

Criptovalute e Criminalità organizzata

di Vittorio Guarriello,

Sostituto Procuratore della Repubblica presso il Tribunale di Campobasso

(Relazione alla base dell'intervento tenuto in occasione dell'evento "*Talk About Mafia*", organizzato dall'Associazione Nazionale Magistrati, svoltosi a Reggio Calabria il 5 giugno 2026).

SOMMARIO: 1. Definizione di Criptovalute. – 2. La tecnologia "*blockchain*". – 3. Criptovalute e criminalità organizzata. – 4. Proposte e soluzioni.

1. Definizione di Criptovalute.

Con il termine criptovalute si intendono valute virtuali, ossia rappresentazioni digitali di valore, decentralizzate, basate sulla crittografia e su registri condivisi.

Più nel dettaglio, esse non sono emesse da uno Stato o da una Banca Centrale e – nella gran parte dei casi – il loro valore è svincolato da quello di una valuta avente corso legale in uno Stato ed è, invece, basato sulla fiducia tra i soggetti privati e sulle dinamiche relative all'interrelazione tra domanda ed offerta.

In particolare, il loro funzionamento si basa sull'utilizzo di chiavi crittografiche asimmetriche¹: la chiave pubblica, simile a un codice IBAN, rappresenta l'indirizzo di ricezione delle criptovalute. Invece, la chiave privata funziona come una sorta di *password* (o PIN di un bancomat) e serve ad autorizzare il trasferimento di fondi.

La gestione delle criptovalute da parte degli utenti avviene, solitamente, mediante portafogli virtuali denominati "*e-wallet*".

Giova precisare che le criptovalute possono essere scambiate, qualora i partecipanti alla relativa transazione vi acconsentano, direttamente tra due dispositivi in modalità *peer to peer* senza necessità di intermediari, al fine dell'acquisto di beni e servizi (come se fossero una vera e propria moneta avente corso legale).

¹ Ossia una coppia di chiavi matematicamente collegate, quella pubblica utilizzata per cifrare i dati e quella privata per decifrarli.

Tuttavia, esse possono essere anche convertite in valute aventi corso legale. Sotto questo profilo, si suole distinguere tra criptovaluta “unidirezionale” (che non può essere scambiata con valute aventi corso legale) e “bidirezionale” (che, invece, può esserlo).

Il *Bitcoin*, ad esempio, è una moneta virtuale “bidirezionale”, in quanto è suscettibile di essere convertita con facilità in valute aventi corso legale e viceversa.

Alcuni Stati, come l’Uruguay, hanno deciso di sperimentare l’utilizzo di monete virtuali sotto il proprio controllo (*e-peso*).

La prima criptovaluta ad essere stata creata, e la più diffusa a livello mondiale, è il *Bitcoin*, implementata nel 2009 da un misterioso inventore (o gruppo di sviluppatori) noto sotto lo pseudonimo di Satoshi Nakamoto.

Altra criptovaluta estremamente diffusa a livello mondiale è “*Ethereum*”, utilizzata principalmente per la creazione e pubblicazione *peer to peer* di “*smart contract*”² e “*Monero*”, nota per l’utilizzo della crittografia al fine di nascondere gli indirizzi di invio, di ricezione e l’ammontare della transazione.

Sotto il profilo della definizione legislativa, inizialmente le criptovalute venivano definite dal decreto legislativo n. 90/2017, in materia di antiriciclaggio, che definiva le criptovalute come “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 o trasferita e archiviata elettronicamente, e che può essere utilizzata a scopo di investimento”.

Invece, più di recente, è stato approvato dal Consiglio dell’Unione Europea il regolamento del 16 maggio 2023 in materia di cripto-attività, che vengono definite come “rappresentazioni digitali di valore o di diritti”.

Da tale ultima definizione, si evince come il legislatore sovranazionale abbia inteso prendere in considerazione, a differenza della definizione di cui al citato decreto legislativo, l’attitudine delle criptovalute a poter essere utilizzate non solo come mezzo di scambio, ma anche come rappresentazione di diritti.

In particolare, tale ultimo aspetto appare particolarmente pertinente rispetto al fenomeno dei *Non Fungible Token (NFT)*, ossia una tipologia di *token*³, che rappresenta un vero e proprio certificato di proprietà digitale su un’opera d’arte.

² Con il termine *smart contract* vengono definiti i contratti digitali memorizzati su una *blockchain*, suscettibili di essere eseguiti automaticamente quando vengono soddisfatti termini e condizioni prestabiliti.

³ Con il termine *token* vengono definiti una sorta di “gettoni digitali”, che possono essere utilizzati per accedere ad un bene o a un servizio o per acquistarlo o venderlo.

2. La tecnologia “*blockchain*”.

Come anticipato, il principio fondamentale su cui è basato il funzionamento delle criptovalute è la c.d. decentralizzazione, ossia l’assenza di un ente centrale che si occupa dell’emissione di valute e della gestione delle transazioni.

Ebbene, ai fini della validazione delle transazioni le criptovalute si basano sulla c.d. tecnologia “*blockchain*”, la più famosa delle quali è quella del *Bitcoin*.

Esse appartengono alla più ampia categoria delle D.L.T. (*Distributed Ledger Technologies*), ossia dei registri elettronici condivisi tra i singoli partecipanti – denominati, in gergo, “nodi” –, su cui possono essere memorizzate transazioni aventi le caratteristiche della verificabilità e dell’immutabilità.

L’inserimento di nuove informazioni non prevede la validazione da parte di un ente centrale di controllo, ma, invece, il raggiungimento di un accordo tra i partecipanti alla rete, tramite i c.d. meccanismi di consenso.

La peculiarità della *blockchain* consiste in una lista di *record*, che viene continuamente implementata con ogni nuovo inserimento, a loro volta inseriti in “blocchi”.

Ciascun blocco contiene, oltre ai dati, un *hash*⁴ crittografico del blocco precedente. Pertanto, i dati in un blocco sono per loro natura immutabili (atteso che per alterare retroattivamente uno di essi servirebbe il consenso della maggioranza della rete), poiché tutti i nodi della rete memorizzano tutti i blocchi e quindi tutta la Blockchain.

Tale tecnologia, che serve ad evitare il fenomeno del c.d. “*double spending*”, ossia che un soggetto spenda due volte la medesima valuta, risulta estremamente utile, come si vedrà, anche dal punto di vista investigativo.

3. Criptovalute e criminalità organizzata.

Come è noto, lo scopo di qualsiasi forma di criminalità organizzata di stampo mafioso è l’accumulazione di ricchezza ed il suo reinvestimento nell’economia legale, al fine di aumentare il proprio consenso sociale.

Pertanto, qualsivoglia strumento che consenta di reinvestire le ricchezze illecitamente accumulate nel circuito economico viene sfruttata dai sodalizi criminali.

In particolare, per quanto attiene alle criptovalute, le mafie hanno saputo sfruttare le potenzialità offerte dalle stesse in termini di anonimato e di rapidità dei trasferimenti, anche transnazionali, di denaro.

⁴ Con il termine *hash* si definisce una stringa alfanumerica generata da un algoritmo matematico. Esso funziona come un’*impronta digitale* univoca per qualsiasi file o dato: se viene modificato anche un singolo carattere, il codice *hash* cambierà.

Giova precisare che le criptovalute sono connotate da caratteristiche di pseudoanonimato, ma non di totale anonimato, nel senso che ogni transazione è registrata in un registro pubblico (la blockchain o le altre forme di D.L.T.) e può essere visualizzata da chiunque.

Le transazioni sono collegate a indirizzi di portafoglio, non a identità personali.

Tuttavia, risulta possibile collegare le transazioni agli effettivi autori, ad esempio mediante servizi di *exchange* che richiedono agli utenti la verifica dell'identità.

Una tra le tecniche maggiormente utilizzate dai *cybercriminali* al fine di rendere non rintracciabili le transazioni in criptovalute è il *mixing*, che funziona mescolando i fondi provenienti da più utenti, al fine di rendere non identificabili gli autori delle transazioni.

Tuttavia, anche tale tecnica non risulta essere totalmente sicura, in quanto i *mixer* (servizi di *mixing*) potrebbero detenere registri delle transazioni dai quali è possibile risalire all'identità dei loro autori.

Per tale ragione, è stata elaborata un'ulteriore tecnica maggiormente complessa, nota come “*chain-hopping*”, finalizzata proprio ad eludere le indagini sulla *blockchain*.

Segnatamente, essa consiste nel trasferire rapidamente i fondi tra diverse criptovalute su *blockchain* differenti, utilizzando servizi noti come “*blockchain bridges*”⁵.

Infine, deve rilevarsi che l'utilizzo delle criptovalute risulta essere estremamente diffuso nella *darknet*, ossia in quella parte di internet nascosta e accessibile unicamente mediante *software* specifici (come TOR o I2P), per acquistare prodotti e servizi disponibili nei c.d. “*hidden service*”, ossia in quei portali nei quali viene venduto materiale illegale (sostanze stupefacenti, armi, materiale pedopornografico) o è possibile commissionare delitti⁶.

L'importanza delle nuove tecnologie per la criminalità organizzata è attestata anche da varie operazioni di Polizia Giudiziaria, che hanno consentito di intercettare conversazioni telefoniche nell'ambito delle quali gli indagati ne parlavano.

Già nel mese di novembre 2018, nell'ambito dell'operazione denominata “Galassia”, coordinata dalle Direzioni Distrettuali Antimafia di Bari, Catania e Reggio Calabria, uno degli intercettati, ritenuto dagli inquirenti contiguo alla criminalità organizzata di tipo mafioso, diceva esplicitamente: “*Io cerco i nuovi adepti nelle migliori università mondiali, tu vai ancora alla ricerca di quattro scemi in mezzo alla strada che vanno a fare così «bam, bam!».* Io cerco quelli che fanno così «*pin, pin!*», che cliccano”, sottolineando, così, l'importanza di avvalersi di soggetti in grado di adoperare le nuove tecnologie.

Successivamente, nel mese di febbraio 2019, nei comuni di Santa Maria Capua Vetere e San Prisco (in provincia di Caserta), i Carabinieri della Compagnia di Santa Maria Capua Vetere hanno dato esecuzione

⁵ R. PATALANO, *Bit-mafie: criptovalute e riciclaggio* in AA.VV. *Modelli di cybersecurity e prevenzione dei cyber crimes Aporie della legislazione vigente, problematiche applicative e prospettive de iure condendo*, Università degli Studi di Napoli Federico II, 2025, pp. 165 e ss.

⁶ I. GABRIELLI, F. TAVERNA, *Criptovalute ed attività investigativa* in AA.VV. *Investigare 5.0*, Piccin Editore, 2024, pp. 419 e ss.

ad un'ordinanza di custodia cautelare, emessa dal Giudice per le indagini preliminari presso il Tribunale ordinario di Napoli, su richiesta della locale Direzione distrettuale antimafia, nei confronti di cinque persone (tre delle quali sottoposte alla custodia cautelare in carcere e due ristrette agli arresti domiciliari), gravemente indiziate, a vario titolo, dei reati di associazione per delinquere finalizzata al traffico illecito di sostanze stupefacenti del tipo marijuana e hashish e detenzione ai fini di spaccio e spaccio di stupefacenti in concorso (artt. 74 e 73 del D.P.R. n. 309/1990, artt. 81 cpv. e 110 c.p.).

L'esecuzione della misura cautelare costituiva l'esito di un'articolata attività investigativa, inizialmente coordinata dalla Procura della Repubblica presso il Tribunale di Santa Maria Capua Vetere e, successivamente, attesa la sussistenza di un reato associativo ricompreso tra quelli enumerati dall'art. 51, comma 3-*bis*, c.p.p., dalla Direzione Distrettuale Antimafia di Napoli.

Le indagini espletate a monte del provvedimento giudiziario – tra la fine del 2015 e la fine del 2018 – hanno fornito agli inquirenti lo spaccato di una tragica realtà di giovani e giovanissimi pusher, diretti ed organizzati da un “capo”, il quale interagiva con i propri sodali e con gli acquirenti di sostanze stupefacenti anche mediante un sistema informatico di messaggistica criptato – denominato “*Surespol*”⁷ – e provvedeva, in parte, all'approvvigionamento di stupefacenti (in particolare, di marijuana), attraverso il servizio postale, formalizzando via internet⁸ gli accordi con i fornitori e pagando gli stessi in moneta virtuale di tipo *bitcoin*, acquistata preventivamente con carte di credito.

Le suesposte modalità operative del sodalizio criminoso sono emerse da un'intensa attività di riscontro – espletata attraverso intercettazioni telefoniche e assunzione di dichiarazioni dei consumatori di sostanze stupefacenti del tipo hashish e marijuana –, che ha consentito di appurare l'esistenza e l'operatività di un'associazione a delinquere composta da undici giovani, sei dei quali minorenni all'epoca dei fatti. I membri del gruppo criminale dediti allo spaccio di sostanze stupefacenti operavano prevalentemente nei pressi dei luoghi di aggregazione dei loro coetanei, in particolare nei pressi delle ville comunali e all'esterno degli istituti scolastici della zona, mentre il loro capo-promotore individuava per sé e per i propri sodali compiti ben precisi nell'approvvigionamento, confezionamento e spaccio delle suddette sostanze, prendendone nota in agende e quaderni.

Tale documentazione dattiloscritta e manoscritta – recante i nominativi dei clienti, l'indicazione delle somme di denaro e dei metodi di pagamento online, rinvenuta nel corso di una perquisizione eseguita presso la sua abitazione – è risultata estremamente utile ai fini della ricostruzione del *modus operandi* dell'organizzazione criminale e a comprovare l'evidente radicamento sul territorio della stessa.

⁷ Dall'analisi della documentazione rinvenuta, è emerso che il capo del sodalizio criminale, a mo' di promemoria, indicava ai propri correi di «installare Surespol», associando al nominativo di ognuno di essi una combinazione alfanumerica (es. M4, M5 ecc.), al fine di evitare la corretta identificazione dell'utilizzatore dell'applicativo

⁸ Nelle more dell'attività d'intercettazione telefonica, emergevano contatti intercorrenti tra il capo del sodalizio e un soggetto, presumibilmente residente in Torino.

L'opera degli inquirenti ha così disvelato un articolato scenario criminale, nell'ambito del quale i soggetti poi attinti dalle misure restrittive sfruttavano le chat crittografate e l'anonimato garantito dall'utilizzo delle criptovalute al fine di perpetrare gravissimi reati in danno della salute pubblica e, in particolare, quella delle nuove generazioni⁹.

Ancora, nell'ambito dell'operazione denominata "Aspromonte Emiliano", condotta dalla Direzione Distrettuale Antimafia di Bologna, è stata intercettata una conversazione telefonica nella quale un appartenente ad una cosca di 'ndrangheta si mostrava interessato all'acquisto di una piattaforma di *bitcoin* localizzata a Panama, al fine di spostare in sicurezza tale criptovaluta.

4. Proposte e soluzioni.

Alla luce di quanto esposto nei precedenti paragrafi, appare evidente che al fine di contrastare l'utilizzo delle valute virtuali da parte della criminalità organizzata allo scopo di riciclare i proventi delle attività illecite, l'aspetto su cui è necessario che intervengano sia il legislatore sia le Autorità istituzionalmente deputate al contrasto di tali fenomeni è l'identificazione degli autori delle transazioni e la deanonimizzazione delle *blockchain*.

Sotto il profilo legislativo, sicuramente appare efficace l'inserimento da parte della normativa antiriciclaggio degli *exchanger* tra gli intermediari finanziari, con tutti i conseguenti obblighi in materia di trasparenza ed identificazione dei clienti.

Per quanto attiene l'aspetto investigativo, invece, certamente appare utile lo sviluppo di sistemi di *blockchain analysis*, tesi a rilevare indicatori di anomalie delle transazioni e ad identificare gli utilizzatori della stessa.

Nondimeno, risulta sempre più necessario investire anche nella formazione in materia di Magistrati ed appartenenti alla Polizia Giudiziaria e nell'integrazione dei predetti sistemi con l'intelligenza artificiale.

⁹ V. GUARRIELLO, S.M. GUARRIELLO, E. MACRÌ, *Cybercrime: una nuova minaccia per la Pubblica Sicurezza in Democrazia e Sicurezza – Democracy and Security Review*, Agosto 2022, pp.13 e ss.