L’evoluzione legislativa ed interpretativa in materia di tassazione di «Crypto-asset». Assestamenti giurisprudenziali, indicazioni di prassi e novità legislative.

Attività antiriciclaggio della Guardia di Finanza. Contrasto all’utilizzo illecito dei crypto-asset.

Ten. Col. Angelo ANCONA

COMANDANTE
NUCLEO di P.E.F.
GUARDIA DI FINANZA
MODENA

Missione istituzionale della Guardia di Finanza

Forza di polizia ad ordinamento militare dipendente dal Ministro dell'Economia e delle Finanze

POTERI

- Polizia tributaria
- Polizia economico-finanziaria
- Polizia valutaria
- Polizia giudiziaria
- Polizia amministrativa

d. lgs. N. 68|2001

legge n. 189|1959

COMPITI

Contrasto frodi fiscali ed economia sommersa Vigilanza sulla spesa pubblica Anti-contrabbando nel settore doganale e dei prodotti energetici	POLIZIA FINANZIARIA
Aggressione interessi economico-patrimoniali della criminalità organizzata ed al riciclaggio Tutela diritti di proprietà e dei consumatori Contrasto ai traffici illeciti Controllo economico del territorio e servizio di pubblica utilità 117	POLIZIA ECONOMICA
Concorso sicurezza ed ordine pubblico	CONCORSUALI
Polizia del Mare	IN VIA ESCLUSIVA

Dati sull'utilizzo dei crypto-asset per finalità illecite

Evoluzione sistema finanziario internazionale: «*FINTECH*» - *tecnologia applicata alla finanza*

Nel 2021 secondo CHAINALYSIS 14 mld di dollari in transazioni illegali di criptovalute, a fronte cmq di movimentazioni complessive del mercato pari a 15.000 mld di dollari

Anche secondo EUROPOL tale valore complessivo rappresenta ancora solo una quota limitata dell'economia criminale rispetto al contante e ad altre movimentazioni

Come vengono utilizzate criptovalute:

- **schemi riciclaggio sempre più complessi;**
- **mezzo di pagamento attività illecite;**
- **Sistemi di frode (c.d. SCAM).**

Da GEN 2020 ad APR 2022 pervenute al NSPV - tramite UIF - oltre 6.500 SS.OO.SS che presentano collegamenti con operazioni in *virtual asset* (su oltre 350.000 segnalazioni complessive), maggiormente provenienti da BANCHE

G.diF. e contrasto agli illeciti nel Mercato dei Capitali

NUCLEO SPECIALE POLIZIA VALUTARIA

ANALISI INVESTIGATIVA **SEGNALAZIONI DI OPERAZIONI SOSPETTE**

ANALISI INVESTIGATIVA INFORMATIVE PROVENIENTI DA **FIU ESTERE**

ISPEZIONI E CONTROLLI NEI CONFRONTI DEI SOGGETTI OBBLIGATI AI SENSI DELLA NORMATIVA ANTIRICICLAGGIO

INDAGINI DI POLIZIA GIUDIZIARIA SU TUTTO IL TERRITORIO NAZIONALE

Referente nazionale per finanziamento del terrorismo, falso monetario e tutela del risparmio, anche a supporto di Reparti del Corpo

RAPPORTI CON AUTORITÀ E ORGANISMI DI VIGILANZA

ELABORAZIONI **PROGETTI** E **ANALISI OPERATIVE DI RISCHIO** IN MATERIA AML/CFT

COOPERAZIONE INTERNAZIONALE **EUROPOL EMPACT 2022 - 2025**
(tra le diverse priorità 2022 - 2025 *..to target the criminal offenders orchestrating cyber-attacks, particularly those offering specialised criminal services online)*

+ Dlg.vo 186/2021 attuativo della DIRETTIVA UE 2019/1153 (Artt. 5-6-7)

La G.diF. opera a tutela del risparmio sotto un duplice profilo:

- **assicurando la tutela degli investitori;**
- **garantendo il corretto funzionamento del mercato capitali.**

GLI OBBLIGHI ANTIRICICLAGGIO

1. **obblighi di adeguata verifica del cliente e del titolare effettivo (artt. 17, 18 e 19 del D.Lgs. n. 231/2007).**
   (1) vi sia un sospetto di riciclaggio o di finanziamento del terrorismo;
   (2) in occasione dell'instaurazione di un rapporto continuativo, del conferimento di un incarico per l'esecuzione di una prestazione professionale;
   (3) in caso di effettuazione di un'operazione occasionale per un importo pari o superiore a 15.000 euro;
   (4) nell'ipotesi in cui venga disposto un trasferimento di fondi superiore a 1.000 euro.
2. **determinazione del titolare effettivo (artt. 20, 21 e 22 del D.Lgs. n. 231/2007);**
3. **obblighi di conservazione (artt. da 31 a 34 del D.Lgs. n. 231/2007);**
4. **obbligo di inoltro, all'Unità di Informazione Finanziaria, di segnalazioni per operazioni sospette (artt. da 35 a 41 del D.Lgs. n. 231/2007);**
5. **obbligo di inoltro all'U.I.F. delle nuove comunicazioni oggettive (art. 47 del D.Lgs. n. 231/2007)** (operazioni considerate a rischio di riciclaggio o di finanziamento del terrorismo sulla base di criteri oggettivi e quindi a prescindere dalla ricorrenza di elementi di sospetto da parte del soggetto obbligato)**.**

Sintesi quadro normativo di riferimento italiano

- **D.Lgs. 21 novembre 2007 n. 231** Decreto Antiriciclaggio (modificato ed integrato dai D.Lgs. 90 e 92 del 2017, e D.Lgs. 4 ottobre 2019, n. 125)
- **NOVITÀ:**
  - **Decreto del Ministero dell'Economia e delle Finanze del 13 gennaio 2022 (istitutivo della Sezione speciale del Registro O.A.M.)**
  - **ESTENSIONE DELL'OBBLIGO DI ADEGUATA VERIFICA AGLI OPERATORI NEL CAMPO DELLE MONETE VIRTUALI per PRESTATORI DI SERVIZI RELATIVI ALL'UTILIZZO DI VALUTA VIRTUALE e PRESTATORI DI SERVIZI DI PORTAFOGLIO DIGITALE**

GLI OBBLIGHI ANTIRICICLAGGIO

D.Lgs. 4 ottobre 2019, n. 125 - modifica ed integra D.Lgs. nn.rr. 90 e 92 del 2017 e 231/2007

Lett. *ff* - PRESTAZIONE DI SERVIZI RELATIVI ALL'UTILIZZO DI VALUTA VIRTUALE

- ***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.***

Lett. *ff-bis* PRESTATORE DI SERVIZI DI PORTAFOGLIO DIGITALE

- ***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.***

GLI OBBLIGHI ANTIRICICLAGGIO

Il Decreto del Ministro dell'Economia e delle Finanze del 13 gennaio 2022, infatti, ha istituito il Registro degli operatori in criptovaluta con specifici obblighi di registrazione e presenza in Italia per i soggetti esteri e di comunicazione alle autorità italiane.

L' art. 8 co. 1 D.Lgs. n. 90/2017 e l'art. 5 co. 2 D.Lgs. n. 125/2019 hanno esteso ai prestatori di servizi relativi all'utilizzo di valuta virtuale ed ai prestatori di servizi di portafoglio digitale le previsioni dell'art. 17 bis del D.Lgs. n. 141/2010 (cambiavalute):

1. **obbligo di iscrizione in una Sezione Speciale del Registro OAM (Organismo Agenti e Mediatori) che è operativa dal 18 maggio 2022 (ed entro i successivi 60 giorni chi già operava deve effettuare la comunicazione che sarà vagliata entro 15 giorni);**
2. **obbligo trasmissione delle negoziazioni effettuate all'OAM.**

Nella Sezione Speciale del Registro sono annotati i seguenti dati:

A. **il cognome e il nome del prestatore di servizi relativi all'utilizzo di valuta virtuale o del prestatore di servizi di portafoglio digitale persona fisica ovvero la denominazione sociale e la sede legale o la sede della stabile organizzazione nel territorio della repubblica in caso di soggetto diverso da persona fisica;**
B. **il codice fiscale ovvero la partita IVA, ove assegnato;**
C. **l'indicazione della tipologia di servizio prestato;**
D. **l'indirizzo dei punti fisici di operatività, ivi compresi gli eventuali sportelli automatici (ATM), e/o l'indirizzo web tramite il quale il servizio è svolto.**

GLI OBBLIGHI ANTIRICICLAGGIO

L'OAM collabora con i soggetti di cui all'art. 21, comma 2, lettera a) del D.Lgs. n. 231/2007 **(Ministero dell'Economia e delle Finanze, Autorità di vigilanza di settore, Unità di Informazione Finanziaria, Direzione Investigativa Antimafia, Guardia di Finanza attraverso il Nucleo Speciale Polizia Valutaria) e con la Direzione Nazionale Antimafia e Antiterrorismo** per agevolare l'esercizio dei rispettivi compiti istituzionali, fornendo, su richiesta, ogni informazione e documentazione detenuta in forza della gestione della Sezione Speciale del Registro, ivi compresi i dati trasmessi all'OAM.

I prestatori di servizi relativi all'utilizzo di valuta virtuale e i prestatori di servizi di portafoglio digitale trasmettono all'OAM per via telematica, con **cadenza trimestrale**, entro il giorno 15 del mese successivo al trimestre di riferimento, i dati relativi alle operazioni effettuate sul territorio della Repubblica Italiana. in particolare:

A. **i dati identificativi del cliente** (cognome e nome; luogo e data di nascita; residenza; codice fiscale/partita iva; estremi del documento di identificazione);
B. **i dati sintetici relativi all'operatività complessiva di ciascun prestatore di servizi relativi all'utilizzo di valute virtuali e prestatore di servizi di portafoglio digitale per singolo cliente alla data dell'ultimo giorno del trimestre di riferimento** (controvalore in euro del saldo totale delle valute legali e delle valute virtuali; numero e controvalore complessivo in euro delle operazioni di conversione da valuta legale a virtuale e da virtuale a legale; numero delle operazioni di conversione tra valute virtuali; numero delle operazioni di trasferimento di valuta virtuale in uscita e in ingresso da/verso il prestatore di servizi relativi all'utilizzo di valuta virtuale; numero e controvalore in euro dell'ammontare delle operazioni di trasferimento di valuta legale in uscita e in ingresso da/verso il prestatore di servizi relativi all'utilizzo di valuta virtuale suddivise per trasferimenti in contante e strumenti tracciabili).

L'OAM conserva i dati trasmessi per un periodo di **10 anni**.

GLI OBBLIGHI ANTIRICICLAGGIO

Al fine di interdire l'erogazione dei servizi relativi all'utilizzo di valuta virtuale da parte dei prestatori che non ottemperino all'obbligo di comunicazione, il **Nucleo Speciale di Polizia Valutaria della Guardia di Finanza e le Forze di Polizia** di cui all'art. 16 co. 1 della L. 121/1981, nell'esercizio delle proprie funzioni nell'ambito dei rispettivi comparti di specialità di cui all'art. 2 del D.Lgs. n. 177/2016, **possono 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, nonché i dati relativi alle operazioni effettuate.

Qualora il Nucleo Speciale di Polizia Valutaria ovvero il Reparto della Guardia di Finanza da esso interessato o le altre Forze di Polizia rilevino l'esercizio abusivo sul territorio della Repubblica Italiana di servizi relativi all'utilizzo di valuta virtuale e/o di servizi di portafoglio digitale, gli stessi accertano e contestano la violazione con le modalità e nei termini di cui alla **Legge n. 689/1981**.

Secondo l'art. 17 bis co. 8 bis del D.Lgs. n. 141/2010 è prevista una sanzione amministrativa da 2.065 a 10.329 euro emanata dal MEF.

SINTESI OBBLIGHI ANTIRICICLAGGIO OPERATORI CRYPTO

- creazione fascicolo cliente.
- adeguata verifica della clientela.
- verifica liste P.E.P. antiriciclaggio.
- valutazione e gestione del rischio di riciclaggio
- conservazione della documentazione antiriciclaggio.
- segnalazione di operazioni sospette.
- comunicazione di violazioni della limitazione del contante.
- adozione di procedure di controllo interno.
- formazione antiriciclaggio criptovalute e blockchain.

- **D.M. 13/01/2022 M.E.F. - ogni 3 mesi, entro 15 giorni di tempo** dal mese successivo al trimestre di riferimento, gli operatori, **trasmettono i dati delle operazioni** effettuate all'OAM, per via telematica, in particolare:
  - gli estremi identificativi di ogni cliente;
  - i dati sintetici sull'attività svolta nel complesso.
  - **OAM, a richiesta, può inoltrare tali informazioni agli attori AML (N.S.P.V., Direzione Nazionale Antimafia e Antiterrorismo ed altri).**

- **obbligo iscrizione** per operatori di servizi legati ad utilizzo valuta virtuale e servizi di portafoglio digitale, sia quelli già operanti, sia quelli che hanno intenzione di operare in Italia ed anche per i **WA**llet **S**ervice **P**roviders (servizi per conservazione, trasferimento e gestione attività connesse alle criptovalute).
- **iscritti rientrano negli obblighi antiriciclaggio previsti ai sensi del D.lgs. n. 231/2007**, includono raccolta e trasmissione delle informazioni sulle operazioni realizzate (inoltrate al MEF e alle Autorità Tributarie).
- costi per iscrizione: 500 € per persone fisiche - 8.300 € per persone giuridiche.
- esercizio abusivo punito con sanzione amministrativa da 2.065 € a 10.329 €.
- **al 19 ottobre 2022 vi sono 74 operatori iscritti.**

CRYPTOASSET e RISCHIO RICICLAGGIO

A fattor comune e con continuità temporale **GAFI/FATF, Autorità Bancaria Europea (EBA), EUROPOL/EU-EROJUST, Banca d'Italia, U.I.F. e Direzione Nazionale Antimafia e Antiterrorismo**, in atti e documenti, hanno individuato i seguenti **principali rischi**:

- in generale, per l'**integrità del sistema finanziario nel suo complesso**, sia per finalità di riciclaggio, finanziamento del terrorismo che per crimini finanziari perpetrati con e per mezzo di questo strumento;
- **pseudoanonimato connesso ai wallet** che, in molti casi, non identificano direttamente il possessore dello stesso, (soprattutto quelli non ufficialmente operanti in Italia).
- trasferimenti cd. ***peer-to-peer***, con transazioni dirette tra utenti che non si servono né di exchangers né di **WA**llet **S**ervice **P**roviders (obbligati agli adempimenti antiriciclaggio), mediante accesso alla rete internet e senza possibilità di tracciamento antiriciclaggio; **rischio aggravato da utilizzo di canali di comunicazione operanti in deep-web** o tra piattaforme web di soggetti terzi che operano come intermediari di fatto.

CRYPTOASSET e RISCHIO RICICLAGGIO

- **sommati ad altri fattori** quali:
  - **natura decentralizzata** del sistema delle criptovalute, mancanza di una vera e propria localizzazione fisica delle attività criminali poste in essere; in particolare spesso non si conosce dove siano localizzate le persone e/o le infrastrutture.
  - **difficoltà tecniche/pratiche** di prevenzione attività fraudolente e individuazione e sequestro/confisca dei cryptoassets;
  - possibilità che le **transazioni** non avvengano solo tra soggetti residenti in Stati diversi, ma anche **da/verso una pluralità di account** che, in realtà, fanno riferimento alla medesima persona (unico utente titolare di più account/wallet contemporaneamente, ma anche altri mix di soluzioni *creative*);
  - **esistenza di espedienti** che consentono un crescente grado di anonimato - **servizi dei cc.dd. *mixers* e *tumblers*** (sistemi mediante i quali la transazione non è ricondotta all'account del soggetto agente, ma viene spezzettata tra una molteplicità di account, celando in via di fatto i due soggetti di riferimento tra i quali avviene lo scambio di criptovalute).

LE TECNICHE INVESTIGATIVE

Un tipico schema di riciclaggio di denaro sporco (*il cd. modello trifasico*)

Accumulazione di denaro sporco

PLACEMENT

Il denaro sporco viene integrato nel sistema finanziario

LAYERING

Trasferimento sul conto bancario della compagnia "x"

Bonifico

Banca Estera

Prestito alla compagnia "y"

Pagamento da "y" di fatture false alla compagnia "x"

Acquisto di beni di lusso

Investimenti finanziari

Investimenti commerciali/industriali

INTEGRATION

LE TECNICHE INVESTIGATIVE

Andando ad analizzare le varie fasi attraverso le quali si configura un'operazione di riciclaggio, si può comprendere come le valute virtuali rappresentino oggi un'opportunità straordinaria per chi voglia reinvestire capitali di provenienza illecita, offrendo una serie di alternative ai metodi tradizionali.

Le modalità con le quali possono essere attuate le tre fasi tipiche di un'operazione riciclatoria sono le seguenti:

1. Nella fase di **COLLOCAMENTO**, un criminale in possesso di denaro contante provento di reato può, con estrema facilità, utilizzare i servizi di *LocalBitcoin Exchanges* per scambiare le banconote con la criptovaluta. In questo caso, per la negoziazione, all'acquirente di moneta virtuale non viene richiesta alcuna informazione circa la propria identità, in quanto chi vende non è tenuto ad effettuare alcuna verifica.

LE TECNICHE INVESTIGATIVE

2. Nella fase successiva, quella di **STRATIFICAZIONE**, in cui bisogna dividere le somme illecitamente accumulate, è possibile dar vita a diversi *account* di criptovaluta, frazionare l'ammontare originale in tante piccole parti e confondere così la tracciabilità delle transazioni. Gli spostamenti da un *account* all'altro, uniti al mantenimento dell'anonimato, sono in grado di cancellare le prove della provenienza illecita del denaro. Per ogni scambio di moneta virtuale tra gli utenti, infatti, vi è un passaggio tra indirizzi *wallet* diversi. Per lo svolgimento di queste operazioni, spesso le organizzazioni criminali utilizzano i c.d. *money mule*, cioè soggetti reclutati per fungere da intermediari nelle fasi del riciclaggio di denaro. Questi non devono far altro che trasferire le somme di denaro ricevute a soggetti terzi ottenendo una percentuale sull'importo trasferito. Sovente, le persone che si prestano a effettuare tali operazioni non sono neanche consapevoli che il denaro trasferito rappresenta il frutto di un illecito, ma svolgono, ciononostante, un ruolo cruciale nel processo di riciclaggio.

3. Nell'ultima fase, cioè quella di **INTEGRAZIONE**, il riciclatore potrebbe mantenere i guadagni illeciti sotto forma di moneta da investire in future transazioni, anche mediante la creazione di siti o compagnie di facciata *online*.
   Uno dei casi più frequenti, infatti, consiste nella realizzazione di società di *e-commerce* in grado di offrire servizi o commerciare beni in maniera fraudolenta e non.
   Un altro metodo utilizzato, altrimenti, consiste nell'aprire, acquistando in criptovaluta, siti legittimi di gioco d'azzardo *online* usando, per il trasferimento dei fondi, false identità o prestanome. In questa maniera, dopo aver investito la moneta virtuale, il ricavato del sito di gioco d'azzardo appare totalmente legittimo.
   Un'ulteriore pratica diffusa in questa fase è quella di incassare, ponendo in essere più operazioni frazionate, denaro contante presso i servizi dove erano stati originariamente scambiati contanti per monete virtuali.

LE TECNICHE INVESTIGATIVE

È plausibile ritenere che, rispetto gli obiettivi investigativi, il sistema bitcoin e i suoi derivati possano offrire un duplice vantaggio tenuto conto che:

a. il **registro delle transazioni** sottostante (cryptoledger) è **pubblico e immutabile**, quindi, "idoneo" allo svolgimento di attività investigative;
b. è possibile eseguire approfondimenti e attività di intelligence sulle transazioni pubblicate nel registro secondo la tecnica "***follow the money***".

Diversi possono essere gli scopi delle investigazioni in ambito bitcoin:

1. **l'identificazione degli indagati;**
2. **l'acquisizione di fonti di prova circa le movimentazioni di bitcoin e la riconducibilità a soggetti specifici;**
3. **il sequestro dei bitcoin.**

Normalmente, ad inizio investigazione, può essere conosciuto l'indirizzo bitcoin che viene generalmente fornito alla vittima per potervi depositare i fondi, in caso di estorsione o truffe.

L'informazione potrà essere "sfruttata" dagli operatori per proseguire le attività d'indagine, mediante l'impiego di specifici tools per:

a. interrogare la *blockchain* selettivamente;
b. svolgere attività di "*follow the money*";
c. sistemi di tracciamento bitcoin.

LE TECNICHE INVESTIGATIVE

La moneta *bitcoin* non è completamente anonima ma **pseudo-anonima**. Questo vuol dire che pur non avendo una connessione tra identità reale dell'autore del misfatto e indirizzo/chiave pubblica che ha ricevuto il pagamento, è possibile esaminare la *blockchain* dove tutte le transazioni sono memorizzate in maniera indelebile ed individuare e seguire lo spostamento di bitcoin in questa ragnatela di collegamenti.

Quindi, anche se non è possibile risalire (direttamente) all'identità della persona le operazioni di *forensics* riescono a **tracciare i pagamenti *bitcoin***.
Per certi aspetti è possibile tracciare l'operazione finanziaria in modo più agevole rispetto alle transazioni bancarie (che richiedono un decreto della magistratura) ancor più complesso se l'operazione bancaria è eseguita da banche ubicate in stati c.d. "canaglia" e/o a scarsa collaborazione giudiziaria/amministrativa.
L'attività è quindi quella di individuare le transazioni oggetto dell'illecito ed esaminarle; cercare di aggregare indirizzi e capire quali indirizzi appartengono alla stessa persona e quali invece rappresentano magari degli *exchange server* dove l'utente ha una identità e dove è possibile indagare e chiedere informazioni.

LE TECNICHE INVESTIGATIVE

Nel caso di indagini in materia di criptovalute, le indagini tecniche da porre in essere sono di tipo tradizionale (su pc, *smartphone*, *tablet*, ecc), effettuate in locale da eseguirsi successivamente al sequestro dei dispositivi.

In primo luogo, in fase di perquisizione è di fondamentale rilevanza la ricerca delle **chiavi private**, consistenti in una stringa alfanumerica e in un corrispondente QR code (*paper wallet*), nonché i **dati di *login* alla piattaforma di *exchange*** o ***wallet* fisici** che possono assumere diverse forme.

LE TECNICHE INVESTIGATIVE

Inoltre ricercheremo **i *software* o le *app*** utilizzati per la gestione delle criptovalute e le **carte di credito** che consentono direttamente la spesa di criptovalute con conversione contestuale in valuta sovrana.

coinbase

bitpanda

BINANCE

kraken

SpectroCoin

LE TECNICHE INVESTIGATIVE

Come eseguire concretamente il **sequestro**, ovvero come spostare le monete virtuali da sequestrare, sottraendole alla disponibilità dell'indagato per porle a disposizione dell'Autorità Giudiziaria?

Nel caso in cui la parte decida di non collaborare, per riuscire ad avere accesso alla valuta sequestrata, incontrando ***wallet hardware* o *software***, la migliore strategia è quella di cercare un ***backup*** del *wallet*. In tal modo, anche se l'istanza del *wallet* utilizzata dalla parte dovesse essere protetta da parole chiave o crittografia, sarà possibile ripristinarne una nuova, con accesso alle medesime monete virtuali e con la possibilità di disporne senza limitazioni.

Per quanto riguarda i ***wallet online***, sarà innanzitutto necessario entrare in possesso delle **credenziali di accesso**, che solitamente si sostanziano in un indirizzo di posta elettronica ed una *password*. Successivamente bisognerà tenere presente che molti *wallet* di questo tipo prevedono obbligatoriamente **tecniche di autenticazione a due fattori**, quali, a titolo esemplificativo, l'inserimento di un codice inviato via SMS per effettuare l'accesso, la richiesta di cliccare su un link inviato all'indirizzo di posta elettronica abbinato all'*account*, oppure l'inserimento di un codice generato casualmente da apposite applicazioni per *smartphone* come *google authenticator*.

LE TECNICHE INVESTIGATIVE

Per procedere alla materiale esecuzione del sequestro (cautela della criptovaluta e del relativo *wallet*), occorre **generare un nuovo indirizzo/stringa ed una nuova chiave privata** al fine di trasferire la disponibilità di criptovaluta dall'indagato all'A.G..

La chiave pubblica e la chiave privata dell'indirizzo generati *ex novo* e contenenti le disponibilità trasferite, saranno custoditi in busta chiusa e suggellata a disposizione dell'Autorità Giudiziaria (*paper wallet*).

In ogni caso, in presenza della chiave privata, la valuta virtuale potrà eventualmente essere cambiata in valuta corrente secondo le indicazioni della Procura competente.

Al riguardo meglio procedere alla generazione degli stessi in modalità offline. Per questo sono disponibili diversi strumenti, tra i quali: bitcoin tool; vanitygen; paper crypto wallet generator offline.

LE TECNICHE INVESTIGATIVE

Significativa la *best practice* emersa dall'attività coordinata dall'A.G. di Firenze.

L'attività d'indagine ha riguardato l'ammanco di un ingente quantitativo di valuta virtuale (equivalenti a circa 160 milioni di euro) da portafogli elettronici (relativi a 57 mila utenze) gestiti da una società specializzata in *trade* di criptovalute con sede in Italia e dell'ulteriore fase di fallimento della stessa.

Il Tribunale di Firenze nel mese di maggio 2018 ha emesso la misura cautelare del sequestro preventivo di bitcoin per un valore di circa 15 milioni di euro rilevando "*il pericolo di depauperamento del patrimonio della fallenda e la possibile dispersione dei mezzi di prova per l'accertamento delle cause e delle responsabilità alla base dell'ammanco*".

L'attività di sequestro è stata perfezionata **con la creazione di un *wallet* (portafoglio elettronico) nella disponibilità esclusiva del Tribunale** sul quale sono confluite, senza rischio di dispersione, le criptovalute. Per custodirne le relative chiavi elettroniche crittografate (pubblica e privata) sono state cautelate onde evitare l'indebita appropriazione da parte di terzi.

LE TECNICHE INVESTIGATIVE

Più controversa appare, infine, la questione di **come trattare le monete virtuali sequestrate**.
Si premette che la Polizia Giudiziaria, come pure il Pubblico Ministero, non possono procedere alla conversione delle monete virtuali in denaro contante, se non a seguito di **esplicito provvedimento del Giudice**, anche in considerazione del fatto che l'art. 183-quater delle disposizioni di attuazione del c.p.p., al comma 3, prevede che:
"*L'Autorità Giudiziaria competente ad amministrare i beni sequestrati è il **Giudice** che ha disposto il sequestro ovvero, se organo collegiale, il Giudice delegato nominato dal collegio stesso. l'opposizione ai provvedimenti adottati, ove consentita, è presentata, nelle forme dell'articolo 666 del codice, allo stesso giudice ovvero, nel caso di provvedimento del giudice delegato, al collegio*".
Il Giudice, in tal caso, laddove ritenga che la **volatilità** delle criptovalute in sequestro sia talmente elevata da comprometterne il valore, potrà procedere ai sensi dell'art. 260, comma 3, del c.p.p. il quale dispone che "*se si tratta di cose che possono alterarsi, l'Autorità Giudiziaria ne ordina, secondo i casi, l'alienazione o la distruzione*".
La Suprema Corte (con sentenza n. 1916 del 16/01/2017), infatti, ha chiarito che "*ai fini della alienazione di cose in sequestro che possono alterarsi (art. 260, comma 3, c.p.p.) rileva anche il progressivo intrinseco deprezzamento del bene in ragione del trascorrere del tempo; ne consegue che è legittima la vendita di una autovettura, oggetto di sequestro per equivalente, in quanto funzionale alla ottimizzazione della fruttuosità della misura ablatoria*".
In definitiva, la Polizia Giudiziaria, in caso di sequestro di criptovalute, dovrebbe fornire all'Autorità Giudiziaria tutti gli elementi conoscitivi opportuni al fine dell'adozione di un provvedimento di conversione in denaro contante delle valute virtuali.

LE TECNICHE INVESTIGATIVE

Per monetizzare le criptomonete sequestrate la soluzione migliore rilasciata dalla prassi operativa è quella dell'esecuzione di **un'asta giudiziaria**.

In tal modo, si può ottenere valuta a corso legale in cambio di criptomonete, senza avvalersi di terzi intermediari (*exchanger*).

L'U.S. Marshall Service, ad esempio, ha messo all'asta oltre 4.000 bitcoin derivanti da diverse operazioni realizzate da varie agenzie tra cui la DEA e la medesima soluzione è stata adottata anche da forze dell'ordine europee.

LE TECNICHE INVESTIGATIVE

1. il sequestro è effettuabile solo se gli investigatori entrano in possesso della c.d. chiave privata;
2. il sequestro va eseguito mediante la creazione di una transazione finanziaria apposita;
3. la transazione deve essere realizzata con rapidità per evitare che l'indagato o terzi, venendo a conoscenza del possesso della chiave privata da parte della Polizia Giudiziaria, possano ostacolare il sequestro;
4. prima di procedere alla transazione, va in ogni caso predisposto uno specifico ambiente di lavoro e va utilizzata una pre-individuata tipologia di *wallet*, principalmente il *paper wallet*, per la generazione di una nuova chiave privata (da gestire a cura della Polizia Giudiziaria);
5. la transazione di sequestro comporta comunque una diminuzione del valore della valuta iniziale, per effetto dell'intermediazione di più soggetti (*miners, exchanger, wallet provider, ecc.*);
6. la nuova chiave privata (della Polizia Giudiziaria) va custodita in busta chiusa - oscurata e sigillata - e concentrata nell'Ufficio Corpi di Reato della Procura della Repubblica competente ovvero, in alternativa, nel magazzino reperti dell'Organo di polizia procedente;
7. al termine delle operazioni, l'ambiente di lavoro informatico deve essere rimesso in sicurezza per evitare di lasciare traccia della chiave privata in possesso della Polizia Giudiziaria;
8. per trasformare la valuta virtuale sequestrata in valuta avente corso legale (anche in caso di successiva confisca) è necessario procedere ad una seconda transazione finanziaria, che comporterà un'ulteriore diminuzione del valore iniziale della valuta sequestrata. Successivamente, si procederà al versamento della valuta convertita sul Fondo Unico Giustizia;
9. nel caso in cui non fosse possibile procedere alla trasformazione della valuta virtuale sequestrata in valuta avente corso legale, bisogna considerare che la prima ha carattere di volatilità e, con il trascorrere del tempo, subisce oscillazioni - positive o negative - non prevedibili.

Grazie per l'attenzione

Ten. Col. Angelo ANCONA