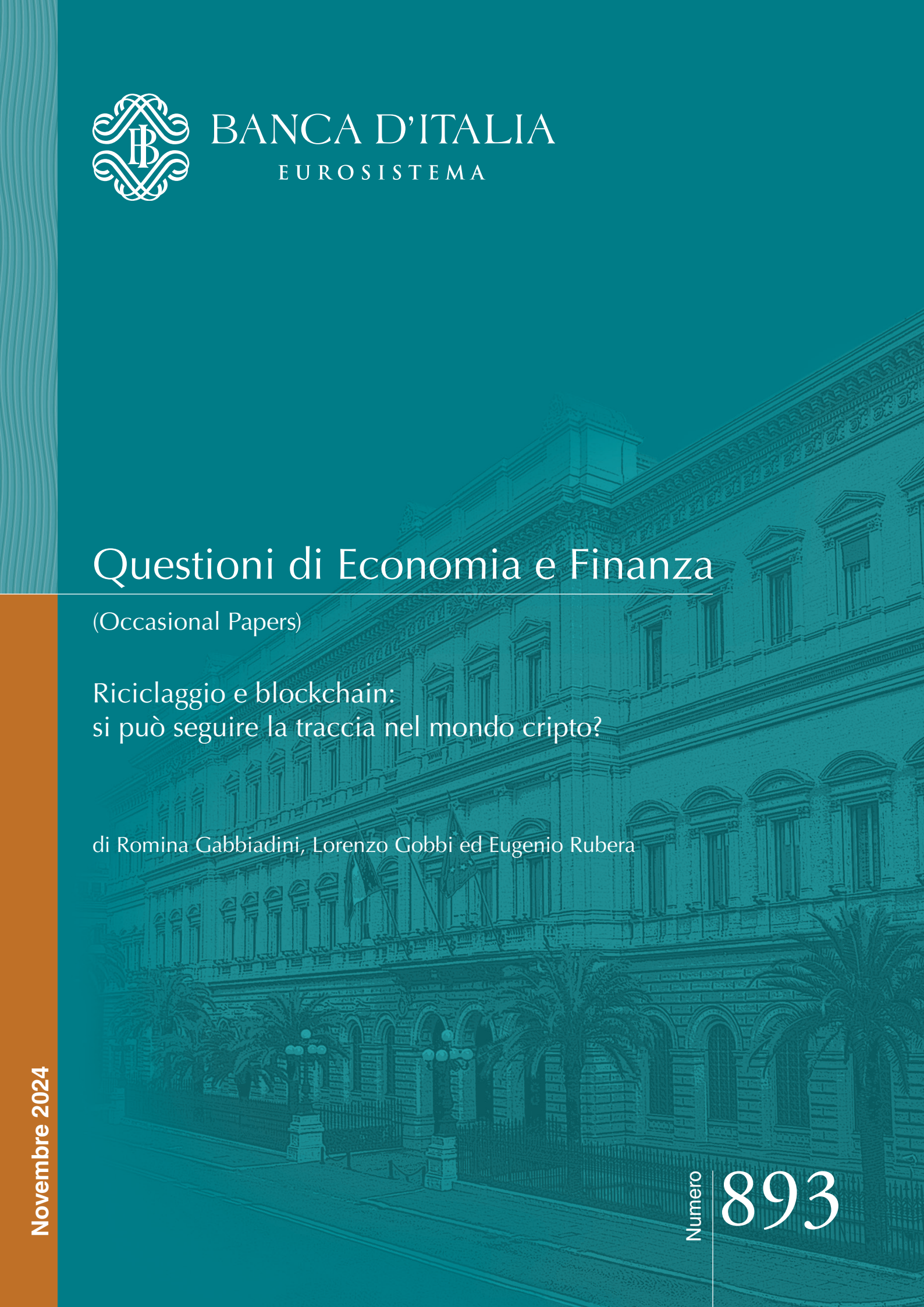
BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

Riciclaggio e blockchain: si può seguire la traccia nel mondo cripto?

di Romina Gabbiadini, Lorenzo Gobbi ed Eugenio Rubera



Novembre 2024

Numero 893

BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

Riciclaggio e blockchain: si può seguire la traccia nel mondo cripto?

di Romina Gabbiadini, Lorenzo Gobbi ed Eugenio Rubera

Numero 893 – Novembre 2024

La serie Questioni di economia e finanza *ha la finalità di presentare studi e documentazione su aspetti rilevanti per i compiti istituzionali della Banca d'Italia e dell'Eurosistema. Le* Questioni di economia e finanza *si affiancano ai* Temi di discussione *volti a fornire contributi originali per la ricerca economica.*

La serie comprende lavori realizzati all'interno della Banca, talvolta in collaborazione con l'Eurosistema o con altre Istituzioni. I lavori pubblicati riflettono esclusivamente le opinioni degli autori, senza impegnare la responsabilità delle Istituzioni di appartenenza.

La serie è disponibile online sul sito www.bancaditalia.it .

ISSN 1972-6643 (online)

Grafica a cura della Divisione Editoria e stampa della Banca d'Italia

RICICLAGGIO E BLOCKCHAIN: SI PUÒ SEGUIRE LA TRACCIA NEL MONDO CRIPTO?

di Romina Gabbiadini*, Lorenzo Gobbi* ed Eugenio Rubera*

Sommario

Il riciclaggio è il processo attraverso il quale la ricchezza di provenienza illecita (denaro, valori, beni) viene occultata, trasferita per dissimularne l'origine e successivamente reinvestita nei circuiti dell'economia legale. Non esiste una quantificazione univoca del fenomeno ma le stime delle diverse istituzioni sono concordi nell'affermarne un'incidenza sull'economia legale significativa e che non evidenzia segnali di contrazione.
Rispetto al mondo tradizionale, nel mercato cripto la misurazione del perimetro del riciclaggio è resa ancora più complessa dalla presenza di ulteriori strumenti che consentono di fare perdere le proprie tracce. La regolamentazione in materia, in ambito nazionale ed europeo, ha pertanto esteso il novero dei destinatari delle norme ai soggetti che prestano servizi in criptoattività, ma permangono spazi non regolamentati perché connessi a modelli di offerta decentralizzati o perché appartenenti ad altre geografie.
Obiettivo del presente lavoro è approfondire le tecniche di utilizzo per finalità di riciclaggio (e di finanziamento del terrorismo) della blockchain e delle criptoattività per valutare l'efficacia delle nuove soluzioni tecnologiche basate su *smart contract* nell'intercettare in DeFi le operazioni anomale.

Classificazione JEL: G18, G23, G28.

Parole chiave: adeguata verifica, AML, blockchain, cripto, DeFi, DLT, riciclaggio, *smart contracts*, *zero-knowledge proof*.

DOI: 10.32057/0.QEF.2024.893

* Banca d'Italia, Divisione Fintech Milano.

1. Introduzione[1]

Il riciclaggio è il processo attraverso il quale la ricchezza di provenienza illecita (denaro, valori, beni) viene occultata e la traccia interrotta attraverso trasferimenti che ne dissimulano l'origine con il fine del successivo reinvestimento nei circuiti dell'economia legale; le azioni di contrasto al fenomeno, oltre a rappresentare un possibile freno alle attività illegali, consentono di limitarne gli effetti distorsivi sulla libera concorrenza, sulla crescita economica e sul benessere dei cittadini.

Proprio a causa della sua natura illecita non esiste una quantificazione univoca del riciclaggio e le stime delle diverse istituzioni divergono. Secondo un'analisi del Fondo Monetario Internazionale, a livello globale i proventi annuali delle attività criminali si attestano in un intervallo compreso tra il 2 e il 5 per cento del PIL mondiale; per l'Italia, secondo l'ISTAT sono pari a circa l'1 per cento del PIL e secondo l'ultima analisi nazionale sui rischi di riciclaggio e finanziamento del terrorismo (*National Risk Assessment* – NRA) potrebbero raggiungere il 12 per cento del PIL[2].

Si tratta quindi di un'incidenza significativa sull'economia legale, che non mostra segnali di contrazione, e le modalità di realizzazione del riciclaggio che le istituzioni nazionali e sovranazionali si trovano a fronteggiare sono in continua evoluzione[3]. Chi ricicla ha dimostrato di sapere utilizzare a proprio vantaggio tecnologie e applicazioni nuove, quali le blockchain e le criptoattività, che consentono il trasferimento di valore tramite circuiti alternativi a quelli più regolamentati.

Le stime relative al riciclaggio attraverso criptoattività – intese come rappresentazioni digitali di valore o di diritti che possono essere emesse, trasferite e memorizzate elettronicamente sulla blockchain – sono rese più complesse dalla presenza di ulteriori modalità che, utilizzate da sole o in combinazione con tecniche più tradizionali, consentono di fare perdere le tracce. Queste modalità sfruttano alcune caratteristiche delle criptoattività, fra cui quelle di immaterialità, di velocità di trasferimento, di problematico assoggettamento a confini e controlli geografici, di difficile riconducibilità al soggetto che le possiede.

Vanno pertanto controllati i punti di passaggio tra la finanza tradizionale e il settore cripto – ovvero i sistemi che consentono di convertire moneta in criptoattività e viceversa – al fine di arginare il trasferimento di capitali illeciti verso e da questo nuovo mercato, nel quale è più facile aggirare i presidi antiriciclaggio in essere.

La regolamentazione in materia, in ambito sia nazionale che europeo, ha esteso il novero dei destinatari delle norme ai soggetti che prestano servizi in criptoattività, ma permangono spazi non regolamentati. Esistono infatti modelli di offerta decentralizzati – in cui la tecnologia sostituisce gli intermediari destinatari degli obblighi (cosiddetta *Decentralised Finance*, DeFi)

[1] Si ringraziano per gli utili commenti Giorgio Gobbi, Giuseppe Zingrillo e i colleghi del Dipartimento Informatica Giuseppe Galano, Matteo Nardelli e Fabiana Rossi, le colleghe dell'Unità di Supervisione e Normativa Antiriciclaggio Maria Colonnello e Concetta Galasso. Si ringraziano inoltre i colleghi della UIF Simone Bonella, Alessia Cassetta, Simone Cortellesi, Marco Militello e Daniele Ruscio per il proficuo confronto.
[2] Cfr. Szego (2023).
[3] Cfr. Eurojust (2022).

– e operatori localizzati in giurisdizioni non collaborative, con regole più lasche, che proprio la tecnologia rende facilmente accessibili anche agli utenti italiani ed europei.

Obiettivo del presente studio è approfondire le tecniche di utilizzo per finalità di riciclaggio (e di finanziamento del terrorismo) delle blockchain e delle criptoattività e valutare l'efficacia del sistema in essere nell'intercettare le operazioni anomale realizzate attraverso le criptoattività.

In particolare, il lavoro analizza gli elementi tecnici[4] utili per comprendere il dibattito in corso relativo alla dicotomia tra trasparenza e anonimato, fornisce alcuni cenni sui principi della normativa antiriciclaggio, contestualizza la rilevanza del fenomeno sulla base dei dati disponibili, illustra come si configurano nel mondo cripto le tre fasi classiche del riciclaggio (piazzamento, stratificazione e integrazione) e fornisce alcune riflessioni sulla applicabilità delle misure antiriciclaggio previste dalla normativa in essere al mondo DeFi, nel quale sono assenti i soggetti destinatari degli obblighi.

2. La blockchain e le criptoattività: alcuni concetti di base e alcuni dati

Il settore finanziario ha dimostrato di saper cogliere le opportunità via via offerte dalla tecnologia. Se da un lato l'innovazione digitale ha aumentato il livello di efficienza degli operatori e ha generato effetti su prodotti, servizi, canali di offerta e soggetti, dall'altro tuttavia ha parallelamente abilitato un'attività illecita tecnologicamente più complessa, capace di sfruttare a proprio vantaggio le nuove tecnologie e le nuove *asset-class*.

Negli ultimi anni, hanno suscitato crescente interesse negli investitori e nel pubblico le DLT (*Distributed Ledger Technologies)*, di cui la blockchain rappresenta la categoria prevalente e più conosciuta[5]. L'utilizzo di crittografia in DLT ha consentito lo sviluppo delle criptoattività (o token) e, con esse, si è profilata la possibilità di creare un nuovo ecosistema finanziario decentralizzato (DeFi), che funziona senza un'autorità fiduciaria centralizzata e senza intermediari, ovvero quei soggetti su cui fa perno la normativa per il contrasto del riciclaggio.

La DLT consiste in un registro elettronico distribuito sulla rete informatica, condiviso tra i partecipanti (detti nodi), su cui possono essere memorizzate transazioni verificabili e immutabili. L'aggiunta di nuove informazioni al registro non richiede la validazione da parte di un ente centrale di garanzia, ma prevede il raggiungimento di un accordo tra i partecipanti alla rete tramite i c.d. meccanismi di consenso. La blockchain è una specifica categoria di DLT caratterizzata dal raggruppamento delle transazioni in blocchi, concatenati in ordine cronologico (la catena, *chain,* appunto), per creare un registro non modificabile di tutte le transazioni effettuate[6].

Sul mercato esistono numerose blockchain, che differiscono per grado di diffusione, per casi d'uso abilitati e per funzionamento tecnico. La pluralità delle soluzioni disponibili non consente di scambiare dati (e quindi, come vedremo, trasferire criptoattività) tra registri diversi;

[4] È disponibile in appendice un Glossario con i principali termini tecnici e acronimi utilizzati.
[5] Cfr. Politecnico di Milano (2024) e Pitchbook (2024).
[6] Le blockchain possono essere distinte tra private o pubbliche, in relazione alla restrizione o meno alla lettura delle informazioni memorizzate sul registro e in *permissioned* e *permissionless*, in relazione alla necessità o meno di un'autorizzazione per scrivere sul registro. Questa analisi si concentra principalmente sulle blockchain pubbliche *permissionless*.

per superare tale frammentazione sono necessarie soluzioni di collegamento[7], come ad esempio i *bridge cross-chain* e gli *atomic swap*.

2.1 La crittografia e i wallet

La crittografia è la tecnologia abilitante per l'esecuzione di transazioni in modalità decentralizzata sulle DLT, che assicura l'autenticità e la protezione delle informazioni. In ambito cripto sono utilizzati diversi protocolli crittografici asimmetrici, basati sull'utilizzo di una coppia di chiavi (pubblica e privata) matematicamente correlate tra loro. Dalla chiave pubblica viene derivata una stringa alfanumerica – detta indirizzo – che può essere condivisa per ricevere criptoattività; concettualmente rappresenta qualcosa di simile all'IBAN nel mondo tradizionale. La chiave privata invece non deve essere condivisa in quanto è ciò che consente di firmare digitalmente e autorizzare le transazioni, ed è concettualmente assimilabile alla password di accesso ad una applicazione di home banking.

Le chiavi e gli indirizzi sono generati e conservati nei *wallet*, ovvero portafogli digitali necessari per operare sulle blockchain. Ciascun utente può possedere una pluralità di *wallet* e in ciascun *wallet* possono essere conservate una pluralità di chiavi, a cui corrispondono diversi indirizzi[8]. I *wallet* si distinguono tra *non-custodial* (o *un-hosted o self-hosted*), e *custodial* (o *hosted*) a seconda che la gestione delle chiavi private faccia capo rispettivamente all'utente o a un soggetto terzo.

2.2 I paradigmi di offerta: CeFi e DeFi

Nel mondo cripto l'offerta di servizi finanziari può avvenire attraverso due diversi paradigmi: quello della finanza centralizzata (CeFi, *Centralized Finance*) e quello della finanza decentralizzata (DeFi, *Decentralised Finance*).

La **finanza centralizzata** consiste in un sistema di nuovi intermediari, che offrono servizi assimilabili a quelli offerti nel mondo tradizionale (TradFi) dagli intermediari vigilati. I principali attori del mondo CeFi sono gli *exchange* centralizzati (CEX), i quali spesso accentrano una pluralità di funzioni che nella finanza tradizionale devono far capo a intermediari diversi[9]. Altri soggetti rilevanti della CeFi sono gli ATM per criptovalute, comunemente utilizzati per la conversione di moneta in criptoattività e viceversa[10], i *broker* OTC, che facilitano le transazioni tra privati mettendo in contatto acquirenti e venditori di criptoattività, e i *mixer* centralizzati, che aumentano la privacy nelle transazioni blockchain.

La **finanza decentralizzata** (DeFi) rappresenta invece una nuova modalità di offerta dei servizi, che non trova parallelo nel mondo finanziario tradizionale, in cui l'utente interagisce, anziché con un soggetto, direttamente con software eseguibili dai nodi della rete che automatizzano azioni predeterminate e irreversibili al ricorrere delle condizioni previste (c.d.

[7] Cfr. anche Buterin (2016).

[8] Possono essere necessari indirizzi diversi per operare su *blockchain* diverse, come ad esempio per Ethereum e Bitcoin.

[9] Alcuni esempi di servizi offerti dai nuovi soggetti nel mondo cripto sono: attività di emissione, commercializzazione, distribuzione e scambio di criptoattività; attività di *broker*, *dealer*, *market maker*, custodia, riconciliazione e *asset management*. Per le implicazioni in termini di rischi della multifunzionalità degli intermediari in criptoattività cfr. Financial Stability Board (2023).

[10] I clienti inseriscono nel dispositivo i contanti che vogliono convertire in criptoattività e l'indirizzo del *wallet* al quale inviare la corrispondente quantità di criptovaluta, al netto di una commissione per il servizio.

smart contract)[11]; questi programmi decentralizzati sono disponibili su blockchain pubbliche *permissionless* (ad esempio Ethereum) e sono alla base del funzionamento degli *exchange* decentralizzati (DEX) e di altri protocolli DeFi, come i *mixer* decentralizzati.

BOX 1 – ***Smart contract* e Bitcoin**

Bitcoin, la criptoattività più nota e longeva, è nata nel 2009 per consentire pagamenti elettronici *peer-to-peer* senza l'intervento di intermediari. Poggia sull'omonima blockchain che, supportando solo linguaggi di programmazione con funzionalità limitate (c.d. *non Turing completi*), non è in grado di eseguire gli *smart contract* più complessi che stanno alla base della DeFi[12]. Attualmente può essere scambiata o in modalità *peer-to-peer* o su *exchange* centralizzati.

Altre blockchain, come per esempio Ethereum, supportano invece linguaggi di programmazione c.d. *Turing completi* e sono in grado di eseguire *smart contract* complessi – come quelli che includono cicli iterativi – che, combinati tra loro, hanno consentito la nascita e lo sviluppo della finanza decentralizzata.

Una differenza significativa tra CEX e DEX attiene alla modalità di funzionamento e in particolare alla possibilità di eseguire operazioni non registrate sulla blockchain. Le operazioni in criptoattività possono infatti essere eseguite sia *on-chain* – sulla base dei meccanismi di funzionamento della blockchain descritti, che attribuiscono alle transazioni quelle caratteristiche distintive di immutabilità e verificabilità di cui si è parlato – sia *off-chain*, ovvero su sistemi di archiviazione tradizionali, esterni ai registri distribuiti e quindi non pubblici.

Mentre i DEX, che come detto funzionano tramite *smart contract*, possono operare esclusivamente *on-chain*, i CEX possono operare anche *off-chain* – ad esempio offrendo, tramite la propria piattaforma, un servizio di scambio di criptoattività tra gli utenti e registrando poi le transazioni su un proprio archivio interno. In altre parole, i CEX possono elaborare le transazioni internamente, anche tramite *order book* simili a quelli della finanza tradizionale, con vantaggi in termini di tempo e costi[13].

L'operatività esclusivamente *on-chain* dei DEX, che da un lato consente di esaminare il codice sottostante gli *smart contract* e di tracciare gli scambi, dall'altro – a causa della necessità di validare tutte le transazioni *on-chain* – può ridurre la velocità di esecuzione delle transazioni e determinare una maggiore incidenza delle *gas fee*[14] sul costo totale della transazione.

[11] Cfr. anche Auer et al. (2023).
[12] Cfr. anche Antonopoulos (2014), Antonopoulos et al. (2018) e Kannengießer et al. (2022).
[13] Quando il CEX opera *off-chain*, l'utente non sostiene commissioni per l'utilizzo della blockchain ma solo per lo scambio (*trading fee*) e/o per specifiche funzionalità (ad esempio deposito e prelievo).
[14] Le *gas fee* (o *network fee*) sono le commissioni corrisposte da un utente ai creatori dei blocchi (validatori) per includere una transazione su blockchain, incentivando il corretto mantenimento del registro e disincentivando attacchi alla rete. È difficile fare una comparazione sulla struttura dei costi delle transazioni effettuate tramite CEX e DEX a causa della pluralità dei fattori considerati nelle politiche di prezzo (ad esempio tipologia di criptoattività scambiate, volume ecc.). Un tentativo di confronto si può ritrovare in KPMG (2021).

2.3 Alcuni dati

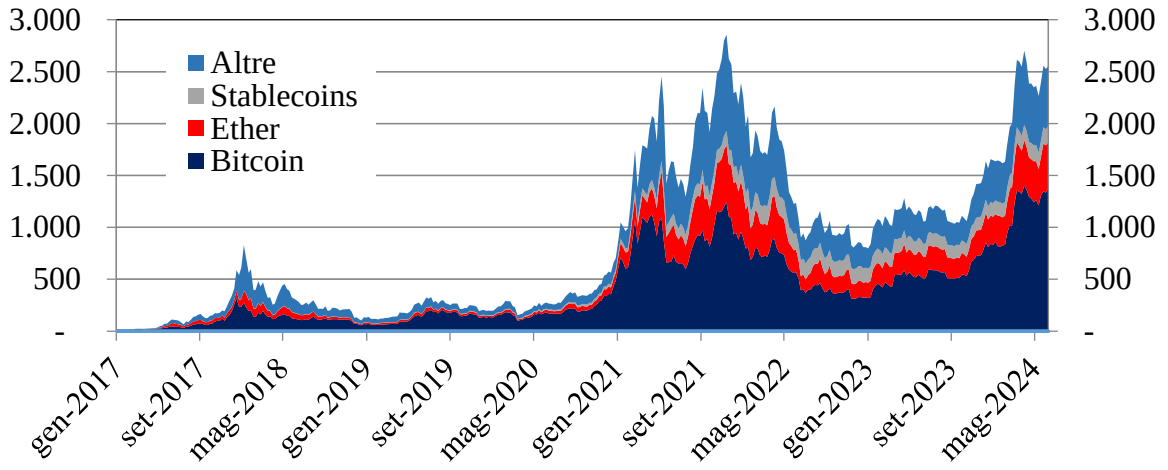
Per apprezzare la dimensione del mercato cripto è possibile guardare al numero delle criptoattività esistenti e alla loro capitalizzazione complessiva[15].

Il numero delle criptoattività esistenti non è univocamente quantificato. I dati disponibili sono talvolta divergenti, a causa dei diversi criteri adottati nel censimento e della relativa facilità con la quale nascono nuove criptoattività, spesso riconducibili a progetti poco robusti, abbandonati o oggetto di frodi e truffe. Si stima che complessivamente siano state create oltre 20.000 criptoattività[16] ma attualmente ne risultino attive meno di 10.000[17].

La capitalizzazione complessiva di mercato è estremamente volatile e il settore appare fortemente concentrato, con la prima criptoattività per diffusione, bitcoin, che ne rappresenta oltre la metà e raggiunge il 70% circa insieme alla seconda, ether; il suo punto di massimo di quasi 3 mila miliardi di dollari è stato toccato nel novembre 2021, si è ridotta a circa 860 miliardi di dollari a dicembre 2022 ed è risalita a circa 2.500 miliardi di dollari ad aprile 2024[18] (Figura 1).

La dimensione del mercato, specie se valutata in rapporto a quella dei mercati tradizionali è ancora contenuta ma appare comunque non trascurabile: bitcoin rappresenta l'ottavo asset per capitalizzazione a livello globale.

Figura 1: capitalizzazione di mercato delle criptoattività – miliardi di dollari, 2017 - 2024

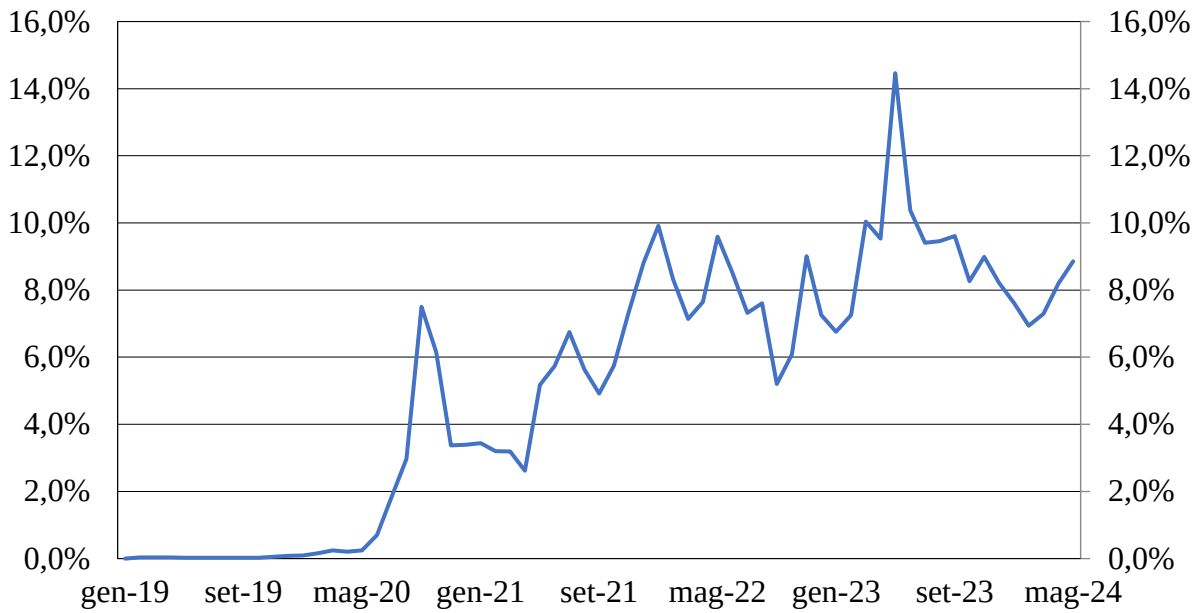


Fonte: Coinmarketcap. Vengono tracciate tutte le criptoattività, incluse le *stablecoin*, ad esclusione degli NFT.

[15] Definita come il prodotto tra le criptoattività in circolazione e il rispettivo prezzo di mercato.
[16] Stima a inizio 2023. Fonte: Financial Conduct Authority.
[17] Fonte: Coinmarketcap e Statista (2024).
[18] Si consideri per confronto che la capitalizzazione di mercato del NYSE a gennaio 2024 era pari a circa 24 mila miliardi di dollari.

È pure interessante esaminare il grado di diffusione dei due paradigmi di offerta. I volumi complessivi negoziati a pronti attraverso CEX superano ampiamente quelli scambiati attraverso DEX: a marzo 2024 il rapporto era di 9 a 1 (2,5 mila miliardi di dollari contro 181 miliardi[19], cfr. Figura 2); inoltre gli scambi a pronti risultano particolarmente concentrati presso pochi grandi soggetti e protocolli decentralizzati: a marzo 2024 la quota di mercato del primo *exchange* centralizzato (Binance) era circa del 50 per cento[20] e il protocollo decentralizzato più rilevante (Uniswap) raccoglieva quasi la metà del totale volumi scambiati a pronti attraverso DEX[21].

Figura 2: Rapporto tra i volumi a pronti negoziati su DEX e quelli negoziati su CEX (%), 2019 - 2024



Fonte: The Block [b]. L'indicatore è calcolato includendo gli *exchange* più grandi per i quali sono disponibili metriche di volumi scambiati.

Va precisato tuttavia che i volumi scambiati a pronti su CEX e DEX costituiscono solo una quota di quelli scambiati complessivamente, in quanto non comprendono ad esempio gli scambi *peer-to-peer*.

3. La normativa antiriciclaggio

L'efficacia dell'attuale sistema di prevenzione è fortemente legata alla collaborazione offerta dal sistema legale a cui i criminali si devono rivolgere per reinserire i proventi illeciti dei reati

[19] Fonte: The Block [a] e The Block [c].
[20] CoinGecko (2024). Si noti peraltro che i volumi riportati dagli *exchange* centralizzati possono essere influenzati da *wash trades*, ovvero operazioni di acquisto o vendita fittizie finalizzate ad accrescere i volumi scambiati presso un *exchange* relativi ad una o più criptoattività (cfr. anche ESMA 2024).
[21] The Block [a].

nell'economia legale. La normativa fa infatti ampio affidamento sulla collaborazione passiva degli operatori, tenuti a rispettare divieti e ad adempiere a specifici obblighi (raccolta e registrazione di informazioni funzionali all'adeguata verifica della clientela), e sulla collaborazione attiva che prevede l'individuazione e la segnalazione delle operazioni sospette.

Le regole sono configurate diversamente per le varie categorie di destinatari della normativa, il cui novero è stato progressivamente ampliato proprio per includere le attività ritenute via via suscettibili di essere utilizzate a fini di riciclaggio, ragion per cui a fianco degli intermediari finanziari e dei professionisti, si trovano ad esempio i prestatori dei servizi di gioco, gli operatori in oro, le case d'asta, nonché da ultimo anche gli operatori in criptoattività.

La normativa italiana a seguito del recepimento della V Direttiva antiriciclaggio ricomprende tra i soggetti obbligati, nella categoria degli operatori non finanziari, i prestatori di servizi relativi all'utilizzo di valuta virtuale[22] – introducendo tra l'altro un'accezione più ampia rispetto a quella europea, che ricomprende nel perimetro anche lo scambio di criptoattività con altre criptoattività[23] – e i prestatori di servizi di portafoglio digitale[24] ossia coloro che offrono i cosiddetti "*hosted wallet*" (cfr. supra). Tutti questi soggetti, per poter operare sul territorio nazionale, sono tenuti a iscriversi in un apposito registro tenuto dall'OAM, divenuto operativo dal mese di maggio del 2022; sono inoltre stati posti a loro carico obblighi di raccolta e trasmissione periodica delle informazioni sulle operazioni realizzate, inclusi gli estremi identificativi di ogni singolo cliente[25].

Il framework nazionale subirà peraltro significative modifiche con la piena entrata in vigore del Regolamento europeo MiCA, che introduce l'obbligo di autorizzazione e il passaporto europeo per i prestatori di servizi in criptoattività e li assoggetta a regole di vigilanza prudenziale. È interessante notare che il meccanismo di autorizzazione unica a livello europeo si rifletterà pure sulle scelte strategiche di localizzazione dei player già presenti sul mercato europeo e quindi sui flussi delle SOS ricevute a livello nazionale[26].

L'insieme degli obblighi posti dal vigente quadro normativo europeo antiriciclaggio in capo agli intermediari (e agli altri destinatari) configura un sistema di raccolta, aggiornamento e

[22] Definiti dal D. Lgs. 231/07 come ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, anche online, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute.

[23] La normativa europea (V Direttiva AML) si limitava a individuare come destinatari degli obblighi i "prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso forzoso".

[24] Definiti dal D. Lgs. 231/07 come ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali.

[25] Gli obblighi di registrazione iniziale e di segnalazione hanno finalità di censimento e di raccolta informativa. L'OAM non dispone di poteri di vigilanza o di intervento ulteriori rispetto a quelli di tenuta del registro, mentre il controllo del rispetto delle disposizioni antiriciclaggio è affidato alla Guardia di Finanza, in quanto chi offre servizi in criptoattività rientra nella categoria degli "operatori non finanziari" ai sensi del d.lgs. n. 231/2007.

[26] Ne deriverà un'esigenza di rafforzamento del sistema di collaborazione tra le FIU (Financial Intelligence Unit) dei diversi paesi affinché venga salvaguardato il patrimonio informativo relativo ai fenomeni in cui sono coinvolti i rispettivi cittadini.

conservazione di informazioni sul cliente e sul titolare effettivo del rapporto[27], sia nella fase genetica della relazione sia nel suo successivo dispiegarsi, che mira a rendere possibile la ricostruzione a posteriori dei passaggi di disponibilità avvenuti tramite il rapporto (metodo della traccia) e di intercettare e valutare, secondo un approccio basato sul rischio, le operazioni non coerenti con il profilo economico del cliente.

Ai fini della presente analisi rilevano pertanto sia i momenti di identificazione e raccolta di informazioni sul cliente e sul titolare effettivo nell'ambito del processo di adeguata verifica[28] (in sede di apertura del rapporto o contatto con l'intermediario) sia la capacità di associare al cliente (e al titolare effettivo) le operazioni da lui successivamente effettuate tramite i rapporti intestati per monitorarne l'operatività.

Nella valutazione dell'efficacia in ambito cripto dell'attuale sistema dei presìdi occorre tenere ben presenti i profili di immaterialità e a-territorialità delle valute virtuali: la tecnologia consente di superare con maggiore facilità la fisicità e i confini geografici delle giurisdizioni, e semplifica quindi il passaggio verso paesi con un quadro regolamentare più lasco. Poiché gli operatori in criptoattività offrono i propri servizi in mercati globali sarebbe dunque auspicabile una armonizzazione delle regole a livello internazionale, anche oltre i confini europei.

4. Lo pseudonimato: inquadramento del problema

Le informazioni archiviate sulle blockchain sono verificabili e immutabili e i registri delle blockchain pubbliche possono essere liberamente consultati; ciò significa che le transazioni e i loro indirizzi di origine e destinazione, pur non essendo associabili a un'identità reale, sono osservabili e analizzabili da chiunque ne abbia interesse[29].

Con il termine pseudonimato si fa riferimento proprio alla possibilità che hanno tutti gli utenti della rete di osservare (e tracciare) i trasferimenti eseguiti su blockchain pubbliche da un indirizzo, senza poter però conoscere l'identità del soggetto a cui quell'indirizzo fa capo. L'eventuale associazione dell'indirizzo all'identità dell'utente renderebbe pubblicamente ricostruibili tutte le transazioni eseguite da quel soggetto utilizzando quell'indirizzo, con evidenti problematiche in termini di privacy, circa ad esempio la conoscibilità delle strategie di investimento di singoli operatori o l'entità del patrimonio in criptoattività di un soggetto.

L'opportunità di operare tramite una pluralità di indirizzi consente agli utenti di accrescere il livello di privacy sulla propria operatività – obiettivo che, si noti bene, può essere del tutto legittimo – purché valga la cosiddetta proprietà di *unlinkability*, e non sia quindi possibile collegare tra loro i diversi indirizzi appartenenti al medesimo soggetto. Molte delle tecniche di riciclaggio utilizzate, anche in combinazione tra loro, mirano proprio a offuscare il

[27] Il titolare effettivo del rapporto è definito dal D. Lgs. 231/07 che recepisce in Italia le Direttive Europee in materia come la persona fisica o le persone fisiche, diverse dal cliente, nell'interesse della quale o delle quali, in ultima istanza, il rapporto continuativo è istaurato, la prestazione professionale è resa o l'operazione è eseguita.

[28] Il D. Lgs. 231/07 dispone l'obbligo di adeguata verifica del rapporto in occasione dell'instaurazione di un rapporto continuativo e dell'esecuzione di un'operazione occasionale che comporti la trasmissione o movimentazione di un importo pari o superiore a 15 mila euro (ovvero a mille euro in caso di trasferimento di fondi ai sensi del Regolamento UE 2015/847).

[29] Fanno eccezione alcune blockchain, come quelle su cui nascono e vengono trasferite le *privacy coin* che permettono di nascondere parte dei dati.

collegamento tra identità e indirizzo e tra la pluralità di indirizzi di uno stesso soggetto, come risulterà più chiaro nella successiva illustrazione delle diverse casistiche.

Nell'industria cripto si sono invero consolidate tecniche, c.d. di *blockchain analytics*[30], tramite le quali operatori specializzati raccolgono e analizzano le transazioni pubbliche su blockchain con il fine di tracciare il percorso delle criptoattività e di individuare le interazioni degli indirizzi con soggetti sanzionati, operatori localizzati in geografie a rischio[31] o soggetti centralizzati. Questi ultimi, destinatari di obblighi antiriciclaggio, rendono possibile l'associazione identità/indirizzo e facilitano quindi la ricostruzione di operazioni concatenate.

Lo pseudonimato a fini di riciclaggio è quindi più facilmente sfruttabile nel mondo DeFi, dove l'assenza di soggetti non attiva quei momenti di controllo funzionali ad associare indirizzi ed identità.

5. Le fasi del riciclaggio di denaro tramite criptoattività

Il processo di riciclaggio si svolge tipicamente in tre fasi successive, dette collocamento, stratificazione e integrazione o, in inglese, *placement, layering* e *integration*.

La fase di collocamento (*placement,* o piazzamento) è quella in cui i proventi dell'attività illecita vengono materialmente collocati presso intermediari finanziari o altri soggetti terzi regolamentati. Si tratta, per chi ricicla denaro, di una fase molto delicata, nella quale la probabilità di destare sospetti e determinare l'avvio di una SOS è particolarmente alta.

Durante la fase di stratificazione (*layering*) il denaro viene poi dissociato dall'attività illecita che lo ha generato tramite una complessa serie di transazioni (o di *strati*, ad esempio trasferimenti, bonifici, prestiti, pagamenti, ecc.), che hanno l'obiettivo di dissimulare l'origine dei fondi.

Infine, nella fase di integrazione (*integration*) il denaro ripulito viene reinserito nell'economia reale attraverso trasferimenti all'apparenza legittimi (tipicamente *investendo* in beni immobili, beni di lusso, aziende e altri valori).

È interessante capire come le criptoattività si inseriscono in questo schema e come il loro impiego, specie se combinato con tecniche tradizionali, renda più complesso il contrasto al riciclaggio. Si noti a questo proposito che le criptoattività possono derivare ai riciclatori dalla conversione di denaro fiat sporco, oppure essere il frutto diretto di condotte illegali (ad esempio vendita di sostanze stupefacenti a fronte di pagamento in criptovalute, furto di cripto, eccetera). Nel primo caso i riciclatori puntano a sfruttare la natura pseudonima delle criptoattività e le maggiori possibilità che esse offrono nella fase di stratificazione, mentre nel secondo caso il riciclaggio nasce direttamente in ambito cripto.

Vanno dunque presidiati i momenti di passaggio fra i due mondi al fine di intercettare lo spostamento di "denaro sporco" nel mercato cripto – per dissimularne l'origine e poi

[30] Per un approfondimento relativo alle possibili applicazioni degli strumenti di blockchain analytics e alle loro modalità di funzionamento cfr. anche Atlam et al. (2024).
[31] La prassi nell'industria di condividere tramite social network gli indirizzi di utenti e servizi malevoli abilita inoltre forme di auto-controllo dell'ecosistema tramite strumenti specifici detti *blockchain explorers*.

reintrodurlo nel sistema finanziario (*on-ramp* e *off-ramp*) – e viceversa la conversione di "criptoattività sporche" in moneta (*off-ramp*).

5.1 Passaggio dal mondo tradizionale all'ambiente cripto (on-ramp)

I sistemi a cui è possibile fare ricorso per convertire moneta in criptoattività (cd. fase di ***on-ramp***) sono i CEX, gli ATM per criptovalute e i *broker OTC*. I DEX – che, come detto, operano unicamente *on-chain* – non possono invece essere utilizzati nella fase di *on-ramp*, poiché non è possibile scambiare moneta su blockchain[32].

I **CEX** consentono di acquisire criptoattività a fronte dell'invio di moneta, principalmente tramite bonifico o carta di pagamento. Le criptoattività vengono accreditate dai CEX su *wallet hosted* ovvero su propri conti interni.

Gli **ATM per criptovalute** sono invece dispositivi fisici usati dai riciclatori per convertire denaro contante[33] in criptoattività, che vengono poi inviate dall'ATM all'indirizzo del *wallet* – *hosted* o *unhosted* – indicato dall'utente, al netto di una commissione per il servizio; in taluni casi si applicano limiti all'entità delle transazioni e alla loro frequenza.

Infine i ***broker OTC***, che rappresentano una fonte di liquidità molto importante per il mercato cripto, vengono utilizzati soprattutto nelle transazioni che coinvolgono grandi volumi di criptoattività[34]. Gli scambi possono avvenire direttamente tra le parti (*peer-to-peer*) oppure con l'intermediazione del *broker*, che mette a disposizione i propri conti (o *escrow account* di terzi), ai quali inviare criptovaluta e denaro prima del regolamento dell'operazione.

Chi ricicla denaro si rivolge in particolare a soggetti che si trovano in Paesi considerati dal GAFI ad alto rischio e/o privi di legislazione antiriciclaggio e a quelli che, pur autorizzati in giurisdizioni cooperative, disapplicano – in tutto o in parte – la normativa (Elliptic, 2023). I riciclatori ricercano infatti piattaforme che operano senza condurre controlli di adeguata verifica, rendendo complesso per le autorità risalire all'identità degli utenti, ma pure operatori autorizzati e in regola con la normativa, spesso servendosi di documenti falsi o di prestanome (*money mules*) nel processo di adeguata verifica. Esistono addirittura siti web in grado di fornire una lista di servizi P2P che operano senza controlli di KYC (ad esempio kycnot.me), che si inquadrano in una logica di "*crime as-a-service*"[35].

L'assenza di territorialità degli asset digitali, unita alle divergenze normative a livello internazionale, rende le criptoattività un mezzo particolarmente appetibile per il riciclaggio di denaro: i riciclatori potrebbero spostare i fondi di origine illecita in giurisdizioni con requisiti antiriciclaggio minimi o inesistenti, e da lì convertirli in criptoattività senza subire controlli di adeguata verifica. Secondo il *Congressional Research Service* americano[36] grazie a

[32] Invero con la recente entrata in vigore del Regolamento MiCA (Regolamento (UE) 2023/1114) diventa possibile scambiare moneta tokenizzata su blockchain.
[33] Possono anche essere utilizzate carte prepagate o altri strumenti tracciati.
[34] Il *broker* OTC può essere associato (*nested*) a un *exchange* che agisce da fornitore di liquidità.
[35] Sul tema della conversione di moneta in criptoattività meritano un cenno in Italia anche i Satoshi Spritz, ovvero eventi pubblici, aperti a tutti, durante i quali i partecipanti possono scambiare *peer-to-peer* bitcoin con beni e servizi, moneta inclusa.
[36] Congressional Research Service, (2022).

meccanismi simili i Russi sono riusciti ad aggirare, almeno in parte, le sanzioni imposte dai Paesi occidentali come conseguenza dell'invasione russa in Ucraina[37].

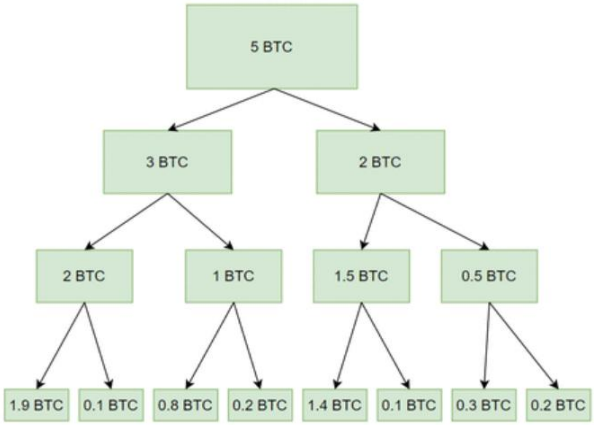
Già in questa fase i riciclatori raggiungono pertanto un certo grado di anonimato.

5.2 Stratificazione

Nel mondo cripto chi ricicla ha a disposizione diversi strumenti per complicare il tracciamento delle transazioni; può utilizzare *mixer*, *privacy coin* e tecniche di *chain hopping* – in combinazione tra loro o anche con meccanismi che assicurano la privacy a livello di rete.

In alcuni casi le criptoattività sono preliminarmente ripartite tra un grande numero di indirizzi, generalmente appartenenti allo stesso *wallet*[38]; si parla in questo caso di "***chain peeling***". Nello schema classico, le criptoattività vengono inizialmente suddivise tra due indirizzi, ognuno dei quali invia le criptoattività ricevute ad altre due destinazioni, e così via fino a ottenere il risultato desiderato[39].

Figura 3: Esempio di chain peeling



Fonte: Medium (2022).

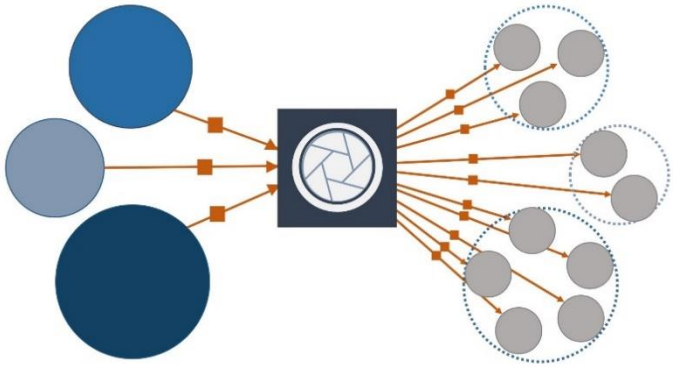
Poiché queste operazioni sono osservabili sulla catena, il *chain peeling* non riduce la tracciabilità dei fondi ma permette di ottenere importi più contenuti e quindi più facili da riciclare[40].

Fra gli strumenti che aiutano a offuscare le tracce rientrano invece i ***mixer*** (o *tumbler*), che raccolgono criptoattività da un numero sufficientemente elevato di utenti, le mescolano tra di loro e utilizzano la massa ottenuta per trasferire agli stessi utenti – ad un nuovo indirizzo o a molteplici nuovi indirizzi – un ammontare di criptovaluta pari a quanto depositato, al netto di una commissione per il servizio[41].

[37] Cfr. Politico (2023).
[38] Cfr. Chainalysis (2021).
[39] Medium (2022).
[40] Cfr. Kaspersky (2023).
[41] I token ricevuti provengono dalla massa e non sono gli stessi che l'utente ha depositato.

Possono funzionare sia in modalità centralizzata che in modalità decentralizzata. In entrambi i casi, nonostante tutte le transazioni siano registrate *on-chain*, risulta difficile, se non talvolta impossibile, collegare l'indirizzo destinatario a quello di origine grazie all'utilizzo di una pluralità di indirizzi di destinazione e anche alla distribuzione delle transazioni in uscita lungo un certo lasso di tempo.

Figura 4: Funzionamento di un *mixer*



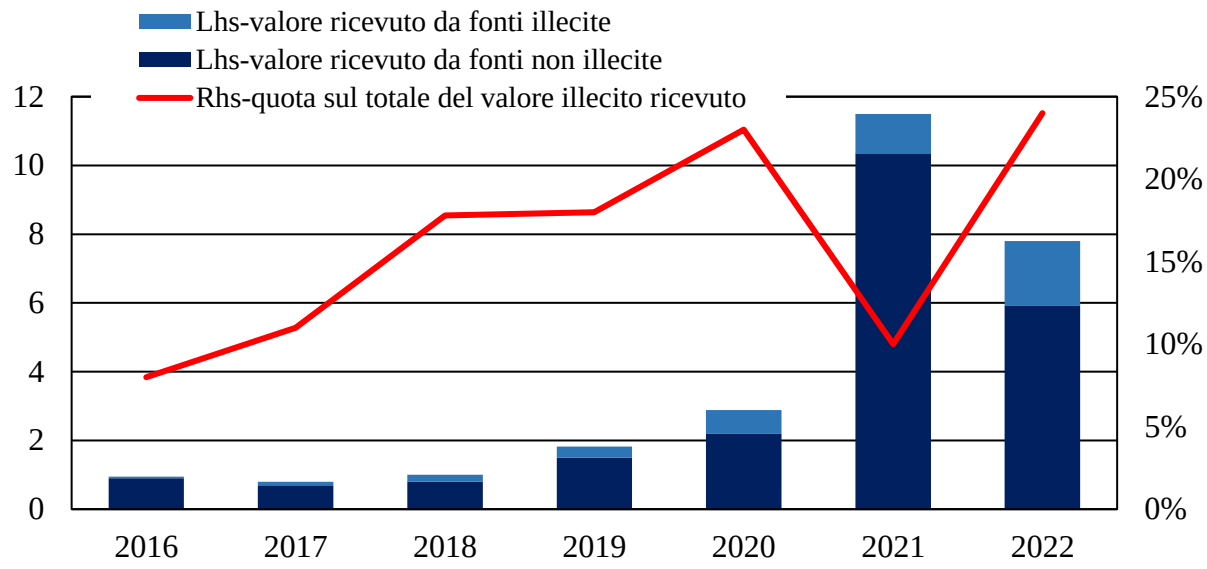
Fonte: Hudson Intelligence, *Mixers and Coinjoin*.

I *mixer* sono di per sé strumenti legittimi, che tutelano la privacy di chi opera in criptoattività[42], ma il loro utilizzo comporta alcuni rischi. I *mixer* centralizzati, per esempio, entrano in possesso dei token dei propri utenti, e conoscono sia i loro indirizzi IP[43] sia il collegamento fra gli indirizzi cripto di origine e quelli di destinazione; i clienti sono pertanto esposti al rischio di frodi e di diffusione delle informazioni, anche a seguito di attacchi cyber.

Il ricorso ai *mixer* per finalità non legali appare in aumento, tanto che il valore delle criptoattività di accertata provenienza illecita ricevuta dai servizi di mixing nel 2022 ha quasi raggiunto i due miliardi di dollari (Figura 5).

[42] Permettono, per esempio, di fare in modo che il saldo e le transazioni di un portafoglio bitcoin non siano ricostruibili da chiunque, o di evitare che, studiando il *ledger* di una criptovaluta, si possano individuare e replicare le strategie di investimento di un altro soggetto.
[43] Salvo quando sono utilizzati servizi VPN o rete TOR (cfr. Glossario).

Figura 5: Valore delle criptoattività ricevute annualmente dai *mixer*, 2016 - 2022 – miliardi di dollari



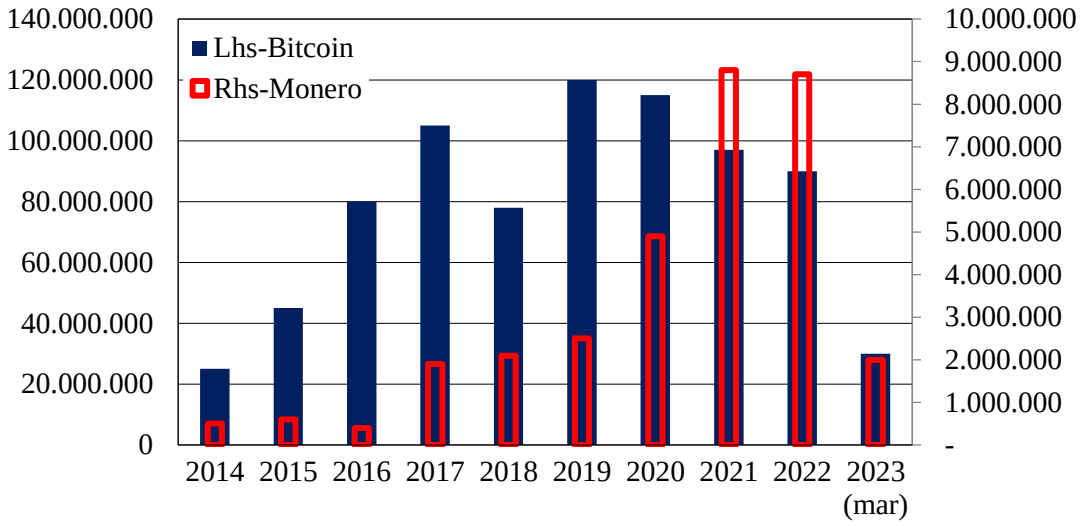
Fonte: Chainalysis (2023) [b].

Le ***privacy coin*** sono particolari criptoattività che, sfruttando diverse tecniche, complicano la tracciabilità delle transazioni. In alcuni casi si servono di firme ad anello per nascondere l'indirizzo da cui ha origine il trasferimento[44], in altri nascondono il destinatario creando indirizzi unici e temporanei per ogni transazione (indirizzi "*stealth*" o nascosti) rintracciabili solo da mittente e destinatario, in altri ancora incorporano sistemi simili a quelli dei *mixer* decentralizzati. Fra le *privacy coin* più comuni, Monero consente transazioni solo in modalità "privata", mentre per Dash e Zcash la scelta della forma anonima è opzionale.

A causa del loro diffuso impiego per finalità illecite (Figura 6) le *privacy coin* sono oggetto di divieti in alcune delle principali economie del mondo (Giappone, Australia, Corea del Sud, Dubai); nell'Unione Europea il Regolamento MiCA impedisce nella sostanza agli *exchange* di ammettere le *privacy coin* alla negoziazione[45].

[44] L'idea di base di una firma ad anello è che un utente può scegliere un gruppo di chiavi pubbliche appartenenti ad altri utenti della medesima blockchain, inconsapevoli, e combinarle con la propria chiave privata per creare una firma. Avendo a disposizione la firma e le chiavi pubbliche dei membri del gruppo, chiunque può verificare che qualcuno nel gruppo ha firmato il messaggio (o la transazione) ma non chi lo abbia firmato in modo specifico.
[45] Art 76 par. 3 del Regolamento UE 2023/1114.

Figura 6: Numero di transazioni per anno, Bitcoin vs Monero, 2014 - 2023



Fonte: Chainalysis (2023) [a].

Un'altra tecnica utilizzata dai riciclatori nella fase di stratificazione, detta ***chain-hopping***, consiste nello scambio delle criptoattività da ripulire con altre criptoattività supportate da una diversa blockchain (ad esempio da Bitcoin a Ethereum) attraverso *exchange* centralizzati[46]. Gli scambi fra criptoattività implementate su blockchain diverse – soprattutto se utilizzati in combinazione con altre tecniche di stratificazione – rendono infatti particolarmente difficile tracciare i movimenti delle criptovalute. Oltre che attraverso gli *swap* appena descritti, il cambio di blockchain può essere realizzato pure per mezzo di ***bridge cross-chain***, che peraltro rappresentano punti critici del sistema poiché i grossi volumi di criptoattività che vi transitano li rendono uno degli obiettivi preferiti dagli hacker[47].

Anche l'utilizzo degli ***exchange***, sia centralizzati che decentralizzati, può avere un ruolo nella fase di stratificazione. Nel caso dei CEX, chi ricicla denaro potrebbe sfruttare la loro operatività *off-chain*, tramite registri interni, che non rende possibile ricostruire l'intera lista delle transazioni effettuate dai clienti sulla sola base dei registri distribuiti. I DEX sono invece utilizzati principalmente da chi intende riciclare criptoattività rubate – spesso non quotate su *exchange* centralizzati e generalmente frutto di attacchi a danno di protocolli di DeFi – per effettuare scambi con criptovalute più liquide – solitamente Ether – o per convertire *stablecoin* in altri asset che, a differenza delle *stablecoin*, non possono essere "congelati" dall'emittente[48].

5.3 Off-ramp e fase di integrazione

Al termine della fase di stratificazione i riciclatori puntano a reintrodurre la ricchezza nel sistema finanziario tradizionale, convertendo le criptoattività in moneta; successivamente alla

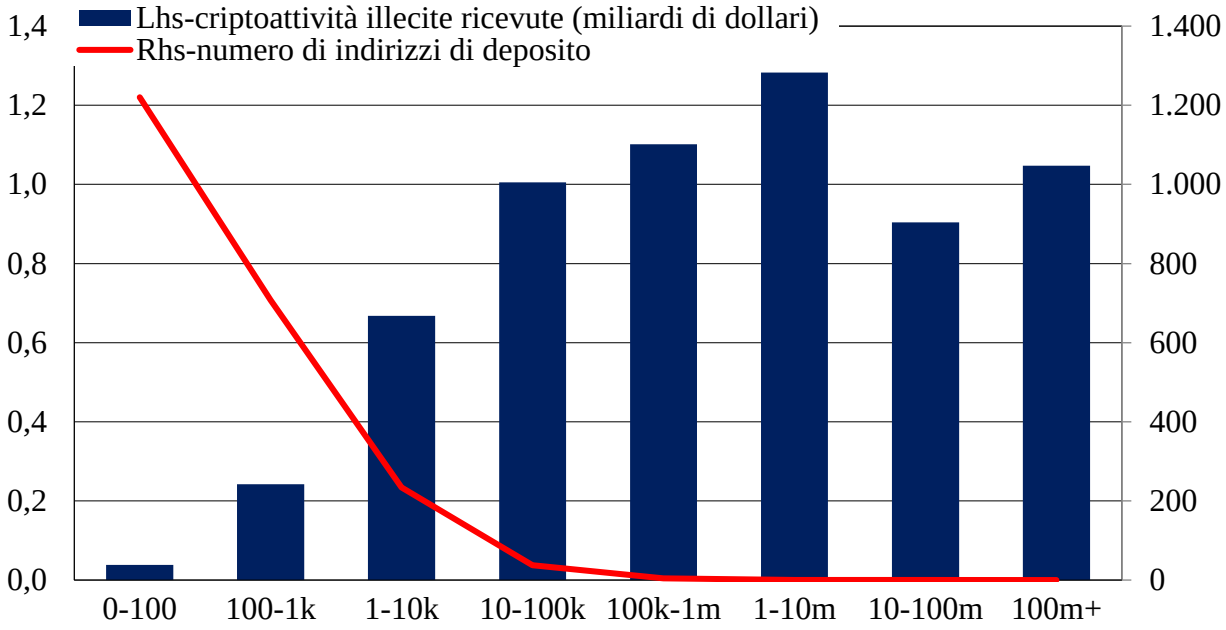
[46] Si tratta di CEX non conformi alla normativa o con sede in Paesi considerati dal GAFI ad alto rischio.
[47] Cfr. Chainalysis (2022).
[48] Cfr. Chainalysis (2023).

conversione non si potranno più utilizzare tecniche di *blockchain analytics* per il tracciamento delle transazioni, ma sarà necessario ricorrere ad analisi di tipo tradizionale.

Nella fase di ***off-ramp*** i riciclatori possono utilizzare in senso inverso tutti i sistemi descritti nell'*on-ramp* (CEX, ATM per criptovalute e *broker* OTC).

L'attività di *off-ramp* delle criptoattività di provenienza illecita sembra essere concentrata nelle mani di pochi soggetti. Secondo Chainalysis nel corso del 2022 quattro indirizzi hanno ricevuto più di un miliardo di dollari in criptoattività di provenienza illecita. I *wallet* che hanno ricevuto piccole quantità di criptoattività con origine illegale (fino a 100 dollari), pur essendo molti (1.220.554) hanno invece permesso di riciclare nel complesso solo 38 milioni di dollari.

Figura 7: Criptoattività di origine illecita ricevute da servizi di *off-ramp*, 2022



Fonte: Chainalysis (2023) [b].

Va detto che talvolta i riciclatori si avvalgono di iniziative di integrazione del mondo cripto con l'economia reale che consentono di utilizzare le criptoattività come strumento di pagamento per l'acquisto di asset di valore (immobili, auto, gioielli, arte, vino ecc.). Alcuni siti web pubblicizzano immobili disponibili per la vendita in cambio di bitcoin – anche in Italia (ad esempio CryptoRealEstate) – altri consentono di scambiare criptovalute con oro fisico (ad esempio Vaultoro), diamanti (ad esempio Antwerpor), automobili (ad esempio BitCars).

Possono inoltre sfruttare le proprietà dei token non fungibili (*non-fungible tokens* o **NFT**), che si differenziano dalle criptoattività sotto due principali aspetti: ogni NFT (i) è unico e (ii) contiene informazioni che lo collegano a un asset al di fuori della blockchain (opere d'arte, fotografie, video, oggetti ecc.). Nel mercato degli NFT non esistono prezzi di riferimento e il

valore di ogni token dipende dalla sua desiderabilità; il prezzo degli NFT è dunque altamente volatile e soggettivo, il che rende questi strumenti particolarmente adatti al riciclaggio[49].

Chi ricicla può infatti acquistare, usando fondi leciti, NFT con prezzi relativamente bassi[50], scambiarli con le criptoattività da ripulire – simulando un'operazione di compravendita a un prezzo molto più alto – e conferire così alle cripto una provenienza all'apparenza legittima[51].

La varietà e l'ampiezza delle opportunità descritte fanno luce su come il mondo cripto possa agevolare l'attività dei riciclatori, offrendo un nuovo insieme di strumenti che possono essere utilizzati da soli o in combinazione con sistemi più tradizionali.

6. I modelli di identità decentralizzata e la *zero-knowledge proof*

I riciclatori che utilizzano criptoattività perseguono due principali finalità, ovvero impedire l'individuazione dell'identità del soggetto che esegue le operazioni e offuscare e interrompere le tracce delle movimentazioni.

Questi obiettivi sono evidentemente comuni a quelli già noti nel sistema finanziario tradizionale, in cui i riciclatori pongono in essere strategie dirette a nascondere i titolari effettivi dei rapporti (ad esempio utilizzando teste di legno, o schermi societari e/o di varia natura), e a disegnare schemi complessi di transazioni in cui diventano difficilmente ricostruibili le reali catene di trasferimento del denaro.

Esiste tuttavia una differenza significativa tra i due ambiti e cioè che solo nel mondo cripto è possibile operare senza interagire con i soggetti obbligati a fini antiriciclaggio, vuoi nell'ambito del paradigma DeFi in cui i soggetti sono sostituiti dagli *smart contract*, vuoi nell'ambito del paradigma CeFi in cui l'operatività con soggetti localizzati in Paesi privi o carenti di legislazione antiriciclaggio è facilitata dalla immaterialità e a-territorialità degli asset[52].

La possibilità di operare sulla blockchain senza una preventiva identificazione, attivando una pluralità di indirizzi potenzialmente indipendenti e non ricollegabili tra loro, rende particolarmente efficace la fase di stratificazione e alquanto problematico, sia per gli intermediari che per le autorità preposte ai controlli, ricostruire la complessiva operatività di un soggetto, per cogliere quegli elementi di incoerenza che possono alimentare il sospetto in fase preventiva o provare le condotte illecite in fase repressiva.

Considerato che la normativa si sta evolvendo per ricomprendere a fini antiriciclaggio i VASP/CASP fra gli intermediari[53], è interessante soffermarsi sull'operatività in ambito DeFi e

[49] Cfr. anche Canepa (2024).
[50] L'operazione è facilitata dal fatto che molte piattaforme per la compravendita di NFT non richiedono l'identificazione degli utenti.
[51] Il prezzo di vendita più alto di quello di acquisto può essere giustificato dalla soggettività dei prezzi nel mercato NFT. Inoltre la natura pseudonima della blockchain fa sì che, se i criminali sono accorti, l'indirizzo di acquisto e quello di vendita non siano riconducibili allo stesso soggetto.
[52] Sono anche possibili scambi diretti di criptoattività P2P, assimilabili allo scambio di contante nella finanza tradizionale, indagabili attraverso gli strumenti di *blockchain analitycs*.
[53] Cfr. pacchetto di misure legislative antiriciclaggio e di contrasto al finanziamento del terrorismo composto dalla VI Direttiva antiriciclaggio, dal Regolamento *Single Rulebook*, dal Regolamento che istituisce l'AMLA (Anti-Money Laundering Authority) e dal Regolamento *Transfer of Funds Regulation recast* (*TFR recast*).

analizzare quali strumenti – alternativi alla collaborazione attiva – possono consentire di rispettare al contempo la natura pseudonima della blockchain e la tutela della privacy.

Quando gli utenti interagiscono con protocolli DeFi le transazioni avvengono tra *smart contract* e *un-hosted wallet*, che non sono stati associati ad una identità nell'ambito di un processo di adeguata verifica. Per attivare anche in questo mercato i controlli sarebbe quindi necessario prevedere l'obbligo di codificare, proprio negli *smart contract*, meccanismi automatizzati di identificazione e di verifica preventiva delle caratteristiche dei soggetti, ad esempio attraverso soluzioni decentralizzate di identità digitale; ciò consentirebbe di rilevare le circostanze suscettibili di incidere sull'instaurazione della relazione e/o sulla classificazione in base al rischio dell'utente (ad esempio residenza in paesi della *black list* del GAFI, qualifica di PEP, eccetera).

Il modello ***Self Sovereign Identity*** **(SSI)** – a cui si ispira anche la revisione della Direttiva europea Eidas – è un modello di identità digitale che attribuisce all'utente il controllo delle proprie informazioni personali, superando la presenza degli *Identity Provider* e offrendo l'opportunità di gestire con presidi di privacy l'identità in rete.

Nel modello SSI un soggetto può dimostrare su blockchain il possesso di informazioni o attributi senza rivelarli – ad esempio dimostrare di essere maggiorenne senza rivelare la propria età anagrafica –, tramite la cosiddetta ***zero-knowledge proof*** (ZKP, prova a conoscenza nulla)[54]. Lo schema prevede la presenza di tre soggetti – l'emittente, il detentore e il verificatore dell'identità – tra i quali deve esistere un rapporto di vicendevole fiducia[55]. In particolare l'emittente rilascia una *Verifiable Credential* (VC) firmata crittograficamente al detentore, che la conserva in uno specifico *wallet* e da cui genera una ZKP utilizzabile presso il verificatore; quest'ultimo esegue poi una serie di prove per verificarne l'autenticità (ad esempio che la VC risulti effettivamente firmata dall'emittente).

L'introduzione del modello SSI in DeFi consentirebbe a ciascun utente di presentare ad uno *smart contract* le ZKP generate – ad esempio relative all'età, alla residenza, alle eventuali cariche politiche, alla presenza di eventuali sanzioni nazionali e internazionali, eccetera – per accedere ai servizi decentralizzati[56]; pertanto la previsione di idonee disposizioni normative o linee guida sull'utilizzo degli *smart contract* in finanza potrebbe ad esempio permettere di inibire l'operatività dei soggetti già sanzionati o segnalati.

Per una effettiva azione di contrasto del riciclaggio, sarebbe tuttavia necessario che le autorità avessero accesso alle informazioni di identificazione qualora l'indirizzo risultasse poi coinvolto in operazioni illecite.

La creazione di un archivio delle identità dei detentori di VC da parte degli emittenti, consultabile dalle autorità ancorché in presenza di specifiche e definite condizioni, sarebbe però poco in linea con la filosofia decentralizzata, oltre a costituire un *single point of failure*. Un'ipotesi alternativa esplorata dall'accademia, che non prevede la creazione di registri

[54] Sono allo studio anche altre applicazioni della ZKP potenzialmente rilevanti ai fini antiriciclaggio, cfr. Buterin et al. (2024).
[55] Il fatto che l'informazione contenuta nella VC sia crittograficamente verificabile non implica che sia vera; sono pertanto imprescindibili uno stretto rapporto di fiducia tra i soggetti e l'affidabilità e solida reputazione dell'emittente. Sui modelli di SSI si veda anche PolygonID e Pauwels et. al. (2022).
[56] Cfr. anche Pauwels (2021) e Pauwels et al. (2022).

centralizzati, ricorre a soluzioni basate su tecniche crittografiche che consentono di salvare *on-chain* una versione cifrata delle VC, decodificabile solo con l'accordo di una pluralità soggetti (ad esempio Garante della Privacy e organi investigativi) e in presenza di un interesse pubblico[57].

L'opportunità di ricostruire l'identità di chi ha eseguito in DeFi transazioni sospette rappresenterebbe senza dubbio un passo avanti, con un potenziale rafforzamento dell'efficacia dei sistemi di analisi forense. D'altra parte, anche qualora divenissero concretamente realizzabili, queste soluzioni sofisticate e complesse non consentirebbero ancora di sostituire la collaborazione attiva degli intermediari per l'individuazione delle operazioni anomale, in mancanza di una classificazione in base al rischio degli utenti e dei titolari effettivi, principio cardine dell'attuale sistema di prevenzione.

Ma se pure divenisse possibile integrare all'interno degli *smart contract* sistemi di ponderazione di tutte le numerose condizioni rilevanti per classificare gli utenti in base al rischio (ad esempio professione e/o settore di attività, geografia, eventuali cariche politiche, ecc.), sarebbe poi alquanto difficile codificare coerenti forme di monitoraggio differenziate per la ricerca di potenziale operatività anomala.

L'attivazione di una pluralità di indirizzi tra loro *unlinkable* per garantire lo pseudonimato, impedisce infatti la ricostruzione della complessiva operatività di un soggetto (e ancor di più di un titolare effettivo) e rende quindi difficile immaginare processi di adeguata verifica nel continuo e di individuazione delle transazioni potenzialmente sospette automatizzati tramite *smart contract*.

7. Conclusioni

La rapida e ampia diffusione delle criptoattività ha generato, anche in ambito antiriciclaggio, un vivace dibattito tra i sostenitori delle cripto, che sottolineano le caratteristiche di tracciabilità e immutabilità delle transazioni garantite dalla tecnologia blockchain, e i loro detrattori che invece evidenziano come, utilizzando criptoattività, i criminali possano operare attraverso indirizzi non associabili a identità reali, specie nel paradigma della finanza decentralizzata in cui le transazioni avvengono senza l'intervento di intermediari.

Mentre in CeFi è possibile individuare i soggetti a cui imporre obblighi antiriciclaggio analoghi a quelli esistenti nella finanza tradizionale – e proprio in tale direzione si sta evolvendo la normativa a livello europeo –, il paradigma dell'offerta decentralizzata pone molteplici sfide circa la possibilità di introdurre meccanismi a tutela della legalità.

Per bilanciare le esigenze di privacy con il presidio del rischio di utilizzi illeciti, il mercato sta sviluppando soluzioni tecnologiche che, in assenza di intermediari e altri soggetti, tentano di codificare negli *smart contract* i necessari sistemi di controllo; in particolare, diverse sperimentazioni utilizzano la tecnologia ZKP che consente una *disclosure* selettiva delle informazioni, affinché l'accesso a specifici servizi decentralizzati possa essere riservato a indirizzi legittimati preservando la necessaria riservatezza.

[57] Cfr. Bruschi et. al. (2021).

Ma allo stato queste soluzioni complesse e di frontiera potrebbero consentire soltanto di estendere l'applicazione degli obblighi di identificazione della clientela al mondo DeFi, limitando l'utilizzo di servizi decentralizzati solo agli indirizzi il cui titolare possieda caratteristiche predeterminate; tuttavia il loro utilizzo non permetterebbe di effettuare l'adeguata verifica nel continuo, che è invece un presidio indispensabile per individuare le transazioni incoerenti con il profilo del soggetto e quindi potenzialmente sospette[58]. Si tratta quindi di tentativi utili per incorporare meccanismi di prevenzione a fini antiriciclaggio nel mondo decentralizzato ma ancora non sufficienti a costruire un presidio efficace.

Qualora in futuro venissero sviluppate soluzioni tecniche idonee a costruire anche in ambito decentralizzato un sistema di controllo del rischio di riciclaggio paragonabile a quello tradizionale, occorrerà considerare pure il rischio insito nella trasparenza degli *smart contract*, il cui codice di funzionamento è memorizzato sulla blockchain, e quindi pubblicamente ispezionabile. La trasparenza degli *smart contract*, infatti, consentirebbe sì di valorizzare la collaborazione attiva con quei soggetti che potenzialmente possono contribuire a migliorare la sicurezza complessiva del sistema (sviluppatori, intermediari, ecc.), ma al contempo certamente agevolerebbe i riciclatori nell'individuazione di modalità di elusione dei presidi, in quanto renderebbe conoscibili tutti i meccanismi di controllo attuati tramite gli *smart contract*; e la natura *open-source* degli *smart contract* richiederebbe inoltre che i codici siano sufficientemente robusti affinché i riciclatori non ne possano compromettere il funzionamento.

In conclusione, quindi, la tecnologia che ha ispirato la filosofia di decentralizzazione ancora non consente di costruire un sistema di controlli a presidio del rischio antiriciclaggio in grado di sostituire la collaborazione attiva degli intermediari; se in futuro l'innovazione riuscirà a sviluppare gli strumenti necessari, si amplieranno le sfide per il regolatore e le autorità di controllo, la cui azione dovrà anch'essa sempre più sfruttare le opportunità offerte dalla tecnologia.

[58] Rilevano inoltre i rischi connessi con le possibili debolezze nelle implementazioni della tecnologia ZKP che potrebbero essere sfruttate dai riciclatori.

APPENDICE

Glossario

ATM per criptovalute: dispositivi fisici per la conversione di moneta in criptoattività (e viceversa) al netto di commissioni per il servizio.

***Atomic swap*:** soluzione di interoperabilità tra blockchain diverse basata su scambi P2P tramite *smart contract* che consentono il regolamento delle transazioni solo se le controparti hanno depositato la corretta quantità di criptoattività da scambiare.

Blockchain: particolare tipologia di tecnologia a registro distribuito (DLT) che – tramite i meccanismi di consenso – permette di validare e raggruppare le transazioni in blocchi concatenati in ordine cronologico al fine di creare un registro non modificabile e verificabile di tutte le operazioni effettuate.

***Blockchain analytics*:** tecniche che sfruttano la trasparenza dei registri distribuiti per tracciare, analizzare e visualizzare transazioni, indirizzi e altri dati con il fine di approfondire le relazioni tra soggetti operanti su blockchain.

***Bridge cross-chain*:** soluzioni di interoperabilità tra blockchain tra le quali si menzionano i *bridge burn and mint* che bloccano l'asset sulla *chain* di partenza prima di crearlo su quella di destinazione e i *bridge lock and mint* che cancellano l'asset prima di ricrearlo sulla *chain* di destinazione.

Chiave privata: stringa alfanumerica necessaria per firmare digitalmente e autorizzare le transazioni; deve essere quindi mantenuta riservata. Dalle chiavi private si derivano tramite una funzione crittografica le chiavi pubbliche, ma non è possibile il passaggio inverso.

Chiave pubblica: stringa alfanumerica che, tramite una funzione crittografica, viene derivata dalla chiave privata e dalla quale a sua volta è ottenuto l'indirizzo.

CeFi (*Centralized Finance*): sistema di nuovi intermediari (CEX, ATM per criptovalute, *broker* OTC, eccetera) che offrono nel mondo cripto servizi assimilabili a quelli offerti da intermediari vigilati nel mondo finanziario tradizionale; possono operare sia *off-chain* che *on-chain*.

CEX (*centralized exchange*): soggetti che consentono lo scambio di criptoattività con moneta e di criptoattività con criptoattività e contribuiscono ai meccanismi di formazione dei prezzi. Offrono una pluralità di servizi in criptoattività quali ad esempio la custodia, la commercializzazione e distribuzione, l'emissione di *stablecoin*, eccetera. I CEX possono operare anche *off-chain* utilizzando un sistema di conti interni privi delle caratteristiche di immutabilità e verificabilità. Da ciò deriva che la ricostruzione delle transazioni complessivamente effettuate dai clienti di un CEX non è possibile analizzando soltanto i registri distribuiti ma richiede l'acquisizione dei registri interni dell'*exchange*.

Criptoattività (o token): rappresentazione digitale di valore o di diritti che possono essere emessi, trasferiti e memorizzati elettronicamente su tecnologie a registro distribuito.

DeFi (*Decentralized Finance*): paradigma di offerta di servizi in criptoattività in cui l'utente non si interfaccia con soggetti ma con *smart contract*, che operano esclusivamente *on-chain*.

DEX (*decentralized exchange*): protocolli decentralizzati che consentono lo scambio di criptoattività con altre criptoattività in assenza di intermediari.

FIU (*Financial Intelligence Unit*): autorità centrale nazionale incaricata di acquisire e – ove previsto – richiedere i flussi finanziari e le informazioni riguardanti ipotesi di riciclaggio e di finanziamento del terrorismo su cui effettua l'analisi finanziaria; grazie ai poteri di cui dispone, valuta la rilevanza dei flussi raccolti ai fini della trasmissione alle autorità competenti con cui può collaborare per l'eventuale sviluppo dell'azione di repressione. Per l'Italia la FIU è l'Unità di Informazione Finanziaria (UIF).

GAFI (Gruppo d'Azione Finanziaria Internazionale): organismo intergovernativo creato nel 1989 in ambito OCSE con lo scopo di definire e promuovere strategie di contrasto del riciclaggio, a livello nazionale e internazionale.

Identità digitale: insieme di dati, associati in modo univoco a una persona fisica o giuridica, che consentono la sua identificazione attraverso un processo elettronico.

***Identity provider*:** soggetti accreditati che erogano e forniscono servizi di identità digitale per consentire l'identificazione degli utenti.

Indirizzo: stringa alfanumerica derivata crittograficamente dalla chiave pubblica utilizzata nelle transazioni su blockchain dagli utenti per indicare la destinazione delle criptoattività e per verificare la firma digitale di una transazione, ovvero verificarne la validità.

Indirizzo IP: codice necessario per navigare in rete associato a ciascun dispositivo; fornisce informazioni sulla sua localizzazione geografica e viene assegnato dal fornitore dei servizi Internet (Internet Service Provider, ISP). Tale indirizzo viene utilizzato dalle autorità per individuare i nodi e ricostruire le operazioni in rete.

Meccanismo di consenso: modalità con cui i partecipanti al registro distribuito si accordano sullo stato del sistema, garantendo la validità delle transazioni e dei blocchi da aggiungere alla catena. Tra i meccanismi di consenso più diffusi ci sono i Proof of Work (PoW), Proof of Stake (PoS) e Proof of Authority (PoA).

***Mixer* (o *tumbler*)**: strumenti che hanno la funzione di aumentare la privacy degli utenti su blockchain. Possono essere soggetti centralizzati o applicazioni decentralizzate (*smart contract*); raccolgono elevate quantità di criptoattività di utenti diversi, le mescolano tra di loro e le redistribuiscono agli stessi utenti – al netto di commissioni di servizio – in modo tale da rendere difficile la ricostruzione della catena dei trasferimenti.

NFT (*non-fungible token*): rappresentazione digitale di un asset esterno alla blockchain (ad esempio opere d'arte, fotografie, video, oggetti ecc.) che possiede quindi caratteristiche di unicità; un NFT non conferisce al proprio detentore il controllo dell'asset collegato (chiunque può scaricare l'immagine o il video associato al token).

On-chain: modalità operativa in cui le transazioni sono eseguite direttamente sulla blockchain. Le transazioni *on-chain* vengono registrate e convalidate sulla blockchain attraverso meccanismi di consenso, diventando verificabili e immutabili.

Off-chain: modalità operativa in cui le transazioni sono eseguite al di fuori della blockchain.

On-ramping**:** conversione di moneta in criptoattività.

Off-ramping: conversione di criptoattività in moneta.

Order book**:** registro elettronico che raccoglie e permette di associare gli ordini di acquisto e vendita al fine di avviare lo scambio fra acquirente e venditore.

Peer-to-peer **(P2P) o** ***Consumer to Consumer*** **(C2C):** modalità di scambio di attività (o di dati) direttamente tra due utenti.

Privacy wallet**:** *wallet* che favoriscono la privacy e l'anonimato dell'utente, ad esempio limitando la tracciabilità delle transazioni effettuate o ostacolandone l'intercettazione da parte dei software di *blockchain analytics*. Possono incorporare meccanismi di offuscamento dell'indirizzo IP tra cui le *Virtual Private Network* (VPN) e il protocollo TOR.

Protocollo decentralizzato: insieme di regole e procedure che disciplinano il comportamento dei partecipanti a una rete decentralizzata. Sono implementate tramite *smart contract*, solitamente *open-source*, il cui codice sottostante può essere quindi esaminato e verificato da chiunque.

Pseudonimato: caratteristica tipica delle tecnologie a registro distribuito per cui gli indirizzi delle transazioni sono visibili a tutti gli utenti della rete ma non sono riconducibili – senza informazioni aggiuntive – all'identità dei soggetti a cui gli indirizzi fanno capo.

Self-Sovereign Identity **(SSI)**: modello di identità digitale decentralizzato implementabile tramite blockchain che attribuisce il controllo delle informazioni all'utente.

Smart Contract**:** applicazioni software eseguite in maniera collettiva e decentralizzata dai nodi di un registro distribuito, che al verificarsi di specifiche condizioni fornite in input automatizzano azioni predeterminate e irreversibili.

TOR (*The Onion Router*): rete di comunicazione che, tramite una architettura a diversi strati di crittografia, ha l'obiettivo di garantire l'anonimato dei propri utenti nel trasferimento dei dati di navigazione tra i nodi della rete. Ad ogni passaggio da un nodo all'altro, la comunicazione viene crittografata e ogni nodo conosce solo il precedente e il successivo della catena di navigazione, ma non il nodo di partenza. La presenza di passaggi intermedi impedisce che il destinatario conosca l'indirizzo IP dell'utente mittente.

Turing Completeness: caratteristica di un linguaggio di programmazione la cui semantica consente di implementare una qualsiasi macchina di Turing, ovvero una macchina che può calcolare in un numero finito di passi qualsiasi funzione computabile. Un linguaggio Turing completo permette di scrivere *smart contract* complessi, come quelli che sono alla base della DeFi. Diversamente, un linguaggio non Turing completo (come quello adottato in Bitcoin) ha funzionalità limitate e non consente di sviluppare applicazioni decentralizzate complesse.

Verifiable Credential **(VC)**: attributo digitale, immodificabile e verificabile, collegato a una identità digitale.

VPN (*Virtual Private Network*): software che consente la creazione di una rete privata tra dispositivi su Internet. Le VPN sono utilizzate per criptare il traffico di rete e per rendere inefficaci i servizi di geolocalizzazione sostituendo l'indirizzo IP dell'utente con quello del VPN provider a cui l'utente si collega.

***Wallet*:** strumenti necessari per operare sulla blockchain che conservano le coppie di chiavi pubbliche e private, consentendo di creare e firmare le transazioni. Possono essere classificati in:

- *Non-custodial* (o *un-hosted*) se la gestione delle chiavi private fa capo all'utente, e *custodial* (o *hosted*) se fa invece capo ad un soggetto terzo.
- *Hot* e *cold* se sono collegati o meno alla rete.
- *Software* e *hardware*, a seconda che siano applicazioni informatiche o dispositivi fisici simili ad una chiavetta USB**.**

***Zero-Knowledge Proof* (ZKP)**: protocollo crittografico tramite il quale un agente (detto *prover*) può provare ad un altro agente (detto *verifier*) che è in possesso di una informazione, senza rivelarla.

Bibliografia

Antonopoulos A.M. (2014), *Mastering Bitcoin*

Antonopoulos A.M., Wood G. (2018), *Mastering Ethereum*

Atlam H., N. Ekuri, M. A. Azad, H. S. Lallie (2024), *Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions*, Electronics 2024, 13, 3568.

Auer R., B. Haslhofer, S. Kitzler, P. Saggese, F. Victor (2023), *The Technology of Decentralized Finance (DeFi)*, BIS Working Papers No 1066

Autorité de contrôle prudentiel et de résolution (2023), *Decentralised" or "disintermediated" finance: what regulatory response?*, Discussion Paper

Binance (2021), *Cosa sono i nested exchange e perché dovresti evitarli?*

Bruschi F., T. Paulon, V. Rana e D. Sciuto (2021), *A privacy preserving identification protocol for smart contracts*, IEEE Symposium on Computers and Communications, ISCC 2021, pagine 1–6, 2021, IEEE, Atene, Grecia

Buterin V. (2016), *Chain Interoperability*

Buterin V., J. Illum, M. Nadler, F. Schär, A. Soleimani (2024), *Blockchain privacy and regulatory compliance: Towards a practical equilibrium*, Blockchain: Research and Applications, Volume 5, Issue 1

Canepa A. (2024), *Il mercato dei non fungible tokens tra arte, moda e gamification*

Chainalysis (2020), *Crypto Money Laundering: How Criminals Cash Out Billions in Bitcoin and Other Cryptocurrencies*

Chainalysis (2021), *3 Common Blockchain Analysis Mistakes that Impede Cryptocurrency Investigations*

Chainalysis (2022), *Vulnerabilities in Cross-chain Bridge Protocols Emerge as Top Security Risk*

Chainalysis (2023) [a], *Privacy Coins 101: Anonymity-Enhanced Cryptocurrencies*

Chainalysis (2023) [b], *The 2023 Crypto Crime Report*

Chainlink (2023), *What Is an Atomic Swap?*

Chand A. (2022), *Medium, What Are Blockchain Bridges And How Can We Classify Them?*

CoinGecko (2024), *2024 Q1 Crypto Industry Report*

Congressional Research Service (2022), *Russian Sanctions and Cryptocurrency*, CRS Reports

Decrypt (2023), *How On-Chain Attestations Unlock Blockchain's Most Valuable Use Cases*

Elliptic (2023), *Preventing Financial Crime in Cryptoassets*, Typologies Report 2023

ESMA (2024), *Draft Technical Standards specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA) – second package, Final Report*

Ethereum (2024), *What are zero-knowledge proofs?*

Eurojust (2022), *Report on Money Laundering, Criminal justice across borders*

Europol (2023), *One of the darkweb's largest cryptocurrency laundromats washed out*

Financial Conduct Authority, *Crypto: The basics*, url

Financial Stability Board (2023), *The Financial Stability Implications of Multifunction Crypto-asset Intermediaries*

Halpin H. (2021), *Holistic Privacy and Usability of a Cryptocurrency Wallet*

Hudson Intelligence, *Mixers and Coinjoin*, url

Kannengießer N., S. Lins, C. Sander, K. Winter, H. Frey, A. Sunyaev (2022), *Challenges and Common Solutions in Smart Contract Development*

Kaspersky (2023), *How cybercriminals launder dirty crypto*

Kocegarovas G. (2022), *Cryptocurrency money laundering risk: the best explanation of a 3-step process*

KPMG (2021), *Crypto Insights#2. Decentralised Exchanges & Automated Market Makers Innovations, Challenges & Prospects*

Medium (2019), *What is OTC cryptocurrency trading?*

Medium (2022), *Crypto Compliance Series | What is Peel Chain*

Newsletter n. 4 – 2019, Le valute virtuali - Rischi di utilizzo anomalo, Unità di Informazione Finanziaria, 2019

Pauwels P. (2021), *zkKYC; A solution concept for KYC without knowing your customer, leveraging self-sovereign identity and zero-knowledge proofs*

Pauwels P., J. Pirovich, P. Braunz e J. Deeb (2022), *zkKYC in DeFi: An approach for implementing the zkKYC solution concept in Decentralized Finance*

Pitchbook (2024), *Crypto Report*

Politico (2023), *Two major crypto exchanges failed to block sanctioned Russians*

PolygonID, *Introduction to PolygonID*

Poltecnico di Milano (2024), Osservatorio Digital Innovation, *Nel 2023 aumentano i progetti Blockchain nel mondo*

Rapporto annuale per il 2022, n. 15 – 2023, Unità di Informazione Finanziaria, 2023

RareSkil (2023), *How Tornado Cash Works (Line by Line for Devs)*

Statista (2024), *Number of cryptocurrencies worldwide from 2013 to January 2024*

Szego B. (2023), *"Nuovi scenari AML: La Banca d'Italia incontra il mercato", intervento del Capo dell'Unità di Supervisione e Normativa antiriciclaggio,* Workshop Banca d'Italia

TechBullion (2023), *Blockchain Privacy Guide: Comparing CoinJoin and Tornado.Cash*

The Block [a], *DEX Volume*, accesso 18 aprile 2024, url

The Block [b], *DEX to CEX Spot Trade Volume (%)*, accesso 18 aprile 2024, url

The Block [c], *Cryptocurrency Monthly Exchange Volume*, accesso 18 aprile 2024, url

Wired (2021), *L'Italia è il Paese perfetto per chi vuole riciclare denaro con i bitcoin*