



IL RICICLAGGIO E ALTRE FIGURE DI REATO COMMESSI MEDIANTE CRIPTOVALUTE – PROFILI SOSTANZIALI E PROCESSUALI

Cesare Parodi

P.A. Procura della Repubblica di Torino

MATERIALI TRATTI DAL VOLUME

C. PARODI-V. SELLAROLI (a cura di) **Diritto penale
dell'informatica, I reati della rete e sulla rete**, Giuffrè
Francis Lefevre, Milano, 2020

LA RETE E IL RICICLAGGIO

Il riciclaggio è una delle fattispecie la cui diffusione è stata “esaltata” dalla possibilità di porre in essere le condotte con modalità telematiche: sia sul piano quantitativo, che su quello “qualitativo”, da intendersi come efficacia - in negativo - delle condotte criminali in oggetto.

Possibilità di operare in rete ha reso più veloci, più semplici, più “delocalizzabili” e per molti aspetti meno “riferibili” a un singolo soggetto, i trasferimenti di valori.

Art. 648 bis c.p.

“Fuori dei casi di concorso nel reato, sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l’identificazione della loro provenienza delittuosa”: sanzionata sia la sostituzione, che il trasferimento che le “altre operazioni” possono trovare nella rete uno scenario ottimale laddove finalizzate a “ostacolare” una provenienza delittuosa.

Il D. Lvo. n. 231/2007 modificato dal D. Lvo. n. 90/2017 e dal D. Lvo. n. 125/2019, che all'art. 2 (Finalità e principi) precisa che le disposizioni del decreto si applicano a fini di prevenzione e contrasto dell'uso del sistema economico e finanziario a scopo di riciclaggio e finanziamento del terrorismo.

Analizzando le finalità del decreto, il suo campo di azione con lo sterminato elenco dei soggetti (intermediari bancari e finanziari, operatori finanziari, professionisti individuali, associati o in società, operatori non finanziari, prestatori di servizi di gioco, solo per fare alcuni esempi) chiamati dall'art. 3 a adempiere agli obblighi previsti, si comprende come proprio **le attività telematiche siano al centro dell'attenzione del legislatore come delle autorità di controllo.**

L'art. 41 d.lgs. 231/2007 impone a un'ampia platea di soggetti (cd. "soggetti obbligati"), costituiti da intermediari finanziari e altri soggetti esercenti attività finanziaria (cfr. art. 11), professionisti (cfr. art. 12), revisori (cfr. art. 13) e altri operatori non finanziari (cfr. art. 14), di portare a conoscenza della UIF, mediante l'invio di una segnalazione di operazioni sospette, ossia le operazioni per le quali **"sanno, sospettano o hanno ragionevoli motivi per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo"**.

Il **sospetto** può essere desunto da caratteristiche, entità, natura delle operazioni, o da qualsiasi altra circostanza conosciuta dai segnalanti in ragione delle funzioni esercitate, tenuto conto anche della capacità economica o dell'attività svolta dai soggetti cui le operazioni sono riferite e deve fondarsi su una valutazione compiuta di tutti gli elementi delle operazioni - oggettivi e soggettivi - a disposizione dei segnalanti, acquisiti nell'ambito dell'attività svolta ovvero a seguito del conferimento di un incarico.

Le possibilità di riciclaggio online

L'offerta di prodotti, servizi e aree di scambio di varia natura in rete rappresenta una straordinaria opportunità per individuare nuove e (almeno apparentemente) sicure metodiche per attuare condotte di riciclaggio, non infrequentemente coinvolgendo soggetti ignari.

RICCA CASISTICA

- **Utilizzo (indebito e anzi “contro” i gestori del servizio) di account PayPal o servizi analoghi;** un sistema che consente di evitare forme di “tracciatura” anche se non è in grado di “supportare” normalmente importi di particolare rilievo. Accredito della somma di provenienza illecita a favore di un account riferibile a un soggetto compiacente, giustificato apparentemente dall’acquisto di beni o servizi, con conseguente restituzione (in tutto o almeno in parte) della somma in questo modo accreditata.
- **Presentazione di fittizie offerte di lavoro, occasionali o addirittura sistematiche.** Soggetti dichiarano di avere accettato apparenti offerte di lavoro - reperite in rete - per svolgere attività di ricezione e ritrasferimento di somme di denaro o beni a fronte del pagamento di un compenso; somme depositate sul loro conto da un operatore generalmente nazionale e che gli stessi “girano” su un conto estero.
- **Riciclaggio sentimentale “** (anziani, vedovi, uomini soli) contattati da giovani e attraenti donna che richiedono la disponibilità a mettere a disposizione i propri conti per operazioni che si riveleranno essere illecite.

- **Casinò online**, presenti in tutto il mondo, in numero sterminato, molti dei quali assicurano un sostanziale anonimato ai giocatori per l'accesso ai servizi offerti. Ampia gamma delle possibilità di pagamento - bonifici, carte di credito e prepagate, trasferimenti diretti, debiti e crediti sulla fattura telefonica utilizzando per deposito e ritiro delle somme i servizi di gestione dei pagamenti anche in valute virtuali.
- **Giochi online di tipo multiplayer**. Piattaforme di gioco di per sé illecite, ma che in concreto consentono forme di riciclaggio, in quanto attraverso le stesse è possibile convertire crediti di gioco in denaro reale; si tratta di aprire più account su varie piattaforme di gioco creando così le condizioni per il trasferimento di denaro.

- La rilevanza del **settore “gioco”** in relazione al fenomeno riciclaggio può essere tratta dal fatto che con il D. Lvo. n. 90/2017 siano state dettate specifiche disposizioni per i prestatori di servizi di gioco nell’ambito del D. Lvo. n. 231/2007.
- **Riciclaggio e traffico telefonico:** le carte SIM sono per molti aspetti assimilabili alle carte di credito e possono essere sia postpagate sia prepagate; costituiscono mezzi portatili e anonimi per trasportare ingenti somme di denaro.

Tecnologia blockchain, monete virtuali e riciclaggio

La tecnologia blockchain e le sue principali applicazioni - prima tra tutte le monete virtuali e i bitcoin in particolare - rappresentano un terreno di approfondimento e confronto di grande rilievo per gli operatori del settore economico-finanziario, anche sotto il profilo della potenziale rilevanza penale delle condotte tenute. Le monete virtuali possono essere considerate in prospettiva uno dei principali strumenti per attuare attività di riciclaggio o autoriciclaggio.

La tecnologia blockchain.

Il successo della tecnologia blockchain deve essere posto in relazione a caratteristiche di affidabilità, immutabilità, irrevocabilità, trasparenza e convenienza.

Blockchain è un libro mastro (Ledger) decentralizzato e crittograficamente sicuro per la gestione di transazioni su reti peer-to-peer. : “protocollo di comunicazione, che identifica una tecnologia basata sulla logica del database distribuito (un database in cui i dati non sono memorizzati su un solo computer ma su più macchine collegate tra loro, chiamate nodi). La Blockchain è un grande database per la gestione di transazioni crittografate su una rete decentralizzata di tipo peer-to-peer decentralizzato che dà il nome a una nuova piattaforma tecnologica, che permette di ridefinire e reimpostare il modo in cui creiamo, otteniamo e scambiamo valore.”

M. BELLINI, “Blockchain: cos’è, come funziona e gli ambiti applicativi in Italia”, in www.blockchain4innovation.it .

Una “catena di blocchi” collegati in rete tra loro, di modo che ogni transazione che avviene attraverso l’algoritmo di base viene validata dalla rete stessa nell’analisi di ciascun singolo blocco. Ogni blocco costituisce un archivio per tutte le transazioni e per tutto lo storico di ciascuna transazione che possono essere modificate solo con l’approvazione dei nodi della rete. Solo con il “teorico” consenso di tutti i nodi della rete le transazioni potrebbero essere modificate, così che le stesse sono di fatto non modificabili.

Tale forma di “organizzazione” (e, di gestione, delle informazioni) assume la forma del cd. distributed ledger, ossia del libro mastro “condiviso” - la cui piena funzionalità si basa non solo sull’efficacia dell’algoritmo di sistema ma anche sulla fiducia reciproca e sul ruolo necessariamente paritario tra tutti i soggetti che agiscono sulla rete - che si oppone alla logica verticistica del centralized ledger, ossia di un sistema centralizzato di gestione delle informazioni.

Le singole transazioni sono validate e correlate da un marcatore temporale, attraverso l'applicazione di funzione algoritmica informatica non invertibile (denominata hash) ogni blocco (contenente le transazioni) viene identificato in modo univoco e collegato con il blocco precedente tramite una procedura di identificazione. La marca temporale consente di associare una data e un'ora certe e legalmente valide a un documento informatico, rendendo tale dato "opponibile" a terzi.

Ogni transazione contiene:

- **le informazioni relative all'indirizzo pubblico del ricevente;**
- **le caratteristiche e l'oggetto dell'operazione;**
- **la firma crittografica che garantisce della sicurezza e dell'autenticità dell'operazione.**

Una volta inserita in rete, nell'ambito di un "blocco", la singola transazione può essere conosciuta e verificata da tutti gli utenti del sistema; la transazione è così autorizzata e validata, divenendo "immutabile".

L'autenticazione e validazione non possono essere effettuate da chiunque; l'inserimento di un blocco di transazioni in una blockchain "passa" attraverso un processo di validazione e crittografazione ("impegnativo" sul piano informatico e computazionale, in quanto richiede una particolare capacità elaborativa) che viene effettuato (a fronte di una remunerazione) a mezzo di appositi algoritmi dai cd "miner".

Risolvendo un complesso problema matematico, il miner aggiunge un nuovo blocco alla catena, così che tutti i partecipanti sanno che è stata verificata la validità di tutte le sue transazioni.

Solo se tale processo è completato senza errori o anomalie il blocco entra a tutti gli effetti nella blockchain, divenendo conoscibile (e accettato) da tutti i "membri" del sistema. Sono i "miner" che "creano" ad. es. i bitcoin.

**.....CONTINUAMENTE NUOVE APPLICAZIONI
DELLA TECNOLOGIA BLOKCHAIN**

Tracciamento genere alimentari
dall'origine alla distribuzione finale

“Autenticazione” di opera artistiche
digitali, in tal modo rese “uniche”

Tutela del diritto di autore per le opere
multimediali

Le cripto valute

Bitcoin e criptovalute stanno alla blockchain come specie rispetto al genus.

Una criptovaluta è fruibile solo conoscendo un determinato codice informatico; non esiste in forma fisica, ma si genera e si scambia esclusivamente per via telematica.

Non è pertanto possibile trovare in circolazione dei bitcoin in formato cartaceo o metallico; le cripto valute non hanno corso legale e possono essere accettate come mezzo di pagamento solo su base volontaria; non sono regolate da enti centrali governativi; sono generalmente emesse e controllate dall'ente emittente secondo regole proprie, a cui i membri della comunità di riferimento accettano di aderire.

Il sito di CONSOB (www.consob.it) ha dedicato una sezione per specificare alcune delle caratteristiche delle monete virtuali, in particolare per chiarire se alle stesse possono essere riconosciute le funzioni di unità di conto, di mezzo di pagamento comunemente accettato e di deposito di valore.

Una valuta virtuale, o criptovaluta, è stata definita una rappresentazione digitale di valore decentralizzata basata sul peer-to-peer, su una blockchain condivisa il cui trasferimento è basato sulla crittografia e le cui regole di emissione sono basate su un algoritmo open source.

CARATTERISTICHE PECULIARI

- nell'insieme di regole (detto "protocollo"), cioè un codice informatico che specifica il modo in cui i partecipanti possono effettuare le transazioni;
- in un "libro mastro" (distributed ledger o blockchain) che conserva immutabilmente la storia delle transazioni; si tratta di un registro aperto e distribuito che può memorizzare le transazioni tra due parti in modo sicuro, verificabile e permanente. I partecipanti al sistema vengono definiti 'nodi' e sono connessi tra di loro in maniera distribuita.
- in una rete decentralizzata di partecipanti che aggiornano, conservano e consultano la distributed ledger delle transazioni, secondo le regole del protocollo.

Non esiste, di fatto, un'interpretazione condivisa o almeno maggioritaria sulla natura giuridica della criptovalute.

Moneta “atipica”, stante l'assenza di un soggetto terzo emittente, o genericamente di un mezzo di pagamento, di beni immateriali, di una versione in chiave digitale dell'istituto del baratto, di una commodity piuttosto che della “manifestazione” di un'obbligazione naturale. Verosimilmente, nessuna di tali categorie può essere ritenuta quella corretta.

Siamo come Darwin alle Galapagos: non poniamoci il problema di attribuire nomi nuovi ad animali mai visti prima.

Per CONSOB

«l'assenza di un quadro giuridico preciso determina l'impossibilità di attuare un'efficace tutela legale e/o contrattuale degli interessi degli utenti, che possono, pertanto, trovarsi esposti a dover subire ingenti perdite economiche, ad esempio in caso di condotte fraudolente, fallimento o cessazione di attività delle piattaforme on-line di scambio presso cui vengono custoditi i portafogli digitali personali (i cosiddetti e-wallets). In un contesto di assenza di obblighi informativi e di regole di trasparenza, le piattaforme di scambio sono altresì esposte a elevati rischi operativi e di sicurezza: esse, infatti, a differenza degli intermediari autorizzati, non sono tenute ad alcuna garanzia di qualità del servizio, né devono rispettare requisiti patrimoniali o procedure di controllo interno e gestione dei rischi, con conseguente elevata probabilità di frodi ed esposizione al cybercrime.»

Monete virtuali e riciclaggio

Le valute virtuali possono essere trasferite, memorizzate o scambiate elettronicamente. Per fare ciò, l'utente deve avere a disposizione un wallet, ossia un portafoglio digitale indispensabile per depositare le criptovalute nella propria disponibilità.

L'installazione su un dispositivo informatico di una app specifica genera un indirizzo, in questo caso un indirizzo bitcoin, che può essere condiviso e che può consentire il trasferimento di monete virtuali. Tale trasferimento viene protetto da una chiave privata, così garantendo che la transazione sia effettivamente stata disposta dalla persona titolare dell'indirizzo, e la sua immodificabilità.

Se i trasferimenti di bitcoin possono avvenire direttamente tra due soggetti che hanno la disponibilità di un wallet, rilievo deve essere riconosciuto anche ad altre figure del settore, ossia i cd “exchanger”. Prestatori di servizi chiamati ad assicurare il “cambio” tra valute virtuali e valute legali, che assumono il ruolo di “traghettatori” tra gli scambi economico finanziari tradizionali e il mondo delle criptovalute.

Attraverso gli interventi apportati al D. Lvo. n. 231/2007 dal D. Lvo. n. 90/17 prima e dal D. Lvo. n. 125/2019 in seguito che l’attenzione del legislatore si è soffermata sui punti d’ingresso e d’uscita dal circuito virtuale, attraverso il processo di conversione di valuta a corso legale in criptovaluta e viceversa.

L'acquisto e il trasferimento di bitcoin può indubbiamente costituire condotta funzionale **a garantire un "ostacolo" all'identificazione della provenienza delittuosa** di denaro o altre utilità di provenienza illecita: sia nei casi in cui le monete rappresentino strumenti di pagamento, sia ove assumano una valenza puramente "speculativa". In questa prospettiva, i bitcoin assumono almeno di fatto il ruolo di moneta (o di "rappresentazione" di un valore), anche se non ufficialmente riconosciuta; una "moneta" - non considerata di per sé illegale - la cui circolazione può essere tracciata e ricostruita con difficoltà non comparabili a quelle delle monete tradizionali.

Valute virtuali e disciplina antiriciclaggio il D. Lvo. n. 90/2017

Il legislatore nazionale ha anticipato, con il D. Lvo. n. 90/2017 (rubricato “Prevenzione dell’uso del sistema finanziario a scopo di riciclaggio e finanziamento al terrorismo” in vigore dal 4.7.2017) le proposte di modifica della IV Direttiva (2015/849 UE) confluite poi nella bozza della V direttiva, in tema di valute virtuali.

In generale, con il D. Lvo. n. 90/2017 i soggetti obbligati:

- - adottano misure di adeguata verifica della clientela proporzionali all’entità dei rischi di riciclaggio e di finanziamento del terrorismo;
- - devono dimostrare alle autorità competenti che le misure adottate sono adeguate al rischio rilevato;
- - devono provvedere all’obbligo di identificazione dei soggetti interessati.

Il legislatore si è reso conto delle criticità, rispetto a una piena efficacia del decreto, derivanti dal sostanziale anonimato delle cripto-valute e dalla conseguente inadeguatezza delle verifiche della clientela e dell'individuazione del titolare effettivo del conto wallet (art. 18 D. Lvo. n. 231/2007).

L'assenza di intermediari finanziari nelle cripto-valute può inoltre favorire operazioni di riciclaggio e di finanziamento al terrorismo, non essendo strutturalmente coinvolti quegli organismi che, nell'economia tradizionale, svolgono le funzioni di controllo e segnalazione di attività sospette alle autorità competenti.

Gli “exchanger” sono considerati soggetti destinatari delle normative antiriciclaggio di cui alla direttiva antiriciclaggio.

Non rientrano nella nuova regolamentazione tutte le transazioni che avvengono senza l’intermediazione degli exchanger e quelle derivanti da attività di mining, nonché quelle relative a exchanger non sottoposti alla normativa antiriciclaggio.

Il D. Lvo. n. 90/2017 ha introdotto due definizioni:

- **Valuta Virtuale** (art.1 cm 2 lett qq): “la rappresentazione digitale di valore, non emessa da una banca centrale o da un’autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l’acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente.”

- **Prestatori di servizi relativi all’utilizzo di valuta virtuale** (art.1 cm 2 lett ff): “ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali, all’utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione in valute aventi corso legale”; tali soggetti, ex art. 3 cm 5 lett. i, sono inseriti tra quelli obbligati agli adempimenti antiriciclaggio.

L'art.35 prevede che i soggetti obbligati - prima di compiere l'operazione - inviano una segnalazione all'UIF - senza ritardo - quando “sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento al terrorismo o che comunque i fondi provengano da attività criminosa. Il sospetto è desunto dalle caratteristiche, dall'entità, dalla natura delle operazioni, dal loro collegamento o frazionamento...in ragione delle funzioni esercitate, tenuto anche conto della capacità economica e dell'attività svolta dal soggetto a cui è riferita”.

Anche soggetti quali professionisti, intermediari finanziari, gli altri operatori non finanziari e i prestatori di servizi di gioco sono attratti agli obblighi antiriciclaggio relativi a valute virtuali.

Indicazioni tanto indirette quanto equivoche potenzialmente applicabili ai trasferimenti di bitcoin sono rilevabili dall'art. 24 del decreto (obblighi di adeguata verifica rafforzata della clientela), ove è previsto che “i soggetti obbligati tengono conto almeno dei seguenti fattori:....b) di rischio relativamente a prodotti, servizi, operazioni o canali di distribuzione quali:

- 2) prodotti o servizi che potrebbero favorire l'anonimato;
- 5) prodotti e pratiche commerciali di nuova generazione, compresi i meccanismi innovativi di distribuzione e l'uso di tecnologie innovative o in evoluzione per prodotti nuovi o preesistenti”.

Con il recepimento della Direttiva (UE) 2018/843 - c.d. V Direttiva - il legislatore è intervenuto sul testo del D. Lvo. n. 231/2007 (già modificato dal D. Lvo. n. 90/2017) delineando una nuova disciplina - tra l'altro - delle operazioni aventi ad oggetto le monete virtuali e degli obblighi dei soggetti che operano in tale settore.

La Quinta Direttiva europea antiriciclaggio (approvata dal Parlamento europeo il 19 aprile 2018), aggiorna la Direttiva (UE) 2015/849, aggiunge (cfr. articolo 2, paragrafo 1, punto 3) le nozioni di «prestatore di servizi di cambio tra valute virtuali e valute legali» e «prestatore di servizi di portafogli digitali», ed estende a tali categorie gli obblighi antiriciclaggio previsti per gli altri soggetti obbligati.

L'articolo 47, paragrafo 1, impegna gli Stati membri ad assicurare che i prestatori di servizi di cambio tra valute virtuali e valute legali, e i prestatori di servizi di portafoglio digitale siano registrati.

Il D. Lvo. n. 231/2007, all'art. 1, prevedeva già la figura dei **prestatori di servizi relativi all'utilizzo di valuta virtuale**: “ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale”.

Il D. Lvo. n. 125/2019 modifica la definizione di cui all'articolo 1, comma 2, lettera ff), **prestatori di servizi di portafoglio digitale** inserendo, dopo le parole «a titolo professionale,» l'indicazione: «**anche online,**» e aggiunge: “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**”.

UNA VICENDA EMBLEMATICA

Indagine avente ad oggetto una **società italiana che gestisce una piattaforma di scambio di criptovalute**; il responsabile della società sarebbe stato indagato per i reati di frode informatica, auto-riciclaggio e bancarotta fraudolenta- per un importo di ca 120 milioni di euro- in danno di oltre 230 mila risparmiatori; allo stesso sarebbe stata applicata la misura cautelare del divieto di esercitare attività d'impresa e di ricoprire uffici direttivi di imprese.

Risulterebbero documentate condotte fraudolente e distrattive in danno di investitori, su piattaforme informatiche e con l'uso di monete virtuali.

Tribunale di Firenze (sentenza n. 18/2019 del 21 gennaio 2019) aveva dichiarato il fallimento della società in oggetto, dalla quale risultava essere stato sottratto un rilevante importo di criptovaluta Nano (XRB).

Numerosi soggetti avevano “affidato” la propria criptovalute alla società menzionata, senza tuttavia che fosse predisposta una gestione “fisicamente” separata dei wallet dei singoli utenti. La valute sarebbero confluite in un unico wallet centrale, le cui chiavi private restavano nella esclusiva responsabilità del gestore della piattaforma. La criptovalute risultavano, pertanto, riferibili ai singoli utenti solo in forza di un dato contabile interno, ma concretamente “confuse” con quelle di pertinenza non solo ai vari clienti, quanto anche allo stesso gestore.

In questo modo le operazioni di scambio sulla piattaforma **non potevano essere gestite autonomamente dagli utenti**, quanto solo dal gestore, in base alle istruzioni ricevute da questi ultimi.

Il sistema della criptovaluta utilizzata **avrebbe processato più volte le medesime transazioni**, in quanto proprio la gestione tramite un unico wallet non avrebbe consentito di rilevare la sussistenza di un saldo preciso e specifico per i singoli utenti.

A nome di alcuni di questi sarebbero state inviate alla rete richieste multiple, in base alle quali si sarebbe progressivamente “svuotato” il patrimonio in criptovaluta della società. La verifica delle transazioni in uscita sarebbe stata effettuata dal **gestore con modalità non adeguate, mediante la sola consultazione del servizio esterno del sistema, senza che lo stesso fosse correttamente sincronizzato** come il nodo gestito direttamente dalla stessa piattaforma, di modo da evitare transazioni già eseguite su input di quest’ultima.

PROFILI PENALI (in corso di valutazione)

Le illecite sottrazioni di criptovaluta sarebbero state **consapevolmente non impedito dal gestore**, non avendo questi implementato la sicurezza della piattaforma con uno dei metodi disponibili resi noti dalla società creatrice della criptovaluta e non avendo informato del verificarsi di ammanchi la società che aveva creato la valuta, la community e gli user.

Omissioni che avrebbero consentito ai beneficiari delle operazioni di ottenere un profitto per complessivo di 11.500.000 XRB circa, pari a 120.000.000 di euro, danneggiando più di 230.000 persone in tutto il mondo.

Ravvisabili in astratto non solo reati fallimentari/
condotte di auto-riciclaggio consequenziali ai reati
che avrebbe determinato un illecito arricchimento,
ma in particolare in ipotesi **il delitto di frode
informatica.**

IPOSTESI 1

Una condotta di frode potrebbe essere ravvisabile laddove **risulti provato un accordo diretto tra il gestore della piattaforma e i beneficiari dei trasferimenti di criptovalute** non riconducibili a una corretta gestione del sistema; transazioni in tale caso realizzate approfittando di una criticità del programma e consentita dalla detenzione delle valute in un unico wallet, con conseguente ripartizione degli “utili” - tra beneficiari delle operazioni e gestore.

L'alterazione in qualsiasi modo del funzionamento di un sistema informatico o telematico finalizzata all'ottenimento di un ingiusto profitto con altrui danno potrebbe essere ravvisata in un **concorso tra il gestore e gli utenti beneficiari della transazioni**. L'alterazione si sostanzierebbe nella sistematica e intenzionale “confusione” tra le criptovalute dei singoli utenti, tale da impedire che transazioni superiori all'importo riferibile ai singoli possano essere rifiutate dal sistema.

IPOTESI 2

Anche senza un previo accordo criminoso, il successo (derivante dal numero e dall'entità delle transazioni) dell'attività trading su una piattaforma determina un significativo profitto derivante dalle "commissioni" correlate ai depositi e al trading.

Non impedire che tale meccanismo si arresti- anche dopo aver preso consapevolezza della sussistenza della progressiva insufficienza dei fondi per la copertura dei wallet personali delle migliaia di utenti della piattaforma- può essere condotta di per sé penalmente rilevante?

La risposta potrebbe essere positiva, ove si consideri che l'alterazione del funzionamento di un sistema può derivare anche del mancato adempimento di attività di organizzazione, controllo e verifica della funzionalità demandate al singolo gestore che con il sistema interagisce.

Un problema concreto: il sequestro delle monete virtuali

Non vi è un'autorità centrale che possa coadiuvare l'Autorità Giudiziaria e la Polizia Giudiziaria nell'esecuzione del sequestro; una situazione che determina potenziali criticità in relazione alla necessità di assicurare le dovute garanzie difensive, sia in relazione alla conservazione in termini giuridicamente inoppugnabili della fonte di prova.

Ogni operazione relativa al sequestro della criptovaluta sia opportunamente pianificata, ove possibile, ed effettuata da personale qualificato, ciò in quanto **il minimo errore potrebbe determinare la perdita della somma** (si pensi, ad esempio, alla digitazione di un indirizzo diverso da quello appena creato per completare il trasferimento della criptovaluta).

Le operazioni effettuate con le criptovalute, proprio per la mancanza di un ente centrale di governo e controllo, non sono annullabili.

PRIMA SITUAZIONE

Un soggetto viene trovato, ad es. durante una perquisizione, in possesso della chiave privata che lo abilita a movimentare una certa quantità di criptovaluta.

Accertata l'esistenza di un wallet e conoscendone la relativa chiave privata, ci si trova di fronte all'esigenza di sottrarre la disponibilità della criptovaluta al soggetto.

Questo potrà avvenire accedendo al wallet di quest'ultimo e spostando la somma verso un altro wallet creato ad hoc, dagli esecutori dell'attività investigativa. Nello specifico si dovrà valutare caso per caso l'opportunità di **creare il wallet più aderente alle necessità contingenti** quale ad esempio un wallet hardware "multi-signature" con un numero di chiavi (PIN) da distribuire a soggetti diversi che poi le deterranno.

A chi affidare le chiavi del wallet?

Al giudice, alla p.g., al consulente del P.M.co al curatore fallimentare? Indubbiamente, tali soggetti, prima o poi, dovranno intervenire per “trasferire” la somma, quantomeno per la restituzione all’avente diritto al termine della procedura.

Necessità di “distribuire” la responsabilità della gestione della somma sequestrata (in particolar modo quando si tratta di ingenti cifre) e minimizzare il rischio di un illecito accesso al wallet con conseguente distrazione della stessa.

... segue:

Qualora dovesse verificarsi la perdita/distruzione/malfunzionamento di questa tipologia di wallet, così come per ogni altro tipo di wallet, sarà sufficiente rigenerarlo a partire dai **seed** (i.e. l'elenco di parole non logicamente collegate necessarie alla generazione o rigenerazione di una coppia di chiavi privata/pubblica, indispensabili ad operare con le criptovalute) , che è opportuno siano conosciuti soltanto dai soggetti designati a detenere le chiavi di accesso.

SECONDA SITUAZIONE

Il soggetto dispone delle credenziali necessarie a operare su una piattaforma online dedita alla compravendita di criptovalute, pur non disponendo di un wallet.

Qualora l'A.G./P.G. sia a conoscenza delle predette credenziali agirà come nei casi di cui al punto precedente, non essendo sufficiente la garanzia data dal cambio password, che potrebbe essere facilmente aggirato dal soggetto, mediante procedura di recupero.

Se non è possibile accedere alla piattaforma con le credenziali del soggetto, bisognerà valutare dove questa abbia sede legale, potendola “aggredire” qualora sia radicata in Italia, o territorio raggiungibile da EIO o **rogatoria internazionale**, così come avviene con un tradizionale istituto di intermediazione finanziaria.

IN CASO DI SEQUESTRO PER EQUIVALENTE ?

Problemi operativi emergono nel caso in cui l'A.G. dispone il sequestro per equivalente di una data somma di denaro. Necessità di "apprensione" di beni - valuta tradizionale e criptovaluta - simili per finalità di utilizzo ma diversi per struttura e profili giuridici

ANALOGIA con sequestro di valute straniere: all'atto della scoperta del possesso di una quantità di criptovaluta da parte dell'indagato, effettuare un cambio, così come avviene per le valute straniere, che fissi in quel momento storico, in cui si esegue il provvedimento di sequestro per equivalente, la conversione della moneta virtuale o di una sufficiente parte di esso tale da soddisfare le esigenze di giustizia.

Le operazioni successive di consolidamento dell'attività svolta potranno essere quelle previste dall'ordinamento per il deposito di somme sequestrate su apposito libretto

GRAZIE A TUTTI

