La regola "follow the money" nello spazio virtuale della blockchain: l'individuazione ed il sequestro di asset digitali.

Lorenzo Savastano
Maggiore della Guardia di Finanza
DOI: 10.54103/milanoup.150.c181

Abstract: La prima parte del lavoro è incentrata sul valore probatorio assunto dalle transazioni elettroniche impresse sul *public ledger* della blockchain. Sarà poi analizzata la "meccanica" delle procedure da seguire per l'esecuzione di una misura cautelare reale su beni digitali coerente con la natura puramente dematerializzata di tali asset. Infine, esploreremo come e in che misura la regola "follow the money" sia ancora in grado di declinare ed esprimere il proprio valore investigativo in un universo in cui il vettore naturale delle indagini sembra essersi capovolto. Il dilemma operativo si pone non tanto sulla ricerca degli indizi e delle tracce del denaro, quanto (necessariamente) sulla loro corretta interpretazione e correlata valorizzazione operativa.

The work's first part focuses on the evidence source and its possible metamorphosis in the virtual asset ecosystem. In particular, we will analyse the probative value assumed by the electronic transactions printed on the blockchain public ledger. The "mechanics" of the procedures to be followed for the execution of an accurate precautionary measure on digital assets will then be analyzed. Finally, we will explore how and to what extent the "follow the money" rule. As illustrated, the operational dilemma in this type of investigation will no longer arise () in the search for clues and traces of the money but (necessarily) in their correct interpretation and related operational valorization.

1. "Following the money": ma dove?

In un celebre convegno svoltosi a Castel Gandolfo tra il 4 ed il 6 giugno 1982, curato dal Consiglio Superiore della Magistratura, dal titolo *Riflessioni ed esperienze sul fenomeno mafioso*, i giudici istruttori Giovanni Falcone e Giuliano Turone presentarono una relazione congiunta sul tema "Tecniche di indagine in materia di mafia". Quel documento pose le basi di un metodo di indagine che – ad oggi – è divenuto un vero e proprio postulato operativo informante ogni indagine

dotata di un sufficiente grado di complessità, basato sulla potenza rivelatrice delle tracce finanziarie che precedono o susseguono la commissione di un reato, e sintetizzabile nella formula anglofona: "follow the money".

Il presente contributo intende focalizzarsi su *come* (e *se*) la regola di matrice falconiana abbia preservato la propria *vis* investigativa nello scenario inedito e trasformativo della tecnologia *blockchain*, rassegnando talune osservazioni teoriche e conseguenti corollari operativi che – *quotidie* – si impongono all'attenzione degli Organi investigativi nella conduzione delle più articolate e complesse indagini di polizia giudiziaria.

Posto questo *azimut* argomentativo, ci sospingeremo sul versante più operativo delle moderne investigazioni economico-finanziarie, scandagliando la "meccanica" delle procedure da seguire per l'individuazione ed il successivo sequestro di una *res* digitale, descrivendo a tal fine le manovre di riciclaggio di capitali illeciti, attuate mediante i protocolli informatici delle *Distributed Ledger Technology* (DLT), maggiormente rilevate sia nella prassi operativa che nell'osservazione scientifica.

Infine, affronteremo i contenuti principali ed operativamente più densi della nuova *travel rule* di matrice europea, vero e proprio architrave su cui poggia la strategia anti-riciclaggio in corso di perfezionamento da parte delle Istituzioni dell'Unione europea, nel settore dei *digital asset*.

Chiuderemo in tal modo una parabola ideale che cinge insieme, in un vincolo strettamente cronologico ed evolutivo, il modello investigativo derivante dal contrasto al fenomeno mafioso – precocemente concettualizzato dal giudice Giovanni Falcone – e le più moderne tecniche di polizia economico-finanziaria attualmente impiegate dalle Autorità di controllo e di vigilanza per inseguire le tracce del denaro, anche quando queste si muovono su terreni inediti, ancora poco presidiati e, soprattutto, *virtuali*.

2. L'individuazione degli asset digitali

In limine, vale ricordare che l'art. 648 *bis* del codice penale punisce, con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000, chiunque «sostituisc(a) o trasferisc(a) denaro, beni o altre utilità provenienti da delitto, ovvero compi(a) in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa», ponendo in essere la condotta prevista e punita dal reato di riciclaggio.

Rifuggendo da un approfondimento di natura normativa e giurisprudenziale del predetto reato, preme evidenziare in questa sede come la condotta tipica del riciclaggio possa essere schematizzata secondo una metodologia diffusa nella prassi operativa e che – per i fini che più pertengono all'oggetto del presente contributo – consenta di far emergere l'impiego di asset digitali in tali manovre.

Nello specifico, le operazioni di *money laundering* possono essere operativamente suddivise in tre fasi facenti parti di un unico processo[1]:

– *placement stage* (fase del collocamento): è il "piazzamento" materiale dei proventi da reato nel sistema economico legale attraverso una qualsiasi operazione di deposito, cambio, trasferimento, acquisto di beni e così via. In questa fase, l'obiettivo principale dei *money lauderer* è tradizionalmente la trasformazione del denaro contante in moneta scritturale, come i saldi attivi dei rapporti finanziari intrattenuti presso Istituti di credito o altri intermediari finanziari.
  Nei sistemi di archiviazione e movimentazione di flussi finanziari dischiusi dalle tecnologie ispirate ai protocolli della blockchain, questa fase coincide con la tramutazione dei capitali di origine illecita in cripto-attività scambiabili su piattaforme online, indipendentemente dalla natura centralizzata (CEX) o decentralizzata delle stesse (DEX);
– *layering stage*: stadio del processo di riciclaggio volto alla dissimulazione dell'origine illecita dei capitali e all'eliminazione delle loro tracce contabili e/o finanziarie, al fine prevalente di ostacolare l'operato degli Organi investigativi o di altre Autorità di controllo.
  Trasmigrata nei sistemi DLT, è questa la fase in cui il "camuffamento" dei connotati illeciti della provvista finanziaria – già convertita in digital asset – assume le caratteristiche tipiche di una delle operazioni comunemente riproducibili nell'ecosistema della finanza decentralizzata, come la compravendita di Non-Fungible-Token (NFT) o – nelle ipotesi più complesse – il convogliamento degli asset digitali in *wallet* costituiti *ad hoc* (come nelle operazioni di *staking*) o – più comunemente – in *liquidity pool* ospitate all'interno di DEX nell'ambito di operazioni di *yield farming* e/o *liquidity mining*;
– *integration stage*: una volta fornita un'apparente (e fittizia) giustificazione all'origine della provvista finanziaria illecita, i riciclatori reintroducono il denaro nell'economia legale, perfezionando in tal modo l'obiettivo del processo di riciclaggio.
  Tipicamente, nel *milieu* dei mercati di digital asset tale operazione si perfeziona mediante la conversione del denaro digitale in valuta *fiat* (ovvero avente corso legale), mediante il coinvolgimento di *Virtual Asset Service Provider* (VASP) svolgenti funzioni di *exchanger*. Attesa la loro funzione ai fini della prevenzione di fenomeni di riciclaggio di denaro e di finanziamento del terrorismo, tali operatori sono stati difatti tra i primi ad essere stati inseriti, unitamente ai cc.dd. *wallet provider*, nell'elenco dei soggetti obbligati al rispetto della normativa antiriciclaggio di cui all'art. 3 del D. Lgs. 21 novembre 2007, n. 231 (c.d. decreto antiriciclaggio), in recepimento

1 Tra la vasta produzione dedicata alla strutturazione di schemi di riciclaggio si cita, su tutti: EUROPOL, *Why is Cash still King?* The Hague, 2015, p. 9 e ss.

della Direttiva n. 2015/849/UE (c.d. V Direttiva antiriciclaggio), avvenuta in Italia con il D. Lgs. 4 ottobre 2019, n. 125.

Posta tale schematizzazione di base, è dunque di tutta evidenza come le caratteristiche tecniche e tecnologiche dei virtual asset rendano gli stessi particolarmente versatili per essere impiegati dai riciclatori per attuare o catalizzare una delle tre fasi di *money laundering* appena descritte.

Si tratta, del resto, di un aspetto di cui è ben consapevole lo stesso GAFI (Gruppo di Azione Finanziaria), organismo internazionale operante sotto l'egida dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) e *policy maker* mondiale nell'elaborazione degli standard normativi e regolamentari nel contrasto alle condotte di riciclaggio di denaro "sporco" e finanziamento del terrorismo che, nel corso del tempo, ha emesso plurimi alert e lineeguid,a per consentire a Governi nazionali ed ai soggetti obbligati al rispetto della normativa antiriciclaggio di poter efficacemente fronteggiare le sfide poste dall'avvento delle nuove tecnologie della decentralizzazione finanziaria, secondo il tralatizio approccio *risk-based*[2].

2.1. Manovre di riciclaggio nei sistemi DLT

Ebbene, alla luce del consolidamento delle prime osservazioni investigative stratificatesi nel settore, è possibile individuare (almeno) tre tipologie di dinamiche riciclatorie perpetrate mediante il ricorso alle specificità della blockchain e, in generale, delle DLT.

Nello specifico, possiamo individuare manovre:

– di *peel chain*: tecnica precipuamente volta ad offuscare la tracciabilità di una transazione effettuata mediante digital asset, che viene "frantumata" in più passaggi coinvolgenti wallet differenti prima di essere destinata ad un exchanger per il "cambio" definitivo in una valuta *fiat*.
  In dettaglio, ad ogni step del processo riciclatorio, una parte del denaro digitale viene ceduta a nodi riconducibili al target finale-titolare effettivo della transazione (c.d. *peel off*). In questo modo, i money launderer rendono estremamente complessa la ricostruzione delle operazioni e – di conseguenza – l'attribuzione del flusso virtuale al o ai soggetti che pongono fattivamente in essere la transazione.
– Una variante del *peel chain* – simile allo *smurfing* di denaro contante – prevede inoltre il trasferimento di grandi quantitativi di valuta virtuale all'interno e all'esterno dei protocolli della *DeFi*, impiegando – indifferentemente – sia exchanger centralizzati sia decentralizzati (come detto: CEX o DEX). Ad esempio, per trasferire 100 ETH, un unico individuo potrebbe realizzare 200 transazioni di 0.5. ETH ciascuna.

2 Da ultimo, si veda "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", del 28 ottobre 2021.

Graficamente, una tipica manovra di *peel chain* può essere così rappresentata[3]:

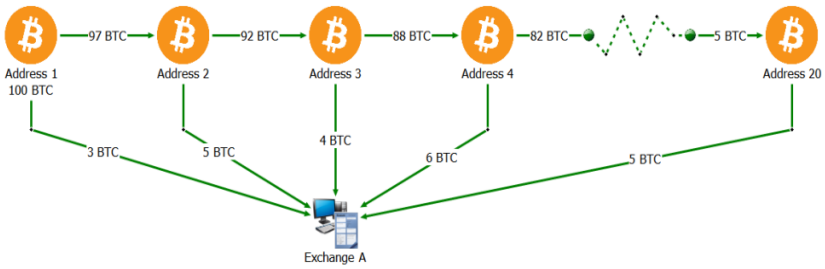

Fig. 1 Civil Action No. 20-606, United States of America, v. 113 Virtual Currency accounts

Sul punto, corre osservare come uno dei principali fattori di profittabilità della manovra, da tenere in considerazione, sia l'importo delle *fee* richieste dalla blockchain impiegata per il perfezionamento della transazione;

– di *chain hopping*: tecnica di offuscamento del flusso di denaro basato sulle potenzialità offerte da talune piattaforme cc.dd. multi-*chain* di *DeFi* che consentono e promuovono l'interoperabilità tra più blockchain (come, ad esempio, *Change Finance* o *Cosmos Network*).
In questi casi i money launderer realizzano molteplici transazioni digitali in un ristretto arco temporale, aumentando – in apparenza – la complessità delle operazioni e rendendo estremamente complessa e dispendiosa l'individuazione del wallet originatore della provvista.
Un caso emblematico di chain hopping è stato osservato nel corso di un'investigazione condotta dall'*Internal Revenue Service-Criminal Investigation* (IRS-CI) statunitense, che ha fatto emergere le condotte un gruppo criminale composto da vari soggetti di nazionalità nord-coreana accusati di aver illecitamente sottratto, nel corso di almeno due attacchi informatici, 250 milioni di dollari di cripto-valuta a diversi exchanger e di aver – conseguentemente – riciclato i proventi mediante un *crypto-trader* OTC (*over-the-counter*) di nazionalità cinese.

3 L'esempio è tratto dalla Civil Action No. 20-606, *United States of America, v. 113 Virtual Currency accounts*, la cui sentenza è stata depositata dal United States District Court for the District of Columbia, il 2 marzo 2020. Nel caso di specie si è trattato di un'investigazione condotta dall'Internal Revenue Service-Criminal Investigation (IRS-CI) statunitense, che ha consentito di ricostruire il riciclaggio di oltre 100 milioni di dollari di criptovalute sottratte illegalmente ad un exchanger ad opera di due soggetti di nazionalità cinese (*cfr. Press Release* del 2 marzo 2020 del US Department of Justice).

L'utilizzo artificiosamente complesso di piattaforme DLT multi-canale da parte degli indagati è ben rappresentato dal seguente schema grafico[4]:

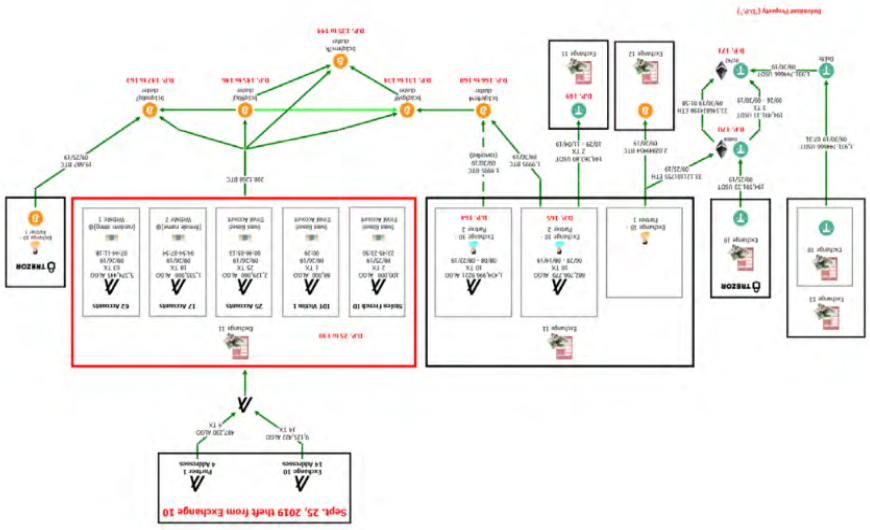

Fig. 2 Civil Action No. 20- 2396, United States of America, v. 280 Virtual Currency accounts

– effettuate mediante il ricorso a *Anonymity-Enhanced Cryptocurrencies* (AEC – come *Mixers* o *Tumblers* e *privacy coin)*, programmi informatici appositamente elaborati per offuscare il registro alla base dei protocolli DLT, rendendo di fatto estremamente complessa la ricostruzione della cronologia delle transazioni riportate sulla blockchain.
Tra le altre, si segnala – per l'ampia risonanza avuta dalla vicenda – la sanzione comminata dal U.S. *Department of the Treasury's Office of Foreign Assets Control* (OFAC) al *virtual service provider* denominato *Tornado Cash,* corrente su *Ethereum*, in grado di offrire servizi di *mixing* delle transazioni e (pertanto) bloccato dal governo degli Stati Uniti per aver consentito il riciclaggio – secondo le accuse – di oltre 7 miliardi di dollari di origine illecita[5].

4 Il caso è stato affrontato nella Civil Action No. 20- 2396, *United States of America, v. 280 Virtual Currency accounts*, la cui sentenza è stata depositata dal United States District Court for the District of Columbia, il 27 agosto 2020 ((*cfr. Press Release* del 27 agosto 2020 del US Department of Justice). La sentenza è integralmente reperibile al seguente link https://www.justice.gov/opa/press-release/file/1253491/download.

5 Si veda, al riguardo, il *press release* dell'OFAC dell'8 agosto 2022, disponibile sul sito ufficiale della prefata Autorità d'oltreoceano.

All'interno della medesima categoria di AEC sono, inoltre, rinvenibili i cc.dd. *privacy coin,* come *Monero*, *Zcash* e *Dash*. Come mostrato dal Dipartimento del Tesoro statunitense nell'ambito del rapporto denominato *National Money Laundering Risk Assessment*, relativo al 2022, tali tipologie di asset digitali sono difatti in grado di oscurare gli elementi chiave di una transazione, grazie all'utilizzo di specifiche tecniche crittografiche, come *ring signatures* (letteralmente "firma ad anello", impiegate per nascondere l'identità dell'originatore della transazione), *ring confidential transaction* (finalizzate a celare l'ammontare effettivo della transazione, sostituendolo con un importo crittograficamente protetto), *stealth address* (tecnologia utilizzata per occultare l'indirizzo digitale del beneficiario, tramite la generazione estemporanea di indirizzi *ad hoc* e *one-time* su cui accreditare l'importo della transazione), protocolli *zero-knowledge proof* (che consentono all'utente di validare una transazione eliminando la necessità di rivelare le informazioni sottostanti, come l'input e l'output del flusso di valuta virtuale).

Nello specifico, sulla blockchain di *Monero*, le transazioni non sono riportate pubblicamente come nella maggior parte delle DLT, ma sono effettuate ricorrendo ad un *one-time wallet* (generati dalla richiamata tecnologia *stealth address*), che consente di occultare ad "entità esterne" gli effettivi mittenti e destinatari del singolo flusso finanziario digitale. Per ogni transazione, difatti, la tecnica *ring signatures* offusca l'origine dei fondi "mixando" (ovvero riunendo e mescolando insieme, all'interno di un unico "contenitore virtuale") la chiave del firmatario della transazione con quelle di altri utenti della piattaforma (denominati *Decoy*), rendendo *de facto* impossibile agli *auditor* l'individuazione del reale disponente della dazione;

– di *Wash trading di NFT* (Non-Fungible-Token): si tratta dell'esecuzione ripetuta di una transazione in cui il medesimo soggetto è presente su entrambi i lati della transazione (*vendor* e *customer*), essendo la medesima entità il possessore dei wallet coinvolti nello scambio. Lo scopo è quello di aumentare artificiosamente i volumi di scambio e – di conseguenza – il valore percepito di un asset. Al riguardo, esemplificativamente, il report di *Chainalysis* del febbraio 2022 riporta, tra gli altri, un caso in cui sono stati individuati 262 users che hanno venduto e ricomprato il medesimo NFT oltre 25 volte, generando un profitto di oltre 8,5 milioni di dollari[6].

Il Wash trading di NFTs può anche essere impiegato come sistema di riciclaggio di capitali di fonte illecita – in modo simile al *digital money muling* osservato al viciniore contesto della *digital economy* – attuato mediante l'effettuazione di transazioni di NFTs, ad un valore appositamente

6 Per un approfondimento sul tema del *wash trading di NFT*: TARIQ S.A. - SIFAT I., *Suspicious Trading in Nonfungible Tokens (NFTs): Evidence from Wash Trading*, 30 aprile 2022, disponibile su SSRN.com.

manipolato, al solo fine di trasferire fondi non monitorati dagli attuali sistemi di prevenzione e di scambio di informazioni anti-riciclaggio[7].

2.2. Tecniche di blockchain analysis

La comparsa di modalità riciclatorie come quelle testé descritte rende necessario, per le Autorità di vigilanza e per gli organi investigativi, dotarsi di strumenti più efficaci e performanti per la conduzione di investigazioni finanziarie, in grado di affiancare e corroborare quelli tipicamente utilizzati in contesti operativi tradizionali. A tal proposito possono succintamente richiamarsi in questa sede:

- tecniche di *ownership analysis*, ovvero l'analisi della catena proprietaria dei wallet verso cui confluiscono gli asset digitali i titolari effettivi dei wallet inseriti in schemi riciclatori e/o evasivi.
  In questo senso, utili elementi per la conduzione di indagini finanziarie potranno pervenire dall'attivazione di mirati canali di scambio informativo con altre giurisdizioni (non solo) europee, anche specificamente dedicati al settore delle cripto-attività, di prossima attivazione.
  Si tratta, in particolare, dei protocolli delineati in ambito OCSE con il c.d. CARF (*Crypto-Asset Reporting Framework*), approvato in agosto e presentato al G20 lo scorso ottobre, e "riprodotti" in ambito europeo con la nuova DAC-8 (*i.e.* l'ottavo emendamento alla Direttiva 2011/16/UE sulla cooperazione amministrativa ai fini fiscali), la cui bozza è stata definitivamente approvata lo scorso dicembre;
- modelli di *clustering algorithms*: anche in abbinamento a tecniche di *pattern analysis*, rese possibili dall'impiego di software capaci di riordinare la complessità delle transazioni riportate su un registro DLT organizzandole classi omogenee di operazioni (*cluster*), raggruppate per caratteristiche soggettive ed oggettive e modalità di effettuazione;
- processi di *e-discovery*: definibili come i procedimenti che – nell'alveo dell'informatica forense – consentono di ricercare ed individuare dati informatici di interesse investigativo (denominati ESI – *electronically stored information*) presenti in archivi digitali, creando copie forensi utilizzabili anche in sede penal-processualistica.
  Al riguardo, un utile ausilio a ricerche di questo tipo può essere offerto dall'impiego di strumenti di *Open Source Intelligence* (OSInt) specificamente dedicati al campo delle *digital currencies*, come l'uso combinato di siti *web* in grado di isolare e descrivere il comportamento di un wallet sospetto.

In generale, è possibile affermare che sovente informazioni sugli *address* Bitcoin e altre valute virtuali sono inferibili da una attenta analisi condotta su

7 *Cfr.* Department of the Treasury, *Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art*, Febbraio 2022, pagg. 25 e ss.

fonti reperibili online (e.g. siti web, piattaforme di microblogging, social media *et similia*), dove gli stessi appaiono indicizzati dai motori di ricerca[8].

A mero titolo esemplificativo, partendo dall'individuazione di un wallet avente un comportamento anomalo, è possibile tracciare la cronologia esatta delle sue transazioni consultando il registro pubblico della relativa blockchain reperibile su internet[9]. Successivamente, impiegando altri strumenti informatici disponibili sulla rete, sarà possibile quantificare la provvista (*balance*) del portafoglio digitale[10] o – qualora risulti proficuo ai fini investigativi – verificare se il medesimo indirizzo è comparso contestualmente su altri siti web o è stato abbinato ad altri indirizzi IP nelle ultime transazioni[11].

Parimenti, sempre ricorrendo a ricerche open source, potrà essere possibile ricostruire il comportamento del wallet investigato, isolando ed enucleando i principali *pattern* di anomalia ricorrenti nella sua recente operatività, nonché le informazioni essenziali sul suo utilizzo, come il flusso totale di criptovaluta da esso transitato che in input che in output [12].

Ebbene, se – come osservato – appare teoricamente possibile ricostruire l'operatività di un wallet di interesse investigativo, decisamente meno agevole risulterà accertare la riconducibilità dello stesso ad un soggetto identificato o identificabile, anche in considerazione dell'ampio uso di pseudonimi o *alias* tra gli utenti delle principali DLT.

Ad ogni modo, atteso il peculiare funzionamento della tecnologia crittografica sottesa al funzionamento della blockchain, nel corso di un'investigazione finanziaria sarà possibile attribuire la piena disponibilità di un wallet ad un determinato soggetto solo qualora quest'ultimo risulti l'effettivo detentore della chiave privata del portafoglio digitale. Solo il possesso *uti domini* di tale strumento consentirà, difatti, la riconduzione all'indagato della ricchezza digitale movimentata o archiviata sul wallet di interesse, fornendo il presupposto necessario ed indefettibile per l'esecuzione di una misura cautelare reale sulle disponibilità digitali dell'indagato.

---

8 Al riguardo, un utile supplemento di indagine potrebbe essere rappresentato dall'utilizzo di software che consentono attività di *crawling* di siti, ovvero un processo mediante il quale un motore di ricerca o un'altra applicazione informatica – comunemente chiamato spider o web crawler – esplora e analizza il contenuto di un sito web, al fine di identificare e indicizzare le informazioni presenti sulle pagine di un sito.

9 Ad esempio, il sito *Blockchain.com*, qualora si tratti di digital asset correnti sulle blockchain di *Bitcoin*, *Ethereum* e *bitcoin cash*.

10 Ricorrendo, ad esempio, al sito Bitref.com che, oltre a fornire la visibilità immediata del *wallet balance*, è in grado di riprodurre anche le ultime 100 transazioni registrate sull'indirizzo.

11 Si tratta di informazioni utili, ad esempio, nel caso di indagini relative a *crypto scam*. Al riguardo un utile tool disponibile online è il sito Bitcoinwhoswho.com, in grado di dare contezza non solo della comparsa del wallet investigato su altri websites, ma anche dell'ultimo indirizzo IP in ordine di tempo ad esso associato.

12 Al riguardo, utili strumenti sono rappresentati – ad esempio – da WalletExplorer.com o, unicamente per i Bitcoin, il sito oxt.me.

3. Il sequestro degli asset digitali

La ricostruzione delle "tracce del denaro" – anche mediante le richiamate tecniche di analisi forense della DLT impiegata dagli utenti – e l'individuazione degli asset digitali costituenti l'oggetto della manovra illecita, sono fasi preliminari (*rectius*: pregiudiziali) al momento finale e più delicato dell'investigazione finanziaria: la fase di *recovery*, ovvero l'esecuzione della misura cautelare reale emessa dalla competente Autorità giudiziaria, che sottragga definitivamente dalla disponibilità dell'indagato la *res* virtuale[13].

A tal fine, come anticipato, è possibile rilevare come la condizione tecnica indispensabile per l'aggressione patrimoniale della provvista digitale sia la materiale disponibilità della chiave privata di accesso all'indirizzo di custodia dei cripto-asset, che potrà alternativamente essere o non essere spontaneamente esibita dall'utente.

In concreto, ponendo il caso operativamente più complesso, ovvero l'ipotesi in cui la parte decida di non collaborare, non fornendo quindi la propria chiave privata per accedere al contenuto del wallet, il recupero dei valori virtuali da porre *in vinculis* potrà avvenire in modo differenziato a seconda della tipologia di wallet rinvenuto.

In particolare, occorre distinguere primariamente tra dispositivi di gestione ed archiviazione di chiavi pubbliche e/o private offline (c.d. *cold hardware wallet* o *cold paper wallet*) e portafogli utilizzati per generare, gestire, archiviare o utilizzare chiavi pubbliche e private connessi ad internet (c.d. *hot wallet*).

Ebbene, mentre nel primo caso risulterà proficuo procedere prioritariamente alla ricerca ed al conseguente sequestro probatorio, ai sensi dell'art. 354 del codice di procedura penale, di copie di backup del wallet o del suo *recovery seed*[14], nella seconda ipotesi prospettata occorrerà porre un'ulteriore *discrimen*, utile ad orientare le scelte operative degli organi inquirenti.

Nello specifico, servirà distinguere tra portafogli digitali:

-non gestiti da specifici VASP (c.d. *hot non-custodial wallet*): in tale scenario sarà necessario entrare in possesso delle credenziali di accesso al software, solitamente consistenti in un indirizzo di posta elettronica ed una password[15]. A tal fine, un utile ausilio investigativo potrebbe essere rappresentato dal ricorso a

13 *Amplius*: SAVASTANO L., *Indagini finanziarie e sequestro di digital asset*, in AA.VV. (a cura di AVELLA F.), *Bitcoin e Cripto-attività*, Il Sole 24 Ore, Milano, febbraio 2023, p. 127 e ss.

14 Il *recovery seed* è la sequenza di parole, la cui lunghezza è variabile a seconda degli standard crittografici utilizzati nell'attivazione del wallet, che consente il recupero dei valori digitali ivi depositati.

15 Tali wallet, in gran parte dei casi, prevedono obbligatoriamente tecniche di autenticazione a due fattori (cd. 2FA – *Two Factor Authentication*), ad esempio mediante l'inserimento di un codice inviato via SMS per effettuare l'accesso, o cliccando su un link inviato all'indirizzo di posta elettronica abbinato all'account, o ancora mediante l'inserimento di un codice generato casualmente da apposite applicazioni per smartphone come *Authy* o *Google Authenticator*.

tecniche di *computer forensics* volte ad esplorare il contenuto di ulteriori device o luoghi fisici e virtuali di archiviazione nella disponibilità dell'indagato, ivi incluso il contenuto della casella di posta elettronica;

-gestiti da specifici *prestatori di servizi di portafoglio digitale*[16] (c.d. *hot custodial wallet*): in tal caso le chiavi private non sono nella disponibilità dirette dell'utente, bensì del provider del servizio di custodia. Nel peculiare contesto di un'indagine di polizia giudiziaria, l'apprensione delle chiavi crittografiche potrà concretamente avvenire in forza di uno specifico provvedimento magistratuale di esibizione di atti e documenti, emesso in forza dell'art. 248 del codice di procedura penale.

Al riguardo, corre evidenziare che – qualora il fornitore del servizio connesso alla valuta virtuale sia stabilito o residente in Italia – potrà farsi riferimento agli operatori inseriti nella sezione speciale dell'elenco dei cambiavalute di cui all'art. 17-*bis* del D. Lgs. 13 agosto 2010 n. 141, detenuto dall'Organismo Agenti e Mediatori (OAM), reso operativo dal D.M. 13 gennaio 2022[17].

Preme rilevare, in proposito, che – anche al di fuori della fase procedimentale delle indagini preliminari – l'art. 6 del decreto da ultimo citato consente al Nucleo Speciale di Polizia Valutaria della Guardia di Finanza, nonché alle Forze di polizia di cui all'art. 16, primo comma, della Legge 1° aprile 1981, n. 121 (*viz.* Guardia di Finanza, Arma dei Carabinieri e Polizia di Stato), nell'esercizio delle proprie funzioni e nell'ambito dei rispettivi comparti di specialità[18], di richiedere all'OAM «i dati e le informazioni inerenti ai prestatori di servizi relativi all'utilizzo di valuta virtuale e ai prestatori di servizi di portafoglio digitale».

In caso contrario, qualora cioè il wallet provider risulti collocato in altra giurisdizione, le modalità operative per accedere ai dati di interesse investigativo (ovvero le generalità del detentore della chiave privata del wallet) potranno essere calibrate differentemente a seconda dello specifico contesto investigativo in cui si rende necessaria l'ablazione dei valori digitali.

In merito, tra i più efficaci canali di scambio informativo ed acquisizione probatoria offerti dai moderni sistemi di cooperazione giudiziaria e di polizia internazionale ed europea, possono senz'altro richiamarsi:

– l'invio di una *rogatoria c.d. attiva*, con i tempi e le modalità disciplinate dall'art. 727 del codice di rito penale, all'Autorità giudiziaria straniera, per il tramite del Ministro della giustizia, in forza di apposite convenzioni

16 I "prestatori di servizi di portafoglio digitale" sono definiti dall'art. 3, comma 2, lett. *ff-bis*) del D. Lgs. n. 23172007 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*»*.

17 Recante: «Modalità e tempistica con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale e i prestatori di servizi di portafoglio digitale sono tenuti a comunicare la propria operatività sul territorio nazionale nonché forme di cooperazione tra il Ministero dell'economia e delle finanze e le forze di polizia».

18 Di cui all'art. 2 del decreto legislativo 19 agosto 2016, n. 177.

multilaterali o bilaterali di assistenza giudiziaria in materia penale, qualora esistenti ed in vigore.

Sulla possibilità del ricorso ad una rogatoria internazionale nel campo delle indagini inerenti a digital asset, si stima utile sottolineare come l'art. 234-*bis* del codice di procedura penale (rubricato "Acquisizione di documenti e dati informatici"), anche in accoglimento degli standard sanciti dalla c.d. Convenzione di Budapest sulla criminalità informatica, ratificata in Italia con Legge 18 marzo 2008, n. 48, preveda apertamente che: «è sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare».

In concreto, difatti, l'art. 29 della citata Convenzione ha previsto che ogni Stato firmatario possa richiedere, tramite il punto di contatto nazionale, ad un altro Stato contraente, di ordinare cautelativamente la conservazione (cd. *freezing*) di dati digitali immagazzinati in un sistema informatico situato nel proprio territorio di pertinenza, al fine di avanzare una successiva richiesta di mutua assistenza per la perquisizione o il sequestro dello stesso;

– l'emissione di un *Ordine Europeo di Indagine* (OEI), di cui alla Direttiva n. 2014/41/UE, recepita in Italia con D. Lgs. 21 giugno 2017, n. 108, definibile come il provvedimento emesso dalla Autorità giudiziaria o amministrativa di uno Stato membro dell'UE (Stato di emissione) per compiere «atti di indagine o di assunzione probatoria che hanno ad oggetto persone o cose che si trovano nel territorio dello Stato o di un altro Stato membro dell'Unione ovvero per acquisire informazioni o prove che sono già disponibili», e soggetto a convalida da parte dell'Autorità giudiziaria dello Stato membro in cui dovrà essere compiuta l'attività d'indagine (Stato di esecuzione).

  In dettaglio, l'OEI può essere applicato per l'esecuzione di qualsiasi atto d'indagine diverso dall'istituzione di una Squadra Investigativa Comune, per la quale specifiche modalità di attivazione e funzionamento sono state dettate dalla Decisione quadro del Consiglio dell'Unione europea n. 2002/465/GAI.

  Dopo aver ricevuto un OEI, lo Stato di esecuzione è dunque tenuto a rispondere rapidamente alla richiesta, potendo opporre un rifiuto solo in determinate e residuali circostanze, per esempio qualora la richiesta sia contraria ai principi di legge fondamentali del Paese o danneggi interessi di sicurezza nazionale. Ad ogni modo, l'organismo che dà esecuzione alla richiesta può scegliere un atto d'indagine alternativo ad un OEI, se ritiene che ciò porterà a risultati simili;

– la richiesta di una misura investigativa prevista dall'art. 30 del Regolamento (UE) n. 2017/1939 del Consiglio, del 12 ottobre 2017, relativo all'istituzione della nuova Procura europea (denominata *European Public Prosecutor's*

Office – EPPO), pienamente attuato in Italia con il D. Lgs. 2 febbraio 2021 n. 9[19].

Si tratta di un provvedimento altamente performante ed efficace nell'ambito di indagini di polizia giudiziaria transnazionali su reati ricadenti nella competenza materiale e territoriale di EPPO[20], rappresentando un definitivo (ed epocale) superamento del principio del "mutuo riconoscimento" a favore della concezione di un'unica giurisdizione unionale ai fini penalistici. Nel contesto della c.d. *cooperazione rafforzata europea*, ogni Procuratore Europeo Delegato (PED) è, difatti, autorizzato a disporre o a chiedere, tra l'altro, «la produzione di dati informatici archiviati, cifrati o decifrati, in originale o in altra forma specificata, inclusi i dati relativi al conto bancario e i dati relativi al traffico», senza che sia necessario ottenere una preventiva convalida del provvedimento da parte dell'Autorità giudiziaria competente dello Stato membro in cui è posto in essere l'atto investigativo.

Ottenuto l'accesso, nelle suindicate modalità, alle disponibilità digitali del wallet*,* mediante l'apprensione della chiave privata dello stesso, lo step successivo per l'esecuzione della misura cautelare sarà infine la predisposizione di un apposito wallet per la custodia delle *res* virtuali da porre nella disponibilità degli organi inquirenti.

È di tutta evidenza, difatti, come l'unica modalità di intervento che consenta di eliminare *in nuce* il rischio che la parte possa accedere al contenuto del wallet in sequestro mediante copie di backup della private key, custodite su altri dispositivi informatici non rinvenuti e cautelati dall'organo inquirente, sia l'effettuazione di una transazione dei valori digitali verso un portafoglio virtuale nell'esclusiva disponibilità dell'Autorità giudiziaria procedente, mediante la contestuale generazione di un nuovo indirizzo (*i.e.* un wallet istituzionale) e l'accurata custodia delle relative chiavi private.

A tal fine, potrà procedersi, alternativamente:

- mediante l'archiviazione del nuovo indirizzo generato dalla polizia giudiziaria e della relativa chiave privata su un supporto fisico, da rimettere successivamente nella disponibilità dell'Autorità giudiziaria;
- affidando ad un terzo custode giudiziario la generazione del wallet verso cui indirizzare i valori virtuali da sequestrare.

In ultimo, in ossequio alle vigenti disposizioni regolamentari e penal-processualistiche, la polizia giudiziaria operante dovrebbe procedere al successivo trasferimento della moneta digitale in sequestro al Fondo Unico Giustizia (FUG), previsto dall'art. 2, comma 2, del D.L. 16 settembre 2008, n. 143 e gestito dalla

19 Avente ad oggetto: «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2017/1939 del Consiglio, del 12 ottobre 2017, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea "EPPO"».

20 Si tratta dei reati di cui alla Direttiva n. 2017/1371/UE, relativa alla protezione degli interessi finanziari dell'Unione europea.

società Equitalia Giustizia S.p.A., anche avvalendosi – qualora necessario – di un exchanger all'uopo autorizzato[21].

4. La nuova travel rule europea

Essere in grado di individuare ed inseguire le tracce del denaro "digitale" anche nel nuovo universo delle DLT, al fine di prevenire e reprimere l'impiego distorto di tale tecnologia per manovre di riciclaggio di capitali illeciti e di finanziamento del terrorismo, è anche una delle priorità dell'Unione europea (UE) che – nel più ampio contesto del pacchetto legislativo antiriciclaggio (c.d. "*AML Package*"), varato dalla Commissione europea il 20 luglio 2021[22] – ha avviato mirati lavori per l'aggiornamento e la rifusione (*rectius*: l'adattamento ai nuovi scenari discussi in questa sede) del Regolamento (UE) n. 2015/847 del Parlamento europeo e del Consiglio, del 20 maggio 2015, riguardante i dati informativi che accompagnano i trasferimenti di fondi all'interno del mercato unico dell'UE. Tali lavori si sono ora formalmente conclusi con l'adozione del nuovo Regolamento (UE) n. 2023/1113 del 31 maggio 2023, la cui trasposizione negli ordinamenti nazionale dovrà avvenire entro il 30 dicembre 2024.

In particolare, l'obiettivo del Regolamento è quello di allineare la normativa unionale con i principi elaborati in materia dal già citato *Gruppo di Azione Finanziaria* (GAFI) che, modificando il 21 giugno 2019 la Nota interpretativa alla sua Raccomandazione n. 15, riguardante il tema delle nuove tecnologie, ha introdotto specifici obblighi di condivisione con le Autorità di settore dei dati informativi richiesti per i prestatori di servizi di attività virtuali (la c.d. "regola di viaggio" o "travel rule").

Si tratta, più in dettaglio, del secondo importante allineamento *de iure condendo* del quadro normativo unionale agli standard elaborati dal prefato Organismo sovranazionale, dopo quello riguardante le definizioni di "cripto-attività" e "servizio per le cripto-attività" [23], recepite all'interno del Regolamento (UE) n. 2023/1114 del 31 maggio 2023, recante *Market in Crypto Asset Regulaton* (MiCAR).

---

21 Al riguardo, corre tuttavia rilevare che, allo stato, non risultano indicazioni di natura legislativa o ministeriale riguardanti le modalità in concreto esperibili per la voltura al FUG delle cripto-attività sequestrate.

22 Il medesimo piano prevede, inoltre, l'aggiornamento della Direttiva n. 2015/849/UE (c.d. IV Direttiva antiriciclaggio), l'istituzione di una nuova Autorità europea antiriciclaggio (c.d. AMLA – *Anti Money Laundering Authority*) ed una proposta di Regolamento concernente un nuovo *set* di regole comuni a tutti gli Stati dell'Unione europea in materia di prevenzione dell'uso del sistema finanziario per scopi di riciclaggio e finanziamento del terrorismo (c.d. *Single Rulebook*).

23 Definita come "*una rappresentazione digitale di valore o di diritti che possono essere trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga*".

Come noto, difatti, già la citata V Direttiva antiriciclaggio aveva introdotto nella legislazione unionale una definizione di "valute virtuali", estendendo l'obbligo di applicazione dei presidi antiriciclaggio alle categorie dei prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso legale (c.d. exchanger provider) e dei prestatori di servizi di portafoglio digitale (c.d. wallet provider). Ora, l'allineamento alle definizioni di matrice internazionale consente di disciplinare ulteriori categorie di prestatori di servizi per le attività virtuali non ancora contemplati dall'attuale assetto normativo e che potrebbero sollevare preoccupazioni in materia di riciclaggio di denaro.

Nello specifico, le prescrizioni contenute nel Reg. (UE) n. 2023/1114 si applicheranno ai prestatori di servizi per le cripto-attività stabiliti o aventi sede legale in UE, ogniqualvolta le loro operazioni, in moneta *fiat* o cripto-attività, comportino un trasferimento di cripto-attività – compresi i trasferimenti di cripto-attività eseguiti per mezzo di cripto-ATM – tra un prestatore di servizi per le cripto-attività e un altro soggetto obbligato (come una banca o un altro ente finanziario), se il prestatore di servizi per le cripto-attività o il prestatore intermediario di servizi per le cripto-attività del cedente o del cessionario ha la sede legale nell'Unione.

Attesa la specificità della materia, al fine di evitare che vi siano asimmetrie tra i pagamenti o i trasferimenti di cripto-attività effettuati all'interno di uno Stato membro ed i pagamenti o i trasferimenti di cripto-attività transfrontalieri, la proposta di Regolamento prevede che tutti i trasferimenti di cripto-attività siano trattati nel rispetto delle stesse prescrizioni previste per i trasferimenti elettronici transfrontalieri, conformemente alla nota interpretativa del GAFI della Raccomandazione n. 16.

Con riguardo al contenuto della travel rule, il nuovo Regolamento fa incombere sul prestatore di servizi per le cripto-attività del cedente la garanzia che i trasferimenti di cripto-attività siano accompagnati non solo dai dati del cedente[24], ma anche dal nome del cessionario e dal numero di conto del cessionario, se tale conto esiste ed è utilizzato per effettuare l'operazione. Specularmente, il prestatore di servizi per le cripto-attività del cessionario dovrà attuare procedure efficaci volte ad accertare l'inclusione – a corredo del trasferimento dei fondi digitali – dei dati informativi relativi al cedente, anche approntando, ove opportuno, un monitoraggio a posteriori o *real time*, per verificare l'eventuale mancanza dei dati informativi prescritti relativi al cedente o al cessionario.

Sebbene l'implementazione della travel rule negli scambi aventi ad oggetto cripto-attività rappresenti senz'altro un passo in avanti decisivo nel contrasto all'utilizzo distorto di tali tecnologie, potenziando sensibilmente la mole di dati

24 In dettaglio: nome del cedente; numero di conto, se tale conto esiste ed è utilizzato per effettuare l'operazione; indirizzo; numero del suo documento personale ufficiale; suo numero di identificazione come cliente o data e luogo di nascita.

a disposizione degli organi investigativi per la conduzione di indagini e dei soggetti obbligati al rispetto della normativa anti-riciclaggio per il rispetto dei presidi *Know-Your-Costumer* (KYC), sono ancora molte le aree di vulnerabilità lasciate scoperte dall'avvento del denaro digitale, come opportunamente evidenziato dal GAFI nell'aggiornamento alle linee-guida *Risk-Based Approach* (RBA) dedicate ai *Virtual Asset Service Providers* (VASP), del 28 ottobre 2021.

Tra queste, si citano, a titolo esemplificativo:

- la mancata adozione o l'implementazione inefficace degli standard previsti dalla travel rule in tutte le giurisdizioni interessate da scambi di cripto-attività (c.d. *sunrise issue*);
- la presenza di transazioni da o verso entità non obbligate al rispetto di presidi antiriciclaggio, come ad esempio wallet privati (c.d. *unhosted wallet*) o VASP situati in giurisdizioni non collaborative e/o non in linea con le regole di condotta stilate dal GAFI. Parimenti sono da considerarsi a rischio scambi monetari c.d. peer-to-peer (P2P), anche quando effettuate in fasi pregresse rispetto a quelle oggetto di specifico monitoraggio;
- tipologie specifiche di asset digitali o di servizi offerti da alcuni VASP, tesi ad offuscare l'origine delle transazioni finanziarie sottostanti, come ad esempio le già mentovate *anonymity-enhanced cryptocurrencies* (AEC), *mixers* e *tumblers*, piattaforme decentralizzate o DEX (*decentralized exchanger*), *privacy wallet* (ovvero wallet in grado di svolgere le funzioni tipiche dei mixer: consentire di unire in un'unica transazione le disposizioni di pagamento di più utenti), nonché servizi di *virtual layering scheme*, che consentono l'inserimento di nodi fittizi (*hidden nodes*) nelle transazioni impresse sulla DLT, riducendo in tal modo la trasparenza negli scambi.

Al riguardo, la proposta di Regolamento approvata lo scorso 20 aprile 2023, prevede che, in caso di trasferimento verso un indirizzo *unhosted*, il VASP del cedente debba ottenere e conservare i dati informativi relativi alla transazione, assicurando che i trasferimenti di cripto-attività possano essere identificati individualmente. Inoltre, qualora il trasferimento di cripto-attività verso un unhosted wallet sia di importo superiore a 1.000 euro, il VASP del cedente sarà tenuto ad adottare, inoltre, misure adeguate per valutare se tale indirizzo sia di proprietà del cedente o da questi controllato (*cfr.* art. 14, par. 5 del Regolamento).

5. Un nuovo vettore investigativo

Nel corso del presente contributo abbiamo esplorato, sebbene succintamente, come e in che misura la regola "follow the money" sia ancora in grado di declinare ed esprimere il proprio valore investigativo nei nuovi sistemi tecnologici ispirati ai protocolli DLT. La risposta è stata sostanzialmente positiva, a patto che i tradizionali strumenti di indagine ed i moderni sistemi di cooperazione giudiziaria e di polizia si integrino adeguatamente con nuovi tool informatici

adatti a leggere e comprendere i sistemi di gestione ed archiviazione delle informazioni tipici della blockchain.

Da tale prospettiva è come se la regola falconiana fosse rimasta integra nel suo significato operativo, ma avesse invertito il suo naturale vettore investigativo. Sul registro della "catena dei blocchi" le informazioni da ricercare sono difatti già presenti, pubbliche, trasparenti: il dilemma operativo in tale genere di investigazioni si pone non più (semplicemente) sulla ricerca degli indizi e delle tracce del denaro, quanto (necessariamente) sulla loro corretta interpretazione e correlata valorizzazione operativa.

Come evidente, in conclusione, il futuro delle investigazioni finanziarie sarà inevitabilmente plasmato dalle modalità di recepimento dei provvedimenti di matrice europea richiamati in questa sede, a partire dalla descritta travel rule. Un processo di traduzione normativa il cui esito non sarà indifferente alle tempistiche di conclusione. Come sempre, infatti, i tempi del diritto rischiano di rivelarsi improvvisamente lenti e macchinosi quando si confrontano con una delle più grandi protagoniste dell'era contemporanea: la tecnologia.