



UNIVERSITA' DEGLI STUDI DI PADOVA
DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI
"M. FANNO"

CORSO DI LAUREA IN ECONOMIA

PROVA FINALE

**"L'UTILIZZO DELLE CRIPTOVALUTE NELL'AMBITO DEI TRAFFICI
ILLECITI: MODALITA' DI UTILIZZO E SCHEMI DI RICICLAGGIO"**

RELATORE:

CH.MO PROF. ANTONIO PARBONETTI

LAUREANDO: DAVIDE DE DONATO

MATRICOLA N. 2035044

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

CAPITOLO I: INTRODUZIONE	4
1.1 <i>I traffici illeciti e gli schemi di riciclaggio</i>	4
1.2 <i>Un nuovo attore: le criptovalute</i>	6
1.2.1 <i>Cosa sono?</i>	7
1.2.2 <i>Come funzionano?</i>	8
CAPITOLO II: MODALITA' DI UTILIZZO DELLE CRIPTOVALUTE	10
2.1 <i>Gli schemi di riciclaggio</i>	11
2.1.1 <i>Le privacy coins</i>	11
2.1.2 <i>I cryptomixers</i>	13
2.2 <i>Gli schemi fraudolenti</i>	14
2.3 <i>Modalità di pagamento</i>	15
CAPITOLO III: L'EVOLUZIONE NORMATIVA, REPRESSIONE E PREVENZIONE	17
3.1 <i>L'evoluzione della regolamentazione</i>	17
3.2 <i>Gli indicatori d'allarme</i>	23
3.3 <i>I paesi ad alto rischio</i>	25
CAPITOLO IV: CONCLUSIONI	27
BIBLIOGRAFIA	29

CAPITOLO I: INTRODUZIONE

Il tema concernente la presenza di traffici illeciti e la creazione di schemi di riciclaggio all'interno del sistema economico mondiale è un argomento giuridico-economico altamente dibattuto al giorno d'oggi, vista la grande frequenza con la quale avvengono questi fenomeni ed i rischi e pericoli che essi arrecano e conseguono. Si tratta di una tematica che trova origine in tempi storici lontani, che negli anni si è mostrata in continua evoluzione, aumentando sempre più il suo peso specifico e rilevanza all'interno dell'economia e delle giurisdizioni, ormai a livello internazionale. Sin dall'inizio, tale materia ha causato non poche difficoltà alle autorità competenti, trovando il suo culmine con l'avvento della digitalizzazione e della globalizzazione, dal momento che le organizzazioni criminali, sempre attente all'introduzione di nuove opportunità, hanno trovato terreno fertile per i fini delle loro attività illecite, creando nuovi schemi e metodi di aggiramento sempre più efficienti oltre che efficaci, servendosi per l'appunto dei nuovi strumenti digitali. Sarà oggetto di questa tesi presentare i nuovi "attori" e i rischi ad essi connessi, analizzarli, comprenderne il funzionamento, esaminare la regolamentazione attualmente in vigore, proporre metodi di contrasto e prevenzione e definire quale direzione normativa perseguire al fine di far fronte a questo pericolo in continua evoluzione oltre che estensione.

1.1 I traffici illeciti e gli schemi di riciclaggio

Per traffico illecito si intende lo scambio di beni o servizi di per sé illegali o scambiati attraverso metodi non contemplati dall'ordinamento giuridico: dal semplice scambio di sostanze stupefacenti fino al traffico di esseri umani, dal traffico di materiali tossici ed inquinanti al traffico di materiali pedopornografici, dal traffico di organi di esseri umani al traffico di materiali volti al finanziamento di attività terroristiche. È possibile affermare che tale fenomeno rappresenti un lato oscuro dell'economia mondiale, ricoprendo sempre maggiormente una parte sostanziosa del sistema, catturando così l'attenzione delle autorità competenti in materia, da diverso tempo impegnate nel contrasto di tali attività. A pari passo con i traffici illeciti vi è l'utilizzo degli schemi di riciclaggio di denaro "sporco", ovvero i meccanismi attraverso i quali gli autori di attività criminali mascherano l'origine illecita dei propri beni o del proprio reddito. Per comprendere al meglio tale fenomeno viene in ausilio l'articolo 648 bis del Codice Penale italiano, all'interno del quale è presente la definizione di riciclaggio di denaro proveniente da reato, il quale viene descritto come quanto segue: "*chiunque 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*"; si tratta quindi di un'operazione economica volta a nascondere l'origine criminosa di beni, denaro o altre utilità e permettere il loro reinserimento all'interno del mercato legale. Muovendo un ulteriore passo, all'interno del supplemento al N.4/2000 della

rassegna dell'arma dei Carabinieri, scritto da Canio Giuseppe La Gala, troviamo le caratteristiche "ontologiche" del riciclaggio, ovvero: l'illegalità dell'operazione (dal momento che il riciclaggio ha per oggetto proventi originati in maniera illecita) e le finalità di occultamento e/o sostituzione (poiché lo scopo è quello di nascondere l'origine dei proventi ed ottenere la loro legittimazione). Una volta definite le funzioni del riciclaggio e le sue caratteristiche, è adesso necessario analizzare integralmente il processo attraverso il quale il denaro proveniente da azioni illegali viene "ripulito" e reinserito all'interno del mercato legale, il quale, secondo il G.A.F.I.¹, si articola in tre fasi:

1. L'introduzione nel mercato, ovvero il collocamento dei proventi attraverso una serie lunga e duratura di operazioni (ad esempio: deposito, cambio, trasferimento, acquisto di beni). Si tratta dunque della fase di raccolta di denaro ed il suo collocamento presso istituzioni o intermediari finanziari direttamente nel mercato.
2. La stratificazione, per la quale si intende il compimento di operazioni di natura per lo più finanziaria volte a separare i proventi illeciti dalla loro fonte. Attraverso questo strato di operazioni di "lavaggio", l'impegno richiesto e le difficoltà per ricostruire il processo di riciclaggio e risalire alla fonte originaria del denaro da parte delle autorità inquirenti sarà maggiormente arduo, creando così una copertura efficace ed una ricchezza anonima, almeno all'apparenza, legittima.
3. L'integrazione, fase nella quale i proventi da reato, una volta ottenuta una facciata lecita, vengono reinseriti all'interno dei circuiti dell'economia. Così facendo, l'ingresso apparirà frutto di un'operazione finanziaria ordinaria, con fondi di provenienza legittima.

È dunque possibile affermare che il fenomeno del riciclaggio sia un complesso sistema processuale, in quanto una singola operazione risulterebbe insufficiente e inefficace per quanto riguarda il fine, ovvero creare un'impronta lecita al denaro proveniente da fonte illecita, soprattutto per merito delle legislazioni antiriciclaggio, anch'esse in continuo aggiornamento, con lo scopo di rendere tale attività obsoleta.

¹ "Gruppo di Azione Finanziaria Internazionale", organismo intergovernativo che ha per scopo l'elaborazione e lo sviluppo di strategie di lotta al riciclaggio dei capitali di origine illecita, costituito nel 1989 in occasione del G7 di Parigi

1.2 Un nuovo attore: le criptovalute

Grazie all'espansione della digitalizzazione e all'evoluzione degli strumenti telematici, nel corso dell'ultimo decennio sono state introdotte all'interno del mercato digitale le valute virtuali, presentate come strumenti finanziari volti all'acquisto di beni e servizi, nonché a finalità di investimento. Considerata l'esponenziale e repentina crescita di tale fenomeno, gli organismi internazionali e le autorità europee hanno iniziato ad esprimere la propria posizione, evidenziando come le caratteristiche intrinseche e proprietà di tali monete possano comportare significativi rischi legati al riciclaggio di denaro e al finanziamento del terrorismo; ne è emersa di conseguenza la necessità da parte delle autorità competenti di redigere una regolamentazione normativa atta alla prevenzione e contrasto di tali rischi.

A tal proposito, l'UIF, nel Comunicato del 30 gennaio 2015, ha sottolineato l'importanza e la necessità di una supervisione specifica per quanto riguarda le operazioni connesse alle valute virtuali da parte dei destinatari degli obblighi antiriciclaggio, in modo da poter identificare eventuali fattori o elementi sospetti, prevenendo così il riciclaggio e il finanziamento del terrorismo. Tale collaborazione tra soggetti obbligati e autorità, negli ultimi anni ha iniziato a produrre risultati tangibili, come evidenziato nella newsletter 5-2022 emanata dall'UIF, il numero di segnalazioni di operazioni sospette riguardanti le valute virtuali è infatti in continua crescita: dai 732 rapporti ricevuti nel 2019 si è registrato un aumento a 3.453 segnalazioni nel 2021, superando le 5.000 segnalazioni nel 2022.

Tra gli elementi di sospetto più frequentemente segnalati vi è l'origine dei fondi impiegati per l'acquisto delle criptovalute, spesso correlata a possibili illeciti fiscali, frodi informatiche o attacchi ransomware; sono stati inoltre riscontrati casi di truffe nel trading online e investimenti effettuati da vittime su piattaforme estere, nella maggior parte dei casi non autorizzate, a seguito di ripetuti contatti telefonici o tramite presunti consulenti finanziari; ulteriori situazioni ricorrenti riguardano le piattaforme di exchange² prive di adeguate strutture organizzative per la tutela dei clienti e il mancato rispetto della normativa antiriciclaggio. Da sottolineare, infine, le segnalazioni da parte di alcuni fornitori di servizi di attività virtuale (VASP) italiani circa l'esistenza di flussi di criptovalute coinvolti in schemi di frode fiscale, attraverso la cessione di crediti fiscali fittizi derivanti da bonus edilizi, i cui proventi venivano utilizzati per l'acquisto di criptovalute.³

Ci troviamo dunque di fronte ad un nuovo attore, destinato a svolgere un ruolo da protagonista all'interno del contesto dei traffici illeciti e degli schemi di riciclaggio.

² Piattaforme digitali che facilitano l'acquisto e la vendita di asset digitali in base ai prezzi di mercato giornalieri.

³ Informazioni raccolte all'interno della newsletter 5-2022 dell'UIF, disponibile su

[<https://uif.bancaditalia.it/pubblicazioni/newsletter/2022/newsletter-2022-5/Newsletter_5_2022.pdf>](https://uif.bancaditalia.it/pubblicazioni/newsletter/2022/newsletter-2022-5/Newsletter_5_2022.pdf)

1.2.1 Cosa sono?

Le criptovalute sono forme di valuta digitale basate sulla crittografia, ovvero sull'applicazione di tecniche aventi la funzione di rendere un messaggio comprensibile esclusivamente ai destinatari autorizzati, utilizzabili unicamente attraverso un codice informatico specifico, noto come "chiave di accesso"; non esistono in forma fisica e vengono generate e scambiate esclusivamente in modalità telematica (motivo per il quale vengono definite "virtuali"), possono essere scambiate attraverso il sistema "*peer-to-peer*" (previo consenso tra le parti coinvolte nella transazione) consentendo così interazioni dirette tra due dispositivi senza la necessità di intermediari, e sono utilizzabili per l'acquisto di beni e servizi, operando come moneta con corso legale in determinati contesti.

Risultano interessanti alcune caratteristiche distintive di tali monete, in particolare:

- Non possiedono corso legale nella maggior parte degli Stati, pertanto il loro utilizzo come metodo di pagamento avviene solo su base volontaria;
- Sono decentralizzate, ovvero non sono sottoposte al controllo di enti centrali governativi; vengono emesse e gestite dagli organismi emittenti secondo regolamenti interni definiti dal cosiddetto "protocollo";
- Utilizzano un registro pubblico, noto come "*distributed ledger*" o "*blockchain*", dove ogni transazione è registrata e può essere consultata da una rete decentralizzata di partecipanti secondo le regole stabilite dal protocollo.

Per una comprensione approfondita della loro natura, è d'ausilio lo studio svolto da Fulvio Fontana all'interno del testo "*Criptovalute e rischi di riciclaggio*", secondo il quale risulta utile differenziare le monete a corso legale dalle criptovalute, ponendo attenzione sulle proprietà delle monete a corso legale, quali: unità di conto, mezzo di pagamento e deposito di valore. Svolgendo un paragone, le criptovalute non riescono a svolgere adeguatamente il ruolo di unità di conto a causa della loro elevata volatilità, i loro prezzi infatti possono subire ampie fluttuazioni anche all'interno della stessa giornata, rendendo difficile la valutazione dei beni e dei servizi. In merito alla funzione di riserva di valore, invece, l'aumento dell'uso delle valute virtuali come mezzi di pagamento può contribuire ad un aumento di valore, visto il numero limitato di monete generate; pertanto, un incremento delle transazioni effettuate in criptovaluta porta ad una valorizzazione delle stesse.

Sempre dal testo di cui sopra⁴, a livello teorico, le criptovalute si avvicinano di più a risorse come l'oro piuttosto che alle monete emesse dalle banche centrali, poiché:

- Entrambi sono limitati;
- Costituiscono un attivo per i detentori;

⁴ FULVIO FONTANA, "*Criptovalute e rischi di riciclaggio*".

- Sono sovranazionali;
- Non possono essere spese direttamente senza l'accettazione della controparte come mezzo di pagamento.

Risulta quindi più appropriato qualificare le criptovalute come "asset", ovvero entità caratterizzate da una valutazione economica soggettiva; tuttavia, sarebbe ancora più adeguato definirle come "criptoasset", interpretandole quindi come rappresentazioni digitali di valore rese uniche attraverso meccanismi crittografici; inoltre, a differenza degli asset tradizionali, che possono essere scambiati sui mercati finanziari convenzionali, i criptoasset possono essere depositati e scambiati unicamente su piattaforme basate su tecnologia DLT⁵, rispettando le regole del protocollo blockchain.

Per concludere, un'ulteriore caratteristica distintiva delle valute virtuali risiede nella loro divisibilità: mentre le valute tradizionali possono essere frazionate fino al centesimo, le criptovalute possono essere suddivise fino al centomillesimo, permettendo così l'utilizzo di questo metodo di pagamento anche per transazioni di importo ridotto, a differenza dei pagamenti in moneta elettronica, che risultano meno praticabili per somme modeste.

Alla luce di quanto esaminato, l'obiettivo primario delle criptovalute risulta quindi l'introduzione di sistemi di pagamento autonomi rispetto ai tradizionali circuiti bancari.

1.2.2 Come funzionano?

Per iniziare a possedere o scambiare criptovalute, è condizione necessaria il possesso di un portafoglio digitale personale ("wallet") contenente due chiavi: una pubblica (la quale identifica in modo univoco il wallet stesso e funge da indirizzo) e una privata (che consente al titolare di gestire le criptovalute depositate o inviate), per poter inviare una criptovaluta a un determinato destinatario è infatti necessario conoscere la chiave pubblica del suo wallet, al contrario, affinché il proprietario di un wallet possa utilizzare la moneta virtuale in esso contenuta è fondamentale che conosca la chiave privata associata al proprio portafoglio.

Di rilevante importanza risulta l'utilizzo della tecnologia Blockchain, un libro mastro distribuito e permissionless⁶ utilizzato dagli enti emittenti di criptovalute, che impiega la tecnologia *peer-to-*

⁵ Con il termine *Distributed Ledger Technologies (DLT)* si fa riferimento a "libri mastri" (o registri) elettronici, distribuiti geograficamente su un'ampia rete di nodi, i cui dati sono protetti da potenziali attacchi informatici grazie al fatto che le stesse informazioni sono ridondate, verificate e validate mediante l'adozione di diversi protocolli (o regole) comunemente accettati da ciascun partecipante.

⁶ Reti aperte che consentono a chiunque di partecipare al processo di consenso senza la necessità di ottenere un'approvazione, un permesso o un'autorizzazione.

*peer*⁷ e memorizza tutte le transazioni effettuate tramite la valuta digitale di riferimento, dalla sua immissione nel mercato fino ad oggi; inoltre, da protocollo, ogni nuovo utente della rete blockchain riceve una copia completa di tutti i blocchi di transazioni validati fino a quel momento. La sua importanza si rileva nella sicurezza che garantisce durante le transazioni: quando un utente desidera effettuare un'operazione, invia una richiesta in broadcast agli altri membri della rete per verificarne la legittimità: se più del 50% della potenza computazionale della rete conferma la proprietà della criptovaluta sull'indirizzo che sta effettuando la transazione e il destinatario accetta il pagamento, la Blockchain verrà aggiornata inserendo la nuova transazione effettuata e solo dopo questi passaggi l'operazione potrà ritenersi conclusa.

Per concludere, è importante evidenziare il fatto che chiunque ha la possibilità di creare una valuta digitale (con relativa conseguenza diretta la possibile esistenza di centinaia, se non migliaia, di criptovalute in circolazione in qualsiasi momento) attraverso un meccanismo noto come “*initial coin offering*” (ICO), una strategia volta alla raccolta di fondi necessari per finanziare un progetto imprenditoriale. Questo processo prevede l'emissione di monete digitali come alternativa agli strumenti finanziari tradizionali, l'offerta di tali monete agli investitori, e l'acquisto tramite denaro contante o altre criptovalute (anche in questo caso, la creazione, l'emissione e il trasferimento dei token avvengono tramite la tecnologia “distributed ledger”).

⁷ Sistema che consente ad un utente di scambiare con altri utenti nel medesimo momento collegati, in regime di assoluta autonomia (senza cioè dover passare per un server centrale, programmi, banche dati, materiali audiovisivi, ecc.

CAPITOLO II: MODALITA' DI UTILIZZO DELLE CRIPTOVALUTE

L'anonimato e la decentralizzazione delle criptovalute sono caratteristiche che forniscono un ambiente favorevole per le organizzazioni criminali, le quali hanno iniziato ad adottarsi di tale nuovo strumento digitale come parte integrante e fondamentale degli schemi di riciclaggio di denaro da loro architettati, ma non solo: si è registrato un crescente impiego delle stesse anche nelle frodi e nel traffico di droga, sono infatti ampiamente utilizzate come mezzo di pagamento per beni e servizi illegali offerti online ed offline. Il fine comune perseguito da chi opera nelle sopracitate attività è quello di nascondere la fonte del denaro utilizzato o dei beni illeciti tramite schemi e processi che si servono delle proprietà delle criptovalute; numerosi indicatori mostrano infatti come i criminali coinvolti nelle frodi facciano forte affidamento sull'uso delle valute virtuali, le quali sono anche il mezzo di pagamento preferito per beni e servizi criminali, come farmaci, sostanze stupefacenti, materiale volto al finanziamento del terrorismo e materiale pedopornografico acquistato online (ciò vale in particolare per le inserzioni sui mercati del dark web, dove rappresentano il principale mezzo di pagamento). Da evidenziare anche l'esistenza di schemi di estorsione portati avanti dai criminali informatici facenti ampio uso di criptovalute, vi sono infatti diverse tipologie di malware⁸ che prendono di mira le criptovalute per furti e per l'estrazione di monete nella rete di vittime ignare della presenza di tali metodi di frode. Nello specifico, all'interno di questo capitolo saranno oggetto di analisi i principali metodi di utilizzo di criptovalute per quanto riguarda il pagamento di traffici illeciti e la creazione di schemi fraudolenti e di riciclaggio.

⁸ termine generico che descrive qualsiasi programma o codice dannoso per i sistemi, il quale cerca di invadere, danneggiare o disattivare computer, sistemi informatici, reti, tablet e dispositivi mobili, spesso assumendo il controllo parziale delle operazioni di un dispositivo.

2.1 Gli schemi di riciclaggio

Le peculiarità delle criptovalute, quali l'impiego della crittografia e l'assenza di un'autorità monetaria centralizzata, costituiscono un'importante opportunità per il riciclaggio e il reimpiego di capitali di provenienza illecita; nello specifico, gli elementi che facilitano l'impiego delle criptovalute nei contesti di riciclaggio risultano essere:

- Anonimità. Tale caratteristica rende non necessaria la fase di collocamento nel processo di riciclaggio;
- Possibilità di creare rapidamente un account a costo zero;
- Possibilità di sviluppare un complesso sistema di riciclaggio con migliaia di trasferimenti economici operati tramite script informatici⁹;
- L'esponenziale e rapido incremento dei tassi di cambio di alcune criptovalute. Talvolta tale crescita supera il 10.000%, rendendo così semplice giustificare un'improvvisa acquisizione di ricchezza.

Attualmente esistono infatti diverse tecnologie correlate alle criptovalute che possono essere inopportuno sfruttate per il riciclaggio, tra le quali spiccano le "*privacy coins*" e i "*cryptomixers*".

2.1.1 Le *privacy coins*

Una *privacy coin* è una categoria di criptovaluta progettata specificamente per assicurare la tutela della privacy e dell'anonimato degli utilizzatori, esse infatti evidenziano un malinteso comune: molte persone suppongono che tutte le criptovalute offrano anonimato totale, quando in realtà la maggior parte possiedono solo carattere pseudonimo. Per comprendere il concetto di pseudonimato, si può esaminare una qualunque transazione in bitcoin, dove vengono registrati i seguenti dettagli:

- Hash¹⁰/ID della transazione;
- Indirizzo del mittente e del destinatario;
- Indirizzo di scambio per gli output non spesi, reindirizzati all'indirizzo di scambio;
- Orario di invio della transazione;
- Importo trasferito.

⁹ Nel linguaggio dei programmatori, uno script è un programma o una sequenza di istruzioni che viene interpretata o portata a termine da un altro programma (invece che dal processore come nei linguaggi compilati).

¹⁰ Classe di algoritmi crittografici che trasformano un dato di lunghezza arbitraria (messaggio) in una stringa binaria (detta "digest") di lunghezza fissa, lunghezza che varia a seconda dell'algoritmo di hash utilizzato.

Nonostante le transazioni in criptovaluta non contengano dati personali o indirizzi IP, il loro carattere pseudonimo consente di dedurre informazioni del mittente o del destinatario tramite l'analisi dei dati e dei modelli di transazioni: le informazioni di cui sopra possono essere infatti impiegate per compromettere la riservatezza delle parti coinvolte nella transazione, rendendo quindi inaccurata l'affermazione secondo la quale le criptovalute siano totalmente anonime. A tal proposito, sono state sviluppate le privacy coins, una tipologia di moneta virtuale che implementa diverse soluzioni progettuali per eliminare o oscurare i dati delle transazioni che potrebbero compromettere la privacy di mittente e destinatario.

Tra queste soluzioni vi sono:

- Le firme ad anello. Tale soluzione permette a un gruppo di utenti di firmare una transazione congiuntamente, rendendo difficile l'identificazione dell'iniziatore;
- L'utilizzo di indirizzi "stealth". È possibile generare indirizzi unici e temporanei per ciascuna transazione, complicando così l'associazione della transazione a un determinato utente.
- Transazioni riservate. Nascondono l'ammontare della transazione al pubblico, offrendo maggiore riservatezza.

Questi elementi contrastano con il funzionamento delle criptovalute tradizionali, in cui il saldo di un indirizzo e le transazioni tra gli indirizzi sono visibili a tutti; tuttavia, il fattore chiave che rende possibile ed efficace l'operatività delle privacy coins è la crittografia "zk-SNARK" (zero-knowledge succinct non-interactive argument of knowledge), nota anche come crittografia a "conoscenza zero": si tratta di una forma di crittografia concepita per fornire agli utenti una protezione della privacy avanzata rispetto a quella generalmente offerta dalla blockchain; essa consente di effettuare transazioni completamente cifrate su una blockchain, rendendole illeggibili per chiunque altro, mentre ne garantisce la validità e legittimità grazie alla tecnologia "Zero Knowledge Proof", la quale permette a una persona A di dimostrare a una persona B la veridicità di un'affermazione X senza rivelare dettagli oltre alla validità dell'affermazione stessa.

Questo approccio alla schermatura delle transazioni contrasta con il sistema delle criptovalute tradizionali, dove indirizzi del mittente e del destinatario e l'importo delle transazioni sono accessibili a tutti; pertanto, le privacy coins rappresentano una categoria di criptovalute che offrono un livello più elevato di anonimato nelle transazioni su blockchain, rendendo la valuta ancor meno tracciabile rispetto alle criptovalute ordinarie, presentandosi così come strumenti fortemente efficaci per attività legate al riciclaggio di denaro.

2.1.2 I cryptomixers

Uno dei metodi più efficaci per celare le tracce delle transazioni in criptovalute, riducendo il rischio di esposizione del portafoglio e l'accumulo di fondi su un indirizzo pubblico, è rappresentato dalla tecnologia dei "cryptomixer". Generalmente, quando si trasferisce una somma di denaro da un indirizzo a un altro, la transazione e gli indirizzi dei partecipanti vengono registrati sulla blockchain con un codice crittografico; al contrario, un mixer di criptovalute modifica gli indirizzi, mescola gli importi e le valute, col fine di rendere il più complesso possibile la rintracciabilità.

Per quanto riguarda il suo modus operandi, il mixer richiede il passaggio per diverse fasi:

- indicare l'importo da inviare a un determinato indirizzo;
- il tempo entro il quale si desidera che la somma arrivi (considerando che un lasso di tempo maggiore diminuisce la possibilità di tracciamento);
- attendere che altri utenti sfruttino il servizio, in modo tale da assicurarsi di disporre di un numero sufficiente di indirizzi e risorse per mescolare le valute, generare una somma da dividere tra i destinatari e inviarla in maniera dilatata nel tempo.

Questo procedimento crea inoltre un nuovo indirizzo di portafoglio al quale verrà inviato l'importo, rendendo così maggiormente complicato per le forze dell'ordine rintracciare un determinato pagamento; nel dettaglio, l'importo destinato agli utenti sarà composto da fondi provenienti da diversi indirizzi e criptovalute, generando più mittenti fittizi per ciascun pagamento sotto un unico indirizzo; inoltre, questi servizi utilizzano canali di comunicazione anonimi, non conservano i registri delle transazioni oltre un certo periodo, sono accessibili pubblicamente tramite Internet e non richiedono informazioni personali, ma piuttosto la creazione di un account privato come condizione necessaria per l'accesso.

Di particolare importanza è inoltre la distinzione tra due tipologie di mixer:

- I mixer centralizzati. Sono servizi privati che ricevono criptovalute dal cliente e restituiscono monete diverse, addebitando una commissione; nel dettaglio, per iniziare una transazione, è necessario inserire il proprio indirizzo e inviare le criptovalute a un indirizzo scelto dal servizio, che mescolerà le monete e invierà importi casuali di bitcoin agli indirizzi forniti fino a restituire l'intero importo al portafoglio del cliente; tuttavia, questa soluzione offre una sicurezza limitata in termini di privacy, poiché i fondi devono essere affidati al mixer senza alcuna garanzia di restituzione.

- I cryptomixer decentralizzati. Si tratta del raggruppamento di quanti più individui possibili, i quali mettono in comune le loro monete per effettuare una grande transazione, restituendo successivamente le monete in modo casuale ai membri del pool; in pratica, più utenti partecipano al gruppo, maggiore è la randomizzazione e la protezione della privacy.

Ai fini dell'analisi condotta, e per una comprensione maggiore circa l'utilizzo della sopracitata tecnologia, risulta interessante il caso "Bitcoin Fog", servizio di coin mixing ideato e creato da Roman Sterlingov. Dopo un'indagine condotta da parte dell'FBI per un periodo di tempo di circa tre anni, la giuria federale di Washington DC ha condannato in data 12 marzo 2024 l'operatore russo-svedese, con l'accusa di aver gestito il più longevo servizio di riciclaggio di denaro tramite bitcoin sul dark web. Alla luce delle prove presentate al processo, Sterlingov sarebbe stato coinvolto nella gestione di Bitcoin Fog dal 2011 al 2021, intervallo di tempo nel quale, attraverso il servizio di mixing, sarebbero stati spostati oltre 1,2 milioni di bitcoin (al momento delle transazioni valutati come circa 400 milioni di dollari) attraverso le tecniche di mixing citate ed analizzate precedentemente, la maggior parte delle quali provenienti dai mercati del darknet e legate a narcotici illegali, crimini informatici, furto d'identità e materiale di abuso sessuale su minori; il mixer aveva infatti acquisito notorietà durante il suo periodo di attività, venendo riconosciuto dai criminali, aventi come fine il mascheramento dei loro proventi illeciti, come la piattaforma di riferimento per il riciclaggio di denaro.

In sintesi, lo scopo di queste tecnologie è quello di "mescolare" fondi di criptovaluta potenzialmente identificabili col fine di oscurarne la provenienza, traendo guadagno dall'applicazione di una commissione (di solito una percentuale dell'importo coinvolto), offrendo anonimato e un tempo di transazione stabilito, incentivando così la fidelizzazione della clientela.

2.2 Gli schemi fraudolenti

La frode rappresenta il reato più frequentemente associato all'uso illegale di criptovalute, costituendo oltre la metà delle transazioni criminali accertate. Solitamente, i criminali coinvolti in frodi sugli investimenti si servono delle criptovalute per veicolare i loro proventi illeciti mediante la creazione di siti web dedicati agli investimenti in criptovalute oppure pubblicizzando investimenti apparentemente redditizi, sollecitando gli investitori a creare conti su piattaforme di trading online; le vittime sono indotte a credere di poter monitorare i propri investimenti tramite queste piattaforme, tuttavia, tale processo si rivela essere un mero raggio.

Esistono altre modalità di creazione di schemi fraudolenti tramite criptovalute, un esempio è la creazione di criptovalute inesistenti ma definite redditizie, finanziate tramite schemi piramidali¹¹. Un report pubblicato da TRM Labs supporta questa tesi, indicando come nel 2022 siano stati spesi complessivamente 7,8 miliardi di dollari in schemi piramidali e Ponzi legati alle criptovalute, affermando quanto segue: *"Le frodi sugli investimenti mirano alla raccolta di fondi per investimenti o progetti fraudolenti; spesso si tratta di false initial coin offerings, security non registrate o piattaforme di investimento ingannevoli. Le frodi connesse alle criptovalute sono aumentate di quasi il 200%, passando da 907 milioni nel 2021 a 2,57 miliardi di dollari nel 2022"*.

Tra gli schemi Ponzi, più rilevanti, perseguiti vi sono Forsage e Trade Coin Club; la prima ha attratto gli investitori promettendo rendimenti elevati tramite contratti su Ethereum e BNB Smart Chain, raccogliendo 974 milioni di dollari attraverso due entità collegate, la seconda invece prometteva alti rendimenti tramite il suo exchange di criptovalute, ottenendo più di 295 milioni di dollari da oltre 100.000 investitori prima del suo collasso. I dati di cui sopra mettono in luce il frequente e diffuso uso illegale di questo nuovo strumento digitale, evidenziandone i rischi e le conseguenze ad esso connesse, oltre alla crescente urgenza circa la necessità di un intervento normativo in materia, al fine di contrastare efficacemente questo fenomeno in rapida crescita.

2.3 Modalità di pagamento

L'utilizzo delle criptovalute è legato anche ai pagamenti relativi all'acquisto di beni illeciti online e rappresentano da sempre il mezzo di pagamento standard per gli utenti delle piattaforme del dark web, sin dai tempi della creazione di Silk Road nel 2011, il primo grande mercato di questo genere (si stima che nel 2020 il volume delle transazioni sui mercati del dark web abbia raggiunto 1,5 miliardi di euro in attività associate alle criptovalute). La necessità, da parte dei criminali, di utilizzare i propri proventi illeciti e aggirare la tracciabilità delle transazioni nei registri pubblici ha reso popolari le tecniche di offuscamento attraverso l'impiego delle valute virtuali; infatti, le caratteristiche tecniche e le proprietà delle criptovalute, quali la decentralizzazione e la sicurezza garantita da algoritmi complessi e blockchain tra tutte, offrono ai criminali numerosi vantaggi; tuttavia, il principale motivo di attrazione non risiede tanto nell'anonimato, quanto piuttosto nella semplicità e praticità d'uso, nonché, in alcuni casi, nell'assenza di supervisione e regolamentazione da parte delle autorità governative.

A supporto della nostra tesi, viene in ausilio il rapporto annuale (2022) riguardante l'uso illegale delle criptovalute prodotto da Chainanalysis, azienda di analisi specializzata nel settore delle

¹¹ Frodi di marketing e di investimento in cui a un individuo viene offerta una distribuzione o un franchising per commercializzare un particolare prodotto.

criptovalute: uno dei dati centrali del documento è il valore complessivo del mercato illegale delle criptovalute: 24,2 miliardi di dollari, importo calcolato sommando tutte le transazioni indirizzate a portafogli considerati sospetti o associati a organizzazioni criminali (all'interno dell'importo sono inclusi anche i furti di criptovalute). Si tratta di una prima stima, destinata ad aumentare con l'incremento delle segnalazioni che Chainalysis riceverà; infatti, nel corso dell'anno precedente, Chainalysis aveva inizialmente stimato un utilizzo di criptovalute in attività illecite di un ammontare pari a circa 20 miliardi di dollari, totale che è aumentato significativamente nel corso del 2023, raggiungendo i 39,6 miliardi di dollari.

L'impiego delle criptovalute per fini illeciti si manifesta dunque principalmente per due motivi: il primo per mascherare le transazioni finanziarie legate a traffici illegali (da anni gli acquisti di stupefacenti o il traffico di armi sfruttano in larga misura le criptovalute per eludere l'intervento del sistema bancario o l'uso del contante), il secondo per eludere gli embarghi imposti dalla comunità internazionale (Chainalysis stima che il 61% dei 24,2 miliardi di dollari affluiti a portafogli illeciti provenisse da Stati o entità soggette a sanzioni internazionali). Le criptovalute, infatti, possono essere trasferite rapidamente senza necessità di un conto bancario tradizionale, rendendole così un mezzo di pagamento allettante per attività illecite, ma va al tempo stesso sottolineato il fatto che tali monete, gli indirizzi associati e i relativi trasferimenti non sono anonimi: ogni transazione è registrata sulla blockchain e può essere consultata da chiunque tramite un blockchain explorer¹²; tuttavia, poiché le transazioni avvengono utilizzando lunghe stringhe di caratteri alfanumerici anziché nomi reali, diventa più complesso identificare i soggetti coinvolti, specialmente nel contesto di operazioni criminali.

Occorre infine considerare la costante evoluzione di questi strumenti digitali e delle metodologie criminali, in particolare con l'emergere delle sopraccitate privacy coins, le quali, per loro progettazione, si dimostrano essere gli strumenti più efficaci per transazioni aventi come oggetto beni o servizi illegali, data la loro totale anonimità rispetto alle criptovalute tradizionali.

¹²Motore di ricerca utilizzato non per la navigazione sul web, bensì per l'ispezione di Blockchain, mostrando i dati relativi alle transazioni in criptovalute, ai wallet e agli smart contract.

CAPITOLO III: L'EVOLUZIONE NORMATIVA, REPRESSIONE E PREVENZIONE

La crescente attenzione verso il fenomeno delle criptovalute come nuovo strumento volto all'utilizzo in attività aventi fini illeciti rappresenta una sfida importante per le forze dell'ordine e le autorità competenti, le quali hanno intrapreso un percorso di informazione e formazione in materia, con lo scopo di intervenire tramite una regolamentazione del settore, servendosi inoltre di collaborazioni con soggetti privati per contrastare questa nuova forma di attività illecita. Sarà oggetto di tale capitolo, l'analisi dell'evoluzione normativa in materia.

3.1 L'evoluzione della regolamentazione

Durante l'introduzione delle criptovalute all'interno del mercato, non esisteva una regolamentazione specifica in materia, inizialmente infatti il Bitcoin fu accolto come un asset digitale sconosciuto e anonimo. L'attenzione giuridica verso tale settore iniziò con l'avvento del Silk Road, un mercato del dark web all'interno del quale era possibile reperire qualsiasi tipo di materiale, come documenti illegali o sostanze stupefacenti, che, come moneta di scambio, imponeva l'utilizzo del Bitcoin, viste le sue caratteristiche intrinseche e l'assenza di un relativo quadro normativo. Tale situazione fece emergere l'urgenza di un intervento normativo in materia da parte delle autorità competenti, le quali per la prima volta videro il pericoloso potenziale dei nuovi asset digitali; non è un caso, infatti, che lo stesso anno, l'Autorità bancaria europea (EBA)¹³ emise un primo avviso pubblico contro le criptovalute, con l'intento di far percepire le pericolosità dietro a questa moneta; tuttavia, una volta svanito l'allarme iniziale, la percezione cambiò: il crollo di Silk Road aveva effettivamente permesso alla criptovaluta di allontanarsi dalla sua reputazione iniziale di strumento di facilitazione per le attività illegali.

Successivamente a questa fase iniziale, chiamata in gergo "*Wild West*", vista l'assenza di una supervisione normativa, il periodo seguente fu caratterizzato da una reazione alle conseguenze di tale assenza: dopo la chiusura di Silk Road, le nuove normative entrate in vigore in America furono infatti in gran parte reazionarie in risposta a quell'evento, lo scopo non era costruire una struttura normativa adeguata e specifica, bensì limitare il più possibile i danni; le agenzie si affrettarono a trovare metodi per protezione dei clienti che erano caduti vittime di truffe e per cercare di impedire che le criptovalute venissero utilizzate con un mero fine illecito. In sintesi, la regolamentazione entrata in vigore dopo i primi anni di operatività delle criptovalute, difficilmente potrebbe essere

¹³ Agenzia dell'UE incaricata di attuare un corpus di norme standard per regolamentare e vigilare sul settore bancario in tutti i paesi dell'UE. Il suo obiettivo è creare un mercato unico dei prodotti bancari dell'UE efficiente, trasparente e stabile.

definita tale, piuttosto dovrebbe essere considerata come una punizione reazionaria alle attività illegali e una corsa all'acquisizione di informazioni attraverso le quali poter salvaguardare i clienti da frodi e truffe.

Dopo tale periodo "reazionario", grazie alla consultazione con gli esperti del settore, diversi input e consigli delle agenzie e rigide protezioni per i consumatori, è stata implementata una regolamentazione in materia a livello globale.

Partendo dagli USA, nel 2023 sono stati apportati degli sviluppi importanti in materia, tra i quali sono degni di nota due progetti di legge in particolare: il "*Financial Innovation and Technology for the 21st Century Act*" e il "*Blockchain Regulatory Certainty Act*". Il FIT21 ha fornito i parametri in base ai quali una criptovaluta debba essere considerata come titolo o come merce, nello specifico:

- La CFTC¹⁴ deve regolamentare e considerare un asset digitale come merce se la blockchain, o registro digitale, di riferimento è funzionale e decentralizzata. Il disegno di legge classifica una blockchain come decentralizzata se nessuna persona ha autorità unilaterale per il controllo della blockchain o il suo utilizzo e nessun emittente o persona affiliata ha il controllo del 20% o più dell'asset digitale. Inoltre, tale legge fornisce alla CFTC un'autorità di regolamentazione esclusiva sui mercati cash o spot per le commodity digitali.
- La SEC¹⁵ deve regolamentare e considerare un asset digitale come titolo se la sua blockchain associata è funzionale ma non decentralizzata. Tuttavia, il disegno di legge stabilisce alcune eccezioni alla regolamentazione SEC per gli asset digitali che limitano le vendite annuali, restringono l'accesso degli investitori non accreditati e soddisfano i requisiti di informativa e conformità.

Per quanto riguarda invece il BRCA, questa esenta da determinati requisiti di rendicontazione finanziaria e di licenza gli sviluppatori di blockchain e i fornitori di servizi blockchain che non assumono il controllo dei fondi dei consumatori. Lo scopo della legislazione attuata, risulta dunque essere quello di ampliare la supervisione del settore e chiarire i ruoli dei diversi enti nella gestione delle criptovalute; al momento però, va sottolineato che dall'emanazioni di tali leggi, gli sforzi legislativi federali si sono generalmente bloccati, non apportando alcun ulteriore progresso in materia.

Spostando il focus sull'Europa, nel maggio del 2023, è stata introdotta la prima regolamentazione completa in materia, nota come MiCA¹⁶, si tratta di una regolamentazione dei mercati delle

¹⁴ Commodity Futures Trading Commissions, agenzia federale indipendente, nata con lo scopo di promuovere l'integrità e la resilienza nei mercati degli USA attraverso un corpo di regole uniformi.

¹⁵ Securities and Exchange Commission, ente federale statunitense preposto alla vigilanza delle borse valori.

¹⁶ "Markets in Crypto-Assets"

criptovalute, la quale istituisce norme di mercato uniformi nell'Unione Europea per le crypto-attività che non sono attualmente regolamentate dalla legislazione vigente sui mercati finanziari. Nello specifico, all'interno sono contenute disposizioni, per coloro che emettono e commerciano criptovalute, riguardanti la trasparenza, la divulgazione e la supervisione delle transazioni, includendo un numero considerevole di misure di livello 2 e 3 che devono essere sviluppate prima dell'entrata in vigore del nuovo regime (entro una scadenza di 12-18 mesi a seconda del mandato); a tal proposito, l'ESMA¹⁷ (in stretta collaborazione con EBA, EIOPA¹⁸ e BCE) ha avviato una consultazione con gli esperti del settore su una serie di standard tecnici, che saranno pubblicati in sequenza di tre pacchetti. Le misure di cui sopra obbligano ogni azienda che emette o scambia crypto asset a dotarsi di una specifica licenza, senza la quale non sarà possibile operare; inoltre, da gennaio 2026, tutti i fornitori di servizi aventi come oggetto le criptovalute dovranno registrare obbligatoriamente il nome di mittenti e beneficiari (indipendentemente dall'importo trasferito) e tutti i wallet self-hosted contenenti una cifra superiore ai 1.000 euro dovranno sottoporsi alla verifica della proprietà del wallet per le transazioni.

A quanto riportato va aggiunta la presenza delle cinque direttive antiriciclaggio emanate dall'UE, delle quali, la quarta e la quinta rivestono un ruolo di particolare importanza, dal momento che entrambe sono state introdotte con lo scopo di rafforzare le misure di prevenzione adottate dagli Stati membri, in linea con le Raccomandazioni del G.A.F.I.¹⁹ del 2012, sottolineando l'importanza di un approccio fondato sul rischio. Tale approccio prevede: l'analisi dei potenziali sospetti di riciclaggio condotta a livello nazionale da parte di ciascuno Stato membro, attraverso specifici approfondimenti sul rischio (national risk assessment), e la combinazione con un'iniziativa sovranazionale coordinata dalla Commissione Europea, finalizzata all'identificazione e alla valutazione dei rischi generati dalle interrelazioni di minacce e vulnerabilità presenti nei vari Stati membri.

Nello specifico, la Quarta Direttiva conferma la rilevanza fondamentale delle Financial Intelligence Unit²⁰ (FIU), le quali hanno il compito di ricevere segnalazioni di operazioni sospette, condurre analisi focalizzate sui casi di rischio ritenuti effettivi e diffondere le informazioni recepite e raccolte. A tal proposito, le disposizioni relative alla cooperazione internazionale sono state recentemente riviste e ampliate, stabilendo la possibilità per le FIU di poter rispondere alle richieste

¹⁷ Autorità Europea degli strumenti finanziari e dei mercati.

¹⁸ Autorità europea delle assicurazioni e delle pensioni aziendali o professionali.

¹⁹ Gli *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, elaborate dal GAFI e compendiate in quaranta Raccomandazioni, rappresentano i principi fondamentali in materia di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo che i paesi sono chiamati a recepire nel contesto dei rispettivi ordinamenti giuridici, amministrativi e finanziari.

²⁰ Unità di raccolta di informazioni finanziarie presente in ciascuno Stato nel rispetto delle norme e dei criteri internazionali, vedasi UIF in Italia. Sono dotate di completa autonomia operativa e amministrativa e sono responsabili della lotta al riciclaggio di denaro e al finanziamento del terrorismo.

provenienti da altri Paesi con gli stessi poteri disponibili per l'analisi a livello domestico, senza tenere conto delle differenze legislative presenti tra i diversi Stati membri; è stato inoltre introdotto l'obbligo di "scambio automatico" di segnalazioni riguardanti operazioni sospette con caratteristiche transnazionali, imponendo alle FIU l'obbligo di inviare tempestivamente alle controparti europee le segnalazioni attinenti ad altri Stati membri.

Per quanto concerne la Quinta Direttiva, questa amplia il novero dei soggetti obbligati al rispetto delle misure antiriciclaggio, includendo tra questi anche gli operatori nel settore delle valute virtuali, e fornisce disposizioni maggiormente dettagliate per quanto riguarda l'adeguata verifica della clientela, con particolare attenzione ai rapporti con controparti provenienti da Paesi considerati ad alto rischio. Tale disposizione mira, inoltre, ad estendere le misure di trasparenza relative alla titolarità effettiva delle società, grazie alla creazione di registri nazionali accessibili e interconnessi, e a potenziare le competenze delle FIU per l'analisi a livello domestico e per la cooperazione.

Infine, per completare il quadro normativo, è stato modificato recentemente il Regolamento UE/2010/1093 in relazione all'European Banking Authority (EBA), confermando la competenza dell'autorità nazionale nel campo dei controlli antiriciclaggio, ma affidando all'EBA nuovi poteri per la valutazione delle autorità di vigilanza nazionali, comprendendo:

- l'esercizio di enforcement e sanzione;
- l'applicazione di poteri di binding mediation²¹
- l'esercizio di poteri sostitutivi in caso di inerzia dei supervisori nazionali;
- l'elaborazione di linee guida per favorire i controlli e sviluppare la collaborazione.

Muovendo un ulteriore passo, l'attenzione si sposta nuovamente su un altro continente, ovvero l'Asia, riconosciuta al momento come leader mondiale nell'uso delle criptovalute, ma risulta interessante il quadro normativo dei diversi paesi, i quali presentano notevoli differenze:

- Il Giappone è aperto all'uso delle criptovalute, riconoscendone sia la funzione di moneta di scambio che di proprietà legale; pertanto, le transazioni in criptovalute e yen sono entrambe gestite dalla Financial Services Agency del paese e i cittadini del paese sono liberi di possedere o investire in criptovalute. Il paese ha recentemente inasprito le regole circa la condivisione delle informazioni dei clienti tra gli exchange di criptovalute, nel tentativo di contrastare il riciclaggio di denaro.
- La Corea del Sud si trova invece in fase di aggiornamento, è stata infatti approvata il *"Virtual Asset Users Protection Act"* nel 2023, una regolamentazione che crea protezioni

²¹ Processo in cui un terzo neutrale, imparziale e indipendente facilita la comunicazione tra le parti coinvolte in una controversia al fine di raggiungere un accordo.

più forti per gli utenti aggiungendo obblighi di tenuta dei registri e trasparenza. Nell'aprile del 2024, inoltre, sono state pubblicate linee guida per quanto riguarda la quotazione degli asset virtuali, le quali prevedono l'impossibilità di quotazione per asset virtuali coinvolti in situazioni hackeraggio (a meno che la causa non sia stata chiaramente identificata) e la possibilità di quotazione di criptovalute estere solo nel caso in cui sia stato pubblicato un white paper o un manuale tecnico per il mercato coreano.

- La Cina risulta essere uno dei paesi più severi in materia, vi è infatti un divieto assoluto su tutte le attività correlate alle criptovalute e a tutte le aziende è vietato fornire qualsiasi servizio avente come oggetto le criptovalute, in quanto considerate attività finanziarie illegali dalla People's Bank of China e dagli enti governativi. A settembre 2021, il paese ha annunciato ulteriori misure severe per combattere l'adozione delle criptovalute in Cina, tra cui un ulteriore controllo delle società che supervisionano le normative.
- Il governo indiano ha cambiato notevolmente il suo punto di vista sulla regolamentazione delle criptovalute nel corso degli anni, ad aprile 2018, la banca centrale indiana aveva infatti imposto un divieto sulla vendita o l'acquisto di criptovalute, per poi essere annullato dalla Corte Suprema. Nel bilancio del 2022, il governo ha chiarito la sua posizione circa le attività digitali, imponendo una tassa fissa del 30% sui profitti ottenuti dal trading o dagli investimenti in criptovalute, insieme a una detrazione fiscale dell'1% alla fonte, non consentendo ai trader e agli investitori di compensare i guadagni con le perdite. È stato inoltre programmato un disegno di legge sulle criptovalute e una regolamentazione delle valute digitali ufficiali (il quale deve essere ancora approvato dal parlamento) con lo scopo di consentire la creazione di una valuta digitale ufficiale da parte della Reserve Bank Of India.

Degna di nota è anche la regolamentazione introdotta dal Brasile nel 2023, coincidente con la nomina della banca centrale come supervisore delle cripto-attività: il "*Virtual Assets Act*" riguarda le linee guida per la fornitura di servizi con asset virtuali e per la regolamentazione dei fornitori di tali servizi. L'atto definisce gli asset virtuali come una rappresentazione digitale di valore che può essere scambiata o trasferita elettronicamente e utilizzata per effettuare pagamenti o per scopi di investimento; nello specifico prevede:

- l'autorizzazione preventiva per la fornitura di servizi;
- i principi guida dell'attività;
- la definizione dei servizi di fornitura di servizi di asset virtuali;

- l'impostazione di nuove responsabilità penali nell'intermediazione di operazioni che comportano frodi, oltre all'aumento delle sanzioni se la pratica avviene nell'ambito delle normative che combattono il riciclaggio di denaro e la criminalità organizzata.

Dopo l'emanazione di tale atto, il governatore della banca centrale brasiliana ha dichiarato di voler imporre una regolamentazione maggiormente stringente in materia.

Per quanto riguarda la Gran Bretagna, questa si è mostrata particolarmente attiva in materia e in continua elaborazione di regole per il settore delle criptovalute. Di rilevante importanza è l'obbligo imposto alle aziende del settore, le quali dovranno essere autorizzate dalla FCA del paese per poter operare, la quale, in accordo con la Bank of England, ha proposto l'introduzione di normative per le stablecoin, monete progettate per avere un valore più stabile rispetto alle criptovalute, avendo il loro valore legato a quello di un altro asset. La Banca d'Inghilterra afferma che la sua regolamentazione avrebbe lo scopo di sfruttare i potenziali benefici che le stablecoin potrebbero offrire ai consumatori e ai rivenditori del Regno Unito, in particolare rendendo i pagamenti più rapidi ed economici, lavorando al contempo sulla protezione dei consumatori prevenendo il riciclaggio di denaro e salvaguardando la stabilità finanziaria.

In conclusione, l'Organizzazione internazionale delle commissioni per i valori mobiliari ha presentato le sue 18 raccomandazioni circa le norme globali sulla gestione delle criptovalute e degli asset digitali, ritenendo necessaria una maggiore coerenza nella regolamentazione e nella supervisione delle attività relative alle criptovalute, data la natura transfrontaliera dei mercati, che crea un "rischio significativo di danni" per gli investitori. A tal proposito, viene in ausilio il rapporto prodotto dal World Economic Forum "*Pathways to the Regulation of Crypto-Assets: A Global Approach*", documento che mira ad un allineamento internazionale su alcune regole relative alle criptovalute come "non solo auspicabile, ma necessario".

"È necessario un approccio globale per massimizzare i vantaggi della tecnologia sottostante e per gestire i rischi", afferma il documento. *"Tuttavia, dati i diversi stadi di maturità del mercato, lo sviluppo di hub regionali e la diversa capacità degli enti regolatori, è prudente concentrarsi in modo olistico anche sull'importante ruolo che le organizzazioni internazionali e gli enti regolatori nazionali/regionali, nonché gli attori del settore, possono svolgere nel garantire un'evoluzione normativa responsabile".*

Dalla disamina condotta si evince dunque la diversità tra i diversi Stati circa il trattamento delle criptovalute: da una ricerca di trasparenza attraverso obblighi di licenza e iscrizione presso registri pubblici (con fini preventivi) all'assoluta non accettazione di tale moneta; affermando però, al

contempo, la ricerca di una direzione normativa comune, basata prima di tutto sulla collaborazione, oltre che prevenzione.

3.2 Gli indicatori d'allarme

Per poter contrastare in maniera efficace l'utilizzo illecito delle criptovalute è necessaria non solo un'adeguata regolamentazione normativa in materia, bensì risulta opportuno produrre e servirsi di indicatori di allarme, volti a segnalare nei tempi più celeri possibili un possibile utilizzo illecito delle valute virtuali, favorendo il lavoro delle autorità competenti e dando loro la possibilità di troncane sul nascere tali attività, prima che la loro tracciabilità ed identificabilità diventi esageratamente complessa.

A tal proposito, nel 14 settembre 2020, il GAFI ha rilasciato un documento intitolato "*Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*", che in parte estende le Linee Guida del 2019. Il Rapporto mette in rilievo una serie di indicatori di anomalia ("*red flag indicators*") che possono suggerire un uso illecito degli asset virtuali, si tratta di segnali utili nel sostegno delle VASPs, delle istituzioni finanziarie, dei professionisti e degli operatori obbligati nell'identificazione e segnalazione di transazioni sospette e nel compimento di una adeguata due diligence sui clienti, così come per l'assistenza alle Autorità di Controllo nell'analisi delle segnalazioni di operazioni sospette e nel monitoraggio complessivo degli obblighi antiriciclaggio.

Il Rapporto specifica, tuttavia, che la semplice elencazione delle condotte esaminate non giustifica automaticamente l'invio di segnalazioni di operazioni sospette; piuttosto, il customer due diligence deve considerare tali comportamenti all'interno di un contesto più ampio e in combinazione con indicatori di rischio tradizionali relativi a clienti, operazioni e prodotti.

Il GAFI identifica in dettaglio sei principali indicatori di anomalia associati a specifiche macroaree di utilizzo sospetto degli asset virtuali, offrendo per ciascuno una dettagliata descrizione dei modelli e comportamenti anomali, corredata da esempi pratici rilevanti osservati negli ultimi anni, nello specifico:

1. Anomalie legate alle transazioni. Possono emergere quando la loro dimensione e frequenza rivelano diverse criticità, come ad esempio un volume elevato di piccoli scambi di asset virtuali o la loro conversione in contanti, oppure ancora, trasferimenti di asset virtuali a più piattaforme VASPs situate in giurisdizioni con rischi elevati in materia di antiriciclaggio.
2. Comportamenti inappropriati nelle transazioni. È il caso di clienti che avviano operazioni incoerenti con il loro profilo, particolarmente in termini di volumi di asset virtuali scambiati o trasferiti, o quando un cliente esegue operazioni con vari tipi di asset virtuali e conti senza una spiegazione logica, inclusa la conversione in valuta corrente con perdite.

3. Utilizzo di tecnologie che favoriscono l'anonimato. Queste tecnologie rendono gli asset virtuali attraenti per attività di riciclaggio di denaro e finanziamento del terrorismo; ciò include clienti che operano con criptovalute potenziate per l'anonimato o utilizzano indirizzi IP o e-mail mascherati, o accedono alle piattaforme VASPs con strumenti che impediscono l'identificazione del titolare del dominio. In generale, le operazioni il cui anonimato ostacola una adeguata due diligence sui clienti sin dal processo di onboarding sono considerate anomale.
4. Soggetti che inviano o ricevono le transazioni, specialmente durante la creazione dell'account, utilizzando indirizzi IP anonimi o più account creati dallo stesso individuo, o quando vi è insufficienza di informazioni per una corretta due diligence sui clienti (informazioni false, incomplete o inesistenti sui clienti, origine dei fondi e destinazione). Si tratta di anomalie che possono derivare anche da discrepanze tra gli indirizzi IP associati ai profili dei clienti e quelli usati per effettuare transazioni. Inoltre, potrebbero esserci casi di individui utilizzati come "mulini per denaro" per riciclare proventi illeciti, come quando una persona con scarsa familiarità tecnologica attiva uno o più account per condurre numerose transazioni, magari di valore non compatibile con il suo profilo economico;
5. Provenienza dei fondi. Qualora risultino potenzialmente derivanti da traffico di droga, frodi, attacchi informatici e attività criminali in generale; il FATF²² identifica come sospetti l'uso di asset virtuali legati a servizi di gioco d'azzardo online, l'uso di carte di credito/debito associate a portafogli di asset virtuali per prelevare grandi quantità di denaro, o grandi depositi di valuta virtuale seguiti da conversioni in moneta legale, indicando un potenziale furto di asset virtuali. Ulteriori rischi possono derivare dalla mancanza di informazioni su origine e proprietari dei fondi, magari usando società di comodo, in connessione con offerte iniziali di nuove criptovalute²³.
6. Contesto geografico. Visto lo sfruttamento, da parte dei riciclatori, delle lacune sistemiche nella conformità agli standard GAFI nel settore specifico degli asset virtuali e dei fornitori di servizi a loro connessi. Molti paesi, infatti, non richiedono ancora l'aderenza ai requisiti antiriciclaggio per i partecipanti nell'ecosistema degli asset virtuali, creando "giurisdizioni a rischio" che vedono la registrazione di VASPs e il sorgere di operazioni provenienti, destinate o in transito in tali regioni.

In conclusione, tale documento sottolinea come gli indicatori di allerta, i quali si concentrano sulle caratteristiche intrinseche e le vulnerabilità legate agli asset virtuali, debbano comunque essere

²² "Financial Action Task Force", si tratta di un'organizzazione intergovernativa fondata nel 1989 su iniziativa del G7 per sviluppare politiche di lotta al riciclaggio di denaro.

²³ È il caso delle Initial Coin Offerings, vedasi capitolo 2.1.1.

considerati nel contesto di una più ampia attività di conformità alle normative antiriciclaggio, conformità che dovrebbe essere basata su un approccio dinamico orientato al rischio e prevedere una collaborazione bidirezionale tra le Autorità di Vigilanza e i soggetti obbligati.

3.3 I paesi ad alto rischio

Analizzando le normative attualmente in vigore e l'evoluzione delle stesse, si evince il modus operandi dei legislatori e la direzione normativa da essi perseguita. Alla luce delle analisi svolte è infatti possibile affermare che la strategia al momento adottata per contrastare l'uso illecito delle criptovalute sia strettamente basata sulla collaborazione, non solo tra i soggetti obbligati e il proprio Stato d'appartenenza, bensì una vera e propria collaborazione internazionale, soprattutto tra gli stati membri dell'Unione Europea. Tale strategia trova le sue fondamenta sull'approccio adottato dall'UE in materia antiriciclaggio, ovvero l'approccio basato sul rischio, avente come fine la prevenzione delle sopraccitate attività illegali, con lo scopo di reprimere le suddette attività sul nascere, in modo tale da evitare il sostentamento di sistemi di riciclaggio e di raggiro prima che diventino talmente complessi e ben strutturati da rendere la loro tracciabilità e identificabilità potenzialmente irraggiungibile. Risulta dunque necessaria ed indispensabile la collaborazione viste le basi di partenza, dal momento che la prevenzione richiede l'accesso al più largo novero di informazioni possibili per poter essere efficace, e l'unico modo è quello di mettere insieme le conoscenze e referenze di tutti i soggetti obbligati residenti in ogni Stato membro e di tutte le autorità di competenza in tale materia. Una volta concordata quindi l'importanza della collaborazione all'interno della strategia attualmente adottata, vi si pone un problema di assoluta rilevanza, ovvero la collaborazione con i paesi aventi legislazioni in materia poco stringenti se non addirittura assenti. Attualmente sono diversi gli stati recanti le suddette caratteristiche, le quali offrono terreno fertile per le organizzazioni criminali o qualsiasi persona operi attività di riciclaggio od illecite attraverso le valute virtuali, non è un caso, infatti, che la maggior parte delle criptovalute vengano trasferite presso conti intestati in paesi aventi legislazioni lasche. Le strade da perseguire per poter fronteggiare a tale situazione non sono molteplici, è possibile produrre un appello volto ai paesi sopraccitati denotando l'importanza di una legislazione solida e ben strutturata ai fini della sicurezza economica globale; ma il problema risiede nel fatto, che nella maggior parte dei casi, le attività di riciclaggio o qualsiasi altra attività legata ai traffici illeciti, rappresentano la fonte di ricchezza economica primaria per i suddetti paesi, i quali difficilmente deciderebbero di farne a meno. In merito a tale situazione, il GAFI, nel giugno del 2023, ha prodotto una lista (in continuo aggiornamento) dei paesi ad alto rischio di riciclaggio e finanziamento del terrorismo, all'interno della quale sono attualmente presenti i seguenti stati: Afghanistan, Barbados, Burkina Faso, Isole Cayman, Repubblica democratica del Congo, Haiti, Gibilterra, Mali, Giordania, Mozambico,

Nigeria, Myanmar, Filippine, Panama, Senegal, Sud Sudan, Sud Africa, Tanzania, Uganda, Tobago, Trinidad, Emirati Arabi Uniti, Yemen, Vanuatu.

Sarà di rilevante importanza l'impegno nel mantenere aggiornata tale lista, dal momento che essere a conoscenza di quali siano i paesi ad alto rischio di riciclaggio e finanziamento del terrorismo risulta fondamentale principalmente per due aspetti: l'applicazione di misure rafforzate di adeguata verifica per i detentori di criptovalute residenti in paesi ad alto rischio (ai sensi del D. Lgs. 231/2007) e la deducibilità dei costi relativi ad operazioni con imprese localizzate in paesi ad alto rischio.

CAPITOLO IV: CONCLUSIONI

Alla luce delle disamine svolte nei precedenti capitoli, si è constatato il crescente utilizzo delle criptovalute per fini illeciti: dalla creazione di nuovi metodi di riciclaggio innovativi, efficienti ed efficaci, all'introduzione di nuove monete per il pagamento di vendite online aventi come oggetto beni o materiali illegali (quali sostanze stupefacenti, farmaci, traffico di organi di essere umani, armi e altri materiali volti al finanziamento del terrorismo) fino ad arrivare alla produzione di schemi fraudolenti. Se da una parte però si è registrato un crescente uso illecito delle criptovalute, dall'altra si evince una crescente attenzione ed impegno da parte delle autorità inquirenti competenti in materia. È il caso dell'emanazione della IV e V direttiva europea antiriciclaggio, la quale ha favorito l'attenzione ed impegno da parte degli stati membri nel produrre un sistema antiriciclaggio maggiormente solido con l'inserimento all'interno dell'ordinamento giuridico di leggi e disposizioni maggiormente stringenti per quanto riguarda la prevenzione dell'illegale uso delle valute virtuali. A quanto sopraccitato si aggiunge inoltre il rilascio del documento "*Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*" da parte del GAFI, contenente indicatori di anomalia associati all'utilizzo sospetto degli asset virtuali, in modo tale da prevenire nei tempi più celeri possibili un errato ed illegale uso delle valute virtuali. È possibile dunque affermare che le autorità competenti abbiano recepito l'urgenza di una regolamentazione normativa in materia, iniziando da subito la lotta alla repressione delle attività di cui sopra, con lo scopo di designare una direzione normativa comune basata soprattutto sulla collaborazione tra i diversi Stati. L'approccio della direzione normativa perseguita è detto "basato sul rischio", il quale prevede una costante valutazione delle potenziali minacce di riciclaggio, l'identificazione delle vulnerabilità all'interno del sistema e l'individuazione dei settori maggiormente esposti a tali rischi. Da tale approccio si evince un ulteriore principio sul quale poggia la direzione normativa, ovvero quello della prevenzione: lo scopo è di reprimere quanto prima possibile la creazione di schemi di riciclaggio e l'utilizzo illecito delle criptovalute prima che l'individuazione e identificabilità diventino eccessivamente complesse se non inutili. A tal proposito va ricordata la creazione di una lista di soggetti obbligati al rispetto delle misure antiriciclaggio, ovvero soggetti tenuti alla collaborazione con le autorità inquirenti, alla diffusione di segnalazioni circa l'esistenza di operazioni sospette, alla conservazione di documenti e informazioni, per garantire la tracciabilità dei flussi finanziari e ad attuare un'adeguata verifica della clientela; notiamo così, come anche in questo caso, i principi cardine siano la collaborazione e prevenzione. Va quindi riconosciuta la validità ed efficienza del sistema di repressione prodotto, ma al tempo stesso ne vanno riconosciuti i limiti con prospettiva critica ed oggettiva, col fine di poter offrire un ausilio in materia, proponendo nuove strade normative da percorrere per poter contrastare e reprimere, nel modo più efficace ed efficiente possibile, le attività illegali legate all'uso delle criptovalute. In primis, è necessario

riconoscere la rischiosa posizione degli Stati aventi legislazioni in materia poco stringenti e vincolanti, è il caso dei paesi presenti all'interno della lista dei paesi ad alto rischio di riciclaggio e finanziamento al terrorismo prodotta dal GAFI; tali paesi rappresentano un ambiente favorevole per le organizzazioni criminali facenti uso illegale delle criptovalute, non è infatti un caso il costante trasferimento di valute virtuali presso tali paesi. Una direzione normativa da poter perseguire a tal proposito potrebbe essere quella di emanare disposizioni, in forza delle quali, nel momento in cui venga avviata una transazione avente come destinatario un conto intestato presso i paesi sopraccitati e come importo quantità ingenti di denaro che superino un certo limite espresso dalle disposizioni, questa venga bloccata, segnalata alle autorità competenti, e successivamente convalidata solo nel caso in cui il mittente giustifichi con prove di giusta causa la transazione. Togliendo l'attenzione dai paesi ad alto rischio, un'altra proposta potrebbe essere quella di negare la possibilità di trasferire tante piccole quantità di denaro (espresse in criptovalute) in una breve frazione di tempo, se non appunto una volta giustificate le transazioni con prove di giusta causa. In sintesi, la direzione normativa proposta è pur sempre caratterizzata dai principi di collaborazione tra i soggetti obbligati, le autorità inquirenti e i diversi Stati, nonché di prevenzione, ma al tempo stesso mira ad essere maggiormente stringente, vincolante ed invasiva, in modo da affrontare con maggior concretezza e prontezza le segnalazioni di operazioni sospette, col fine di garantire il giusto utilizzo delle criptovalute, trovando il giusto compromesso tra la privacy e l'invasività.

Un'ultima proposta potrebbe essere quella di creare delle valute virtuali centralizzate, aventi le stesse caratteristiche intrinseche delle criptovalute, ma regolate dagli enti preposti di ciascun stato emittente. Risulta ovvio che così facendo si andrebbe a perdere l'essenza della criptovaluta stessa ed il motivo del suo successo, ovvero essere regolata da un ente terzo, estraneo alle banche centrali, ma si avrebbe la quasi totale sicurezza che chiunque acquisti tali monete, operi l'acquisto con il mero fine d'investimento.

In conclusione, dunque, l'impegno nelle attività di antiriciclaggio e repressione dell'utilizzo illecito delle criptovalute da parte delle autorità inquirenti e degli enti preposti è sicuramente valido e riconosciuto, ma al tempo stesso risulta necessario un continuo aggiornamento ed impegno in materia, nonché l'emanazione di nuove norme ed il perseguimento di una direzione normativa maggiormente stringente, basata non solo sulla prevenzione, bensì sull'interventismo immediato; dal momento che le organizzazioni criminali e qualsiasi persona svolga attività illecite mediante l'uso delle criptovalute, sono in continuo aggiornamento ed evoluzione, pronti a servirsi nell'immediato di qualsiasi metodo innovativo, volto al raggirare e sfruttamento di buchi normativi presenti all'interno degli ordinamenti giuridici dei diversi Stati.

i

BIBLIOGRAFIA

CANIO GIUSEPPE LA GALA, Rassegna dell'arma dei carabinieri, *“Il riciclaggio di denaro, strumenti contrati e misure patrimoniali”*, supplemento al n.4/2000 della rassegna dell'arma dei carabinieri, periodico trimestrale – “spedizione in A. P. ART. 2 comma 20/C legge 662/96 – filiale di Roma”

UNITA' DI INFORMAZIONE FINANZIARIA PER L'ITALIA, *“normativa antiriciclaggio”*, [online] disponibile su <<https://uif.bancaditalia.it/normativa/norm-antiricic/index.html?com.dotmarketing.htmlpage.language=102>>

EUROPOL SPOTLIGHT , *“Cryptocurrencies: Tracing The Evolution Of Criminal Finances”*, [online] disponibile su <<https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf>>

UNITA' DI INFORMAZIONE FINANZIARIA PER L'ITALIA, comunicazione del 28 maggio 2019, [online] disponibile su <https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Comunicazione_VV_2019.pdf>

UNITA' DI INFORMAZIONE FINANZIARIA PER L'ITALIA, 2022. Newsletter n.5 *“Aggiornamenti in materia di virtual asset”*, [online] disponibile su <https://uif.bancaditalia.it/pubblicazioni/newsletter/2022/newsletter-2022-5/Newsletter_5_2022.pdf>

FULVIO FONTANA, *“Criptovalute e rischi di riciclaggio”*, [online] disponibile su <<https://www.antiriciclaggiocompliance.it/app/uploads/2020/08/Fontana.pdf>>

CONSOB, *“Le conoscenze finanziarie di base: le criptovalute”*, [online] disponibile su <<https://www.consob.it/web/investor-education/criptovalute>>

MINISTERO DELL'ECONOMIA E DELLE FINANZE, *“Prevenzione dei reati finanziari: Comitato di Sicurezza Finanziaria”*, [online] disponibile su <https://www.dt.mef.gov.it/it/attivita_istituzionali/prevenzione_reati_finanziari/comitato_sicurezza_finanziaria/>

NETWORK DIGITAL 360, 25 maggio 2022. “*Cryptomixer: cosa sono e come funzionano i sistemi per il riciclaggio delle criptovalute*”, [online] disponibile su

<<https://www.cybersecurity360.it/nuove-minacce/cryptomixer-cosa-sono-e-come-funzionano-i-sistemi-per-il-riciclaggio-delle-criptovalute/>>

COINTELEGRAPH, 29 giugno 2023. “*Billions lost in crypto Ponzi schemes in 2022*”, [online] disponibile su <<https://it.cointelegraph.com/news/billions-lost-in-crypto-ponzi-schemes-in-2022>>

UNITED NATIONS, “*Money laundering through cryptocurrencies*”, [online] disponibile su <<https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/laundryingproceeds/moneylaundrying.html>>

COMPUTER WEEKLY, 25 gennaio 2024. “*Criptovalute e traffici illeciti: nel 2023 giro d'affari da 24 miliardi*”, [online] disponibile su

<<https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/laundryingproceeds/moneylaundrying.html>>

SKRILL, “*Che cos'è una privacy coin?*”, [online] disponibile su

<<https://www.skrill.com/it/crypto/the-skrill-crypto-academy/advanced/che-cose-un-privacy-coin/#:~:text=Una%20privacy%20coin%20%C3%A8%20un,la%20maggior%20parte%20%C3%A8%20pseudonima>>

DARIO MARCHETTI, 2022. Guida alle privacy coin: cosa sono e a cosa servono. *Tuttotech*

[online]. Disponibile su <<https://www.tuttotech.net/fintech/guida-privacy-coin-cosa-sono.html>>

Raccomandazioni FATF. 21 giugno 2019. “*Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*”

FATF, Settembre 2020. “*Virtual assets Red Flag Indicators of Money Laundering and Terrorist Financing*” [online]. Disponibile su <<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf>>

SOPHIE CAMP, 25 luglio 2024. The evolution of crypto regulations. *Fideum* [online]. Disponibile su <<https://www.fideum.com/blog/the-evolution-of-crypto-regulations>>

WORLD ECONOMIC FORUM, 2 maggio 2024. Cryptocurrency regulations are changing across the globe [online]. Disponibile su <<https://www.weforum.org/agenda/2024/05/global-cryptocurrency-regulations-changing/>>

ESMA. “*Markets in Crypto-Assets Regulation (MiCA)*” [online]. Disponibile su <<https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica>>

GUNEET KAUR, 15 settembre 2023. An overview of the cryptocurrency regulations in Asia. *Cointelegraph* [online]. Disponibile su <<https://cointelegraph.com/learn/an-overview-of-the-cryptocurrency-regulations-in-asia>>

CONGRESS.GOV. “*H.R.4763 – Financial Innovation and Technology for the 21st Century Act*” [online]. Disponibile su <<https://www.congress.gov/bill/118th-congress/house-bill/4763>>

CONGRESS.GOV. “*H.R.1747 – Blockchain Regulatory Certainty Act*” [online]. Disponibile su <<https://www.congress.gov/bill/118th-congress/house-bill/1747>>

ⁱ Per la stesura di tale elaborato, sono state utilizzate 9.568 parole