema distribuisce l'ultima copia del libro mastro a tutti i partecipanti della rete.

Figura 1.4: Funzionamento della blockchain



[Fonte: *Blockchain Structure*, ResearchGate]

1.2.4 I diversi usi della Blockchain

La tecnologia *blockchain* è impiegata per numerosi scopi differenti ed è applicata in svariati settori.

- Criptovalute: l'utilizzo predominante della *blockchain* riguarda le criptovalute; quando vengono acquistate, spese, trasferite o scambiate, ogni transazione viene registrata su una *blockchain.*

- Smart Contract: sono contratti ad esecuzione automatica che, quando sono rispettate determinate condizioni, entrano istantaneamente in vigore senza necessità di intermediari.

- Voto elettronico: la *blockchain* permette il funzionamento di un sistema di votazione sicuro, veloce e trasparente.

- Servizi bancari e finanziari: la *blockchain* viene utilizzata per numerose transazioni bancarie rendendo il trasferimento di denaro molto più rapido e flessibile.

- Trasferimento di asset: la tecnologia *blockchain* viene spesso utilizzata per registrare e trasferire la proprietà di asset, sia digitali che fisici, come immobili, veicoli e opere d'arte.

Questo processo diventa così molto più veloce e immediato, eliminando la necessità di pratiche manuali.

- Gestione dei dati sanitari: tramite la *blockchain* è possibile conservare dati medici e altri dati sensibili in maniera sicura, migliorando la privacy e la sicurezza dei pazienti.

- Giochi e intrattenimento: questa tecnologia viene spesso utilizzata per creare asset digitali, come gli NFT, che vengono utilizzati in giochi, programmi o altri contenuti creativi.

1.2.5 Vantaggi e svantaggi della blockchain

I principali vantaggi dati dalla *blockchain* sono:

- Riduzione degli errori: tramite questa tecnologia il margine di errore nelle transazioni digitali viene ridotto drasticamente in quanto ogni attività deve essere verificata in più fasi e da più nodi in tutta la rete; essendo tutto tracciato e registrato è impossibile che qualche errore o anomalia non venga rilevato.

- Sicurezza: grazie alla struttura decentralizzata, la *blockchain* è estremamente sicura ed è praticamente impossibile immettere transazioni fraudolente o falsificate nel database in quando sarebbe necessario hackerare tutti i nodi e manipolare tutti i registri dell'intera rete.

- Velocità: il funzionamento moderno della *blockchain* consente di essere attiva 24 ore su 24, 7 giorni su 7, e su scala internazionale, così da garantire un servizio sempre efficiente ed estremamente rapido che elimina i tempi di attesa che normalmente sono previsti da banche o intermediari pubblici che devono confermare e verificare ogni attività manualmente.

I principali svantaggi dati dalla *blockchain* sono:

- Costi energetici: la *blockchain* consuma un enorme quantità di energia, principalmente a causa del processo di *mining* che chiede una potenza di calcolo significativamente maggiore rispetto a un singolo database o foglio di calcolo; il funzionamento della *blockchain*

comporta dunque un impatto molto negativo sull'ambiente a causa delle ingenti emissioni di anidride carbonica

- Complessità tecnica: essendo la *blockchain* un meccanismo molto elaborato che richiede la conoscenza di concetti complessi come crittografia e algoritmi matematici, non è accessibile ad aziende ed individui che non dispongono di un'adeguata formazione tecnica e teorica.

- Rischio di attività illegali: essendo un sistema altamente protetto e sicuro, la *blockchain* è spesso utilizzata per svolgere attività e traffici illeciti. Viene sfruttata l'elevata privacy e riservatezza del database per evitare intercettazioni e tracciamenti.

1.3 Storia delle criptovalute

Le criptovalute hanno colpito e trasformato il mondo finanziario sin dalla loro nascita. Nate dall'idea di un sistema decentralizzato che potesse autonomamente governare e gestire le transazioni digitali, le criptovalute si sono evolute nel tempo influenzando pian piano tutti i settori del mercato globale. In questo sottocapitolo verranno ripercorse le varie tappe dell'evoluzione delle criptovalute a partire dalla nascita di Bitcoin fino ad oggi.

1.3.1 L'idea di criptovaluta

Bitcoin è riconosciuta come la prima criptovaluta ad essere creata e inserita nel mercato. Tuttavia, l'idea di queste monete virtuali è nata molto prima, e molti progetti precedenti, che hanno fallito, hanno successivamente portato alla sua creazione.
David Chaum è riconosciuto dalla maggior parte degli studiosi come una figura cruciale nello sviluppo primitivo delle criptovalute. Con il suo paper intitolato "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups[1]", pubblicato nel 1982, gettò le prime basi per lo sviluppo della blockchain. Chaum fu il primo a elaborare e dimostrare la possibilità di scambiare token digitali in modo veloce e sicuro tramite la crittografia, senza il bisogno di un'autorità centrale.

[1] Chaum, D., 1982. *Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups.* Ph.D. Dissertation, University of California, Berkeley.

In seguito, Chaum creò una valuta digitale chiamata "eCash", in cui cercò di applicare i suoi studi e le sue teorie in maniera pratica. Tuttavia, il progetto esaurì i fondi e non ebbe una notevole diffusione. Nonostante ciò, fu di esempio e ispirazione per molti sviluppatori che negli anni seguenti tentarono di creare token digitali capaci di funzionare e di imitare la stabilità del prezzo dell'oro.

1.3.2 La nascita e lo sviluppo di Bitcoin (2008-2010)

Bitcoin è nato durante la crisi finanziaria del 2008. In quell'anno, Satoshi Nakamoto pubblicò il famoso *whitepaper* "Bitcoin: A Peer-to-Peer Electronic Cash System[2]".
Satoshi Nakamoto rimane tutt'oggi uno dei più grandi misteri nel panorama delle criptovalute in quanto non venne mai identificata questa figura e collegata ad una persona o ad un'organizzazione specifica. Secondo molti esperti, colui che creò Bitcoin decise di rimanere anonimo così da non influenzare e contaminare il successo della sua invenzione.
In questo documento venne presentato il Bitcoin come una nuova valuta digitale basata sul meccanismo *peer-to-peer* e sul meccanismo di consenso *proof-of-work*.
All'inizio del 2009 Bitcoin divenne per la prima volta disponibile al pubblico quando Satoshi Nakamoto pubblicò i primi 50 Bitcoin, dando inizio alla pratica del *mining* di criptovalute. In quel periodo solo programmatori ed appassionati del settore vennero a conoscenza e si interessarono a questa nuova tecnologia che nell'arco di pochi anni divenne considerata rivoluzionaria.
Nel primo anno di diffusione, il Bitcoin non aveva un valore economico chiaro. Una delle prime transazioni celebri fu l'acquisto di 10.000 bitcoin per soli 50 dollari da parte di Gavin Andresen, uno degli sviluppatori. Un altro evento significativo di questo periodo fu l'acquisto di due pizze al prezzo di 10.000 bitcoin da parte di Laszlo Hanyecz, un altro sviluppatore; il valore di quelle due pizze sarebbe stato, qualche anno dopo, durante il picco massimo di Bitcoin, di 600 milioni di dollari.

[2] Nakamoto, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Figura 1.5: L’evoluzione del prezzo di Bitcoin negli anni

[Fonte: SoFi, 2023]

1.3.3 La crescita del mercato delle criptovalute (2010-2014)

Tra il 2010 e il 2014, il mercato delle criptovalute ha conosciuto una crescita esponenziale, specialmente dopo che Forbes ha parlato di Bitcoin in un articolo nel 2011[3].

Con la diffusione e il successo iniziale di Bitcoin, sono emerse molte nuove valute elettroniche, chiamate "*altcoin*" in quanto alternative a Bitcoin. La maggior parte di queste nuove valute offriva miglioramenti tecnici rispetto a Bitcoin, e la più celebre di quel periodo fu Litecoin.

La crescita esplosiva di Bitcoin e delle valute digitali continuò negli anni seguenti, attirando sempre più l'attenzione dei media, degli investitori e degli appassionati. Entro la fine del 2013, Bitcoin raggiunse un traguardo significativo in termini di valore, passando da pochi centesimi a 1.000 dollari.

La principale piattaforma di scambio di criptovalute in quegli anni era Mt. Gox, che, nel periodo di massima popolarità, subì numerose violazioni della sicurezza e attacchi hacker, portando al furto di 850.000 Bitcoin e causando ingenti danni e perdite per molti utenti.

---

[3] Greenberg, A., May 2011. *Crypto Currency*, Forbes.

A seguito di questi attacchi hacker e della diffusione di molte piattaforme illegali per lo scambio di Bitcoin, come Silk Road, il mondo delle valute digitali subì molte critiche e un generale danno d'immagine. La struttura anonima e decentralizzata delle criptovalute rendeva impossibile il tracciamento di queste movimentazioni illegali e degli attacchi alla sicurezza.
Nonostante questi ostacoli, il periodo 2010-2014 ha gettato le basi per il successivo sviluppo del mercato delle criptovalute, dimostrando il potenziale rivoluzionario della tecnologia *blockchain*.

1.3.4 La rivoluzione di Ethereum e gli smart contract

Nel 2015 venne lanciata Ethereum, la prima valuta virtuale aggiornata e innovativa dopo Bitcoin.
Questo fu il primo e vero progetto con ambizioni differenti rispetto a tutte le precedenti *altcoin*. Ethereum ha introdotto una nuova dimensione: gli *smart contract*, i cosiddetti "contratti intelligenti". Questa tecnologia ha consentito lo sviluppo di applicazioni decentralizzate complesse ampliando notevolmente le possibilità di utilizzo della *blockchain*, oltre alle semplici transazioni finanziarie. Le innovazioni portate da Etehreum comportarono una rapida ascesa della nuova valuta che diventò così la seconda criptovaluta più grande al mondo.

1.3.5 L'ascesa della popolarità della criptovalute

Tra il 2017 e il 2018, il prezzo del Bitcoin è aumentato vertiginosamente, passando prima a 10.000 dollari e poi a 20.000 dollari, grazie alla diffusione di numerose piattaforme di exchange e trading che hanno reso l'accesso al pubblico molto più semplice. Tuttavia, questo aumento è stato seguito da un forte calo caratterizzato anche da significative discussioni tra gli sviluppatori.
Nel frattempo, Ethereum ha continuato a crescere, portando la nascita degli NFT e lo sviluppo di progetti DeFi[4] come exchange decentralizzati.
Nel 2020, dopo un periodo di calo e stagnazione, il mercato delle criptovalute ha ripreso slancio. Il Bitcoin ha raggiunto un valore di 70.000 dollari, supportato dall'adozione da parte di grandi multinazionali come Tesla. Successivamente, il mercato ha vissuto notevoli turbolenze a causa

[4] DeFi: "*Decentralized Finance*", si riferisce a sistemi e applicazioni di finanza decentralizzata basati sulla tecnologia *blockchain.*

di gravi fattori macroeconomici e del crollo di alcune *stablecoin*[5], che hanno nuovamente bloccato la crescita del settore.
Successivamente, il mercato delle criptovalute ha ritrovato un equilibrio, continuando la sua ascesa e diffusione in numerosi settori come il gioco d'azzardo, i videogiochi, lo sport e la finanza. Con la continua digitalizzazione del mondo, le criptovalute rivestono oggi un ruolo fondamentale nella semplificazione di molte attività e nello sviluppo di nuovi prodotti, rappresentando un possibile futuro del denaro.

1.4 Le principali criptovalute

Ad oggi le criptovalute più rilevanti e più diffuse sono le seguenti:

- Bitcoin (BTC): Bitcoin è la prima criptovaluta creata al mondo, lanciata nel 2009 e ancora oggi rimane la più celebre. Funziona su una *blockchain* propria, con le transazioni validate da una rete decentralizzata di *miner* e il meccanismo di consenso *Proof of Work* (PoW). Viene utilizzata principalmente come metodo di pagamento e come riserva di valore. Ad aprile 2024, Bitcoin vantava una capitalizzazione di mercato di 1,31 trilioni di USD.

- Ether (ETH): Ether venne lanciata nel 2015 da Vitalik Buterin ed è la criptovaluta nativa della *blockchain* Ethereum. Anch'essa pera su una *blockchain* propria ma senza un limite massimo di emissione (a differenza di Bitcoin che ha fissato il limite massimo di offerta a 21 milioni di bitcoin) permettendo la creazione teoricamente infinita di monete. Questa moneta è caratterizzata principalmente dall'innovazione degli *smart contract*, dalle applicazioni decentralizzate (dApps) e da un'ampia comunità di sviluppatori.

- Binance Coin (BNB): Binance Coin è la criptovaluta nativa dell'Exchange Binance, il più grande exchange al mondo dal 2024. Venne lanciata nel 2017 da Changpeng Zhao. Gli utenti di Binance possono usufruire di commissioni ridotte quando pagano in BNB, incentivando così l'adozione della moneta. Per mantenere il valore di BNB stabile, Binance periodicamente "brucia" una percentuale delle monete in circolazione.

- Tether (USDT): Tether è una *stablecoin*, progettata per mantenere un valore stabile agganciato a un asset esterno, in questo caso il dollaro statunitense. Venne lanciata nel 2014

[5] Stablecoin: criptovalute ancorate ad un asset stabile come il dollaro o l'euro

da tre fondatori statunitensi. Ogni USDT è teoricamente supportato da un dollaro USA, riducendo la volatilità tipica delle altre criptovalute.

- Solana (SOL): SOL è la criptovaluta nativa della piattaforma Solana, che anch'essa utilizza una *blockchain* propria. Venne fondata nel 2020 da Anatoly Yakovenko. Solana è nota per la sua capacità di eseguire fino a 50.000 transazioni al secondo e per questo molto utilizzata nel mondo del trading online. Le caratteristiche principali di questa criptovaluta sono l'elevata velocità delle transazioni e i bassi costi.

- XRP (XRP): XRP opera sulla rete Ripple ed è spesso definita la "criptovaluta delle banche" poiché è stata progettata per soddisfare specifiche esigenze del settore finanziario. Utilizza un algoritmo di consenso unico differente dai canonici *Proof of Work* (PoW) *o Proof of Stake* (PoS). È stata programmata per garantire trasferimenti di denaro in tempo reale, a livello internazionale e con bassi costi di commissione.

- Cardano (ADA): ADA è la criptovaluta della blockchain Cardano, soprannominata "criptovaluta di terza generazione". Venne fondata nel 2017 da Charles Hoskinson. Cardano divide la propria *blockchain* in due livelli distinti per migliorare la velocità delle transazioni. Questa piattaforma è basata principalmente su ricerca accademica a e revisione tra pari e sul meccanismo di consenso *Proof of Stake* (PoS). Ha uno sviluppo più lento rispetto ad altre piattaforme a causa della progettazione scientifica e accurata che sta alla base del meccanismo.

- USD Coin (USDC): USD Coin è una *stablecoin* ancorata al dollaro statunitense, simile a Tether, ma con una maggiore trasparenza finanziaria e processi di audit migliorati. Viene mantenuto il valore stabile di 1USD per 1 USDC. Lanciata nel 2018, USDC mira a ridurre i rischi associati alle criptovalute, permettendo agli utenti di ritirare i loro fondi digitali in cambio di contanti equivalenti in qualsiasi momento. Viene utilizzata molto nel trading e nelle applicazioni DeFi per la sua stabilità, trasparenza e affidabilità, nonostante i potenziali rischi derivanti dalla regolamentazione attorno al dollaro statunitense a cui è ancorata.

- Aave (AAVE): Aave è una piattaforma decentralizzata che opera sulla *blockchain* di Ethereum utilizzando *smart contracts* per facilitare prestiti e finanziamenti in criptovalute. La piattaforma consente agli utenti di guadagnare interessi sui depositi e di prendere in prestito asset, richiedendo un deposito superiore al valore del prestito. Il token nativo,

AAVE, viene utilizzato per la governance della piattaforma e la riduzione delle commissioni, contribuendo alla sicurezza e alla partecipazione degli utenti.

CAPITOLO 2

L'UTILIZZO DELLE CRIPTOVALUTE IN AMBITO DI OPERAZIONI ANOMALE

Nel capitolo secondo viene analizzato, nello specifico, l'utilizzo delle criptovalute in ambito di operazioni anomale e traffici illeciti in relazione a quanto previsto dai regolamenti e dall'unità di informazione finanziaria della Banca d'Italia. Vengono presentate le varie normative nazionali e internazionali che vigilano in questo ambito, le diverse operazioni illegali che si riscontrano maggiormente e le tecniche di analisi e tracciamento utilizzate per limitarle.

L'approfondimento presentato in questa tesi si basa principalmente su quanto previsto dall'Unità di Informazione Finanziaria per l'Italia (UIF).

Il documento intitolato "Utilizzo anomalo di valute virtuali[6]", redatto dall'Unità di Informazione Finanziaria per l'Italia, affronta il crescente fenomeno delle valute virtuali, con particolare riferimento ai rischi connessi al loro utilizzo anomalo. Le valute virtuali stanno guadagnando popolarità come mezzi di scambio volontari per l'acquisto di beni e servizi, sebbene non siano riconosciute come moneta legale. Esse vengono utilizzate principalmente nel commercio elettronico e nelle attività di gioco online. Tuttavia, l'utilizzo di queste valute può esporre a significativi rischi di riciclaggio di denaro e finanziamento del terrorismo. Tali preoccupazioni sono evidenziate da istituzioni internazionali ed europee, tra cui il Gruppo d'Azione Finanziaria Internazionale (FATF), l'Autorità Bancaria Europea (EBA) e la Banca Centrale Europea (ECB).

Le operazioni con valute virtuali si svolgono prevalentemente online tra soggetti di diversi stati, inclusi paesi o territori a rischio. L'anonimato di chi opera in rete e dei beneficiari delle transazioni complica ulteriormente l'identificazione di tali soggetti. Inoltre, i fornitori di servizi legati all'uso, scambio e conservazione delle valute virtuali non sono soggetti alle normative antiriciclaggio, esentandoli dall'obbligo di verifica della clientela, registrazione dei dati e segnalazione delle operazioni sospette. Questo scenario può favorire comportamenti illeciti e ostacolare le attività di prevenzione.

Durante il 2014, l'Unità di Informazione Finanziaria ha ricevuto segnalazioni di operazioni sospette legate ad acquisti o vendite di valute virtuali. Tali operazioni erano considerate opache per vari motivi, tra cui il profilo soggettivo del cliente, la natura delle controparti spesso estere,

[6] Unità di Informazione Finanziaria per l'Italia, 2023. Utilizzo anomalo di valute virtuali. *Banca d'Italia*.

e le modalità di esecuzione delle operazioni, come l'uso di contante o carte di pagamento prepagate.

Per prevenire l'uso delle criptovalute a fini di riciclaggio e finanziamento del terrorismo, il decreto legislativo 231/2007[7] impone agli intermediari finanziari e agli operatori di gioco di prestare particolare attenzione alle operazioni connesse alle valute virtuali. Devono essere valutati con attenzione i prelievi e versamenti di contante, le movimentazioni di carte di pagamento e le operazioni di acquisto e vendita di valute virtuali, specialmente se realizzate in breve tempo e per importi significativi. Le operazioni sospette devono essere segnalate tempestivamente all'Unità di Informazione Finanziaria, specificando il fenomeno nella sezione apposita della segnalazione.

Infine, è essenziale che i soggetti obbligati alla segnalazione sensibilizzino il proprio personale e i collaboratori, fornendo indicazioni operative adeguate alla valutazione delle operazioni sospette, contribuendo così alla collaborazione attiva nel contrasto di queste movimentazioni illegali.

2.1 Regolamentazione delle Criptovalute

La regolamentazione del mercato delle criptovalute è un tema di crescente rilevanza sia a livello nazionale che internazionale, dato l'uso crescente di questo settore per il finanziamento di attività illecite come il riciclaggio di denaro, il finanziamento del terrorismo e il traffico di droga e armi. Le normative volte a regolamentare e prevenire tali operazioni anomale sono sempre più rigide e applicate sia a livello europeo che globale.

2.1.1 Regolamentazione delle Criptovalute in Italia

L'Italia si è dimostrata uno dei paesi più attivi e attenti in termini di regolamentazione e tutela del mercato delle criptovalute.

[7] Decreto Legislativo 21 novembre 2007, n. 231: Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione.

In Italia, la regolamentazione in materia di *crypto-assets* è stata anticipata con il Decreto Legislativo n.90/2017[8], che ha modificato il D.lgs. 231/2007 in linea con la V Direttiva Antiriciclaggio dell'UE.
Questo decreto introduce nuove misure per prevenire le più frequenti operazioni illecite, tra cui il riciclaggio di denaro e il finanziamento del terrorismo.
I principali obblighi e direttive imposti da questo decreto sono:

- Obblighi di identificazione (KYC[9]): il decreto prevede un ampliamento degli obblighi per gli intermedi finanziari, per le banche e i professionisti, al fine di verificare e identificare l'identità degli utenti prima di avviare qualsiasi transazione o movimentazione.

- Registro degli operatori: è stato introdotto l'obbligo di registrazione presso l'Organismo degli Agenti e dei Mediatori (OAM) per gli operatori che offrono servizi in ambito di criptovalute e portafogli digitali.

- Segnalazioni: è stato previsto un rafforzamento degli obblighi di segnalazione di movimentazioni o transazioni sospette all'Unità di Informazione Finanziaria (UIF).

- Valutazione del Rischio: è stato rafforzato l'obbligo per gli enti soggetti alla normativa di eseguire valutazioni del rischio di riciclaggio o finanziamento al terrorismo e applicare consone misure di prevenzione.

- Sanzioni: sono state introdotte sanzioni più severe per la violazione degli obblighi antiriciclaggio, con vari gradi di penalità in base alla gravità del caso.

- Formazione: il decreto prevede un aumento degli obblighi per gli enti interessati in termini di formazione e informazione dei dipendenti sulle misure di prevenzione.

[8] Decreto Legislativo 25 maggio 2017, n. 90: Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006. (17G00104).

[9] KYC: "Know Your Customer", procedimento utilizzato per verificare l'identità del cliente

Oltre al D.lgs. 90/2017, svolge un ruolo fondamentale nella regolamentazione del mercato della criptovalute in Italia, la Consob.
La Consob è la Commissione Nazionale per le Società e la Borsa e svolge un ruolo chiave nella regolamentazione delle valute digitali con l'obiettivo di custodire un ambiente trasparente e sicuro per gli investitori.
Ha avuto grande importanza l'iniziativa della Consob che nel gennaio 2020 ha pubblicato un articolo titolato "Offerte iniziali e gli scambi di cripto attività[10] ". In questo rapporto viene proposto un nuovo quadro normativo per le *Initial coin offerings* (ICO) e per gli scambi di *crypto-assets*.

La Consob ha definito che la qualificazione giuridica delle criptovalute deve seguire la seguente classificazione: *security tokens*, *payment tokens* e *utility tokens*; ogni categoria è soggetta a normative e regolamenti differenti in base alle diverse caratteristiche e utilizzi.

- Security tokens: sono criptovalute utilizzate come strumenti finanziari e sono soggette alle stesse normative che regolano i titoli finanziari tradizionali; rappresentano una partecipazione in un'azienda, un diritto a ricevere interessi o dividendi su un asset sottostante come una società, un immobile o altri flussi di entrate finanziarie. I *security tokens* sono tenuti al rispetto di stretti requisiti di *disclosure* e trasparenza come previsto per i titoli finanziari ai sensi della Direttiva sui Mercati degli Strumenti Finanziari (MiFID II). Oltre alla direttiva appena citata, i *security tokens* sono soggetti alle normative antiriciclaggio e di identificazione del cliente (AML/KYC).

- Payment tokens: sono criptovalute utilizzate come mezzo di pagamento per l'acquisto di beni o servizi; a differenza dei *security tokens*, non rappresentano un diritto agli utili o alla governance di un'impresa. Questa categoria di criptovalute è soggetta alla Direttiva sui Servizi di Pagamento (PSD2)[11] e alle normative AML/KYC.

- Utility tokens: sono criptovalute che forniscono l'accesso ad un servizio o un prodotto specifico all'interno di una *blockchain*; non sono progettati per essere usati come mezzo di scambio e non rappresentano una partecipazione ad un'impresa o un diritto agli utili.

[10] Consob, 2020. *Rapporto finale su "Le offerte iniziali e gli scambi di cripto-attività"*.
[11] Direttiva (UE) 2015/2366 del Parlamento Europeo e del Consiglio relativa ai servizi di pagamento nel mercato interno.

Avendo una funzionalità meno soggetta al rischio, gli *utility tokens* sono regolati da normative meno rigide e stringenti rispetto alle precedenti categorie.

Questa classificazione da parte della Consob mira ad aumentare la sicurezza nel mercato delle criptovalute garantendo maggior trasparenza agli investitori e assicurando che ciascuna tipologia di token sia regolata da appropriate normative in base alle diverse caratteristiche e funzionalità.

Oltre alla Banca d'Italia e alla Consob, il Ministero dell'Economia e delle Finanze (MEF) svolge un ruolo fondamentale nella regolamentazione del settore delle criptovalute in Italia. Gli obiettivi sono garantire sicurezza e legalità, prevenire operazioni illecite, assicurare trasparenza fiscale registrando e tassando adeguatamente ogni transazione, promuovere l'innovazione e lo sviluppo del settore.

2.1.2 Regolamentazione delle criptovalute in Europa

L'Unione Europea (UE) ha adottato un approccio proattivo per la regolamentazione del mercato delle criptovalute cercando di introdurre delle normative mirate alla stabilità finanziaria, all'innovazione del settore, alla protezione degli investitori e alla prevenzione da operazioni illegali.
La regolamentazione degli stati membri dell'UE in termini di criptovalute si basa sul regolamento MiCA[12], che offre un quadro normativo generale sulle regole da rispettare al fine di mantenere un ecosistema sicuro, trasparente e volto all'innovazione tecnologica.
Il regolamento MiCA, proposto alla Commissione Europea nel 2020, entra definitivamente in vigore nel 2024, diventando l'iniziativa più significativa e concreta al fine di gestire e regolamentare il settore delle criptovalute.

Il MiCA è costituito da 126 articoli dedicati all'emissione e all'offerta al pubblico delle criptovalute e si basa sui seguenti punti chiave:

[12] Regolamento (UE) 2023/1114 relativo ai mercati delle cripto-attività (MiCA)

- Autorizzazioni e Requisiti di Licenza: le imprese che offrono servizi in ambito di cripto-attività devono ottenere una licenza ufficiale per poter operare all'interno dell'UE; in questo modo solo utenti registrati e con licenza possono operare nel mercato.

- Definizioni: questo regolamento definisce le varie categorie di cripto-attività al fine avere delle normative specifiche per ogni diverso asset digitale. La nuova classificazione predisposta dalla MiCA vede tre categorie di *crypto-assets*: i token di moneta elettronica (EMT), i token collegati ad attività (AMT) e i token residuali.

- Protezione dei Consumatori: proteggere i consumatori dai rischi di questo settore è uno tra gli obiettivi fondamentali del MiCA che propone varie disposizioni per la trasparenza delle informazioni, pratiche di marketing e procedure per gestione di problematiche e reclami.

- Trasparenza: il MiCA impone obblighi di trasparenza per cui gli emittenti di cripto-attività devono fornire un *whitepaper* preciso e dettagliato. Questo documento contiene tutte le informazioni necessarie sul progetto, inclusi i dati rilevanti e i rischi associati all'asset emesso. Il *whitepaper* deve inoltre fornire informazioni sui meccanismi di sicurezza, le strategie di governance e l'utilizzo del progetto, rendendo più facile la comprensione e la valutazione dell'investimento per gli investitori, oltre a facilitare la prevenzione di potenziali rischi.

Il regolamento MiCA si rivolge principalmente alle criptovalute diverse dagli strumenti finanziari, come *utility tokens* e *monetary tokens*. L'obiettivo di questo regolamento è colmare una lacuna legislativa nel sistema dell'UE, garantendo l'integrazione di questi nuovi strumenti digitali nel quadro di regolamentazione finanziaria e di gestione dei rischi per le imprese attive nell'UE. Questo era necessario poiché, prima del regolamento, la situazione normativa europea era molto frammentata e ogni paese adottava le proprie leggi e restrizioni, rendendo difficile una coesione generale tra i diversi stati.
Le opinioni della community riguardo all'applicazione di questa normativa sono generalmente positive, ad eccezione di alcuni critici del settore che vedono il regolamento come un ostacolo per l'evoluzione del mercato, portando effetti negativi. Queste restrizioni potrebbero rallentare e complicare alcune transazioni tra wallet di exchange o prelievi di grandi somme di cripto che prima avvenivano in maniera immediata.

Oltre al MiCA, un altro elemento fondamentale del quadro normativo dell'UE è il Quinto Pacchetto Antiriciclaggio (5AMLD)[13]. Emanata nel 2018, la Quinta Direttiva Antiriciclaggio rappresenta un significativo avanzamento nella lotta contro il riciclaggio di denaro e il finanziamento del terrorismo. Una delle principali novità è l'accesso pubblico ai registri di trasparenza, permettendo a chiunque di ottenere informazioni sui beneficiari effettivi delle entità registrate.

La direttiva estende l'obbligo di conformità a nuove categorie di soggetti, come i fornitori di servizi di portafoglio elettronico e di cambio di valute virtuali, i commercianti d'arte, gli agenti immobiliari per affitti superiori a 10.000 euro mensili e i consulenti fiscali. Questi soggetti devono ora registrarsi e verificare l'iscrizione al registro di trasparenza, segnalando eventuali discrepanze. Inoltre, la creazione di una piattaforma europea che interconnette i registri di trasparenza nazionali facilita lo scambio di informazioni a livello continentale.

La 5AMLD impone ulteriori obblighi per le transazioni con paesi esteri ad alto rischio, richiedendo informazioni aggiuntive sui partner commerciali e i beneficiari effettivi. Una delle innovazioni chiave è l'obbligo per tutti gli Stati membri dell'UE di mantenere registri centrali con informazioni precise e aggiornate sui titolari effettivi delle società o altre entità giuridiche; questi registri devono essere accessibili alle autorità competenti e alle unità di informazione finanziaria.

L'implementazione della 5AMLD comporta un aumento degli adempimenti burocratici per le imprese, che devono adeguarsi alle nuove norme per evitare sanzioni. È cruciale per le aziende monitorare attentamente gli sviluppi legislativi e adottare misure appropriate per proteggere i propri interessi. La maggiore trasparenza e i nuovi obblighi mirano a prevenire l'occultamento di attività criminali dietro strutture societarie complesse e a migliorare la cooperazione internazionale nella lotta contro il riciclaggio di denaro e il finanziamento del terrorismo.

In sintesi, la Quinta Direttiva Antiriciclaggio rafforza il quadro normativo esistente, ampliando la portata delle misure preventive e incrementando la trasparenza delle transazioni finanziarie. Le imprese devono conformarsi ai nuovi obblighi e prestare attenzione agli aggiornamenti legislativi per garantire una piena aderenza alle normative.

[13] Direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio, del 30 maggio 2018, che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE (Testo rilevante ai fini del SEE).

2.1.3 Regolamentazione delle criptovalute negli Stati Uniti

Gli Stati Uniti hanno adottato un approccio normativo frammentato per il mercato delle criptovalute, affidando la regolamentazione a diverse agenzie come la Securities and Exchange Commission (SEC), la Financial Crimes Enforcement Network (FinCEN) e la Commodity Futures Trading Commission (CFTC), ognuna con un ruolo specifico.

La SEC governa i mercati dei titoli finanziari negli Stati Uniti e ha un ruolo fondamentale nella regolamentazione delle criptovalute, in particolare riguardo alle *Initial Coin Offerings* (ICO). La SEC considera molte criptovalute come titoli finanziari e quindi soggette alle normative del "Securities Act[14]" del 1933 e del "Securities Exchange Act[15]" del 1934. Ha intrapreso numerose azioni contro emittenti di criptovalute non registrati, sottolineando l'importanza di una vigilanza intensificata per garantire la sicurezza e la protezione degli investitori.

La CFTC regola i mercati dei *futures*[16] e delle materie prime e ha classificato Bitcoin ed Ethereum come *commodities*, conferendo l'autorità di supervisionare i derivati delle criptovalute. La CFTC controlla le transazioni del mercato degli asset digitali e ha emesso regolamenti per definire chiaramente quando una movimentazione si considera effettivamente consegnata. Collabora con altre agenzie federali e internazionali per gestire le pratiche illegali nel mercato delle criptovalute e affrontare le sfide delle nuove tecnologie emergenti.

La FinCEN protegge il sistema finanziario da utilizzi illeciti e promuove la sicurezza nazionale attraverso la raccolta e la diffusione di informazioni finanziarie. Ha emanato normative specifiche per il settore delle criptovalute, focalizzandosi sui requisiti antiriciclaggio (AML) e know-your-customer (KYC). FinCEN ha chiarito che le entità che gestiscono e scambiano criptovalute devono essere considerate come aziende di servizi monetari (MSB) e devono rispettare obblighi di registrazione e conformità alle normative AML e KYC. L'attenzione di FinCEN verso il mercato delle criptovalute è stata recentemente intensificata, riconoscendo il loro potenziale crescente rischio nel finanziamento del terrorismo.

---

[14] United States Congress, 1933. *Securities Act of 1933*. Pub. L. No. 73-22, 48 Stat. 74. Washington, D.C.: Government Printing Office.

[15] United States Congress, 1934. *Securities Exchange Act of 1934*. Pub. L. No. 73-291, 48 Stat. 881. Washington, D.C.: Government Printing Office.

[16] Futures: contratti finanziari che obbligano l'acquisto o la vendita di un asset a un prezzo predeterminato in una data futura.

2.1.4 Istituzioni internazionali ed europee

Le principali direttive in ambito di criptovalute e prevenzione da attività illegali sono evidenziate da istituzioni internazionali ed europee, tra cui il Gruppo d'Azione Finanziaria Internazionale (FATF), l'Autorità Bancaria Europea (EBA) e la Banca Centrale Europea (ECB).

FATF

Il Financial Action Task Force (FATF) svolge un ruolo cruciale nella regolamentazione delle criptovalute e nella prevenzione del riciclaggio di denaro ("Antimoney Laundering" AML). Questo organismo intergovernativo indipendente sviluppa politiche mirate a proteggere il sistema finanziario globale da attività illecite, tra cui il riciclaggio di denaro, il finanziamento del terrorismo e la distribuzione di armi di distruzione di massa. L'importanza del FATF nella regolamentazione delle criptovalute è emersa con l'evoluzione del mercato dei beni virtuali, che ha visto il FATF rispondere all'ascesa delle criptovalute con l'emissione di definizioni chiave e l'identificazione dei potenziali rischi AML e CFT. Questo sforzo è culminato con una guida pubblicata nel 2015 che ha identificato i punti critici di connessione tra le attività di valuta virtuale e il sistema finanziario tradizionale. Successivamente, nel 2018, il FATF ha aggiornato le sue raccomandazioni per includere esplicitamente le attività finanziarie connesse ai beni virtuali, introducendo le definizioni di "bene virtuale" ("*virtual asset*" VA) e "fornitore di servizi di beni virtuali" ("*virtual asset service provider* VASP), imponendo nuove regolamentazioni e sistemi di monitoraggio. La guida del FATF[17] sottolinea l'importanza di un approccio basato sul rischio esortando i paesi e i VASP a comprendere e mitigare i rischi di riciclaggio di denaro e finanziamento del terrorismo. Le criptovalute anonime, le piattaforme e gli scambi decentralizzati, e i wallet di privacy rappresentano sfide significative per via della loro capacità di ridurre la trasparenza e aumentare l'oscuramento dei flussi finanziari. Per affrontare queste problematiche, il FATF ha emesso una nota aggiuntiva che chiarisce ulteriormente come applicare i requisiti FATF ai VA e ai VASP, enfatizzando la necessità di una regolamentazione e supervisione efficaci per mitigare i rischi AML/CFT. La cooperazione internazionale è inoltre essenziale, vista la natura globale delle attività e una supervisione efficace richiede l'autorità di condurre ispezioni, ottenere informazioni e imporre sanzioni. In sintesi, il FATF, attraverso le sue raccomandazioni aggiornate e un approccio basato sul rischio, svolge un ruolo

[17] FATF (2019), *Linee guida per un approccio ai virtual asset e ai prestatori di servizi in materia di virtual asset basato sul rischio,* FATF.

fondamentale nella regolamentazione delle criptovalute, promuovendo la trasparenza e la sicurezza del sistema finanziario globale.

EBA

L'Autorità Bancaria Europea (EBA) svolge un ruolo chiave nella regolamentazione delle criptovalute e nella lotta contro il riciclaggio di denaro nell'Unione Europea (UE). Istituito nel quadro normativo finanziario dell'UE, il mandato dell'EBA, include il monitoraggio delle attività finanziarie innovative, la fornitura di consulenza sulla delimitazione del perimetro normativo e l'assicurazione del corretto funzionamento del settore bancario dell'UE. Nonostante la loro crescente popolarità, le criptovalute generalmente ricadono al di fuori dell'ambito delle normative finanziarie tradizionali dell'UE. Questo vuoto normativo pone sfide significative, inclusi rischi legati alla protezione dei consumatori, all'integrità del mercato e alla stabilità finanziaria. L'EBA è stata attivamente impegnata nella valutazione dell'applicabilità delle leggi esistenti sui servizi finanziari dell'UE alle cripto-attività. I risultati indicano che la maggior parte delle cripto-attività non si adattano perfettamente agli attuali quadri normativi come la Direttiva sul Denaro Elettronico (EMD2) o la Direttiva sui Servizi di Pagamento (PSD2). Di conseguenza, molte attività legate alle cripto-attività, comprese le piattaforme di trading e i servizi di custodia dei wallet, rimangono non regolamentate a livello dell'UE. Questa ambiguità normativa ha portato ad approcci divergenti tra gli Stati membri dell'UE, potenzialmente minando la coerenza del mercato interno e ponendo rischi per i consumatori e la stabilità finanziaria. In risposta a queste sfide, l'EBA ha emesso diverse raccomandazioni. Una raccomandazione chiave è che la Commissione Europea conduca un'analisi costi-benefici completa per determinare la necessità e l'ambito delle azioni normative a livello dell'UE riguardanti le cripto-attività. Questa analisi dovrebbe considerare gli ultimi sviluppi degli organismi internazionali come il Financial Action Task Force (FATF), che fornisce linee guida globali sull'antiriciclaggio (AML) e sul finanziamento del terrorismo (CFT). L'EBA sostiene il rafforzamento del quadro AML/CFT dell'UE per includere in modo completo le cripto-attività. L'EBA intende sviluppare un modello di monitoraggio comune per aiutare le autorità competenti nazionali a raccogliere e riportare dati sulle attività di cripto-attività. Questa iniziativa mira a migliorare la comprensione e la supervisione dei mercati delle criptovalute e a supportare lo sviluppo di un approccio normativo coerente in tutta l'UE.

BCE

La Banca Centrale Europea (BCE) gioca anch'essa un ruolo importante nella regolamentazione delle criptovalute e nella prevenzione del riciclaggio di denaro nell'Unione Europea. La BCE si occupa di mantenere la stabilità finanziaria del settore, garantire l'efficacia della politica monetaria e supervisionare i sistemi di pagamento. Nonostante le cripto-attività, a causa della loro alta volatilità e mancanza di sostegno da parte delle banche centrali, attualmente non minaccino significativamente la politica monetaria, la BCE monitora attentamente il settore per prevenire potenziali rischi futuri. La BCE sottolinea la necessità di regolamentare gli scambi di cripto-attività e i fornitori di *wallet* di custodia per prevenire il riciclaggio di denaro e il finanziamento del terrorismo, come previsto dalla Quinta Direttiva Antiriciclaggio (AMLD5). Inoltre, collabora con organismi internazionali come il Financial Stability Board (FSB) e il Financial Action Task Force (FATF) per sviluppare un approccio unico e coordinato alla regolamentazione delle criptovalute. Questa cooperazione è fondamentale per evitare l'arbitraggio normativo nei diversi paesi.

2.2 Operazioni anomale e traffici illeciti

Le caratteristiche distintive delle criptovalute, come il sistema decentralizzato e l'assenza di autorità centrali, le rendono particolarmente appetibili per attività criminali come riciclaggio di denaro, furti, frodi e traffico di sostanze e armi. In questo sottocapitolo sono descritte le principali attività illegali legate al mercato delle criptovalute.

2.2.1 Riciclaggio di denaro

Il riciclaggio di denaro tramite criptovalute rappresenta una nuova e complessa sfida per le autorità di regolamentazione e le forze dell'ordine, poiché sfrutta le caratteristiche intrinseche delle criptovalute per mascherare l'origine illecita dei fondi. La natura decentralizzata e pseudonima delle criptovalute, come Bitcoin e Monero, facilita il processo di "pulizia" del denaro ottenuto illegalmente, rendendo difficile l'identificazione e la tracciabilità dei fondi. Questo fenomeno è caratterizzato da diverse tecniche e fasi, ciascuna delle quali sfrutta specifiche caratteristiche delle criptovalute, che arricchiscono il panorama del

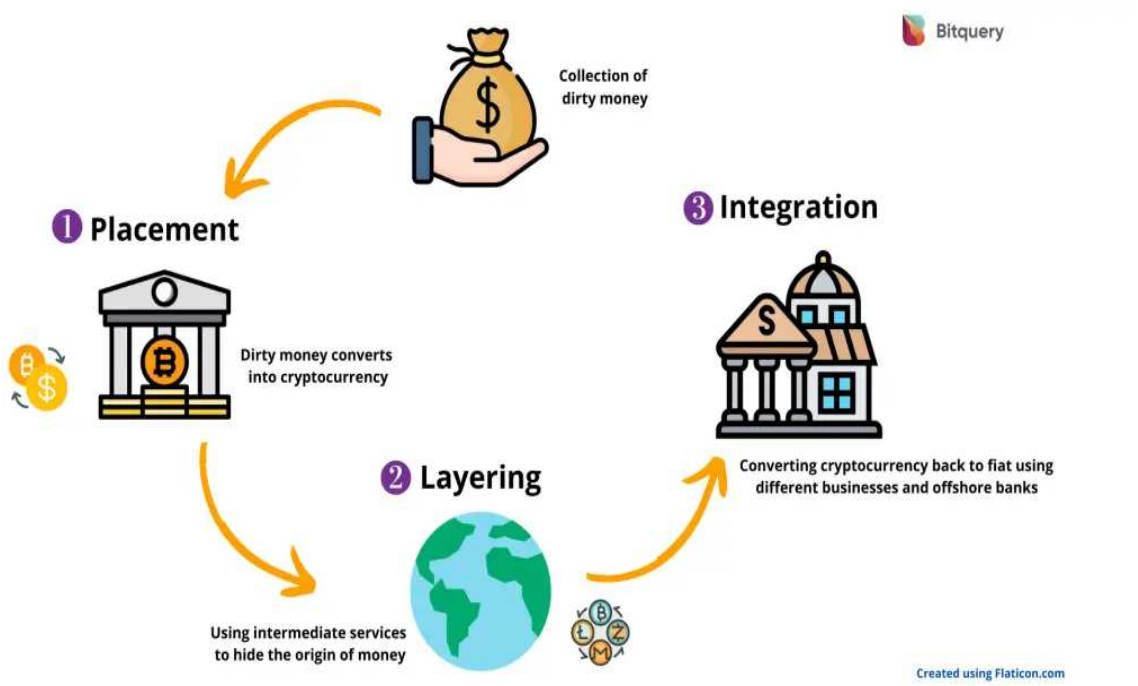
CyberLaundering, ossia il riciclaggio di denaro basato sull'utilizzo di tecnologie informatiche e telematiche.

Il processo di riciclaggio di denaro tramite criptovalute può essere suddiviso in tre fasi principali: *placement, layering e integration*. Durante la fase di *placement*, i proventi illeciti vengono introdotti nel sistema finanziario tramite l'acquisto di criptovalute utilizzando exchange, spesso non regolamentati, carte di credito prepagate, o altre forme di pagamento anonime, come voucher o conti digitali. L'utilizzo di exchange decentralizzati (DEX) è particolarmente diffuso in questa fase, poiché tali piattaforme non richiedono verifiche di identità rigorose (KYC - Know Your Customer) e operano senza un'entità centrale, rendendo più difficile l'identificazione dell'utente. Una volta che i fondi illeciti sono stati convertiti in criptovalute, questi possono essere trasferiti attraverso vari conti digitali o wallet, solitamente appartenenti al criminale o a una rete di complici, per confondere ulteriormente le tracce e scollegare la somma di denaro dalle attività illecite.

Nella fase di *layering*, le criptovalute vengono movimentate attraverso una serie di transazioni complesse per nascondere l'origine dei fondi. Questa fase può coinvolgere l'uso di tecniche avanzate come il "*chain hopping*", ovvero la conversione continua di una criptovaluta in un'altra attraverso vari exchange per rendere la tracciabilità ancora più difficile. Inoltre, l'uso di servizi di *mixing*, o *tumbler*, è comune: questi servizi mescolano le criptovalute di diversi utenti in modo da offuscare la provenienza originale dei fondi, rendendo estremamente difficile il collegamento tra la criptovaluta iniziale e quella finale. In aggiunta, si possono utilizzare strumenti di anonimizzazione come i "*coinjoin*", che combinano le transazioni di più utenti in una sola, complicando ulteriormente il tracciamento. L'uso di server proxy o di Tor per mascherare gli indirizzi IP degli utenti aggiunge un ulteriore livello di anonimato, proteggendo l'identità di chi effettua le transazioni.

La fase di *integration* coinvolge l'integrazione dei fondi "puliti" nel sistema economico legale attraverso investimenti in attività legali, partecipazioni a *Initial Coin Offerings* (ICO), o l'acquisto di beni e servizi con criptovalute, che possono poi essere convertiti in valuta tradizionale. Questa fase rappresenta la finalizzazione del riciclaggio, dove i fondi, ormai difficilmente tracciabili, vengono inseriti nel circuito economico legittimo. Le criptovalute, grazie alla loro crescente accettazione per l'acquisto di beni e servizi, offrono ai criminali un'ampia gamma di opzioni per integrare i fondi riciclati nell'economia legale. In alcuni casi, i fondi riciclati vengono anche utilizzati per finanziare ulteriori attività criminali o per investimenti speculativi nel mercato delle criptovalute stesse, contribuendo ulteriormente a nascondere l'origine primitiva dei fondi.

Figura: 2.1 Processo di Riciclaggio di denaro



[Fonte: *Cryptocurrency Money Laundering Explained, Bitquery*]

Le criptovalute hanno incentivato il fenomeno del *CyberLaundering*, introducendo nuove dinamiche nel riciclaggio di denaro. Con la diffusione delle valute digitali si è sviluppata una modalità di riciclaggio di denaro definita "riciclaggio digitale integrale". A differenza del "riciclaggio digitale strumentale", dove il denaro viene convertito in criptovalute per poi essere movimentato, nel riciclaggio digitale integrale tutte le fasi del processo avvengono online. Il denaro "sporco" è già in forma digitale e il riciclatore può operare senza alcun contatto con il contante, utilizzando esclusivamente strumenti e piattaforme digitali. La riduzione dei tempi di transazione, la facilità di accesso globale alle criptovalute e la possibilità degli scambi "*peer to peer*", facilitati da un sistema decentralizzato, rendono il trasferimento del denaro più sicuro e meno soggetto a controlli da parte delle autorità, che potrebbero essere limitate nella loro capacità di tracciare e bloccare tali transazioni. Questo ha spinto le autorità a sviluppare nuove tecnologie e strategie per contrastare il riciclaggio di denaro tramite criptovalute, ma la continua evoluzione del settore rappresenta una sfida costante e complessa.

2.2.2 Finanziamento del terrorismo

L'uso delle criptovalute nel finanziamento del terrorismo è un fenomeno in crescita che sfrutta le caratteristiche principali delle valute digitali, come l'anonimato e la difficile tracciabilità, per facilitare e potenziare le operazioni finanziarie delle organizzazioni terroristiche jihadiste. La diffusione di criptovalute come il Bitcoin, grazie alla sua decentralizzazione e pseudo-anonimità, è stata rapida tra i gruppi terroristici, poiché permette di eludere le tradizionali misure di controllo finanziario. Questo uso è particolarmente evidente su piattaforme di comunicazione criptate come Telegram, che offrono sicurezza e anonimato per la coordinazione delle attività terroristiche come propaganda, reclutamento e raccolta fondi. Questa applicazione consente una comunicazione anonima e sicura, attraverso canali pubblici e chat segrete, rendendola uno strumento efficace per evitare le intercettazioni delle autorità.

Organizzazioni come le Brigate Izz ad-Din al-Qassam (IQB) e altre campagne, come Madad, hanno dimostrato l'efficacia delle criptovalute nel raccogliere fondi attraverso infrastrutture di portafogli virtuali. Queste organizzazioni utilizzano metodi sofisticati per generare indirizzi unici per ciascun donatore, complicando notevolmente il tracciamento dei fondi. Un processo spesso utilizzato è quello della creazione di "*cascading addresses*", dove ogni transazione si dirama verso nuovi indirizzi, rendendo complesso per gli investigatori seguire il flusso del denaro. Inoltre, l'uso di mixer, come Wasabi Wallet e CoinJoin, aggiunge un ulteriore livello di anonimato, frammentando e mescolando le transazioni in modo che sia praticamente impossibile distinguere l'origine e la destinazione dei fondi.

Nonostante gli sforzi delle piattaforme come Telegram per limitare l'uso a fini terroristici, le misure adottate sono spesso insufficienti a fermare tali attività. Le criptovalute, attraverso la tecnologia *blockchain*, hanno aperto nuove frontiere nel finanziamento del terrorismo grazie alla loro capacità di effettuare transazioni pseudo-anonime. L'introduzione di monete digitali come Monero, Zcash, e Dash, note per il loro elevato livello di anonimato, è stata accolta con favore dai terroristi, che cercano di nascondere i propri flussi finanziari destinati all'acquisto di armi, esplosivi o all'organizzazione di operazioni logistiche.

L'uso di software di anonimizzazione del traffico, mixer centralizzati e *peer-to-peer*, come TOR e I2P[18], aggiunge ulteriori livelli di oscurità alle transazioni, rendendo il tracciamento molto difficile per le autorità. Questo metodo, chiamato "*onion routing*", maschera l'identità dell'utente e la sua posizione, rendendo estremamente complicato per le forze dell'ordine risalire alla fonte dei fondi.

[18] TOR e I2P sono due reti anonime decentralizzate utilizzate per proteggere la privacy online e garantire comunicazioni e servizi sicuri.

Le forze dell'ordine hanno risposto sviluppando diverse tecniche di de-anonimizzazione per contrastare queste attività. Tali tecniche includono l'analisi delle transazioni *blockchain* per identificare schemi sospetti e collegare indirizzi Bitcoin a singoli utenti. Questo processo è facilitato dall'uso di tecniche avanzate di *machine learning* e dall'incrocio dei dati con altre informazioni disponibili pubblicamente o acquisite tramite collaborazioni internazionali. L'analisi comportamentale delle transazioni può rivelare pattern che, quando combinati con altre indagini, portano all'identificazione dei responsabili.

Nonostante la volatilità del mercato delle criptovalute e le implicazioni religiose che associano queste monete al gioco d'azzardo, proibito dall'Islam, l'emergere di aziende conformi ai precetti della sharia sta contribuendo a rendere le criptovalute sempre più accettabili per i donatori musulmani. Aziende come OneGram e Stellar offrono soluzioni finanziarie che rispettano la legge islamica, rendendo più facile per i donatori utilizzare criptovalute senza violare i loro principi religiosi. Questi strumenti, tuttavia, vengono attentamente monitorati per evitare che vengano abusati per il finanziamento del terrorismo.

L'uso delle criptovalute per il finanziamento del terrorismo, tuttavia, non è privo di sfide. La trasparenza e tracciabilità intrinseche della tecnologia *blockchain* rendono difficile nascondere le attività illecite a lungo termine. Ad esempio, il governo degli Stati Uniti ha intrapreso azioni contro conti di criptovalute legati ad Hamas, sequestrando numerosi siti web e conti associati alle Brigate Izz al-Din al-Qassam per riciclaggio di denaro e occultamento di supporto materiale per il terrorismo. Le autorità hanno utilizzato l'analisi della *blockchain* per tracciare i movimenti finanziari e smantellare le reti di finanziamento.

Le sfide regolatorie persistono, in particolare nell'imporre la conformità tra gli exchange basati all'estero e le piattaforme finanziarie decentralizzate. Il quadro normativo statunitense, radicato in leggi come il Bank Secrecy Act (BSA)[19] e il USA PATRIOT Act[20], impone rigidi requisiti antiriciclaggio e di contrasto al finanziamento del terrorismo (AML/CFT) per le imprese di servizi monetari e, per estensione, per i fornitori di servizi di risorse virtuali. Tuttavia, l'evoluzione rapida del settore delle criptovalute richiede aggiornamenti continui e adattivi delle normative per mitigare i rischi posti dall'uso illecito delle criptovalute.

---

[19] United States Congress, 1970. *Bank Secrecy Act*. Pub. L. No. 91-508, 84 Stat. 1114. Washington, D.C.: Government Printing Office.

[20] United States Congress, 2001. *USA PATRIOT Act: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*. Pub. L. No. 107-56, 115 Stat. 272. Washington, D.C.: Government Printing Office.

2.2.3 Truffe e frodi

Le truffe con le criptovalute rappresentano una crescente minaccia nell'era digitale, sfruttando l'anonimato e la decentralizzazione caratteristici di queste tecnologie. Tra ottobre 2020 e marzo 2021, circa 7.000 persone hanno perso oltre 80 milioni di dollari a causa di frodi legate alle criptovalute. Negli anni seguenti le percentuali di frodi e truffe sono diminuite, ma rappresentano ancora oggi una grande minaccia per il settore.

I truffatori utilizzano una varietà di metodi sofisticati per ingannare gli investitori e rubare fondi, approfittando della mancanza di regolamentazione e delle discrepanze normative tra paesi. Tra le truffe più comuni vi sono i siti web falsi che imitano piattaforme di scambio o portafogli digitali legittimi, inducendo le vittime a inserire dati sensibili e trasferire criptovalute a indirizzi fraudolenti. Un altro metodo diffuso è il *phishing*, dove i truffatori inviano e-mail ingannevoli che sembrano provenire da servizi di criptovaluta affidabili, convincendo gli utenti a fornire le loro chiavi private.

Gli schemi di "*pump and dump*" sono particolarmente diffusi nel mondo delle criptovalute. In questi schemi i truffatori acquistano una grande quantità di una criptovaluta a basso costo, diffondono false informazioni per gonfiare artificialmente il prezzo e poi vendono tutto al prezzo massimo, lasciando gli altri investitori con perdite significative. Un esempio emblematico di questo tipo di frode è la criptovaluta ispirata alla serie TV "Squid Game", che ha visto il suo valore crollare da 2.856 dollari a zero, con gli sviluppatori che hanno sottratto 3,3 milioni di dollari. Le app false rappresentano un'altra minaccia, con software apparentemente legittimi disponibili sugli store ufficiali che, una volta installati, rubano dati o criptovalute.

Le truffe possono anche prendere la forma di endorsement falsi da parte di celebrità, dove i truffatori utilizzano nomi e immagini di persone famose per legittimare le loro frodi. Elon Musk è uno degli esempi più comuni, con truffatori che creano falsi account sui social media o video su YouTube, promettendo rendimenti elevati per gli investimenti in Bitcoin. Un altro esempio molto frequente sono i giveaway truffa, i quali sono particolarmente ingannevoli e, promettendo di restituire o moltiplicare le criptovalute ricevute, riescono a fregare migliaia di utenti. Anche il ricatto e l'estorsione sono metodi comuni, con i truffatori che minacciano di divulgare informazioni sensibili a meno che non vengano pagati in criptovaluta.

Un altro tipo di truffa molto diffusa riguarda il *cloud mining*, dove le vittime vengono indotte a investire in servizi di *mining* che si rivelano essere inesistenti o non redditizi. Le offerte di moneta iniziale (ICO, *Initial Coin Offering*) fraudolente, invece, raccolgono fondi promettendo la creazione di nuovi token che poi non vengono mai sviluppati.

Per difendersi da queste truffe, è essenziale adottare un approccio critico e informato. Gli investitori dovrebbero diffidare da promesse di guadagni garantiti, fare ricerche approfondite su qualsiasi progetto o piattaforma, verificare l'esistenza di un *whitepaper* dettagliato e controllare l'identità dei membri del team.
Mantenere segrete le chiavi di accesso del proprio portafoglio digitale e scaricare solo app da fonti ufficiali sono ulteriori misure preventive efficaci.
Affidarsi a polizze assicurative private può ulteriormente aumentare la sicurezza. In caso di sospetto di truffa, è cruciale agire rapidamente contattando la propria banca, cambiando le password compromesse e denunciando l'accaduto alle autorità competenti.
Riconoscere i segnali di frode, tra cui errori tipografici, promesse di rendimenti elevati, contratti restrittivi e manipolazione psicologica, è essenziale per proteggersi. La crescente incidenza delle frodi con criptovalute sottolinea l'importanza di una vigilanza costante e di misure di protezione avanzate per salvaguardare gli investimenti in questo settore in rapida evoluzione.

2.2.4 E-commerce illegali e Dark Web

Il Dark Web rappresenta una parte nascosta e criptata di Internet, accessibile esclusivamente attraverso specifici software come TOR (Onion Router). Questa sezione della rete è nota per ospitare una vasta gamma di attività illegali, dalla vendita di droghe e armi al traffico di dati rubati e documenti falsi. A differenza del Deep Web, che comprende contenuti non indicizzati ma spesso innocui, il Dark Web è configurato per garantire l'anonimato degli utenti tramite l'uso di domini, server criptati e nodi distribuiti. La navigazione avviene attraverso il browser Tor, che cifra i dati in modo che ogni nodo nella rete conosca solo il nodo immediatamente precedente e successivo, rendendo estremamente difficile tracciare l'origine del traffico.
Le criptovalute, e in particolare il Bitcoin, svolgono un ruolo cruciale nel funzionamento del Dark Web. Grazie alla loro natura decentralizzata e alla capacità di fornire un certo grado di anonimato nelle transazioni, le criptovalute sono diventate il mezzo di pagamento preferito per gli scambi commerciali in questo ambito. Bitcoin è spesso utilizzato per la sua diffusione e la relativa facilità d'uso, ma anche altre criptovalute come Monero, che offre un livello ancora maggiore di privacy, stanno guadagnando popolarità. Il Bitcoin consente transazioni che, sebbene registrate su una blockchain pubblica, non rivelano l'identità degli utenti.
I mercati del Dark Web, definiti "*dark markets*", operano come versioni illegali e nascoste dei classici e-commerce tradizionali.

Uno dei più noti mercati del Dark Web è stato Silk Road, un "mercato anonimo" dove si compravano e vendevano illegalmente droghe, armi, carte di credito, passaporti, materiale pedopornografico e altri beni illeciti utilizzando Bitcoin. Creato nel 2011, Silk Road è diventato un simbolo di questo mercato nero operante sul web, a cui potenzialmente chiunque potrebbe accedere. Il gestore del sito decise di utilizzare Bitcoin come valuta per effettuare le transazioni sulla piattaforma, permettendo agli utenti registrati di creare e gestire i loro wallet direttamente sui server di Silk Road. Il sistema di pagamento del sito prevedeva l'uso di conti di garanzia, gestiti da Silk Road, per assicurare che le transazioni avvenissero in modo corretto prima di effettuare effettivamente lo scambio di denaro e il trasferimento dei Bitcoin al portafoglio del venditore. Ulteriori misure, come l'uso di servizi chiamati "Tumbler", erano impiegate per mantenere l'anonimato durante i pagamenti, creando false transazioni randomiche collegate in modo complesso alla transazione reale del sito.

Nonostante le precauzioni adottate, le forze dell'ordine monitorano costantemente queste attività per identificare e perseguire i responsabili di operazioni illegali e hanno migliorato le loro capacità di tracciare le transazioni *blockchain* e di identificare gli utenti, portando a numerosi arresti e chiusure di e-commerce illegali. Silk Road, per esempio, è stato chiuso dall'FBI nel 2013, e il suo fondatore, Ross Ulbricht, è stato condannato all'ergastolo.

La complessità del Dark Web e l'uso delle criptovalute richiedono una conoscenza approfondita dei meccanismi di sicurezza e dei rischi associati. Gli utenti devono essere consapevoli delle implicazioni legali e dei pericoli potenziali, incluso il furto di dati personali e le possibili conseguenze penali derivanti dall'accesso e dall'utilizzo di questi mercati oscuri. Navigare nel Dark Web comporta significativi pericoli, tra cui l'esposizione a contenuti illegali e potenzialmente dannosi e la possibilità di essere vittime di truffe e cyberattacchi.

Mentre le criptovalute offrono numerosi benefici per le transazioni legittime, il loro utilizzo nel Dark Web continua a rappresentare una sfida significativa per le autorità e una questione critica nel dibattito sulla regolamentazione delle nuove tecnologie digitali.

CONCLUSIONI

In questo elaborato sono state esaminate le criptovalute sotto molteplici prospettive, evidenziandone sia le caratteristiche positive che le potenziali insidie. Il primo capitolo ha fornito una panoramica delle criptovalute, mettendo in luce la loro natura decentralizzata, la sicurezza garantita dalla crittografia, e il potenziale rivoluzionario della blockchain. Questi elementi conferiscono a queste valute virtuali un ruolo sempre più centrale nell'economia digitale globale, rappresentando un mezzo di scambio che potrebbe, in futuro, competere ancor di più con le valute tradizionali.

Tuttavia, il secondo capitolo ha messo in evidenza come le stesse caratteristiche che rendono le criptovalute così promettenti possono anche essere sfruttate per scopi illeciti. La loro capacità di garantire l'anonimato e di operare al di fuori dei tradizionali sistemi finanziari ha aperto la porta a una serie di attività illegali, come il riciclaggio di denaro, il finanziamento del terrorismo e altre forme di frode. Le criptovalute, pur essendo un mezzo di scambio così rivoluzionario ed innovativo, rappresentano quindi una sfida significativa per le autorità di regolamentazione e per le forze dell'ordine, che devono continuamente aggiornare le proprie strategie al fine di fronteggiare questi molteplici rischi.

In conclusione, se da una parte le criptovalute rappresentano una straordinaria innovazione con il potenziale di trasformare profondamente il mondo della finanza tradizionale, dall'altra il loro utilizzo porta continui rischi e sfide che non possono essere sottovalutati. La regolamentazione del settore sarà cruciale per garantire che i benefici delle criptovalute possano essere pienamente sfruttati, limitando al contempo i pericoli connessi al loro abuso. [21]

[21] Per la stesura del presente elaborato sono state utilizzate 10630 parole.

BIBLIOGRAFIA E SITOGRAFIA

- Sekar, G., & Kumar, B., 2023. The Impact of Cryptocurrencies on Anti-Money Laundering and Counter-Terrorist Financing. *Journal of Emerging Technologies and Innovative Research (JETIR)*, Volume 10, Issue 8, pp. e830-e837.
- Leuprecht, C., Jenkins, C., & Hamilton, R., 2023. Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*, 30(4), pp. 1036-1054.
- Dion-Schwarz, C., Manheim, D., & Johnston, P. B., 2019. Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats. *RAND Corporation*, Santa Monica, Calif.
- Unità di Informazione Finanziaria per l'Italia, 2023. Utilizzo anomalo di valute virtuali. *Banca d'Italia*.
- Chainalysis, 2024. The 2024 Crypto Crime Report: The Latest Trends in Ransomware, Scams, Hacking, and More. *Chainalysis Inc.*
- Subashi, R., 2024. Cryptocurrencies and Money Laundering. *Balkan Journal of Interdisciplinary Research*, 10(1), pp. 55-62. https://doi.org/10.2478/bjir-2024-0005.
- European Banking Authority (EBA), 2019. Report with advice for the European Commission on crypto assets. *European Banking Authority*. https://www.eba.europa.eu/
- ECB Crypto-Assets Task Force, 2019. Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures. *ECB Occasional Paper Series*, No 223, May 2019. https://www.ecb.europa.eu/
- Financial Action Task Force (FATF), 2021. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. *FATF/OECD*, Paris. http://www.fatf-gafi.org/
- Fontana, F., 2023. Criptovalute e rischi di riciclaggio. *Approfondimenti giuridici*, pp. 1-375.
- Rosen, L.W., Tierno, P., & Miller, R.S., 2023. Terrorist Financing: Hamas and Cryptocurrency Fundraising. *Congressional Research Service*. https://crsreports.congress.gov
- Surace, V., 2020. Il ruolo delle criptovalute nel sistema di finanziamento delle organizzazioni terroristiche. *Analytica for Intelligence and Security Studies*, Torino.
- Dyntu, V., & Dykyi, O., 2018. Cryptocurrency in the System of Money Laundering. *Baltic Journal of Economic Studies*, 4(5), pp. 75-81. https://doi.org/10.30525/2256-0742/2018-4-5-75-81.

- Esposito, E., 2019. Antiriciclaggio e Criptovalute. *Università Cattolica del Sacro Cuore, Milano*.
- CONSOB, 2024. Criptovalute: cosa sono e quali rischi si corrono. *CONSOB - Commissione Nazionale per le Società e la Borsa*. https://www.consob.it/web/investor-education/criptovalute
- Kriptomat, 2024. Breve storia delle criptovalute. *Kriptomat*. https://kriptomat.io/it/criptovalute/breve-storia-delle-criptovalute/
- Polverini, G., 2023. C'è vita oltre il Bitcoin: evoluzione delle criptovalute e nuove sfide per le banche centrali. *Agenda Digitale*. https://www.agendadigitale.eu/cittadinanza-digitale/ce-vita-oltre-il-bitcoin-evoluzione-delle-criptovalute-e-nuove-sfide-per-le-banche-centrali/
- Wikipedia, 2024. Criptovaluta. *Wikipedia, L'enciclopedia libera*. https://it.wikipedia.org/wiki/Criptovaluta
- Schoenmaker, S., 2022. Da enfant prodige a adolescente difficile: storia di Bitcoin dal 2008 al 2022. *Forbes Advisor Italia*. https://www.forbes.com/advisor/it/investire/criptovalute/da-enfant-prodige-a-adolescente-difficile-storia-di-bitcoin-dal-2008-al-2022/
- Osservatori Digital Innovation, 2023. Blockchain: la storia dal Bitcoin a Web3 in 8 tappe. *Osservatori Digital Innovation*. https://blog.osservatori.net/it_it/blockchain-storia-bitcoin-web3
- European Central Bank (ECB), 2018. Cryptocurrencies and tokens. *European Central Bank*. https://www.ecb.europa.eu/paym/groups/pdf/fxcg/2018/20180906/Item_2a_-_Cryptocurrencies_and_tokens.pdf
- Young Platform, 2024. Crittografia. *Young Platform Glossario*. https://youngplatform.com/glossary/cryptography/
- Coinbase, 2024. Cos'è la crittografia? Coinbase. https://www.coinbase.com/it/learn/crypto-basics/what-is-cryptography
- Cripto Investire, 2024. Crittografia: La sicurezza della Blockchain. *Cripto Investire*. https://www.criptoinvestire.com/come-funziona-la-crittografia-nelle-blockchain.html
- Forbes Advisor Italia, 2023. Che cos'è la blockchain? *Forbes Advisor Italia*. https://www.forbes.com/advisor/it/investire/criptovalute/blockchain-cosa-sapere/
- Amazon Web Services (AWS), 2024. Cos'è la tecnologia Blockchain? *Amazon Web Services*. https://aws.amazon.com/it/what-is/blockchain/
- Worldcoin, 2024. History of Cryptocurrency: the idea, journey, and evolution. *Worldcoin*. https://worldcoin.org/articles/history-of-cryptocurrency

- Culicchi, R., 2023. Cripto-asset: il punto sulle regole in Europa e Italia. Agenda Digitale. https://www.agendadigitale.eu/cittadinanza-digitale/pagamenti-digitali/cripto-attivita-le-principali-iniziative-regolamentari-e-la-situazione-in-italia/
- Italia, 2017. Decreto Legislativo 25 maggio 2017, n. 90. *Gazzetta Ufficiale della Repubblica Italiana*. https://www.gazzettaufficiale.it/eli/id/2017/06/19/17G00104/sg
- Andersen, 2019. CONSOB publishes its final report on ICO. *Andersen Italia*. https://it.andersen.com/en/consob-publishes-its-final-report-on-ico/
- European Securities and Markets Authority (ESMA), 2024. *European Securities and Markets Authority (ESMA)*. https://www.esma.europa.eu
- Coindesk, 2024. US Treasury says it wants to better money-laundering regulations around crypto, other illicit finance. *Coindesk*. https://www.coindesk.com/policy/2024/05/16/us-treasury-says-it-wants-to-better-money-laundering-regulations-around-crypto-other-illicit-finance/
- Nieder, J., 2024. Cos'è il MiCA e cosa prevede il regolamento europeo sulle crypto? *Young Platform Blog*. https://youngplatform.com/blog/news/mica-crypto-cos-e-cosa-prevede-regolamento-europeo/
- European Union, 2018. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018. *EUR-Lex*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843
- Deloitte, 2024. The Transparency Register: Latest Developments Due to the 5th EU Anti-Money Laundering Directive. *Deloitte Germany*. https://www2.deloitte.com/dl/en/pages/legal/articles/transparenzregister-5-eu-geldwaescherichtlinie.html
- Chainalysis, 2023. Assessing Terrorism Financing On-Chain is Crucial and Complex. *Chainalysis Blog*. https://www.chainalysis.com/blog/assessing-terrorism-financing-on-chain/
- Kaspersky, 2024. Le più comuni truffe di criptovaluta e come evitarle. Kaspersky *Resource Center*. https://www.kaspersky.it/resource-center/definitions/cryptocurrency-scams
- Bitpanda Academy, 2024. Che cos'è la darknet e cosa ha a che fare con il Bitcoin? *Bitpanda Academy*. https://www.bitpanda.com/academy/it/lezioni/che-cose-la-darknet-e-cosa-ha-a-che-fare-con-il-bitcoin/
- Canelli, E., 2022. Bitcoin e Dark Web: esistono ancora piattaforme per acquistare merce illegale? *Crypto.it*. https://www.crypto.it/2022/09/30/bitcoin-dark-web/
- IT Impresa, 2023. Dark Web: cos'è, come accedere e cosa si trova. *IT Impresa Blog*. https://www.it-impresa.it/blog/dark-web/

- CryptoWiki, 2023. Dark Web e criptovalute. *CryptoWiki on Substack*. https://cryptowiki.substack.com/p/dark-web-e-criptovalute