BITCOIN FORENSICS E INTELLIGENCE SULLA BLOCKCHAIN

PAOLO DAL CHECCO – FABIO PASCUCCI – GIOVANNI RECCIA – MARCO STELLA

ASPETTI GIURIDICI, ECONOMICI, FISCALI ED INVESTIGATIVI DELLE CRIPTOVALUTE

IISFA

BITCOIN FORENSICS E INTELLIGENCE SULLA BLOCKCHAIN

ASPETTI GIURIDICI, ECONOMICI, FISCALI ED INVESTIGATIVI DELLE CRIPTOVALUTE

A cura di
PAOLO DAL CHECCO, FABIO PASCUCCI,
GIOVANNI RECCIA, MARCO STELLA

CREDITI

Chiuso in redazione nel mese di Novembre 2019

Information Systems Forensics Association Italian Chapter
Via Federico Cesi n. 72, 00193 Roma (RM)

ISBN della versione cartacea 9788832189001
ISBN della versione e-book 9788832189018

IISFA è la prima ed unica associazione italiana

con focus specifico sulla "Information Forensics". L'associazione, senza scopo di lucro e aperta a tecnici e giuristi, ha come mission la promozione della materia attraverso la divulgazione, l'apprendimento e la certificazione, riconosciuta tra l'altro in ambito internazionale. Le attività ruotano intorno ad un codice etico e alla possibilità di far parte di un network di specialisti, con lo scopo altresì di costituire insieme, nel medio periodo, un punto di riferimento nello specifico settore, allo stato sottolineato da forti individualità. Per altre informazioni: www.iisfa.it.

PRESENTAZIONE

La lettura di Bitcoin Forensic e Intelligence sulla Blockchain, volume scritto da G. Reccia, P. Dal Checco, F. Pascucci e M. Stella, consente di comprendere molti aspetti legati alle criptovalute.

Le criptovalute, un recente risultato molto raffinato dell'evoluzione dell'Informatica in alcuni dei suoi aspetti, pur assicurando un elevato livello di sicurezza nelle operazioni finanziarie, diventano un pericolo quando le transazioni riguardano attività poco lecite e spesso criminali.

Esse non sono un pericolo di per sé, ma

permettere l'anonimato quasi assoluto a chi le utilizza, consentono di concludere ogni genere di affare, lecito e/o illecito: traffico di armi, di stupefacenti, di esseri umani e di organi, contrabbandi, richiesta di riscatti per sequestri di beni o di persone, riciclaggio di monete sporche, e così via.

Inoltre, molte di queste attività si svolgono nel cyberspace non visibile (dark web), che ormai occupa regioni virtuali dalle dimensioni confrontabili con quello visibile. Il cd. dark web è difficilmente tracciabile e scarsamente indicizzato dai motori di ricerca per le difficoltà che ci sono nel farlo. È quindi evidente la semplicità con cui la criminalità (un soggetto anonimo) può

portare a compimento i propri affari, in uno spazio incontrollato, pressoché indisturbata.

Il libro, con puntualità, esamina importanti aspetti teorici e i corrispondenti aspetti tecnico-applicativi non ignorabili da chi deve contrastare il malaffare. Quindi siamo di fronte ad un manuale prezioso che non trascura gli aspetti operativi da tenere in conto quando, nel rispetto della legge, si svolgono indagini e si inseguono tracce e prove di atti compiuti.

Si tratta di un'opera importante e credo unica nel suo genere, un punto di partenza solido nel presentare una metodologia di indagine e di acquisizione delle prove nell'ambito

delle monete virtuali e delle blockchains.

Il libro non è mai astratto e nella sua lettura si avverte l'esperienza diretta degli Autori, professionisti protagonisti di indagini di notevole rilevanza, che operano in scenari in continua e rapida evoluzione, dove le tecnologie digitali richiedono competenze specialistiche crescenti e rendono il loro lavoro sempre più impegnativo.

Il libro è ben scritto ed è chiaro, la sua lettura è coinvolgente e consente di mettere a fuoco concetti apparentemente incomprensibili ed indica alcune metodologie che, se adottate o imitate nei principi, risultano efficaci nel contrasto alla criminalità, non solo

finanziaria. Sarà inevitabile in una società sempre più digitalizzata appropriarsi di questi strumenti.

INTRODUZIONE

Il tema delle criptovalute e, più in particolare, la prima e più famosa criptomoneta, il bitcoin, è stato l'oggetto principale di approfondimento della presente trattazione.

L'approccio al tema che è stato adottato ha riguardato molteplici aspetti: si è infatti passati dai più ricercati aspetti di natura giuridica ed economica a quelli di tipo operativo nonché tecnico, grazie anche all'esperienza maturata sul campo dagli autori.

Il valore aggiunto che, a parere di chi scrive, emerge nell'opera, si può individuare negli approfondimenti

tecnici che caratterizzano la ricerca di informazioni attraverso lo studio della struttura della *blockchain* e delle modalità pratiche, oltre che tecniche, di come procedere al sequestro di oggetti particolari come lo sono le criptomonete.

Il testo è stato articolato in quattro parti ben distinte ma che aiutano a ottenere una visione di insieme sulla complessità della criptovaluta *bitcoin* e, di conseguenza, del paradigma sottostante alle principali criptomonete nel loro genere.

A tal proposito, giova evidenziare che, seppur molteplici sono le opere che trattano dell'argomento in maniera più o meno approfondita lo specifico tema,

sotto i più svariati profili economici, finanziari o giuridici, difficilmente ci si trova di fronte a un manuale unico che consente di avere una visione di insieme anche su aspetti di natura più marcatamente pratici, operativi e tecnici volti a comprendere anche quei meccanismi più nascosti o meno conosciuti ai più, ma in ogni caso utilizzabili da chiunque, per affrontare in maniera quanto più ampia e condivisa il tema delle criptovalute.

Sul punto, ad esempio, è risultato utile descrivere il funzionamento di *bitcoin* oltre che descrivere la sua struttura e quella della relativa *blockchain*: ciò ha consentito di ipotizzare schemi visuali e relazionali utili a supportare la

comprensione dei dati che essa raccoglie e conserva per essere poi riutilizzati in ambito investigativo. A ciò si aggiunge l'esperienza operata sul campo per poter definire quali modalità siano da considerarsi le più idonee per procedere, ad esempio, con il "congelamento" giudiziario di una tale tipologia di strumenti innovativi.

L'opera, in ultima analisi, nella *prima Parte* affronta tematiche e implicazioni di natura giuridica e fiscale del bitcoin.

Nella *seconda Parte* sono descritti contesti operativi in cui è stato riscontrato un utilizzo particolarmente avanzato del bitcoin e di altre criptovalute, oltre che la naturale simbiosi tra questi "oggetti" e il *dark*

web.

Nella *terza Parte* è stato introdotto un possibile metodo di investigazione e di ricerca delle informazioni mediante lo studio e la modellazione del protocollo utilizzato per la costruzione del *bitcoin*, traendo innovativi risultati sotto il profilo dell'*intelligence* mediante l'applicazione di tecniche di *social network analysis*.

Nella *quarta Parte*, grazie anche alle numerose esperienze dell'autore esperite sul campo, si è cercato di fornire un metodo di approccio al sequestro e alla confisca delle criptomonete laddove sia ritenuto essenziale per gli esiti di una investigazione.

In sintesi, l'opera rappresenta un

compendio di ricerca e di diverse esperienze sul campo che consentono di approcciare al mondo delle criptomonete con praticità e, nel contempo, con rigore scientifico dettato da metodi e tecniche tipiche della ricerca scientifica.

Marco Stella

GLI AUTORI

Giovanni Reccia è Colonnello della Guardia di Finanza. Plurilaureato, abilitato alle professioni di avvocato e revisore dei conti, ha acquisito i master di II livello presso L'Università La Sapienza di Roma in "Strategia globale e Sicurezza", presso la Scuola Superiore dell'Economia e Finanze in "Etica nella pubblica amministrazione e contrasto alla corruzione", presso la Scuola Superiore di Amministrazione Pubblica in "Gestione della produzione e conservazione documentale", presso l'Istituto Studi Legislativi in

"Consulenza Legislativa". È titolato dell'Alta Formazione presso l'Istituto Alti Sudi Difesa ed ha svolto incarichi di docenza presso la Scuola di Polizia Economica e Finanziaria e nel corso "Antiriciclaggio" dell'Università La Sapienza di Roma. È stato a capo del Servizio Informatica e dell'Ufficio Telematica del Comando Generale del Corpo (2009-2013) nonché Comandante della Provincia di Latina (2013-2016). Ha condotto indagini di polizia a contrasto della criminalità organizzata, del riciclaggio e del finanziamento al terrorismo, nonché dell'evasione fiscale internazionale e dei reati economico-finanziari. Dal 2017 quale Comandante del Nucleo Speciale Frodi Tecnologiche

e Privacy si occupa di contrastare il cyber crime ed opera a tutela della privacy.

Paolo Dal Checco ha conseguito Laurea in Informatica e Dottorato di Ricerca, durante il quale si è occupato di crittografia e sicurezza delle reti e degli elaboratori, operando per alcuni anni in ambito di direzione tecnica allo sviluppo di sistemi di protezione delle comunicazioni. Da circa dieci anni si occupa essenzialmente di perizie informatiche forensi come consulente d'informatica forense in processi penali e civili, su evidenze digitali acquisite da smartphone, computer, reti, profili social network, email o altri supporti.

Con il suo Studio d'Informatica Forense offre da anni servizi in materia di digital, mobile, network forensics ad Aziende, Studi Legali o privati ma anche a Pubblici Ministeri, Giudici e Forze dell'Ordine in Tribunale o Procura come CTP, CTU o ausiliario di Polizia Giudiziaria. Fornisce consulenza informatica anche in ambito di D. Lgs 231, GDPR, protezione dei dati e sicurezza informatica. Specializzato oltre che in informatica forense anche nelle attività investigative sulle criptovalute come ad esempio i Bitcoin e sulle attività di Open Source Intelligence OSINT sulle fonti aperte. Collabora con l'Università di Torino e di Milano, oltre che con Centri di

Ricerca ed Enti di Formazione per docenze a contratto in Corsi, Master o Perfezionamento.

Fabio Pascucci è Ufficiale Superiore della Guardia di Finanza, laureato in Giurisprudenza, Scienze Politiche, Economia e Scienze della Sicurezza Economico Finanziaria. Con esperienza diretta nel contrasto alla criminalità organizzata negli incarichi svolti sul territorio nazionale, presso il Nucleo di Torino e quello di Bolzano, è attualmente impiegato presso il Comando Generale della Guardia di Finanza nel campo dell'informatica. Nella stessa branca, è stato in servizio per un periodo pluriennale presso il

CED interforze del Ministero dell'Interno e nel campo dell'informatica logistica e addestrativa del Corpo, ove ha svolto numerosi incarichi di insegnamento e partecipato a molteplici gruppi di lavoro applicati allo specifico settore.

Marco Stella è Ufficiale Superiore della Guardia di Finanza, con esperienza diretta nel settore del contrasto alla criminalità organizzata negli incarichi svolti in un Comando territoriale della Calabria, presso la Presidenza del Consiglio dei Ministri - Ufficio del Commissario di Governo per la gestione e la destinazione dei beni confiscati alle organizzazioni criminali nonché al

Servizio Centrale Investigazione Criminalità Organizzata della Guardia di Finanza. Attualmente è impiegato presso il Comando Generale della Guardia di Finanza e si occupa di informatica applicata alle operazioni ed alle investigazioni. Laureato in Scienze della Sicurezza Economico-Finanziaria e in Ingegneria Informatica nonché in possesso di certificazioni internazionali nello specifico settore, è autore di articoli e pubblicazioni nello specifico settore di analisi criminali e informatica forense.

PARTE I

DEFINIZIONI E CARATTERISTICHE DEI *BITCOIN*

1.

1. LA NATURA GIURIDICA DEI BITCOIN

a cura di Fabio Pascucci

1.
2.

Sommario: 1.1 Inquadramento generale – 1.2 La *Blockchain* – 1.3 Il *mining* – 1.3.1 Conviene fare il *mining*? – 1.3.2 I rischi di investire in *bitcoin* – 1.3.3 Le ICO – 1.4. Definizione giuridica dei *bitcoin* – 1.4.1 Prodotto digitale, bene immateriale – 1.4.2 Mezzo di pagamento o strumento di investimento – 1.4.3 La

pronuncia della Corte di Giustizia Europea e la recente sentenza della Corte d'Appello di Berlino – 1.5 *Smart contracts*.

3.
4.

1. **1.1 INQUADRAMENTO GENERALE**

Con il termine "Bitcoin" si intendono due concetti che vanno tenuti distinti e separati. Il primo, identificabile con la B maiuscola, indica un "protocollo informatico di comunicazione", ossia l'algoritmo che ne è alla base e il fenomeno mondiale che da esso si è

sviluppato. Il secondo, che chiameremo bitcoin (b minuscola), identifica invece una "moneta", cioè uno strumento finanziario utilizzato per compiere una serie di particolari forme di transazioni online. Pertanto, la parola "Bitcoin", con iniziale maiuscola, viene riferita alla tecnologia e al network sottostante, mentre il termine "bitcoin", scritto con iniziale minuscola, indica la valuta stessa [1].

La evidente difficoltà del giurista a fornire una definizione di bitcoin deriva dalla problematicità di enucleare una disciplina della materia, nonché dall'individuazione esatta di un fenomeno che per sua natura sfugge a strutture di caratterizzazione in cluster

univocamente identificabili. Come evidenziato nella letteratura di riferimento [2] il Bitcoin è un protocollo, cioè un insieme di regole che servono a definire il funzionamento del software utilizzato da un network di computer che dialogano tra loro in maniera paritaria (peer-to-peer), con lo scopo di creare e gestire la valuta bitcoin. Le transazioni sono convalidate dalla tecnologia associata al funzionamento del network, senza il coinvolgimento di soggetti terzi con il ruolo di intermediari.

Secondo la teoria dei giochi, è razionale l'individuo che, oltre a conseguire il proprio obiettivo con le risorse di cui dispone, prende in considerazione i

comportamenti degli altri agenti. Di conseguenza, se ciascuno perseguisse il proprio interesse personale, conseguirebbe la situazione più efficiente per tutti. La nostra economia appare non più incentrata su sistemi di produzione (beni tangibili), bensì su sistemi finanziari di trasferibilità di capitali (beni intangibili). Secondo il pensiero neoliberista, i protagonisti nei mercati sono i privati che, in concorrenza tra loro, soddisfano in modo efficiente la domanda e l'offerta di risorse.

La tendenza è verso un mercato sempre più aperto e deregolato, in cui i privati possono interagire per soddisfare i propri interessi. Il sistema finanziario

ben evidenzia, in molti casi, la subordinazione sociale nei confronti del sistema bancario.

Satoshi Nakamoto, il creatore del Bitcoin[1], in occasione della pubblicazione del whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System" nel 31 ottobre 2008" afferma: "una versione puramente peer-to-peer di denaro elettronico permetterebbe di spedire direttamente pagamenti online da un'entità ad un'altra senza passare tramite un'istituzione finanziaria. Le firme digitali offrono una soluzione parziale al problema, ma i benefici principali sono persi se una terza persona di fiducia è ancora richiesta per prevenire la doppia spesa. Proponiamo

una soluzione al problema della doppia spesa mediante l'utilizzo di una rete peer-to-peer".

Pertanto, il bitcoin si caratterizza per essere svincolato dal controllo di un'Autorità centrale, nonché per essere libero dall'intermediazione bancaria. È basato su un sistema decentralizzato, senza organismi centrali, con l'intento potenziale di sottrarre il potere di controllo della moneta alle banche centrali e agli Stati. Non essendo emesso da una banca o un'autorità centrale, chi se ne serve può farlo direttamente, in qualunque paese del mondo, senza passare attraverso intermediari. Non facendo ricorso a un ente centrale, tantomeno a meccanismi

finanziari sofisticati, il valore è determinato unicamente dalla leva domanda e offerta [3].

Bitcoin è open-source: la sua progettazione è pubblica e ognuno può prendere parte al progetto. Utilizza un database distribuito tra i nodi della rete che tengono traccia delle transazioni e sfrutta la crittografia per gestire gli aspetti funzionali, come la generazione di nuova moneta e l'attribuzione della proprietà [4].

2. 1.2. LA *BLOCKCHAIN*

Uno dei pilastri costitutivi del Bitcoin è

la Blockchain, ossia un database che viene mantenuto da tutti i partecipanti alla rete e che contiene tutte le transazioni effettuate dall'assegnazione della prima moneta. Dunque, è un database condiviso, decentralizzato, distribuito e criptato, secondo precise regole di sicurezza. È in grado di garantire l'assoluta immutabilità e incorruttibilità di tutte le informazioni; è aperto e trasparente per tutti i partecipanti, che possono vedere tutto e in qualsiasi momento, a patto che soltanto gli stessi partecipanti possano modificare l'archivio, unicamente con il consenso di tutti.

Ne consegue che la Blockchain è una tecnologia che permette la creazione e la

gestione di un grande database distribuito per la conduzione di transazioni condivisibili tra più nodi di una rete. È un archivio strutturato in blocchi (contenenti più transazioni) che sono tra loro collegati in rete in modo che ogni transazione avviata sulla rete debba essere validata dalla rete stessa nell'analisi di ciascun singolo blocco. La Blockchain risulta così costituita da una catena di blocchi che contengono ciascuno più transazioni. Le transazioni sono affidate ai Nodi, che vedono, controllano e approvano tutte le transazioni, creando una rete che condivide su ciascun nodo l'archivio di tutta la Blockchain. Ciascun blocco è un archivio per tutte le transazioni e per

tutto lo storico, modificabile solo con l'approvazione dei nodi della rete. Pertanto, le transazioni possono essere considerate immodificabili, se non attraverso una nuova autorizzazione delle stesse da parte di tutta la rete. Il concetto di immutabilità della transazione si basa appunto sulla irreversibilità delle transazioni sulla Blockchain, per cui non è possibile per un utente sovvertire l'ordine delle operazioni. Per poter riprodurre un'operazione sarebbe necessario possedere una potenza di calcolo paragonabile alla somma della potenza di calcolo di tutti i partecipanti alla rete. Allo stato attuale, il network dei bitcoin ha una potenza di calcolo superiore alla

somma dei primi 500 supercomputer operanti a livello globale; pertanto, sarebbe molto complesso sferrare un attacco alla rete anche da parte di uno stato sovrano [3].

3. 1.3. IL *MINING*

Esistono tre modi per ottenere bitcoin: acquistarli su un servizio di exchange; accettarli come metodo di pagamento per beni o servizi; crearne di nuovi attraverso il "mining".

Quest'ultimo è un processo che permette di aggiungere ulteriori fascicoli al registro pubblico della Blockchain.

Come abbiamo visto, la Blockchain assicura che ogni transazione possa essere confermata e che ogni utente nella rete possa accedere in qualsiasi momento al libro contabile. Svolge, inoltre, il compito di distinguere le transazioni legittime da quelle illecite, impedendo che le medesime unità di bitcoin vengano utilizzate più volte dallo stesso utente.

Come tenere traccia di tutte le transazioni ovvero come essere certi che un singolo bitcoin venga usato univocamente e non speso in due operazioni distinte? L'unico modo per sincronizzare tutti i database è il mining, ossia trasformare le transazioni in una stringa (secondo un procedimento di

matematica crittografica) e incollare l'hash in fondo al database stesso.

Ci sono ricompense (in bitcoin, ovviamente) per coloro che, mettendo a disposizione il loro computer, elaborano le transazioni correttamente.

In particolare, la generazione e l'attribuzione di nuove unità di valuta (nuovo circolante in forma di bitcoin) viene premiata con un riconoscimento accordato dalla rete agli utenti (miners) che contribuiscono, in concorrenza fra loro, alla sua gestione e alla sua sicurezza [5].

Mettendo a disposizione le capacità di calcolo del proprio computer, i miners offrono la possibilità di verificare, tramite la soluzione di complesse

operazioni matematiche, l'univocità e la sicurezza delle transazioni effettuate [6]. Il mining rappresenta la procedura di verifica che viene effettuata sfruttando la potenza di calcolo dei computer o dei dispositivi che vengono messi a disposizione dai "minatori".

Nel sistema bitcoin, con programmata emissione di un numero finito di "monete, i miners sviluppano la catena delle transazioni e ricevono altri bitcoins in cambio del loro lavoro di implementazione e certificazione elettronica [7].

L'infrastruttura tecnologica sulla quale viaggia il flusso di transazioni tra gli utenti (distributed ledger technology) sostituisce l'attività di regolazione

dell'offerta di valuta – funzione tipica dell'Autorità monetaria centrale – e si autogestisce. Questa tecnologia permette alle criptovalute che ne fanno ricorso di non avere un organo centrale al comando, ma di avvalersi della distribuzione potenzialmente diffusa della nuova moneta creata. Quindi, una ripartizione espansa di monete decentralizzate, considerato che il mining è liberamente accessibile, anche se risulta nella pratica abbastanza concentrato, a causa dei costi e dei mezzi necessari per lo svolgimento.

Nuove monete vengono generate automaticamente seguendo un algoritmo predefinito che caratterizza l'evoluzione della base monetaria nel tempo.

L’assegnazione di nuove monete agli utenti viene effettuata attraverso un complesso sistema che permette di riconoscere gli utenti che maggiormente concorrono alla sicurezza della rete bitcoin creando un meccanismo incentivante che rende la rete più sicura nel tempo.

Il mining di criptovalute può essere effettuato in tre modalità differenti:

in prima persona, ovvero sfruttando il proprio hardware: può apparire il metodo più proficuo, tuttavia bisogna considerare che nella maggior parte dei casi è richiesta una potenza di calcolo molto considerevole, non essendo sufficiente il pc di casa. e che quindi non basta il computer che abbiamo in

salotto. Se si considera il mining come un'attività amatoriale, si corre il rischio di farla diventare l'opzione più dispendiosa, considerato il costo energetico elevato, che potrebbe non far recuperare nemmeno i soldi spesi per l'acquisto della strumentazione.

messa a disposizione di un gran mettendo a disposizione la propria potenza di calcolo tramite una mining pool: la potenza richiesta si raggiunge con la numero di dispositivi. In questo caso i ricavi saranno proporzionati alla potenza di calcolo offerta;

affittare la potenza di calcolo tramite il cloud mining: si ricercano i siti che mettono a disposizione dei pacchetti da acquistare in cambio di un ritorno

economico. Potrebbe apparire la soluzione più semplice, tuttavia bisogna tener conto dei rendimenti economici potenzialmente negativi, ovvero investire più soldi di quelli che si riesce a far fruttare dal valore delle criptovalute generate.
Da notare che, nei primi due casi, bisogna considerare tra i costi, non solo quello della corrente consumata, ma anche quello dei componenti hardware soggetti ad una elevata usura, causata dalle condizioni di sforzo estreme degli apparati.

1.3.1 Conviene fare il *mining*?

Per generare e ottenere bitcoin, gli utenti

devono prendere parte alla rete in modo attivo, contribuendo con la potenza di calcolo del proprio computer alla sicurezza della rete stessa. Ogni utente può ricevere una ricompensa in bitcoin in base alla potenza computazionale che aggiunge alla rete.

Di solito non è vantaggioso cimentarsi in un settore così complesso come il mining, senza avere minimamente idea delle strumentazioni e delle strutture organizzative necessarie, e più passa il tempo e sempre meno lo sarà. L'elevatissima complessità raggiunta dai calcoli del mining ci evidenzia che è totalmente controproducente supportare il processo con semplici computer di media potenza. La probabilità che un

certo utente riceva la ricompensa in monete dipende dalla potenza computazionale che aggiunge alla rete relativamente al potere computazionale totale della rete.

Considerato che la quantità di operazioni mediamente necessarie a chiudere con successo un singolo blocco è diventata talmente elevata da richiedere grandi quantità di risorse in termini di energia elettrica e potenza computazionale, la maggior parte dei "minatori" si unisce in strutture chiamate "mining pool", dove tutti i partecipanti mettono in comune le proprie risorse, spartendosi poi i blocchi generati in funzione del contributo di ognuno.

In questo consorzio, ogni partecipante

cede una parte di risorse del proprio computer per eseguire calcoli complessi. Una volta che una persona si sarà unita al pool e avrà creato il proprio account personale, dovrà scaricare un programma in Java per svolgere le operazioni di calcolo, soprattutto crittografie. Ogni volta che un pool trova la soluzione alla crittografia, il sistema lo premia con pacchetti da bitcoin. Le monete poi sono ripartite tra i vari membri, in base al contributo e le risorse messe a disposizione.

Per diventare un miner sono quindi necessari: un pc, una connessione Internet, un wallet specifico per bitcoin, e Java installato sul proprio hard disk. Il

tipo di sistema operativo non è importante: Windows, Linux o Mac, ognuno di questi ha software appositi per fare mining. All'inizio i bitcoin potevano essere minati semplicemente attraverso l'utilizzo delle classiche CPU dei normali desktop computer. Con l'aumentare della difficoltà di risoluzione del blocco si è passati all'adozione delle GPU ovvero delle schede grafiche fino ad allora dedicate prevalentemente al gaming e a scopi professionali quali editing o simulazione e modellazione complesse. Negli ultimi tempi tutto ciò non basta più, in quanto la difficoltà di creazione di un nuovo blocco cresce esponenzialmente al diminuire di bitcoin disponibili. È

quindi necessario ricorrere per lo meno all'utilizzo di più schede grafiche collegate fra di loro o optare per l'utilizzo degli ASIC, acronimo di Application Specific Integrated Circuit, ovvero hardware progettato appositamente per il mining di bitcoin.
Chi decide di utilizzare un normale microprocessore dovrà assicurarsi di avere una scheda grafica con memoria dedicata e un processore ad alte prestazioni. Viene consigliato di destinare una macchina dedicata con buone ventole di raffreddamento ed essere pronti a veder salire la bolletta dell'energia elettrica. Servono investimenti ingenti per iniziare, mentre il ritorno economico è tutto da scoprire.

Il processo di generazione ed estrazione dei token dei bitcoin dalla sua Blockchain avviene mediante un algoritmo di hashing che viene fatto girare continuamente dai computer adibiti al “mining,rig”.

Quest’ultimo processo viene sviluppato tramite GPU RIG, ovvero dei computer che sfruttano le capacità di calcolo di una scheda video per fare mining di molte cryptomonete. I rig di GPU possono essere usati sia in delle farm che per fare mining a livello domestico. Negli ultimi anni sono sorte parecchie mining farm, veri e propri capannoni privati pieni di hardware dedicato al mining con una potenza di calcolo davvero elevata. Queste farm nascono

solitamente in nazioni dove il costo della corrente è relativamente basso. Una nazione molta ambita per questo tipo di attività è l'Islanda, che offre il clima ideale ed energia a basso costo grazie all'abbondanza di fonti geotermiche ed impianti idroelettrici.

Dal punto di vista tecnico, ogni rig armato di GPU comprende in media 6/8 schede video. La GPU è ottima per eseguire operazioni ripetitive, e l'algoritmo di hashing è una di queste. Più se ne riescono a montare sul rig e maggiori saranno i bitcoin che si potranno minare.

Per fare un esempio concreto: in media, ogni GPU consuma tra i 100 e i 250 watt (l'algoritmo di hashing è intorno ai 100

watt) per cui bisogna fare bene i conti di ciò che serve.

Gli altri comuni componenti del computer, come ad esempio CPU (Central Processing Unit, ovvero il processore) e la RAM (Random Access Memory, la memoria volatile) non servono granché nel processo di mining.

Minare bitcoin da casa è da tempo considerato un'utopia, perché è necessario disporre di server ultrapotenti e un consumo di energia elettrica spropositato. Quindi il miraggio di poter minare bitcoin e ricevere ricompense con il computer installato nella cameretta di casa è ormai svanito. Fare mining con un semplice computer domestico di alta

qualità può far guadagnare circa 0,00001000 BTC al giorno, ovvero nemmeno 0,00400000 BTC all'anno (meno di 2€ annuali).

Il primo blocco emesso ha garantito 50 bitcoin nel lontano 2009, dimezzandosi a 25 nel 2012 e ancora a 12.5 nel 2016, continuando progressivamente a diminuire. Il numero di bitcoin creati per blocco era, come detto, di 50 BTC. Tale quantità è stata programmata per diminuire nel tempo secondo una progressione geometrica con un dimezzamento del premio ogni 4 anni circa. Così dimensionata, questa serie comporta che in totale verranno creati esattamente 21 milioni di bitcoin nel giro di 130 anni circa, con l'80% degli

stessi creati nei primi 10 anni.

1.3.2 I rischi di investire in *bitcoin*

Con la progressiva riduzione della ricompensa di generazione nel tempo, la fonte di guadagno per chi effettua "mining" è diventata la commissione della transazione inclusa nei blocchi, anziché la generazione stessa di moneta. L'introito per i minatori è passato dalla produzione della moneta alle commissioni di transazione fino ad arrivare a un punto in cui il provento cessa di essere elargito: per l'elaborazione delle transazioni, c'è unicamente una remunerazione per le commissioni di transazione stesse.

Un'alternativa può essere il cloud mining, che consiste nel processo di acquisto del potere computazionale (hash power) di computer che si trovano in data center dedicati al mining.

Il vantaggio principale di questo approccio si concretizza nella possibilità di non avere una conoscenza approfondita dell'hardware per il mining, tantomeno acquistare dispositivi costosi e difficili da ottenere. Inoltre, non si deve far fronte ai costi della corrente elettrica, alla manutenzione ed al calore sviluppato dalle macchine che si avrebbe minando "in casa". Noleggiare "hash power" significa investire a distanza sul mining di crypto, senza dover intervenire in prima

persona; tuttavia i profitti potranno risultare inferiori rispetto al mining classico.

Molto diffuso, poi, è il trading con bitcoin, considerato il mezzo per scambiare valore in maniera efficiente, anonima e sicura tra gli abitanti della Cultura Digitale. Quest'ultima considera le prospettive di crescita del valore del bitcoin come indubbiamente immani; la Blockchain è ritenuta il futuro dei pagamenti e delle transazioni finanziarie.

Anche la Digital Community, pur considerando il bitcoin trading non necessariamente più pericoloso rispetto ad altri strumenti di speculazione finanziaria, mette in guardia sul rischio

che questo mezzo può esporre l'investitore che cerca un metodo per fare facilmente soldi. È vero che i bitcoin hanno creato più milionari di qualunque altro asset finanziario, ma chiunque affermerebbe che per guadagnare con i bitcoin ci vuole sempre la scelta adeguata della piattaforma più conveniente e anche un minimo di impegno.

Sono in molti a pensare che il trading di bitcoin sia una truffa, proprio perché oggettivamente si possono guadagnare ingenti somme di denaro anche con criptovalute fake che nascondono schemi ponzi o con exchange di criptovalute, che funzionano perfettamente per qualche tempo e poi chiudono, senza

lasciare traccia.

Il vero problema del trading con bitcoin, tuttavia, è l'oscillazione "da ottovolante" del suo valore. Basti pensare che a metà dicembre 2017 toccava il picco storico a un passo da 20mila dollari, con una capitalizzazione di 329miliardi di dollari, per arrivare un anno dopo a circa 3mila dollari con una capitalizzazione evaporata a 56miliardi di dollari, con un crollo verticale dell'85%[2].

Il valore del bitcoin è molto instabile perché è dato unicamente dai flussi di domanda e offerta.

Qualsiasi bene scambiato ha un valore d'uso che permane anche se gli scambi cessano o si diradano. L'oro può essere

comprato come bene di investimento ma ha un uso industriale, oltre a quello ben noto legato alla gioielleria. I prodotti agricoli e l'energia hanno il loro valore concreto ben consolidato nei mercati regolamentati. Anche le valute straniere hanno un contenuto reale, poiché permettono di assicurarsi una quantità ragionevolmente certa di beni o di servizi nel Paese di cui costituiscono la moneta avente corso legale. Come tale, permette di avere un cambio ragionevolmente certo rispetto ad altre valute, a meno di eventi catastrofici, quali guerre, espropri o altri similmente traumatici. L'avere corso legale assicura che il denaro potrà senza dubbio essere speso e il soggetto che lo detiene farà

affidamento su un'adeguata riserva di valore, che, in qualsiasi momento, potrà essere impiegata per ottenere in cambio beni, servizi, o un'altra valuta di caratteristiche similari.

Il valore di qualsiasi bene scambiato su un mercato è dunque radicato in un valore d'uso.

Ciò non avviene per le criptovalute, che non possiedono alcun radicamento reale oltre alla mera disponibilità di qualcuno ad acquistarle in cambio di un altro bene che sia reale, immateriale, o valutario.

Esse dipendono da una infrastruttura che - sebbene diffusa - è privata e non soggetta ad alcun obbligo di servizio. Tale infrastruttura è inoltre soggetta ad una serie di esternalità che ne

condizionano l'esistenza. Ad esempio, il costo della corrente elettrica; se quest'ultima ha un'impennata di costo, i calcoli crittografici estremamente complessi, che sono alla base dell'autenticazione dei blocchi in una Blockchain, divengono estremamente gravosi o addirittura antieconomici.

Purtroppo, il sistema Bitcoin è stato anche utilizzato per attività illecite perché è anonimo e non prevede la presenza di un'autorità centrale che possa raccogliere dati identificativi. Registri, saldi e transazioni sono archiviati su ogni computer. Non vi è dunque un'autorità centrale che può autenticare l'accesso alla Blockchain [8].

1.3.3 Le ICO

L'esplosione del fenomeno criptovalute ha portato con sé quello delle ICO (acronimo di "Initial Coin Offering"), ovvero letteralmente "offerta iniziale di moneta".
Il termine "Initial Coin Offering" è stato evidentemente mutuato da quello di "Initial Public Offering" ossia di un'offerta pubblica di strumenti finanziari da parte di un soggetto emittente (azioni, obbligazioni ecc.). In realtà, si dovrebbe parlare più correttamente di "Token Generation Event", ossia di un evento di generazione di token, dato che tali token

possono rappresentare diritti diversi.
Come le IPO (dall'inglese “Initial Public Offering”) sono Offerte Pubbliche iniziali, ossia offerte al pubblico dei titoli di una società che intende quotarsi per la prima volta su un mercato regolamentato, così, partecipando ad una ICO, si offrono al team autore dell’offerta i finanziamenti per un progetto, ottenendo in cambio dei token, ovvero una nuova criptovaluta, solitamente alla base del progetto stesso.
Mentre le IPO sono promosse generalmente da un'impresa il cui capitale è posseduto da uno o più imprenditori, o da un ristretto gruppo di azionisti (ad esempio investitori

istituzionali o venture capitalists), che decide di aprirsi ad un pubblico di investitori più ampio contestualmente alla quotazione in Borsa, le ICO lanciano sul mercato una nuova moneta, nel caso specifico una criptovaluta, che permette di finanziare progetti attraverso la vendita di una moneta ancora inesistente.

ICO è un concetto recentemente emergente di progetti di crowdfunding (raccolta di fondi) nei settori cryptocurrency e Blockchain. Si tratta di un evento, talvolta definito "crowdsale", in cui vi è un'offerta iniziale di una moneta che verrà ufficialmente emessa in futuro: un'azienda rilascia la propria crittografia con uno scopo di

finanziamento. Di solito rilascia un certo numero di crypto-tokens e poi vende questi token al pubblico destinatario, più comunemente in cambio di bitcoins, ma può anche essere denaro.

Di conseguenza, la società ottiene il capitale per finanziare lo sviluppo del prodotto e i membri del pubblico ricevono le loro azioni di cripto. Inoltre, hanno la completa titolarità di queste azioni.

Da notare che, per un'Offerta Pubblica Iniziale, le azioni della società indicano sempre una quota di proprietà nella rispettiva società; per le ICO, invece, i crypto-tokens possono essere utilizzati in alcuni progetti per trasferire poteri di voto – una quota maggiore di gettoni che

danno più potere di voto –, ma più spesso i gettoni sono un'unità di valuta che può essere inviata ad altri utenti e scambiata con altre valute.

Le IPO, inoltre, sono fortemente regolamentate dai governi di ogni Paese, con obblighi cogenti per le società che vogliano quotare le proprie azioni. Al contrario, il crowdfunding di cryptocurrency è in gran parte scevro dai regolamenti governativi, per cui ogni "organizzazione" lanciare un ICO in qualsiasi momento, con poca preparazione di documentazione e soprattutto rivolgendosi a chiunque voglia partecipare, senza particolari studi o approfondimenti, ma solo contribuendo con le proprie risorse

finanziari. È bene valutare che, come detto, non vi è alcuna regolamentazione predefinita, di conseguenza nessun organo di vigilanza che valuti l'affidabilità di un progetto: per questo è facile imbattersi in una truffa.

Il primo rischio riguarda la strutturazione economica dell'offerta. Non è sempre ben chiaro ancora cosa gli investitori ottengano in cambio di "coin". Gli investitori non sanno bene cosa stanno comprando e questo li espone facilmente a delle truffe. Oggi chi compra "coin", lo fa perlopiù per rivenderli sul mercato secondario a un prezzo maggiore. Il secondo rischio è tecnologico: le modalità usate al momento per quasi tutte le ICO sono

ancora inaffidabili, insicure, non scalabili, tecnicamente fragili o immature. Il terzo è di natura legale: molte società stanno lanciando ICO per aggirare, di fatto, tutte le normative sugli strumenti finanziari.

Recentemente, i membri del Parlamento europeo si sono riuniti per gettare le basi di un primo quadro normativo riguardante le Initial Coin Offering. È allo studio un nuovo disegno di legge che potrebbe rappresentare il primo passo per la nascita di uno standard europeo per la vendita di token. Promotore del disegno di legge è Ashley Fox, deputato al Parlamento europeo (MEP).

Come dichiarato dallo stesso Fox,

l'obiettivo dei legislatori è quello di creare un sistema di regolamentazione per ICO più affidabili ed efficaci, all'interno di un più ampio e variegato mercato che non sempre può garantire regole certe e trasparenti. Si sottolinea la necessità, dunque, di un controllo più rigoroso sull'intero processo di raccolta dei capitali. Per questo motivo si rende più che mai necessaria la creazione di una serie di norme che possano garantire la sicurezza, permettendo alle aziende di sfruttare a fondo tutti i benefici. Il Parlamento europeo, infatti, ha approvato la bozza di normativa della Commissione europea sull'Investments crowdfunding (cioè lending ed equity crowdfunding), che include, tra le altre

modifiche, anche quella riguardante l'aumento a 8 milioni del tetto di raccolta.

Una ICO è una forma di crowdfunding, senza dubbio diversa, ma pur sempre una forma di crowdfunding e, come tale, necessita di certezze normative.

L'urgenza di un intervento legislativo si giustifica già di per sé considerando che quella delle ICO è un fenomeno che ha fatto registrare un vero e proprio boom: nel secondo trimestre del 2018 infatti la raccolta di capitale è arrivata a toccare la cifra record di 8 miliardi di dollari con un aumento, rispetto al trimestre precedente, del 150%.

Tramite il crowdfounding, l'azienda (di solito una startup) offre la possibilità a

tutti gli utenti di finanziare il progetto, fornendo in cambio dei token che saranno scambiabili sulle piattaforme di trading.

I token sono normalmente distinti in:

security token, rappresentativi di diritti economici legati all'andamento dell'iniziativa imprenditoriale (ad esempio, il diritto di partecipare alla distribuzione dei futuri dividendi) e/o di diritti amministrativi (ad esempio, diritti di voto su alcune materie);

utility token, rappresentativi di diritti diversi, legati alla possibilità di utilizzare il prodotto o il servizio che l'emittente intende realizzare (ad esempio, licenza per l'utilizzo di un software ad esito del processo di

sviluppo).
Quando si parla di ICO bisogna pensare a un modello a metà tra la raccolta fondi e il mercato della Borsa. Come avviene ad esempio su Kick starter, i finanziatori scommettono su progetti che non hanno ancora avuto la validazione del mercato; mentre, in Borsa, chi investe acquista una quota dell'azienda che può crescere nel tempo. Dunque, chi promuove l'ICO emette token digitali su una Blockchain pubblica: l'investitore paga con la moneta della Blockchain scelta e acquista una parte dei token messi a disposizione (idealmente paragonabili alle azioni del mercato borsistico). In alcune ICO vengono messi a disposizione dei sistemi di conversione,

in modo tale che l'investitore possa pagare in euro. In un secondo momento lo startupper e l'investitore possono convertire i token in valuta tradizionale sulle piattaforme di exchange tradizionali, oppure con transazioni private.

Uno startupper può avere diversi vantaggi da un ICO. Rispetto a un venture capital[3] o business angel[4], il processo di raccolta è più veloce e non è soggetto a "frizioni" burocratiche. Inoltre, chi cerca fondi può rivolgersi a una platea molto più ampia, non solo professionisti del settore, ma anche piccoli investitori che vogliono finanziare un progetto con pochi euro. Trattandosi di progetti molto rischiosi,

tuttavia, per gli investitori c'è la possibilità di avere ritorni importanti grazie alle fluttuazioni speculative, ma anche il rischio di perdere gran parte del capitale investito in poco tempo.

Le ICO hanno attirato numerosi investitori nel campo delle valute virtuali, in quanto permettono di fatto di ottenere monete non ancora esistenti a prezzi assolutamente vantaggiosi. Si nasconde, tuttavia, qualche insidia, considerato che il progetto o la moneta che si finanzia potrebbero risultare un fallimento o costituire una truffa, per scarsa regolamentazione delle procedure.

È bene tenere sempre a mente che l'azienda ottiene il capitale per

finanziare lo sviluppo del piano e i membri ricevono le loro ricompense, solo se lo stesso avrà successo.

Generalmente una ICO presenta un soft cap e un hard cap, che rappresentano rispettivamente l'obiettivo minimo e quello massimo della raccolta di fondi. Qualora il soft cap non venga raggiunto, la ICO potrebbe procedere in diversi modi, che vanno dalla restituzione dei soldi fino alla messa in commercio delle poche monete vendute. Esiste poi una road map, nella quale vengono descritti tutti i punti cardine e gli obiettivi che il progetto mira a raggiungere in un preciso momento. Al termine della ICO, che può giungere in una data prefissata o una volta raggiunto l'hard cap, la nuova

moneta viene effettivamente lanciata sul mercato e diventa quindi liberamente scambiabile e commerciabile tramite alcuni exchange.

Ogni ICO presenta inoltre un whitepaper, ovvero un documento nel quale vengono spiegati tutti i singoli aspetti che riguardano il progetto e la nuova moneta. Si tratta di un aspetto fondamentale in fase di valutazione di un eventuale investimento.

La maggior parte delle ICO, oltre ad avere un sito internet dal quale poter accedere e quindi partecipare, presentano numerosi canali social e di comunicazione che permettono di mantenersi informato su tutti gli eventi di rilievo.

Solitamente la ICO apre con un pre-sale, ovvero la possibilità ai primi che intendono finanziare il progetto, di ottenere token ad un prezzo ancora più vantaggioso rispetto a color i quali parteciperanno in seguito.
È prassi che, quando si vuole prendere parte ad una ICO, sia necessario sottostare a determinati vincoli imposti dall'azienda, che rilascia il token:

- la soglia minima di finanziamento che accettano;
- il tetto massimo del capitale che intendono ricevere;
- il numero di token che intendono rilasciare;

- il periodo di tempo di durata della raccolta;
- la data del lancio del progetto, nonché le restanti informazioni utili per ogni ICO, sempre reperibili sul sito ufficiale.

Queste indicazioni prendono spunto da uno dei provvedimenti più rilevanti sulle Initial Coin Offering, che ha dato il via all'adozione di accorgimenti da parte di altri legislatori, ovvero quello del 25 luglio 2017 della U.S. Security and Exchange Commission relativo al Report di investigazione n. 81207 su The DAO.

La vicenda di The DAO è stata uno dei primi eventi di ampia rilevanza relativo alla tecnologia Blockchain.

The DAO era una "Decentralized autonomous organization", ossia un'organizzazione creata su Blockchain Ethereum (Ethereum – ETH - è una piattaforma decentralizzata del Web 3.0 per la creazione e pubblicazione peer-to-peer di contratti intelligenti - smart contracts – vgs 1.4.1). Ethereum è diverso da bitcoin, in quanto consente di creare contratti intelligenti, che possono essere descritti come denaro digitale altamente programmabile[5].

The DAO era caratterizzata dal fatto di non essere formalmente definita (ossia era un'organizzazione senza una sede,

senza una personalità giuridica, senza veri e propri amministratori). I creatori di The DAO avevano l'obiettivo di raccogliere capitali (tramite lo scambio di DAO Tokens a fronte di ETH) da investire su progetti che venivano previamente vagliati da un comitato e successivamente posti in votazione ai possessori di DAO Token. Per far questo, avevano provveduto alla creazione di:

- un sito Internet per fornire informazioni;
- un whitepaper in cui veniva descritto il progetto,
- audit del codice sorgente degli smart

contracts utilizzati;

- accordi con alcuni "exchange" per permettere lo scambio dei token una volta acquisiti.

Nel giro di pochi mesi gli organizzatori di The DAO riuscirono a raccogliere circa 150 milioni di dollari. Il 18 giugno 2016 veniva violato l'indirizzo in cui erano stati allocati gli ETH ricevuti dall'organizzazione e in poche ore furono persi circa 70 milioni di dollari.

La vicenda portò ad una scissione della Blockchain Ethereum ed alla creazione di due nuove Blockchain (oggi suddivise in Ethereum classic - quella più antica -

ed Ehthereum).

La SEC, nell'analizzare la vicenda, si pose innanzitutto l'obiettivo di qualificare la fattispecie, soprattutto per comprendere la riconducibilità o meno della stessa nell'alveo dell'attività di collocamento di strumenti finanziari. A tale scopo, fece appello ai principi articolati in una decisione della Corte Suprema statunitense del 1946 (caso SEC v. W. J. Howey Co), principi oggi conosciuti come il test Howey.

Questo "test" prevede che per comprendere se la fattispecie concreta possa essere definita un "contratto di investimento" è necessario riferirsi alla sostanza e non alla mera forma contrattuale, dovendo essere considerato

come contratto di investimento qualsiasi "investimento di denaro in un'impresa con la ragionevole aspettativa di profitti derivanti da sforzi manageriali o imprenditoriali di altri".

Nel caso di The DAO la SEC, alla fine, ha evidenziato che:

- non è necessario che l'investimento sia "monetario", ma può essere effettuato con altra tipologia di contribuzione di valore. Nel caso di The DAO gli investitori avevano appunto scambiato ETH (che avevano un valore determinato sul mercato)

in cambio di DAO Tokens;

- l'investimento era stato effettuato con un'aspettativa di profitto (che generalmente possono essere dividendi, pagamenti periodici, incremento di valore). Tutti i materiali promozionali di The DAO evidenziavano che l'obiettivo era quello di creare un'entità con scopo di lucro, la quale avrebbe dovuto finanziare progetti in cambio di un ritorno

sull'investimento;

- l'aspettativa di ritorno dell'investimento dipendeva da sforzi gestionali altrui, dato che l'organizzazione di The DAO sulle decisioni in merito ai progetti da finanziare era assolutamente verticistica. I fondatori dell'organizzazione ed i curatori (ossia delle persone da essi selezionate per la loro capacità ed esperienza) monitoravano costantemente le attività,

salvaguardavano gli interessi degli investitori e decidevano quali progetti dovevano essere sottoposti al voto. D'altra parte, la comunità degli investitori era numerosa e frammentata, tale da risultare assai difficoltoso organizzare dei "sindacati di voto" o tentare una concertazione dello stesso.

Tali considerazioni hanno indotto la SEC a ritenere i DAO Token strumenti finanziari, specificando, nel suo "Report of Investigation" del 25 luglio 2017, che

i token fossero delle “securities”, e, in quanto tali, dovessero essere assoggettate al Securities Act del 1933 ed al Securities Exchange Act del 1934.

In tali casi ai token vengono collegati i diritti assimilabili a dei titoli (“security-like”), quali, ad esempio, il diritto alla restituzione di una obbligazione o la partecipazione al fatturato o agli utili della start-up (“revenue sharing” o “profit sharing”), oppure i diritti di voto all’interno della stessa start-up.

Ne deriva l’obbligo per l’ente emittente di registrare le offerte e le vendite degli strumenti (obbligo non rispettato dagli organizzatori di The DAO con violazione della Sezione 5 della richiamata normativa) e,

correlativamente, l'obbligo di registrazione per i soggetti che offrono piattaforme di scambio (trading) dei suddetti token quali "national securities exchange".

I promotori di una ICO devono essere in grado di dimostrare che la valuta virtuale o il prodotto non sono uno strumento finanziario o che, qualora rientrino in tale categoria, siano stati soddisfatti tutti i requisiti previsti dalla legge. Anche nel caso dell'offerta di valute (e quindi tipicamente di prodotti che non garantiscono profitti con lo stesso meccanismo degli strumenti finanziari) il documento chiarisce che la valutazione circa il loro inquadramento nell'ambito della Securities law deve

essere svolta comunque tenendo conto delle loro caratteristiche e del loro uso. Ciò in quanto, dopo la pubblicazione del Report del 25 luglio 2017, molte ICO hanno cercato di enfatizzare l'uso "commerciale" del token proposto, al fine di sottrarre l'offerta dall'alveo della Securities law, parallelamente accentuando il potenziale di vendita su mercati secondari e prospettando così la possibilità di generare profitti da tali rivendite.

Se la società che emette il token evita di dare determinate caratteristiche al token stesso (cosa che avviene nella maggioranza dei casi) questo verrà definito come una criptovaluta che ha una funzione di pagamento di specifici

servizi, pur mantenendo tuttavia inalterata la sua funzione monetaria (i token sono trasformabili in qualunque momento in altra criptovaluta od utilizzabili come moneta per taluni scambi).

Pur non costituendo una vera e propria regolamentazione del fenomeno si può dire che il Report SEC del 25/7/2017 ha svolto la funzione di spartiacque. Nel periodo immediatamente successivo alla sua emissione, si sono infatti susseguite varie prese di posizione delle autorità di controllo di numerosi Paesi.

Il 4 settembre 2017 la People's Bank of China disponeva il divieto di Initial Coin Offering e la sospensione delle attività di scambio dei token sugli

exchange (ed in genere la compravendita di criptovalute a fronte del pagamento in moneta avente corso legale), con obbligo di restituzione delle somme per quelli già collocati sul mercato, approccio seguito dalla Corea del Sud il 29 settembre 2017.

Alcuni Paesi hanno assunto posizioni simili a quelle della SEC[6], altri si sono concentrati nel ricordare l'applicabilità delle leggi nazionali a seconda della tipologia di token emesso[7], altri ancora si sono limitati ad emettere avvisi agli investitori (come il Regno Unito) oppure addirittura annunciando la volontà di avviare delle Initial Coin Offering di "valuta nazionale" (come l'Estonia), pur riprendendo l'approccio adottato dalla

SEC relativamente alle ICO private.

Per quanto riguarda la Comunità Europea, è stata pubblicata sulla Gazzetta Ufficiale dell'Unione Europea (L 156 del 19.06.2018) la Direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio, del 30 maggio 2018, che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE. La direttiva non si focalizza in realtà solo sulla moneta virtuale, in quanto elaborata e approvata come misura antiriciclaggio, ma regolamenta anche l'anonimato; nel fare questo, riconosce e definisce le

criptovalute.
La definizione ruota attorno al concetto di valute virtuali, le quali entrano dunque a titolo ufficiale a far parte della legislazione europea: "una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente".
Non vengono mai citate le parole criptovalute, o bitcoin, ma è più che evidente che la direttiva si riferisca

proprio ad esse.
Di fatto con questo testo la UE riconosce ufficialmente le criptovalute, dando loro uno status giuridico differente rispetto a quello delle valute fiat[8], e costringe gli Stati membri a fare altrettanto. Tale definizione, entrando a far parte del diritto comunitario, impone agli Stati Membri di recepirla quale canone interpretativo: la nuova direttiva è entrata in vigore il 9 luglio 2018 e gli Stati membri devono rendere cogenti le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi ad essa entro il 10 gennaio 2020.
Tra le novità più importanti emerge anzitutto la limitazione dei pagamenti

anonimi tramite carte prepagate, ivi inclusi gli exchange per le criptovalute: abbattere il paventato anonimato delle monete virtuali significa omologarle alle valute reali, cambiando in modo radicale il modo in cui tali monete sono recepite agli occhi di quanti le utilizzano nel tentativo di eludere il Fisco o tentare investimenti speculativi o finanziamenti illegittimi. Gli exchange che abiliteranno lo spostamento di denaro virtuale dovranno pertanto identificare le persone che si celano dietro agli account ed avranno altresì l'onere (del tutto omologo a quello degli esistenti istituti bancari) di segnalare ad apposite autorità eventuali manovre sospette.

Sebbene le valute virtuali possano

essere spesso utilizzate come mezzo di pagamento, potrebbero essere usate anche per altri scopi e avere impiego più ampio, ad esempio come mezzo di scambio, di investimento, come prodotti di riserva di valore o essere utilizzate in casinò online. L'obiettivo della direttiva è coprire tutti i possibili usi delle valute virtuali.

Ecco il motivo per cui viene introdotta la riflessione relativa alla correlazione tra anonimato e flussi di denaro verso le cellule terroristiche: "i prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso legale (vale a dire le monete e le banconote considerate a corso legale e la moneta

elettronica di un paese, accettate quale mezzo di scambio nel paese emittente) e i prestatori di servizi di portafoglio digitale non sono soggetti all'obbligo dell'Unione di individuare le attività sospette. Pertanto, i gruppi terroristici possono essere in grado di trasferire denaro verso il sistema finanziario dell'Unione o all'interno delle reti delle valute virtuali dissimulando i trasferimenti o beneficiando di un certo livello di anonimato su queste piattaforme. È pertanto di fondamentale importanza ampliare l'ambito di applicazione della direttiva (UE) 2015/849 in modo da includere i prestatori di servizi la cui attività consiste nella fornitura di servizi di

cambio tra valute virtuali e valute legali e i prestatori di servizi di portafoglio digitale. Ai fini dell'antiriciclaggio e del contrasto del finanziamento del terrorismo (AML/CFT), le autorità competenti dovrebbero essere in grado di monitorare, attraverso i soggetti obbligati, l'uso delle valute virtuali. Tale monitoraggio consentirebbe un approccio equilibrato e proporzionale, salvaguardando i progressi tecnici e l'elevato livello di trasparenza raggiunto in materia di finanziamenti alternativi e imprenditorialità sociale".

Laddove sono esplicitati i rischi rivenienti dall'anonimato che caratterizza molte monete digitali, si evidenzia la conseguente necessità di

prevedere che i prestatori di valuta si conformino alla disciplina prevista dalla nuova direttiva (si dice, in questo caso, che costoro saranno dei "soggetti obbligati"), applicando – fra l'altro – i controlli previsti dall'adeguata verifica del cliente.

Per contrastare tali rischi le unità nazionali di informazione finanziaria dovrebbero quindi poter ottenere informazioni che consentano loro di associare gli indirizzi della valuta virtuale all'identità del proprietario di tale valuta.

L'anonimato non è completamente debellato, ma soltanto – pur se fortemente – limitato: gli scambi sono lecitamente consentiti con le carte

prepagate al di sotto di soglie minime di spesa, pari a 150 euro per gli acquisti in negozio e pari a 50 euro per gli acquisti online. Al di sopra di tali soglie, entrano invece in vigore tutte le prescrizioni finalizzate ad uno stretto monitoraggio dei flussi di danaro per poter ricostruire eventuali illeciti nell'ottica del miglior "follow the money".

Il Parlamento Europeo ha inserito nel testo anche una definizione in grado di perimetrare l'ambito d'azione degli intermediari che consentono operazioni con valuta virtuale. La direttiva, infatti, aggiunge anche la figura del "prestatore di servizi di portafoglio digitale", ossia il "wallet", definendolo come "un soggetto che fornisce servizi di

salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali". Laddove non fosse possibile identificare il "proprietario" del wallet (perché, ad esempio, in possesso solo di un paper wallet), una de-anonimizzazione del soggetto che si accinge a convertire la criptovaluta potrebbe avvenire ad opera dell'exchange provider [9].

Uno sviluppo estremamente interessante può essere rappresentato dall'opportunità offerta agli Identity Provider di rilasciare delle credenziali che consentano di accedere al wallet, in modo tale che la generazione delle chiavi pubbliche[9] in esso riprodotte sia

riconducibile a un soggetto opportunamente identificato [8].

Le valute virtuali, comunque, non dovrebbero essere confuse con:

- la moneta elettronica, come definita dalla cosiddetta II direttiva sulla moneta elettronica, la "EMD2" del Parlamento europeo e del Consiglio"[10];
- il più ampio concetto di "fondi", come definiti dalla cosiddetta direttiva PSD2 del Parlamento europeo e del Consiglio[11];

- il valore monetario utilizzato per eseguire operazioni di pagamento nel perimetro di dispensa previsto per i cc.dd. "strumenti a spendibilità limitata[12] e per le operazioni effettuate tramite l'impiego del credito telefonico[13];
- le valute di gioco che possono essere utilizzate esclusivamente all'interno di un determinato ambiente di gioco.

Maggior trasparenza e maggior controllo, dunque, per una normativa nata per limitare le possibilità di finanziamento del terrorismo, ma che avrà conseguenze ben più incisive a livello di sistema nell'istituto delle criptovalute.

Quindi, a breve, il Giappone non sarà più l'unico grande paese ad aver riconosciuto ufficialmente le criptovalute, ma entro il 2020, si aggiungeranno anche Germania, Francia, Italia, Spagna e tutte le altre nazioni che fanno parte dell'Unione Europea.

Ergo, la moneta "fiat", che istituisce un sistema monetario che permette una creazione di denaro teoricamente illimitata e a costo zero per lo Stato, non

potrà sottrarsi al confronto con la moneta virtuale.

I sostenitori delle criptovalute, sanno benissimo che la moneta “fiat” ha tre caratteristiche obbligatorie:

- è un monopolio dell’autorità riconosciuta, ad esempio lo Stato, che agisce in solido con la sua Banca Centrale. Lo Stato dunque si troverà al vertice del sistema bancario e della piramide monetaria.
- non è convertibile, cioè non deve essere emessa nei limiti del possesso di

un dato materiale (ad esempio, l'oro). Dal 1971 è stato abolito il Gold Standard, perciò in tutto il mondo le monete non devono più essere emesse nei limiti dell'oro di cassa degli Stati. Quindi le monete sovrane non hanno più un limite teorico di emissione;

- è fluttuante: lo Stato non si impegna più a garantire una promessa di pagamento fissa in moneta estera. Il valore della moneta sui mercati

internazionali può quindi variare e lo Stato stesso può modificarlo, a seconda delle necessità.

In virtù di ciò, declinano un indice di argomenti a favore della moneta virtuale, che possono essere riassunti nei seguenti passi:

- la criptovaluta non richiede intermediazione: chi ottiene la moneta ha un modo sicuro di mantenerne il possesso, senza doverla prestare ad una banca. Bisogna ribadire, infatti, che nel sistema attuale i cittadini

non sono affatto proprietari dei soldi che possiedono, eccetto che del contante (il cui utilizzo è sempre più limitato dalle leggi statali). I soldi tenuti in banca sono, come specificato anche dal codice civile, di proprietà della banca, e i correntisti figurano come creditori. Per le criptovalute, il reale proprietario della moneta è chi ottiene la moneta stessa e non rappresenta un mero creditore di una

banca;

- non ci sono costi di intermediazione, ad eccezione della bassa commissione per la creazione dei blocchi della Blockchain;
- non è necessario fidarsi di un ente che garantisca il valore del denaro scambiato;
- il denaro non è sequestrabile e la transazione è riconosciuta da chiunque accetti il protocollo;
- i costi di transazione sono fissi e molto bassi;

- i tempi di transazione sono veloci e non variano in base alla distanza geografica o alla diversa giurisdizione;
- non è modificabile arbitrariamente la quantità[14];
- non ci sono effetti redistributivi fra creditore e debitore dovuti ai cambiamenti dei tassi di interesse decisi arbitrariamente da un ente centrale, che può perseguire interessi di parte
- non c'è rischio di crisi

sistemica scatenato da un'eccessiva cessione di credito.

In conclusione, detti sostenitori affermano che lo Stato ha minori strumenti di controllo sull'economia, pertanto, può lasciare spazio a un più efficiente equilibrio di libero mercato. Non ci sarebbe il rischio di spirali inflattive, bolle speculative e cicli di boom e recessione, che comportano instabilità, inefficienza ed effetti redistributivi. Quest'ultimi non seguono criteri meritocratici o di utilità sociale, perciò possono essere economicamente inefficaci e moralmente controversi.

4. 1.4. DEFINIZIONE GIURIDICA DEI *BITCOIN*

Dal quadro sopra esposto, si comprende agevolmente come non sia affatto di immediata individuazione la categoria giuridica all'interno della quale declinare la fattispecie del bitcoin.

Gli operatori oscillano tra tre diverse qualificazioni circa la natura delle cosiddette criptovalute:

- mezzo di pagamento;
- commodity (un vero e proprio bene);
- security (un'obbligazione o un

titolo rappresentativo di un bene o servizio).

Ergo, si individuano tre tipi di moneta:

- merce (commodity money);
- moneta rappresentativa (representative money);
- moneta fiat (fiat money).

La cripto moneta integra le tre funzioni, ma non è moneta merce, dato che non ha valore intrinseco, non è moneta rappresentativa, poiché non ha alcun sottostante e non rappresenta nulla se non sé stessa, e non è nemmeno moneta fiat, non essendo stata emessa da alcun

ente.

Il Comitato IVA, Organo consultivo della Commissione Europea istituito ai sensi dell'art. 398 della Direttiva 2006/112/CE (c.d. "Direttiva IVA") non considera il bitcoin come una tipologia di "moneta elettronica", in quanto la medesima viene definita come "il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento".

La moneta elettronica, infatti, viene emessa in cambio di fondi espressi in unità di calcolo tradizionali (ad

esempio, euro), preservando così un legame con le valute aventi corso legale [10]. La moneta elettronica può essere emessa solo da determinate categorie di soggetti individuati dall'art. 1, par. 1, della Direttiva 2009/110/CE, quali banche, istituti di moneta elettronica e Stati membri. In dottrina, un ulteriore elemento di differenziazione della moneta elettronica rispetto al bitcoin è individuato nel fatto che la seconda non può assolvere la condizione di costante rimborsabilità (e, quindi, conversione in valuta legale) richiesta dall'art. 11 della citata Direttiva [11].

Già nel 2015 la Banca d'Italia definiva le valute virtuali come "rappresentazioni digitali di valore, utilizzate come mezzo

di scambio o detenute a scopo di investimento, che possono essere trasferite, archiviate e negoziate elettronicamente", avvertendo, tuttavia, che l'utilizzo del termine "valuta" veniva utilizzato semplicemente per identificare il fenomeno comunemente noto sotto tale denominazione, non volendo esprimere alcun giudizio sulla natura di tali strumenti [12].

Secondo alcune tesi, i bitcoin non sarebbero riconducibili al concetto di "moneta", poiché non rientrerebbero in alcuna delle ricostruzioni offerte dalle diverse teorie.

Per la teoria statalista, è lo Stato sovrano che crea la moneta sotto la sua autorità, attribuendole il potere

liberatorio delle obbligazioni pecuniarie (corso legale) e l'impossibilità per il creditore di rifiutarla come mezzo di pagamento (corso forzoso).

I bitcoin non potrebbero essere considerati moneta in base a tale teoria, in quanto strumenti privi del potere liberatorio ipso jure: ad oggi, infatti, nessuno Stato li ha riconosciuti come moneta avente corso legale o forzoso nel proprio ordinamento giuridico. Di conseguenza, un pagamento in bitcoin non potrebbe avere la forza liberatoria per il debitore e il creditore potrebbe sempre rifiutare di ricevere un pagamento in bitcoin, a meno che non abbia precedentemente stabilito con il debitore l'utilizzo di tale strumento [13].

Nella teoria economica, invece, la moneta viene definita in chiave essenzialmente funzionale. Secondo questa lettura, la moneta assolve tre funzioni principali:

- mezzo di scambio (può essere utilizzata per l'acquisto di beni e servizi);
- riserva di valore (ha l'attitudine ad assicurare la conservazione nel tempo del proprio potere di acquisto, potendo essere oggetto di risparmio per la spendita futura);
- unità di conto

(costituisce lo strumento di misurazione del valore dei beni, dei servizi e di altri attivi patrimoniali) [1].

Sul punto, sebbene le opinioni non siano univoche, sembra più convincente la tesi secondo cui i bitcoin sarebbero in grado di assolvere solo parzialmente le suddette funzioni [14].

Per monete tradizionali, infatti, si intendono le monete aventi corso legale: sono mezzi di pagamento stabili grazie all'azione delle banche centrali, ma soprattutto per effetto del loro riconoscimento legislativo. Ai sensi dell'art. 1277 del Codice Civile (debito

di somma di danaro), il creditore che le riceve è obbligato per legge a considerare il debito estinto dal pagamento in moneta legale. Pertanto, sembrerebbe che la moneta virtuale non sia assimilabile alla moneta tradizionale, trattandosi di uno strumento di scambio "convenzionale", utile allo scopo sino a quando non vi sia qualcuno disposto ad accettarlo [15].

La funzione di "mezzo di scambio" sarebbe, infatti, ostacolata dal fatto che bitcoin è uno strumento fondato su basi meramente convenzionali e ad oggi ha ancora un basso livello di accettazione tra il pubblico generale. Inoltre, l'alta volatilità dei tassi di cambio renderebbe bitcoin inutilizzabile come "riserva di

valore", anche nel breve termine. Per di più, la bassa accettazione e l'alta volatilità messe insieme finirebbero per rendere i bitcoin inadeguati per l'utilizzo come "unità di conto", considerata l'impossibilità di fare affidamento sul relativo potere di acquisto [16].

Nel settore delle criptomonete non vi è ancora nulla di specifico e le osservazioni sono frutto di ragionamenti comparatistici con discipline già presenti nel nostro ordinamento al fine di comprendere se quella determinata disciplina possa essere applicata, in qualche modo, al mondo delle criptovalute, ovviamente senza presunzione di esaustività né

completezza data l'incertezza della materia.

Allo stato attuale, quindi, nonostante i bitcoin abbiano un'apparenza tecnica molto simile alla moneta scritturale e/o elettronica, non sarebbe possibile qualificarli come "valuta" (poiché non hanno corso legale), né come "moneta" (in quanto non assolvono perfettamente le funzioni richieste dalla teoria economica) [17].

Altri autori condividono una terza tesi, c.d. teoria sociale, secondo cui la moneta sarebbe un fenomeno sociale, poiché direttamente riconducibile alla volontà delle parti, libere di stabilire come disciplinare le proprie transazioni. In tal senso, "bitcoin dovrebbe

considerarsi moneta, seppure non avente corso legale.

1.4.1 Prodotto digitale, bene immateriale

Il bitcoin, data la sua natura incorporea, potrebbe essere visto come un bene immateriale, ovvero una merce o un prodotto memorizzabile in forma digitale (digital product) [10].
Secondo l'articolo 810 del Codice Civile, “sono beni le cose che possono formare oggetto di diritti”. Tradizionalmente, immateriali sono i beni che non hanno consistenza fisica, ma che posseggono un valore economico (opera dell’ingegno, marchi ecc.);

tuttavia, il concetto di “cosa” richiede materialità. Inoltre, se è indubbio che le monete virtuali abbiano un valore economico, siano oggetto di transazione e posseggano una natura dematerializzata, maggiori perplessità suscitano in merito alla loro fungibilità, dato che la propria stringa alfanumerica è unica. Ad adiuvandum, atteso che la dottrina tradizionale ritiene che possano essere comprese nella pur ampia categoria dei beni immateriali solo quelle entità che realizzino un apporto creativo e soddisfino l’ulteriore requisito della riproducibilità [18], non essendo le criptovalute opera dell’ingegno, si reputa che possano considerarsi quali beni fungibili.

In soccorso giunge anche il Working Paper n. 854 del 2015 del Comitato IVA, in cui si può individuare una certa preferenza per la qualificazione come "effetto commerciale", inteso come strumento che implica il trasferimento di denaro, attese le conseguenze che comporterebbe una categorizzazione nella branca dei prodotti digitali: l'uso continuativo dei bitcoin negli scambi commerciali potrebbe essere considerato come l'esercizio di un'attività economica (intesa come sfruttamento di un bene immateriale), il che implicherebbe l'acquisizione dello status di soggetti passivi ai fini IVA per gli utilizzatori dei bitcoin.

Dunque, non sembrerebbe praticabile la

via del semplice inserimento dei bitcoin all'interno della categoria dei "beni giuridici", stante l'impossibilità di un pacifico inquadramento degli stessi sia tra i "beni materiali" (giacché, difatti, non esistono nella realtà, se non come sequenza numerica su di un computer), sia tra i "beni immateriali" (tenuto conto che questi ultimi sono tipici: il diritto sul bene immateriale esiste se esiste una norma che lo riconosce) [19].

D'altro canto, neppure l'assimilazione del bitcoin alla nozione di "documento informatico" ai sensi del Codice dell'Amministrazione Digitale (D. Lgs. n. 82/2005) sarebbe fondata, in quanto concernente un concetto del tutto distinto. L'art. 1, co. 1, lett. p) del D.

Lgs. n. 82/2005 descrive il documento informatico come "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti", ossia, come qualcosa che non ha valore in sé, ma solo in collegamento con l'atto, il fatto o il dato giuridicamente rilevante di cui fornisce una rappresentazione. Come evidenziato in dottrina, "nel caso del bitcoin, invece, lo script digitale che lo costituisce non rappresenta alcunché, ma risulta essere un valore e come tale spendibile per la soddisfazione di interessi del proprietario dello stesso" [20].

In linea con le caratteristiche della tecnologia utilizzata dalla Blockchain, il bitcoin potrebbe essere inquadrato alla

stregua di un documento informatico – provvisto di un suo valore di uso e di scambio per effetto del consenso sociale all'accettazione quale mezzo di pagamento – recante dati ed informazioni giuridicamente rilevanti e sottoscritto da una progressione di firme elettroniche attestanti, con una sorta di catena di diritti, l'avvenuta validazione della propria e dell'altrui legittimazione al perfezionamento di una certa transazione. Conseguentemente, "il Bitcoin sarebbe idoneo a garantire, seppur su basi pseudonime, la legittimazione e l'adempimento automatico del possessore, in quanto elementi negoziali direttamente incorporati quali dati e rappresentazioni

informatiche giuridicamente vincolanti ex ante, e non lasciati al solo (mutevole) giudizio ex post sulla meritevolezza degli scopi economici conseguibili con il loro utilizzo" [13]. Ma tale inquadramento appare meramente ricognitivo di alcune caratteristiche delle valute virtuali e sfugge l'esigenza di offrire una disciplina protettiva e regolatoria dei diversi interessi ad esse sottese [21].

1.4.2 Mezzo di pagamento o strumento di investimento

Sebbene l'Autorità di Vigilanza non abbia voluto prendere posizione sulla qualificazione giuridica delle

criptovalute, le indicazioni preliminari dalla stessa fornite sembrano aver preannunciato le due strade poi effettivamente intraprese dalla dottrina al fine di valutarne l'inquadramento nell'ambito dell'ordinamento nazionale: una prima, che tende a valorizzare l'utilizzabilità delle criptovalute come mezzo di pagamento, e una seconda che analizza il fenomeno dalla prospettiva dell'investitore, tenendo conto dello scopo di investimento che può caratterizzare l'operatività in valute virtuali [1].

Secondo il Working Paper della Direttiva IVA, il bitcoin, operando quale strumento di pagamento, dovrebbe rientrare nella nozione di effetto

commerciale (negotiable instrument), in linea con la giurisprudenza della Corte di Giustizia[15]. Potrebbe, però, emergere una criticità in merito alla trasferibilità della valuta virtuale: gli effetti commerciali attribuiscono, infatti, il diritto ad esigere una somma di denaro, mentre il bitcoin può essere scambiato contro denaro solo su base volontaria, ovvero solo se viene accettato da un altro soggetto [10].

Il Comitato IVA, inoltre, solleva dubbi sull'idoneità del bitcoin ad assolvere la funzione di riserva di valore, per la mancanza di un'Autorità di vigilanza e supervisione, nonché per l'elevata volatilità che rende concreto il rischio di una bolla finanziaria. Sempre ad

avviso del Comitato, il regime di esenzione previsto dall'art. 135, par. 1, lett. E9, della Direttiva IVA per "le operazioni, compresa la negoziazione, relative a divise, banconote e monete con valore liberatorio" deve intendersi riferito esclusivamente alle valute aventi corso legale e non alla valuta virtuale, che rappresenta un mezzo di pagamento basato unicamente sull'accettazione volontaria di coloro che lo utilizzano [22].

La moneta virtuale potrebbe astrattamente essere qualificata come strumento finanziario. In effetti, essa può essere "estratta" o acquistata anche con finalità di investimento dei propri risparmi, per guadagnare dall'atteso

aumento di valore della stessa; inoltre, esistono siti ove è possibile acquistare e vendere monete virtuali come se fossero veri e propri titoli azionari [15]. Tuttavia, in ossequio a quanto disposto dalla Sezione C dell'Allegato I del Testo Unico in materia di intermediazione Finanziari (TUF) "gli strumenti di pagamento non sono strumenti finanziari". Ne deriva che, se da un lato le monete virtuali possono avere anche finalità di investimento, dall'altro in esse predomina la funzione di mezzo di pagamento [23].

Più plausibile sembrerebbe, invece, la collocazione dei bitcoin nella categoria dei "prodotti finanziari", identificati dall'art. 1, comma 1, lett. u) del TUF

come “gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria…”.

Secondo tale definizione, il genus dei prodotti finanziari è rappresentato dalla somma di due sottocategorie, una relativa agli “strumenti finanziari”, tendenzialmente “chiusa” e formata dagli strumenti tipizzati dal legislatore nell’art. 1, comma 2, del TUF, e l’altra relativa ad “ogni altra forma di investimento di natura finanziaria”, di carattere “aperto” e destinata ad essere “riempita” di volta in volta attraverso un’opera di interpretazione e analisi del caso concreto.

Come la CONSOB[16] ha già avuto modo di chiarire, rientrano in quest’ultima

sottocategoria le proposte di investimento che implicano la compresenza dei seguenti tre elementi:

- impiego di capitale;
- aspettativa di rendimento di natura finanziaria;
- assunzione di un rischio direttamente connesso e correlato all'impiego di capitale.

L'Autorità di Vigilanza, in particolare, si è in presenza di un "investimento di natura finanziaria" ogniqualvolta il risparmiatore impieghi il proprio denaro con un'aspettativa di profitto, mentre si è in presenza di un "investimento di

consumo" quando la spesa è finalizzata al godimento del bene, ossia, è volta a trasformare le proprie disponibilità in beni reali idonei a soddisfare in via diretta i bisogni non finanziari del risparmiatore. A parere della CONSOB "per configurare un investimento di natura finanziaria, non è sufficiente che vi sia accrescimento delle disponibilità patrimoniali dell'acquirente (cosa che potrebbe realizzarsi attraverso talune modalità di godimento del bene come ad esempio con la rivendita del diamante) ma è necessario che l'atteso incremento di valore del capitale impiegato (ed il rischio ad esso correlato) sia elemento intrinseco all'operazione stessa". Ciò che rileva, quindi, è l'effettiva e

predeterminata promessa, all'atto dell'instaurazione del rapporto contrattuale, di un rendimento collegato al bene [17].

Ne deriva che, qualora l'acquisto di bitcoin dovesse assumere la funzione di "investimento di natura finanziaria" nei termini sopra esposti, la causa concreta dell'acquisto (e quindi del rapporto contrattuale instaurato tra il venditore e il compratore della criptovaluta) potrebbe determinare l'attrazione dei bitcoin nella nozione di "prodotto finanziario" ex art. 1, comma 1, lett. u) del TUF, con tutte le conseguenze che ne derivano in punto di disciplina applicabile (in particolare, la normativa in materia di sollecitazione del pubblico

risparmio ai sensi degli artt. 94 e ss. del TUF e le regole riguardanti la promozione e il collocamento a distanza di prodotti finanziaria ex art. 32 del TUF e relative disposizioni attuative) [11].

Parte della dottrina si è interrogata se le criptomonete potessero rientrare nella nozione di "strumento di pagamento" di cui all'art. 1, comma 1, lett. s) del D. Lgs. n. 11/2010, riscontrando poi una possibile obiezione nell'"interpretazione corrente della direttiva sui servizi di pagamento che ne limita la portata ai soli pagamenti denominati in moneta legale" [24].

Negli Stati Uniti, la normativa ha dettagliatamente disciplinato la tassazione e gli oneri dichiarativi circa

le criptovalute, già nel 2014, con la Notice 2014-21, in cui le criptovalute vengono considerate non come mezzi di pagamento, bensì quali commodity soggette a dichiarazione e tassazione ogniqualvolta generino plusvalenze.

Inoltre, in base alla giurisprudenza della Corte di Giustizia[17], uno strumento può qualificarsi come titolo se:

- l'acquisizione dello strumento comporta un trasferimento di diritti relativi all'emittente;
- il trasferimento di tale strumento ha natura finanziaria, nel senso che esso può essere scambiato per denaro o

beni.

Alle operazioni che prevedono l'utilizzo del bitcoin può essere attribuita natura finanziaria, posto che la valuta virtuale possa essere considerata come uno strumento con un valore nominale idoneo a essere scambiato. Tuttavia, non risulterebbe soddisfatto l'ulteriore requisito richiesto per la qualificazione come titolo, in quanto il bitcoin non attribuisce al suo possessore alcun diritto, credito o altra pretesa nei confronti del soggetto emittente o di altra entità [10].

1.4.3 La pronuncia della Corte di Giustizia Europea e la recente

sentenza della Corte d'Appello di Berlino

La Corte di Giustizia dell'Unione Europea, Sez. V, con la sentenza C 264/2014, in data 22/10/2015, ha statuito che la valuta virtuale bitcoin non è un bene materiale, bensì "un mezzo di pagamento utilizzato in maniera corrispondente a mezzi legali di pagamento".
Precisa la Corte che "La valuta virtuale bitcoin, essendo un mezzo di pagamento contrattuale, non può essere considerata, da una parte, né come un conto corrente né come un deposito di fondi, un pagamento o un versamento. D'altra parte, a differenza dai crediti, dagli

assegni e dagli altri effetti commerciali, di cui all'articolo 135, paragrafo 1, lettera d), della direttiva IVA, essa costituisce un mezzo di pagamento diretto tra gli operatori che l'accettano".

Inoltre, "le valute virtuali sono diverse dalla moneta elettronica come definita dalla citata direttiva 2009/110/CE, in quanto, a differenza di tale moneta, nel caso delle valute virtuali i fondi non sono espressi nell'unità di calcolo tradizionale, ad esempio in euro, ma nell'unità di calcolo virtuale, ad esempio il 'bitcoin'" (cit. Corte di Giustizia dell'Unione Europea, n. 264/14).

Pertanto, la Corte, facendo leva sul principio di neutralità fiscale, giunge ad

assimilare i mezzi di pagamento contrattuali ai mezzi di pagamento legali.

Ne discende che, se consideriamo la valuta virtuale quale strumento finanziario, le sue funzioni sono due:

- solutoria;
- strumento d'investimento.

Per la funzione solutoria, in accoglimento della teoria della c.d. funzione sociale della moneta [25] la scelta della tipologia di danaro utilizzabile viene rimessa ai singoli individui, i quali, volontariamente, possono scegliere anche valute non aventi corso legale.

Per la funzione di strumento di investimento, venendo in rilievo la tutela del consumatore quale contraente debole, si applicano le norme previste in tema di intermediazione finanziaria e/o del Codice del Consumo.

Di fatto le più recenti pronunce e prese di posizione amministrative assimilano le criptovalute a mezzi di pagamento, se non a vere e proprie valute.

Nella stessa direzione l'Agenzia delle Entrate italiana con la Risoluzione 72/E del 2 settembre 2016, che porta ad un livello ulteriore il ragionamento della Corte di Giustizia UE, arrivando ad equiparare le criptovalute alle valute straniere.

L'Agenzia delle Entrate, in assenza di

una normativa specifica applicabile al sistema delle valute virtuali, ha ritenuto che la citata sentenza dei Giudici europei debba costituire un punto di riferimento sul piano del trattamento tributario, tanto che l'attività di compravendita di criptovalute per conto terzi, svolta in modo professionale ed abituale, costituisca un'attività economica rilevante ai fini IVA, IRES e IRAP; mentre l'acquisto e la vendita per conto proprio assume rilevanza ai fini delle imposte dirette.

Il Tribunale di Verona, sempre in assenza di una normativa specifica del settore, con sentenza n. 195 del 24 gennaio 2017, ha ritenuto che la compravendita di valute virtuali, come il

bitcoin, vada qualificata alla stregua di uno strumento finanziario, costituito da una moneta, sfruttabile per compiere transazioni, possibili grazie ad un software open source e ad una rete peer to peer.

Il giudice adito, constatando l'assoluta mancanza di qualsiasi forma contrattuale scritta, nonché di qualsivoglia informativa precontrattuale, applicava alla fattispecie concreta la tutela consumeristica di cui agli artt. 67 e ss. del Codice del Consumo, dichiarando la nullità del contratto e l'obbligo di restituire quanto ricevuto [15].

L'operazione di cambio di valuta tradizionale, contro unità di valuta virtuale bitcoin e viceversa, effettuate a

fronte del pagamento di una somma corrispondente al margine costituito dalla differenza tra il prezzo di acquisto delle valute e quello di vendita praticato dall'operatore ai propri clienti, è qualificabile, dal lato dell'operatore, come attività professionale di prestazioni di servizi a titolo oneroso, svolta in favore di consumatori.

La predetta compravendita è un'operazione ad alto rischio per il risparmiatore, con il conseguente obbligo, per colui che ne pubblicizzi la vendita, in proprio o per conto terzi, di informare, preliminarmente, l'utente interessato all'acquisto sui rischi connessi all'investimento (c.d. informativa precontrattuale), così come

stabilito dagli artt. 67 e ss. del Codice del Consumo in tema di commercializzazione a distanza di servizi finanziari ai consumatori; in particolar modo, il promotore dell'operazione di vendita è tenuto all'applicazione delle disposizioni più rigorose previste dalla normativa di settore che disciplina l'offerta del servizio o del prodotto interessato.

L'indagine circa la qualificazione giuridica delle criptovalute ci sta portando, finora, verso la possibilità di considerarle alla stregua di "monete", seppur virtuali.

Ci si potrebbe la domanda se l'istituto della proprietà e del possesso si possano applicare al mondo delle

criptomonete.

Nel nostro ordinamento vigono i concetti giuridici della proprietà, possesso e detenzione ove la proprietà rappresenta uno stato di diritto, mentre il possesso e la detenzione sono due stati di fatto.

Il nostro Codice Civile, infatti, all'art. 832 contempla espressamente la proprietà[18] come il diritto principale tra i c.d. diritti reali[19] ed attribuisce al titolare una signoria piena ed esclusiva sul bene che ne è oggetto.

Come sappiamo, la proprietà è un diritto imprescrittibile, ai sensi dell'art. 948 c.c. terzo comma; mentre l'art. 1140 c.c. definisce il possesso come "il potere di fatto sulla cosa che si manifesta in

un'attività corrispondente all'esercizio della proprietà o di altro diritto reale. Si può possedere direttamente o per mezzo di altra persona, che ha la detenzione della cosa".

La proprietà, pertanto, è un vero e proprio diritto soggettivo, che permette al suo titolare di esercitare una posizione giuridicamente di vantaggio rispetto alla generalità dei consociati.

Considerato che il possesso viene concepito nel nostro ordinamento come relazione materiale con una cosa e non come esercizio di fatto di un apparente diritto, si può già percepire come non sia di agevole definire la detenzione di una criptovaluta, in quanto bene non tangibile e immateriale.

Se facciamo, però, riferimento al principio espresso dall'art. l del Protocollo n. l della Convenzione per la Salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, volto a garantire il pacifico godimento del possesso, sia stato reputato applicabile anche al possesso di beni immateriali ed opere intellettuali, si potrà sicuramente sostenere l'applicabilità dell'istituto del possesso al bene della cripto moneta, sia essa custodita fisicamente in un paper wallet o un wallet hardware, sia considerata software o presente online con accesso tramite password[20].

Recentemente, la Corte di Appello di Berlino ha dovuto pronunciarsi in merito ad una sanzione comminata a spese di un

exchange tedesco che operava senza licenza.

È bene tener presente che, in precedenza, l'Autorità federale di vigilanza finanziaria (BaFin) della Germania aveva classificato il bitcoin come uno strumento finanziario. In particolare, il Federal Financial Supervisory Authority (BaFin) aveva contraddistinto il bitcoin come unità di conto nel Testo Unico Bancario, cosa che rendeva obbligatorio in Germania il permesso per commerciare criptovalute. La sentenza ha escluso tale classificazione e ha deciso che la criptovaluta non soddisfa questa definizione, ai sensi della legge bancaria tedesca (KWG).

Secondo la pronuncia, “il trading con bitcoin non è punibile perché bitcoin non è uno strumento finanziario ai sensi del KWG”.

A causa della natura decentralizzata del bitcoin, non regolata da una banca centrale o da qualsiasi altra autorità pubblica, lo stesso non può essere considerato come una moneta fiat e le norme KWG non devono essere ritenute valide per quanto riguarda gli scambi in bitcoin.

La Corte d'Appello di Berlino, nello specifico, ha respinto un procedimento penale contro l'operatore di una piattaforma di commercio bitcoin locale, mentre l'esecuzione tedesca aveva arrestato l'amministratore per aver

facilitato gli scambi di strumenti finanziari come il bitcoin senza ottenere un permesso BaFin. Mentre il distretto Berlin-Tiergarten aveva condannato l'imputato per la fornitura di servizi finanziari, il tribunale regionale di Berlino ha annullato la sentenza, affermando che BaFin interpretava erroneamente lo status giuridico del bitcoin. La Corte d'appello della divisione criminale 4th di Berlino ha avvalorato la sentenza della Corte regionale, confermando che i regolatori tedeschi estendono la portata del diritto penale al bitcoin senza sincronizzarlo con gli atti bancari.

Dunque, né la banca centrale né alcuna autorità pubblica emettono bitcoin. La

valuta digitale manca di riconoscimento generale e di un valore stabile che potrebbe consentire al suo uso di confrontare beni o servizi. Pertanto, non può ottenere lo status di unità di conto – o strumenti finanziari – contrariamente a quanto è stato applicato dal BaFin.
La sentenza ha anche messo in luce le questioni relative alla vendita e all'acquisto di bitcoin in Germania, stabilendo che il commercio di bitcoin non è soggetto a permessi o licenze.

1.5 *SMART CONTRACTS*

Come noto, il perfezionamento di alcuni atti richiede l'intervento di una parte

terza le cui dichiarazioni (es. notaio) o risultanze (es. Registri immobiliari) hanno il valore di certificare erga omnes quanto dichiarato o registrato (sono le c.d. Third Trusted Parties). Gli atti pubblici, pertanto, necessitano sia della pubblicità dichiarativa (necessaria a far sì che il relativo contratto sia opponibile ai terzi, ad esempio, la trascrizione dell'acquisto di un immobile nei registri immobiliari), sia della pubblicità costitutiva (necessaria alla costituzione dell'accordo stesso, ad esempio, l'iscrizione dell'ipoteca nei registri immobiliari).

Gli smart contracts, invece, non hanno più bisogno della presenza di Third Trusted Parties per legittimare le

transazioni.

I “contratti intelligenti”, digitalizzati, distribuiti e immutabili, regolano la sfera giuridico-patrimoniale fra più parti, rendendo le clausole contrattuali, parzialmente o totalmente automatizzate.

Si tratta, dunque, di protocolli informatici auto ottemperanti, che servono a far rispettare l’esecuzione di un contratto.

Uno smart contract potrebbe essere definito come un documento informatico, ai sensi dell’art. 1 lett. p) del decreto legislativo D. Lvo n. 82/2005 (Codice dell’amministrazione digitale – C.A.D.) secondo cui è documento informatico “il documento elettronico che contiene la rappresentazione informatica di atti, fatti

o dati giuridicamente rilevanti".

Ai sensi dell'art. 20 comma 1 bis del C.A.D. uno smart contract potrebbe, dunque, soddisfare il requisito della forma scritta, sia per la facoltà di libera valutazione da parte del giudice di tale elemento sia in quanto, in alcune ipotesi, lo stesso potrebbe essere direttamente riferibile alle parti che lo hanno stipulato, tramite l'associazione alle firme elettroniche degli stessi.

Il termine "smart contract" venne coniato per la prima volta nel 1996 da Nick Szabo [26]; quindi ancor prima dell'introduzione della Blockchain.

L'idea originaria era quella di creare una serie di clausole che potevano essere incorporate nell'hardware e nel

software con cui ci relazioniamo, in modo da rendere gravoso l'inadempimento. Partendo dal funzionamento degli automi finiti (ossia dei circuiti che realizzano le espressioni booleane) Szabo proponeva l'introduzione di contratti da agganciare ai diritti di proprietà di beni digitali, regolati automaticamente proprio dai contratti, in modo da ridurre le ipotesi di inadempimento e i rischi per le parti.

L'autore suggeriva anche l'uso di tecniche crittografiche e di firme elettroniche per rendere sicure le transazioni nonché riconducibili ai soggetti che le ponevano in essere.

Quando si utilizza il termine smart contract, si fa riferimento di solito a due

principali categorie concettuali:
una inerente agli aspetti operativi, ovvero ai software che tipicamente sono attestati su una Blockchain. In questo caso detti software eseguono automaticamente alcune azioni inerenti ad obbligazioni e diritti e possono controllare determinati asset su un registro condiviso;
l'altra riferita a come gli Smart contract possano essere espressi e realizzati tramite il software. Questo comporta l'analisi di come possano essere redatti i contratti e come il linguaggio legale possa essere interpretato.
Tramite l'utilizzo della Blockchain, si potrebbe riuscire a sintetizzare le due categorie, realizzando contratti che siano

automatizzabili ed eseguibili da un computer, ma al contempo protetti dalla disciplina normativa che potrebbe andare a colmare quelle parti di accordo che non sono automaticamente eseguite all'interno della Blockchain stessa.

Sappiamo, dunque, che i "contratti intelligenti" si basano sulla tecnologia Blockchain (o, parimenti, la distributed ledger technology) che ne assicura la sicurezza, in quanto tutti i nodi controllano che nel libro mastro sia effettivamente eseguito ciò che è previsto dallo smart contract. La Blockchain rende le transazioni sicure, non hackerabili, né manomissibili. Pertanto, gli accordi stipulati vengono conclusi non per via di un contratto

scritto, bensì di un codice crittografico che al suo interno contiene i termini e le condizioni pattuite dalle parti, in forma digitale.

Considerato che con gli smart contracts non servono più intermediari (notai, giudici, avvocati ecc.) tantomeno una terza parte che certifichi il valore del contratto e lo risolva in caso di inadempienza, in quanto auto eseguibile, si possono conseguire dei risparmi in termini di tempo, nel redigere il contratto, e in termini di costi nel dover far redigere l'atto da qualcuno qualificato, nonché farlo rispettare.

Qualche difficoltà potrebbe verificarsi davanti ad un tribunale, per far rispettare un contratto che sia redatto unicamente

sulla base di un linguaggio di programmazione. È percepibile la complessità da parte del giudice di poter immediatamente comprenderne il significato, sia in termini strettamente giuridici sia, soprattutto, in termini di traduzione delle clausole contrattuali in linguaggio informatico, in quanto contengono formule complesse, che non si limitano a prevedere l'esecuzione di una certa azione al verificarsi di un determinato evento.

Se solo si tiene a mente la complessità dei sistemi giuridici, le specificità di un sistema rispetto ad un altro e le esperienze ed i tentativi di standardizzazione anche all'interno di un solo contesto, appaiono evidenti gli

ostacoli ed i problemi che sarebbe necessario superare.

Oggi sono presenti varie proposte che si concentrano prevalentemente nella formalizzazione di soluzioni per riuscire ad adeguare le complessità del linguaggio giuridico alle esigenze di una interpretazione "automatica" da parte di un computer (ad es. Common Accord[21], Legalese[22], Monax's Dual integration[23] ed i Ricardian Contract[24]).

Riepilogando, le caratteristiche principali degli smart contracts sono le seguenti:

- forma digitale;
- i singoli articoli, i termini e le condizioni

contrattuali esistono solo sotto forma di codici crittografici;

- questi "codici" possono essere letti non solo da persone, ma direttamente anche da hardware, quindi da oggetti (c.d. "Internet of Things");
- irrevocabili e immutabili: una volta "sottoscritto", il relativo accordo non può essere risolto e/o modificato dalle parti fino alla completa esecuzione del contratto, come originariamente voluto: il

contratto viene eseguito in modo totalmente automatico;

- distribuiti all'interno della Blockchain, che ne garantisce la sicurezza.

Detti contratti funzionano, quindi, secondo la logica "If this than that", o, più brevemente, "If, Then", ossia al verificarsi di una determinata condizione, si avrà un'azione, certificata e automatizzata.

Nella Blockchain non ci sono terze parti, non c'è un arbitro, ma semplicemente una transazione tra A e B. Lo smart contract, una volta scritto e lanciato, è immutabile (non si può modificare) e

distribuito (installato dentro la Blockchain, ove se ne conosce il codice e l'algoritmo, per cui, ogni variazione testimonierebbe che la transazione è falsa).

Gli smart contracts sono quindi i "mattoncini" di ogni "blocco" della "catena di blocchi" (Blockchain): in ogni blocco vengono "impacchettati" n smart contracts (cioè n codici crittografici). Successivamente, il blocco ("Blocco 1") diviene definitivo e immutabile: non potrà mai essere cancellato né modificato. L'unica opzione ammissibile al fine di dare efficacia al complesso contrattuale è che si passi al blocco successivo ("Blocco 2").

Ciò avviene mediante l'elaborazione di un complesso calcolo matematico, che soltanto i miners possono risolvere., ossia – come detto – gli operatori dotati di computer aventi un eccezionale potere computazionale.

In competizione tra loro, i miners cercano di risolvere l'articolato problema nel più breve tempo possibile: il primo tra questi che vi riesce, valida il passaggio al blocco successivo (e riceve, come premio, una piccola fee - ricompensa). La corretta soluzione del problema, immediatamente verificata da tutti gli altri miners, legittima la registrazione del passaggio dal Blocco 1 al Blocco 2, identica, in ognuno dei registri condivisi (distributed ledgers).

Di blocco in blocco, è possibile ricostruire il "percorso" di un determinato flusso di valore (si tratti di valore monetario, titoli ecc.).

Secondo il diritto italiano, un contratto per essere valido deve avere determinati requisiti, stabiliti dall'art. 1325 del codice civile, ossia l'accordo tra le parti, la causa, l'oggetto e la forma.

Pertanto, uno smart contract dovrebbe contenere gli elementi di cui al citato articolo di legge, peccato che all'interno di una Blockchain questi elementi risultino quantomeno di difficile individuazione e interpretazione: basti pensare quali difficoltà potrebbe avere un giudice nel pronunciarsi su vertenze di contratti che si presentano sotto forma

di codice crittografico.

Tuttavia, lo smart contracts conterrà la disciplina delle prestazioni che il predisponente si impegna ad effettuare al verificarsi di determinati eventi.

L'esecuzione sarà automatica, indipendentemente dalla vera e propria manifestazione di consenso dell'altra parte. Ai fini delle transazioni in bitcoin, lo smart contract provvede al trasferimento di asset digitali al verificarsi di una condizione specifica, quale il ricevimento di una criptovaluta.

Così, in una ICO, finalizzata alla creazione di un progetto, un soggetto A mette a disposizione l'idea per arrivare alla realizzazione del progetto, mentre, il soggetto B fornisce del denaro per il

raggiungimento dell'obiettivo. Lo smart contract opera automaticamente al conseguimento dello scopo, erogando all'investitore la "ricompensa" pattuita.

La varietà del contenuto semantico dei contratti è talmente vasta che, pur aumentando la complessità dei parametri per trasfondere le intenzioni delle parti in un linguaggio eseguibile, non servirebbe comunque a trovare una soluzione definitiva.

Articolare delle clausole attraverso la definizione di parametri può apparire semplice per quelle previsioni che afferiscono ad eventi o elementi numericamente certi (un termine, l'applicazione di un interesse, il pagamento di una somma) ma di certo

non può considerarsi una metodologia immediata e risolutiva per il contenuto di qualsiasi contratto.

La semplice trasposizione delle regole contrattuali in un codice software potrebbe non risolvere il problema.

Un processo di integrazione tra un contratto legale specifico e un contratto intelligente eseguito su un archivio dati distribuito potrebbe contribuire a individuare alcuni parametri considerati "dati primitivi" e altri di natura più complessa, come liste, fino a contenere vere e proprie espressioni intese come funzioni (ad esempio il calcolo degli interessi giornalieri).

La doppia integrazione porterebbe a una procedura automatica in cui un contratto

intelligente verrebbe collegato a un documento che potrà essere eseguito direttamente da un tribunale.

Si tratta solamente di un'ipotesi di soluzione se si vuole andare nella direzione di rendere i "contratti intelligenti", utili per automatizzare molte relazioni basate sui dati. Tuttavia, per essere esecutivi, i contratti intelligenti devono funzionare nei quadri giuridici esistenti, in cui tali quadri esistono già, eliminando un grado di incertezza nell'applicazione.

2. IL TRATTAMENTO FISCALE DEI BITCOIN

a cura di Fabio Pascucci

Sommario: 2.1 Inquadramento generale – 2.2 Ambito imposte indirette – 2.3 Ambito imposte dirette – 2.4 Disciplina ai fini della normativa antiriciclaggio.

2.1 INQUADRAMENTO GENERALE

La questione relativa al trattamento dei bitcoin è talmente sentita che, nel G20 tenutosi a Buenos Aires lo scorso 20 marzo 2018, sono stati posti vari temi sul tavolo, tra i quali il fenomeno delle criptovalute. In quell'occasione, è stato rivolto un invito generale a tutte le istituzioni a continuare a monitorare l e attività connesse alle valute del web, nonché valutare i loro rischi con una risposta multilaterale, se necessario.

Nelle more di interventi decisivi da parte degli Stati ed in assenza di una disciplina armonizzata, gli organi amministrati e giurisdizionali cercano continuamente di colmare le lacune in materia, fornendo soluzioni differenti

agli interrogativi avanzati dai contribuenti, soprattutto, sulla tassazione dei bitcoin.

Nel nostro Paese, dobbiamo distinguere, ovviamente, tra trattamento ai fini IVA e quello ai fini imposte dirette.

2.2 AMBITO IMPOSTE INDIRETTE

Alla questione di quale regime fiscale applicare alle criptovalute, le amministrazioni tributarie di alcuni Stati europei hanno cominciato a dare risposte, solo a partire dalla primavera del 2013.

Le giurisdizioni si sono mosse in ordine sparso fino al 2015, alcune sostenendo

che le criptovalute fossero beni immateriali (pertanto, ogni scambio tra soggetti Iva doveva essere assoggettato ad Iva) altre che fossero assimilabili a denaro (con conseguente trattamento Iva completamente diverso) assumendo così posizioni opposte, con la conseguenza inevitabile di valutare alcune criticità da parte di chi avesse voluto utilizzare i bitcoin come mezzo di pagamento/scambio intracomunitario.

Con la nota sentenza UE C-264/14, la Corte di Giustizia dell'Unione Europea ha interpretato autenticamente l'art. 135, par. 1, lett. e) della Direttiva 28 novembre 2006, n. 112, optando per l'esenzione della valuta virtuale dal campo di applicazione dell'Iva.

La pronuncia prende le mosse dalla controversia secondo la quale, il Sig. Hedqvist risultava titolare di un'attività di cambio esercitata con il supporto di una società di intermediazione, consistente nella compravendita di bitcoin in cambio di valute tradizionali, ottenendo un profitto dalla differenza tra i prezzi di acquisto e di vendita applicati.

La Commissione Tributaria svedese, adita dal Hedqvist, si era espressa chiaramente il 14 ottobre 2013 a favore dell'esenzione della sua attività dal pagamento dell'Iva.

L'Amministrazione finanziaria, di contro, non si era fermata, tanto da interpellare la Corte di Giustizia

Europea sull'interpretazione degli articoli 2 paragrafo 1 e 135 paragrafo 1 della Direttiva 2006/112/ce per chiarire il tema dell'assoggettamento o meno ad Iva del margine di guadagno derivante da operazioni di cambio valuta (da bitcoin in moneta tradizionale e viceversa) che il privato intendeva effettuare con la mediazione di una società

Secondo la Corte, la possibilità di inserire l'attività contestata tra le cessioni di beni doveva essere esclusa, in quanto i bitcoin non erano un "bene materiale", nel senso indicato dall'articolo 14 della Direttiva. I bitcoin rappresentano una valuta virtuale, generata in rete e scambiata tra gli utenti

attraverso un “indirizzo bitcoin” (equiparabile al numero di un conto corrente bancario) e che la Banca Centrale Europea ha definito “a flusso bidirezionale”, differente dalla moneta elettronica perché espressa in unità di calcolo virtuale e non tradizionale.

Pertanto, la valuta virtuale non ha altre finalità oltre a quella di mezzo di pagamento. Detta moneta, infatti, non trasferisce alcun diritto di proprietà e viene utilizzata unicamente per il cambio fra vari mezzi di pagamento.

Conseguentemente, le operazioni di “cambio valuta” non ricadono nella nozione di “cessione di beni” (art. 14 Direttiva Iva) piuttosto costituiscono prestazioni di servizi, ai sensi dell’art.

24 della citata Direttiva, effettuate a titolo oneroso.

L'attività del convenuto, dunque, si configurava come una prestazione di servizi a titolo oneroso ex articolo 2 paragrafo 1 lettera c) della Direttiva, in quanto tra il titolare e gli utenti ricorreva una relazione diretta ed un rapporto giuridico sinallagmatico ove "il compenso ricevuto dal prestatore costituisce il controvalore effettivo del servizio prestato al beneficiario".

L'esenzione dall'imposta deriva dalla natura stessa della criptovaluta: se la moneta virtuale viene accettata e utilizzata come mezzo di pagamento alternativo a quello legale a fronte di una somma pagata come differenza tra i

prezzi di acquisto e vendita, le attività di cambio di bitcoin in moneta tradizionale e viceversa, rientrano a pieno titolo tra le attività esenti dall'applicazione dell'Iva per le transazioni compiute all'interno del territorio europeo.

La Corte comunitaria ha sostenuto, quindi, che solo il contenuto dell'articolo 135 paragrafo 1 lettera e) della Direttiva Iva, concernente "divise, banconote e monete con valore liberatorio", avrebbe potuto giustificare l'esclusione delle operazioni sui bitcoin dal pagamento dell'Iva.

Le esenzioni sono state introdotte con l'obiettivo di risolvere le difficoltà sulla determinazione della base imponibile e l'importo stesso dell'Iva in Europa.

Le valute, nessuna esclusa, non possono essere né consumate, né diversamente sfruttate come beni, ma possono esclusivamente essere utilizzate per la loro funzione propria, ossia rendere agevole lo scambio di beni e di servizi all'interno di un determinato sistema economico (funzione propria di tutti mezzi di pagamento); ciò a prescindere dal vincolo legale (moneta tradizionale) o contrattuale-volontario (bitcoin) posto a presidio dell'efficacia liberatoria del mezzo di pagamento utilizzato (c.d. principio di neutralità dell'imposta) [15].

2.3 AMBITO IMPOSTE DIRETTE

Relativamente al trattamento della moneta virtuale ai fini delle imposte dirette, l'Agenzia delle Entrate, con la Risoluzione n. 72/E/2016, ha chiarito, in ossequio a quanto affermato dalla Corte di Giustizia dell'Unione europea nella predetta sentenza 22 ottobre 2015, causa C-264/14, che l'attività di intermediazione di valute tradizionali con bitcoin, svolta in modo professionale ed abituale, è rilevante agli effetti dell'Iva, Ires ed Irap ed è soggetta agli obblighi di adeguata verifica della clientela, di registrazione e di segnalazione.

È necessario distinguere tra società di capitali e persone fisiche non in regime di attività di impresa. Per le prime, la

cessione di valuta virtuale concorre alla determinazione del reddito di impresa per un importo pari al differenziale tra il prezzo di acquisto e quello di vendita. Tale elemento di reddito è ascrivibile ai ricavi (o ai costi) caratteristici di esercizio dell'attività di intermediazione esercitata e, pertanto, contribuisce quale elemento positivo (o negativo) alla formazione della materia imponibile soggetta ad ordinaria tassazione ai fini Ires e Irap. I bitcoin che a fine esercizio rimangono "in cassa", ossia nella disponibilità (a titolo di proprietà) della società, dovranno essere valutati secondo il cambio in vigore alla data di chiusura dell'esercizio e tale valutazione assumerà rilievo ai fini

fiscali, ai sensi dell'art. 9 del Testo Unico delle Imposte sui Redditi, approvato con D.P.R. 22 dicembre 1986, n. 917 (TUIR). Secondo l'Agenzia delle Entrate, il valore normale dei bitcoin potrebbe corrispondere alla media delle quotazioni ufficiali rinvenibili sulle piattaforme online in cui avvengono le compravendite di moneta virtuale [15].

In relazione, invece, ai clienti di tali società – persone fisiche che detengono i bitcoin al di fuori dell'attività di impresa – l'acquisto è esente da tassazione ai fini Irpef, in quanto considerato alla stregua di una operazione "a pronti", il cui pagamento avviene immediatamente al momento

della consegna, mancando la finalità speculativa.

Alla luce di quanto affermato nel 2016, quindi, poteva ritenersi che le persone fisiche che utilizzano bitcoin, al di fuori dell'attività di impresa, non fossero soggette a tassazione e che le società che svolgono l'attività di intermediarie non fossero gravate dai tipici obblighi del sostituto d'imposta (es. certificazione unica e modello 770).

Gli esperti del settore, tuttavia, avevano iniziato a domandarsi se bisognasse tener conto di quanto stabilito dall'art. 67, comma 1-ter del Testo Unico delle imposte sui redditi (c.d. TUIR), il quale indica il limite oltre il quale la plusvalenza diviene rilevante ai fini

fiscali, concorrendo a formare il reddito imponibile.

Ebbene, nel mese di aprile 2018, in risposta ad istanza di interpello del 22 gennaio 2018, l'Amministrazione finanziaria ha fugato ogni dubbio al riguardo: le cessioni a pronti di valuta virtuale non danno origine a redditi imponibili, mancando la finalità speculativa, salvo generare un reddito diverso, qualora la valuta ceduta derivi da prelievi da portafogli elettronici (wallet) per i quali la giacenza media superi un controvalore di euro 51.645,69 per almeno sette giorni lavorativi continui nel periodo di imposta, ai sensi dell'art. 67, comma 1, lettera c-ter), del TUIR e del comma 1-

ter) del medesimo articolo.

La “giacenza media”, sottolinea l'Agenzia, deve essere verificata rispetto all'insieme dei wallet detenuti dal contribuente indipendentemente dalla tipologia degli stessi (paper, hardware, desktop, mobile, web).

Ulteriore novità, nell'interpello in esame, riguarda il trattamento dei bitcoin ricevuti “a titolo gratuito”. L'Agenzia precisa, in maniera concisa, che il costo iniziale da considerare è quello sostenuto dal donante, ai sensi del comma 6, dell'art. 68 del TUIR.

Per quanto riguarda i redditi derivanti da operazioni realizzate sul mercato “FOREX” e da “Contract for Difference” (CFD), aventi ad oggetto

valute virtuali, gli stessi devono essere considerati redditi diversi ai sensi dell'art. 67, comma 1, lettera c-quater), del TUIR.

2.4 DISCIPLINA AI FINI DELLA NORMATIVA ANTIRICICLAGGIO

La recente esplosione del mercato delle monete virtuali, in particolare nel 2017, ha, da un lato, acceso prepotentemente i riflettori su questo nuovo settore, dall'altro, evidenziato ancor di più i noti problemi di trasparenza che interessano le criptovalute, Quest'ultime, infatti, sono state viste, fin dalla loro prima diffusione, con molto sospetto per

questioni legate al riciclaggio e al finanziamento di attività illecite. D'altronde la possibilità di usufruire di mezzi di pagamento in grado di garantire l'anonimato delle parti, oltre a non necessitare dell'intervento di un istituto bancario, né nella fase di deposito né durante la transazione, potrebbero ben rappresentare un'opportunità per coloro che intendono portare avanti operazioni legate al riciclaggio.

Per quanto riguarda l'attività di "cambia-valute virtuali", l'Italia è stato il primo paese dell'Unione Europea che ha recepito la IV Direttiva antiriciclaggio, mediante il Decreto legislativo 25 maggio 2017, n. 90, che ha introdotto l'obbligo di iscrizione in

una sezione speciale del registro dei cambiavalute (intervenendo sulla normativa prevista dal D. Lgs. 13 agosto 2010, n. 141, articolo 17-bis).

La IV Direttiva ha introdotto un aspetto fondamentale quale quello del c.d. "approccio basato sul rischio", prevedendo, infatti, nei suoi considerando che "dovrebbe essere adottato un approccio olistico basato sul rischio, che non costituisce un'opzione indebitamente permissiva per gli Stati membri e per i soggetti obbligati: implica processi decisionali basati sull'evidenza fattuale, al fine di individuare in maniera più efficace i rischi di riciclaggio e di finanziamento del terrorismo che gravano sull'Unione

e su coloro che vi operano".

Con l'introduzione del Risk Based Approach, viene elaborato un metodo, condotto su tre livelli distinti, in maniera sistematica e con il coinvolgimento di soggetti diversi:

1. Risk Assessment a livello europeo (art. 6, IV Direttiva): è richiesto alla Commissione europea di:

1. individuare le minacce transfrontaliere con potenziali impatti sui mercati nazionali;
2. elaborare una relazione che identifica, analizza e valuta tali

rischi, aggiornarla ogni due anni e metterla a disposizione degli Stati membri;
3. formulare raccomandazioni agli Stati membri riguardo alle misure idonee ad affrontare i rischi;

2. Risk Assessment a livello nazionale (art. 7, IV Direttiva): è richiesto agli Stati membri di:

1. identificare, valutare, comprendere e mitigare i rischi di riciclaggio e finanziamento del terrorismo;
2. designare un'Autorità, ovvero istituire in meccanismo, al fine di

coordinare il risk assessment;

3. svolgere periodicamente il risk assessment;
4. utilizzare le risultanze del risk assessment europeo per la conduzione delle analisi;
5. mettere tempestivamente a disposizione dei soggetti obbligati le informazioni maggiormente rilevanti per il proprio risk assessment;

3. Risk Assessment a livello dei soggetti obbligati (art. 8, IV Direttiva): è richiesto ai soggetti obbligati di:

1. svolgere il risk assessment interno, adottare misure volte a individuare, valutare e mitigare il rischio di riciclaggio e di finanziamento del terrorismo;
2. documentare, aggiornare e mettere a disposizione delle autorità competenti le valutazioni del rischio.

La IV Direttiva, come detto, è stata recepita dal legislatore italiano con il D. Lgs. 90/2017, che ha disciplinato l'approccio basato sul rischio agli artt. 14, 15 e 16.

È stato previsto, infatti, che:

1. il Comitato di Sicurezza Finanziaria ("CSF") sia l'autorità diretta a identificare, analizzare e valutare il rischio nazionale di riciclaggio e finanziamento del terrorismo;
2. le autorità di vigilanza di settore e gli organismi di autoregolamentazione individuano i requisiti dimensionali e organizzativi in base ai quali i soggetti obbligati, rispettivamente vigilati e controllati, adottano specifici presidi, controlli e procedure per la valutazione e gestione del rischio di riciclaggio e finanziamento del terrorismo;

3. i soggetti obbligati dovranno documentare, aggiornare e mettere a disposizione delle autorità competenti e degli organismi di autoregolamentazione il risk assessment effettuato.

Al fine di disciplinare l'operatività delle valute virtuali, il Legislatore le ha distinte dalle valute legali, definendole 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 e trasferita, archiviata e negoziata elettronicamente".

La definizione è utilizzata nel decreto legislativo in esame al fine di dichiarare applicabili le norme in esso previste ai "prestatori di servizi relativi all'utilizzo di valuta virtuale, limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso". Costoro sono obbligati al rispetto della normativa antiriciclaggio, tramite:

1. adeguata verifica della clientela;
2. conservazione dei dati e delle informazioni;
3. segnalazione delle operazioni sospette [27].

In sostanza, nel momento in cui un soggetto (tipicamente un exchanger, preposto all'acquisto e alla vendita per conto terzi di moneta virtuale in cambio di moneta avente corso legale) opera in Italia, deve iscriversi nell'elenco dei cambia valute (art. 17 bis, comma 8 bis del decreto legislativo 13 agosto 2010, n. 141) e deve applicare quanto previsto dalla disciplina cd. Antiriciclaggio, sia relativamente agli obblighi di adeguata verifica della clientela sia alla segnalazione delle operazioni sospette.

In particolare, i soggetti obbligati in presenza di un elevato rischio di riciclaggio o di finanziamento del terrorismo applicano misure rafforzate di adeguata verifica della clientela.

1.

1. Parte II

LE CRIPTOVALUTE E IL *DARK WEB*

1. IL MERCATO DELLE VALUTE VIRTUALI

a cura di Giovanni Reccia

Sommario: 1.1 *Bitcoin*, *Monero* e le altre – 1.2 Riciclaggio e criptovalute, aspetti internazionali – 1.3 Antiriciclaggio per la valuta virtuale in alcuni Paesi del mondo.

1. 1.1 *BITCOIN*, *MONERO* E LE ALTRE

Negli ultimi anni il mercato delle valute virtuali è cresciuto notevolmente ed ha visto l'ingresso di nuove e differenti virtual currency. Ad oggi, infatti, è possibile stimare la presenza in rete di circa 1600 valute virtuali, alle quali è riconducibile un mercato del valore di circa 170 miliardi di dollari[25]. Pur essendo tali informazioni in continuo aggiornamento, rappresentano un importante elemento da tenere in considerazione per comprendere le dimensioni del mercato delle valute

virtuali.
La piattaforma Web coinmarketcap.com offre una panoramica costantemente aggiornata delle valute virtuali attualmente in circolazione, nonché del relativo volume degli scambi. Tendenzialmente la quasi totalità delle valute virtuali oggi in circolazione si basano su reti decentrate, il che non consente di identificare gli utenti di una transazione o rende, comunque, questa operazione poco agevole.
Pur essendo il mercato in esame ampiamente dominato dai Bitcoin, sono degne di attenzione altre tipologie di valute virtuali, tra le quali Monero, Ethereum, Ripple e Litecoin. Ognuna di queste criptovalute ha ottenuto un ampio

successo negli ultimi anni e il loro utilizzo è diffuso anche in alcuni mercati legali presenti sul Web, sia grazie ai sistemi ed alle tecnologie che garantiscono l'affidabilità delle transazioni sia per il valore che alcune di queste valute ha ottenuto già dai primi mesi di vita.

Bitcoin

Il bitcoin può essere considerato la criptovaluta per eccellenza, essendo la prima valuta virtuale introdotta sul mercato. Il funzionamento dei bitcoin, come precedentemente riportato, si basa sulla tecnologia Peer to Peer (P2P) che consente il trasferimento della valuta da un utente, possessore di un wallet

bitcoin, ad un altro senza l'intervento di enti centrali. I wallet (portafoglio) sono software che possono essere gestiti online (wallet online), possono essere installati sul PC o sullo Smartphone (wallet software) oppure si trovano già preinstallati in apposite chiavette USB (wallet hardware). I wallet online richiedono una registrazione ad un sito web (es. Coinbase) fornendo e-mail, telefono, dati personali e scansione di un documento valido, e la gestione dei propri indirizzi (quindi dei propri bitcoin) è completamente demandata al sito. In questo caso non si conoscono le chiavi private dei propri indirizzi detenute esclusivamente dal sito web per cui bisogna avere piena fiducia nei

confronti di chi fornisce il servizio. Semplicemente ricordandosi le credenziali d'accesso al sito, si possono gestire i propri bitcoin da qualsiasi dispositivo in qualsiasi parte del mondo. Tuttavia se il sito dovesse chiudere, i bitcoin sarebbero persi per sempre. I wallet software, ossia quelli installati su PC, hanno il vantaggio della gestione locale dei bitcoin e rispetto ai wallet online vi è un maggiore controllo avendo in locale le chiavi private. L'accesso al software è controllato unicamente da una password scelta dall'utente, tuttavia se si perde o si danneggia il PC senza aver fatto un backup si perderanno per sempre i bitcoin. I wallet hardware si presentano

come piccole calcolatrici, permettono la gestione completa dei bitcoin come gli altri tipi di wallet, tuttavia se si perdono o si danneggiano i bitcoin non potranno essere recuperati.

Le operazioni effettuate con i bitcoin e con i relativi wallet sono fondamentalmente pubbliche[26], ma restano anonimizzate le informazioni relative agli utenti interessati, incarnando a pieno il profilo della criptovaluta. Ad oggi è la moneta virtuale maggiormente commercializzata ed utilizzata, sia per le transazioni lecite sia per quelle illecite, favorite, queste ultime, dal consistente grado di anonimizzazione e di affidabilità della cifratura utilizzata.

Il grado di anonimizzazione di bitcoin viene considerato da alcuni obsoleto, soprattutto in relazione alle nuove criptovalute, essendo lo stesso "compromesso" dalla possibilità di associare il wallet ad una persona fisica, qualora quest'ultima ponga in essere azioni che rendano pubblico l'indirizzo del predetto portafoglio. Per tale motivo, pur restando il bitcoin la prima valuta virtuale per volume di scambi, il suo utilizzo in traffici illegali vede la concorrenza di altre criptovalute.

La spina dorsale del protocollo e della tecnologia Bitcoin è, come detto, la Blockchain. Tutti i blocchi che la compongono sono numerati a partire da

zero (il primo che è stato generato) e non ne esistono due con lo stesso numero. Ogni blocco, al suo inizio, contiene il numero del blocco precedente (o meglio la sua hash), così da occupare un preciso posto rispetto agli altri creando in questo modo una catena di blocchi. La Blockchain è in continua crescita, ogni 10 minuti viene aggiunto un nuovo blocco ad opera dei miner, che entrano in una speciale area comune detta mining pool, in attesa della conferma (fino a quando una transazione non viene confermata essa non dà diritto al passaggio di BTC). I miner scelgono a caso dal mining pool un certo numero di transazioni, ancora da confermare, e provano a creare un blocco risolvendo

un problema matematico. I miner partecipano ad una gara a tempo perché solo il più veloce di loro, ossia quello che per primo creerà un blocco "valido" si aggiudicherà una "ricompensa" (attualmente 12,5 BTC per il servizio di intermediazione). Un blocco è composto da:

- l'hash del blocco precedente in modo da poterlo posizionare correttamente all'interno della catena (quando un miner cerca di creare un nuovo blocco questo valore sarà l'hash dell'ultimo blocco generato, quello più

recente che ancora non ha successori):

- un certo numero di transazione prese a caso dal *mining pool* (in realtà la scelta non è del tutto casuale ma influenzata dalle commissioni);
- una speciale transazione che non ha ingressi ma solo un indirizzo di uscita, quello del *miner* per un importo di 12,5 BTC;
- un campo detto *nonce*.

La "gara" prevede di calcolare l'hash

del blocco così formato e, affinché sia considerato un blocco valido, tale valore di hash deve iniziare con 18 zeri. Il miner sostituisce ripetutamente e velocemente il valore del campo nonce fino a che, per tentativi successivi, ottiene per primo un valore di hash del blocco che rispetti il vincolo del numero degli zeri iniziale (la quantità di zeri è detta "difficoltà"). Il protocollo Bitcoin modula, in automatico, la difficoltà (numero di zeri) in base alle performance dei sistemi di calcolo, in modo da stabilizzare la produzione di nuovi blocchi mediamente ogni 10 minuti. Il calcolo di un siffatto hash richiede altissime prestazioni tecnologiche, di conseguenza attualmente

i miner utilizzano veri e propri server farm o sistemi distribuiti. È attualmente impensabile fare mining in proprio. L'attività del miner consente di fatto la generazione di criptovaluta, diversamente dalle valute FIAT, la coniazione di bitcoin è già predeterminata e cesserà nel 2140 al raggiungimento di 21 milioni di bitcoin. Il modo in cui funzionano le transazioni Bitcoin fa sì che esse siano pubblicamente tracciabili, tramite un'analisi della blockchain. Questo comporta che a partire da un indirizzo Bitcoin "attenzionato" è possibile seguire il flusso di bitcoin, transazione dopo transazione, fino a raggiungere un indirizzo noto, ad esempio un

cambiavalute, e identificare così l'utente (follow the money).

Invero il mixer Bitcoin separa i collegamenti tra flussi di bitcoin. Chi si rivolge ad un mixer per ripulire bitcoin fornisce uno o più indirizzi "puliti" mai utilizzati ed effettua una o più transazioni provenienti da indirizzi sospetti. Il mixer, che dispone di un consistente quantitativo di bitcoin e di numerosi indirizzi, riversa sugli indirizzi puliti, i bitcoin provenienti da altre transazioni estranee trattenendone una percentuale per il servizio. Il mixer rende casuale l'importo delle transazioni e aggiunge ritardi alle transazioni stesse. In genere non c'è nessun collegamento tra le transazioni

originali e l'indirizzo finale dei bitcoin. Il mixer è come un grande "frullatore" che riceve in ingresso numerose transazioni, le scompatta, le riunisce o le ritarda allo scopo di mescolarle e interrompere i flussi ordinari di bitcoin.

Ethereum

Ethereum è una piattaforma decentralizzata sviluppata nel 2013 per la gestione di "smart contracts", definite - dal sito Web ufficiale ethereum.org - come applicazioni che "eseguono esattamente ciò per le quali sono state programmate, senza alcuna possibilità di interruzioni, censure, frodi o interferenze di terze parti".

In sostanza Ethereum potrebbe essere

considerata come la piattaforma, ovvero la blockchain, che consente, tra l'altro, lo scambio di valuta, Ether, mediante una serie di transazioni che creano un vero e proprio mercato, concorrenziale a quello dei bitcoin. Così come per i bitcoin, anche per Ethereum le transazioni avvengono sfruttando la rete Peer-to-Peer, risultando assenti autorità centrali che influiscono sulle transazioni e garantendo l'anonimato degli utenti in esse coinvolti.

Gli smart contracts, citati da Etherum, invece, sono dei veri e propri programmi che eseguono un codice, ovvero un programma che, al verificarsi di determinate condizioni, consente i trasferimenti di Ether da un utente

all'altro. Questo sistema innovativo, inoltre, consente, oltre allo scambio di Ether, l'esecuzione di ulteriori servizi[27], normalmente previsti su Internet, puntando a diventare una alternativa alla rete Internet.

Notevoli sono, invece, le differenze tra i Bitcoin e gli Ether, essendo questi ultimi, ad esempio, caratterizzati dall'assenza di un limite massimo di token presenti sul mercato. Ancor più notevole è la velocità con la quale vengono risolti i blocchi di Ethereum, in media 12 secondi, a fronte dei 10 minuti circa previsti per bitcoin. Tutte le caratteristiche appena citate fanno di Ethereum la seconda piattaforma per volume di scambio di valuta virtuale

sulla rete.

Ripple

Con il termine Ripple viene definita sia la valuta virtuale sia la piattaforma, ovvero il protocollo utilizzato per le transazioni. Ripple Transaction Protocol (RTXP), il "Protocollo Ripple" ($XRP) è stato sviluppato nel 2012 per consentire l'esecuzione di transazioni finanziarie in maniera gratuita e riguardanti sia la valuta tradizionale sia altre tipologie di valori.

Anche la rete Ripple è di tipo decentrato, mediante l'utilizzo della tecnologia Peer-to-Peer e garantisce, così come per le altre valute virtuali, l'anonimato degli attori coinvolti nella

transazione. Tale valuta è inoltre garantita da una serie di misure di sicurezza tali da evitarne la duplicazione o la falsificazione. Così come per Ethereum, anche il sistema utilizzato da Ripple riduce i tempi delle transazioni a pochi secondi, a fronte dei dieci minuti medi di Bitcoin.

Litecoin

Litecoin è una delle prime valute virtuali introdotte subito dopo l'avvento dei bitcoin. Creata nel 2011, differisce rispetto al bitcoin soprattutto per la velocità di elaborazione delle transazioni, seppur superiore rispetto ad Ethereum e Ripple, oltre al maggior numero di token immessi nel mercato

(circa 84 milioni di monete).
Dai portali ufficiali della moneta virtuale in esame, si legge che "Litecoin è una rete di pagamenti globali, open source, pienamente decentralizzata e senza autorità centrale. La matematica garantisce la rete stessa trasferendo agli individui la sovranità sul controllo delle proprie finanze".
Così come per tutte le altre criptovalute analizzate, Litecoin utilizza una rete decentrata, Peer-to-Peer, per gli scambi di valuta e consente, inoltre, la notevole riduzione dei costi previsti per ogni transazione. La rete utilizzata, seppur più veloce e conveniente, è comunque molto simile a quella dei Bitcoin, essendo il Litecoin nato originariamente

per migliorare il funzionamento degli stessi Bitcoin. Anche per i wallet Litecoin, infatti, viene utilizzata la cifratura mediante l'utilizzo delle chiavi private.
Il potenziamento delle misure di sicurezza e le ottimizzazioni apportate negli ultimi anni per Litecoin[28] ne consente oggi un utilizzo ancora molto diffuso, seppur notevolmente superato da altre criptovalute come Ethereum.

Monero

Seppur ad oggi il volume di scambi di Monero risulta più basso rispetto alle altre criptovalute citate, è comunque necessario un approfondimento di tale valuta, essendo, molto utilizzata per i

traffici illegali realizzati sulla rete, soprattutto relativi alla vendita di droghe.

Tale basso utilizzo è probabilmente dovuto alla crescente attenzione degli investigatori verso i bitcoin, il che ha consentito ad altre criptovalute, come Monero, di circolare "indisturbate" o comunque con ridotta considerazione. Inoltre, a differenza dei concorrenti, per Monero viene utilizzato un sistema che, "mescolando" più transazioni rende estremamente complessa l'identificazione degli utenti che la utilizzano, un meccanismo simile ai mixer per bitcoin.

Proprio sul sito Web della valuta in esame, infatti, si legge: "*Monero is a*

secure, private, and untraceable cryptocurrency. It is open-source and accessible to all. […] *Your accounts and transactions are kept private from prying eyes*". In sostanza Monero assicura la sicurezza della valuta, ma soprattutto la riservatezza ovvero l'anonimato delle transazioni. Anche per Monero bisogna far riferimento ad una rete decentrata, nella quale le transazioni vengono registrate su una blockchain, ma si differenzia notevolmente dalle altre criptovalute in quanto utilizza firme e transazioni anonime che oscurano gli importi e gli utenti delle stesse. La tecnologia utilizzata da Monero genera sulla blockchain indirizzi casuali e utilizzati

una sola volta che non consentono, quindi, l'associazione degli stessi ad uno specifico utente. Oltre a non esservi la possibilità di individuare chi riceve o invia la moneta, a differenza degli altri sistemi, per Monero sarà impossibile conoscere anche l'ammontare dell'operazione, rendendo ancor più elevata la difficoltà di identificazione degli attori coinvolti in una transazione.

1.2 RICICLAGGIO E CRIPTOVALUTE, ASPETTI INTERNAZIONALI

La necessità di fornire credibilità e competitività al sistema economico

comporta l'esigenza di tutelare il corretto andamento dei mercati con l'attenzione dovuta ai flussi finanziari al fine di scongiurare l'inserimento nel circuito economico di soggetti ovvero organizzazioni dedite al crimine a danno degli imprenditori onesti e dei risparmiatori.

Ai reati tipici connessi all'usura, al traffico di stupefacenti, allo sfruttamento dell'immigrazione clandestina, alle frodi fiscali svolte in una cornice nazionale, si affianca un'attività illecita che supera i confini nazionali e che va a sfociare in paesi non cooperativi nello scambio di dati o notizie.

Questa attività illecita costituisce proprio le condotte di riciclaggio e di

reimpiego dei proventi illecitamente conseguiti sui territori nazionali, con accumuli di patrimoni e conseguente annacquamento dei mercati, specialmente finanziari. Pertanto le azioni di contrasto non possono prescindere, da un lato, da una ricostruzione delle movimentazioni finanziarie, dall'altro, dall'aggressione ai patrimoni illecitamente accumulati attraverso l'esecuzione di provvedimenti esecutivi reali.

Il riciclaggio è un reato a carattere economico ma ha antichi legami con l'imprenditorialità illecita in connessione non solo con la criminalità organizzata ma anche con singoli soggetti o imprese. L'elemento

scriminante per tutti è lo scopo di lucro, cioè organizzazione finalizzata alla commissione di uno o più reati che producono dei proventi volti a finanziare l'impresa stessa o a permettere investimenti in altre attività delittuose o lecite per la creazione di altro profitto.

Stime inerenti ai capitali riciclati a livello nazionale ed internazionale ne sono state elaborate diverse e talvolta contrastanti. Il Fondo Monetario Internazionale (FMI)[29] lo ha individuato in circa il 5% del Prodotto Interno Lordo (PIL)[30] a livello mondiale, mentre per l'Italia si fa riferimento a circa il 10% del PIL nazionale. Se è vero peraltro che il volume d'affari delle

organizzazioni criminali è indicato in 170 miliardi di euro all'anno, che la corruzione in Italia costa allo Stato circa 60 miliardi di euro l'anno, che l'economia sommersa vale il 16% del PIL mentre l'evasione fiscale ammonta a 120 miliardi di euro annui, è evidente che il riciclaggio assume valori altissimi in termini di costi nazionali.

L'impresa illecita non si distingue da quella lecita se non per il compimento di reati, rimanendo una struttura che può avere una base locale, nazionale o sovranazionale. Ciò la rende partecipe del vivere civile ed il suo agire appare all'esterno in modo lecito, muovendosi in un mercato libero che è terra di conquista e dove la concorrenza utilizza

i medesimi meccanismi della società civile. È ovvio che l'impresa criminale realizza una concorrenza sleale proprio per effetto della continua commissione di reati, quali violenza, minaccia, corruzione, tuttavia rimane un operatore nel mondo globalizzato dell'economia fin tanto che non se ne individuano le illiceità.

L'apertura dei mercati e la loro internazionalizzazione hanno consentito peraltro alle organizzazioni criminali di affinare i propri strumenti assumendo sempre più scelte di tipo imprenditoriale con diversificazione degli investimenti ed inserimento nell'alta finanza. Ciò è stato reso possibile anche per lo sviluppo delle

nuove tecnologie informatiche che consentono l'effettuazione di operazioni finanziarie transnazionali con velocità e contemporaneamente con la possibilità di eliminazione, con la medesima velocità, di dati di riconoscimento.

Il riciclaggio può avvenire con diverse modalità, attraverso persone fisiche o giuridiche, enti con o senza personalità giuridica e la sua ricostruzione non può essere inquadrata in modelli specifici attesa la sua dinamicità ed inserimento in contesti continuamente in evoluzione. Se da un lato vigono ancora tipologie di trasferimento del denaro attraverso moderni "spalloni" (cash currier) che occultano il denaro sui mezzi di trasporto, a differenza dei vecchi

“spalloni” che con sacchi aggiravano il confine attraverso sentieri di montagna, l’uso del sistema bancario e finanziario è stato il mezzo più praticato dai riciclatori nel corso degli anni, mentre oggi è sempre più individuabile un meccanismo che confonde i proventi illeciti con quelli leciti (commingling). In tale panorama le novità sono proprio l’effettuazione di operazioni di cybericiclaggio mediante l’uso illecito dei sistemi di pagamento elettronico o in valuta virtuale (bitcoin) ovvero attraverso sistemi “organizzativo-finanziari” di tradizione non occidentale basati su di uno stretto rapporto di fiducia tra le persone (Hawala).

Sotto tale profilo vengono individuate

quattro diverse fasi storiche del riciclaggio:

- monetario (anni settanta), basato sul forte utilizzo di denaro contante;
- bancario (anni ottanta), agevolato dall'abolizione delle misure restrittive alla circolazione dei capitali e dall'aumentata varietà degli strumenti e servizi disponibili;
- finanziario (anni novanta), canalizzato sull'intermediazione finanziaria;
- extra finanziario

(attuale), fondato sul ricorso a professionisti ovvero operatori non finanziari, nonché connotato da circuiti alternativi rispetto agli intermediari finanziari abilitati (*money transfer*, piattaforme per criptovalute ed *hawala*).

Proprio la constatazione del possibile continuo spostamento di "risorse illecite" dal mondo bancario e finanziario ad ambiti meno esposti all'azione di controllo, hanno visto gli Stati e gli Organismi sovranazionali muoversi verso un'azione di contrasto a

carattere soprattutto preventivo. In ogni caso l'opportunità di trasferire in giurisdizioni diverse tra loro le varie fasi di cui si compone il riciclaggio e l'esistenza di regimi diversi di controllo amministrativo nei vari Paesi, favoriscono l'occultamento di somme di denaro di provenienza illecita. Allo stesso tempo alcuni intermediari finanziari tendono a stabilirsi in luoghi in cui il diverso ordinamento giuridico comporta minori oneri. È il caso dei cc.dd. "paradisi fiscali"[31] (e non solo fiscali) o Paesi off-shore, territori che per attrarre capitali hanno un basso livello di controllo, detengono una tassazione privilegiata, favoriscono l'effettuazione di operazioni finanziarie

con altri Paesi tutelando ancora il segreto bancario e garantiscono l'anonimato per le operazioni in valute virtuali. L'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE)[32] afferma che nei paradisi fiscali si annidano 7000 miliardi di dollari di cui 1600 connessi ad attività delittuose[33].

È in tale contesto che possiamo in generale individuare il riciclaggio come quella serie di operazioni atte a riutilizzare il denaro o i beni derivanti da attività illegali e che normalmente si distingue in tre momenti:

- collocamento (*placement*), cioè

l'introduzione dei proventi illeciti nel sistema economico;

- stratificazione (*dissimulation*), che è il compimento di operazioni commerciali o finanziarie volte a far perdere la traccia dell'origine o provenienza illecita del denaro;

- riutilizzo (*conversion*) del denaro illecito che viene reimpiegato nell'economia legale.

Già nel 2015 con il recepimento

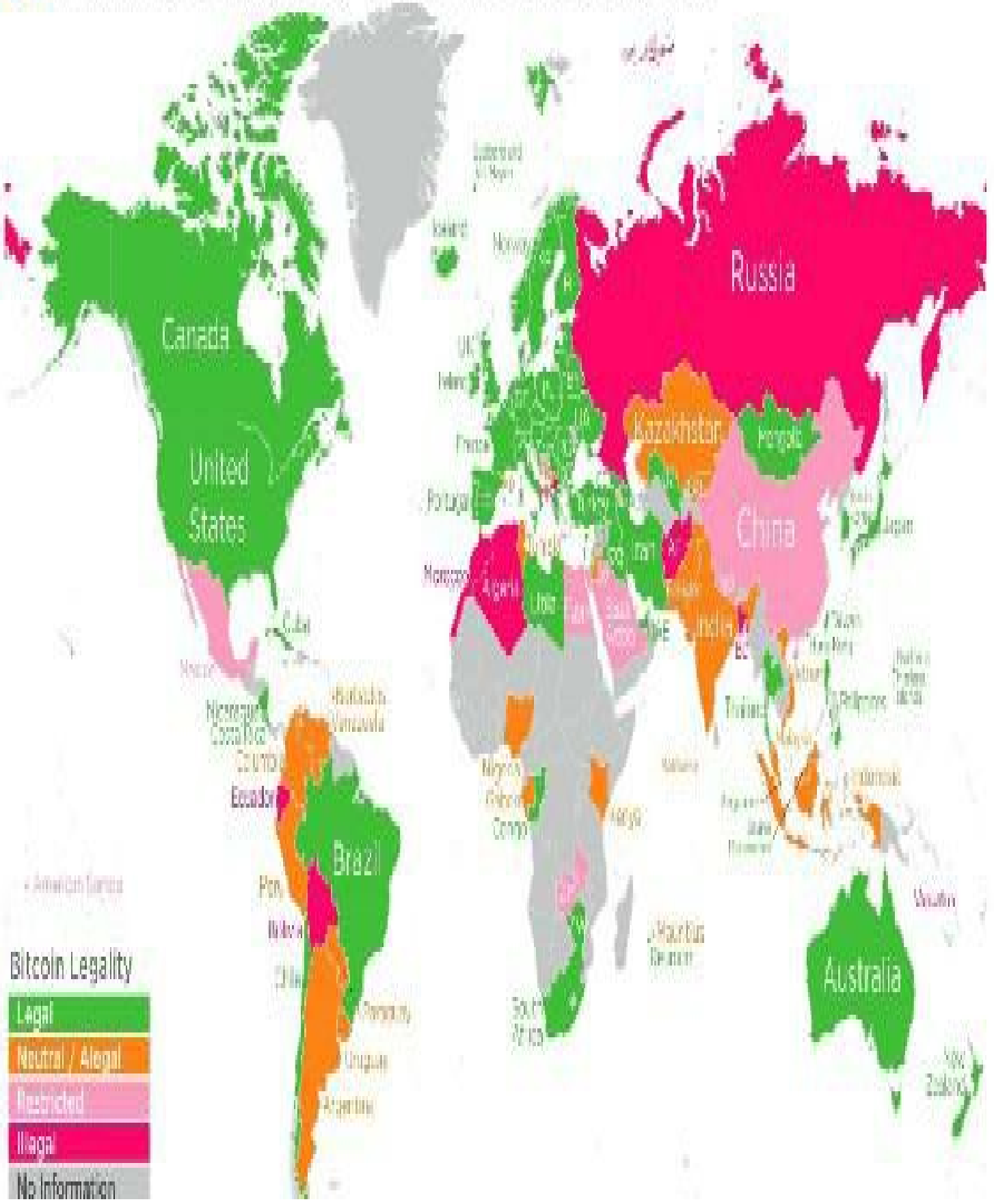
dell'accordo FATCA[34] degli Stati Uniti d'America, l'Italia ha fatto un passo avanti nel processo di scambio di informazioni antifrode fiscale a livello internazionale, seppur limitatamente agli USA e secondo un'impostazione unilaterale standardizzata da parte dell'Agenzia fiscale USA.

Allo stesso tempo con il D. Lgs. n. 32/2017[35] è stata approvata la Direttiva 2015/2376/UE inerente allo scambio automatico obbligatorio di informazioni nel settore fiscale tra gli Stati membri dell'Unione Europea, ciò ad evidenziare come sia alta l'attenzione ai redditi che si spostano tra i diversi Paesi.

Tale attenzione[36] va necessariamente ad

incrociarsi e saldarsi con il sistema antiriciclaggio, tenuto conto che l'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) ha varato nel 2014 il Common Reporting Standard (CRS), uno standard globale consistente nello scambio obbligatorio di informazioni fiscali tra le amministrazioni finanziarie dei Paesi a partire dal 2017, volto ad un'azione di contrasto all'evasione fiscale transnazionale[37].

Bitcoin Legality Around the World



Il modello di accordo CRS persegue gli stessi scopi del FATCA americano, ma a differenza di quest'ultimo vengono richiesti a tutti gli istituti finanziari un adeguamento dei processi di identificazione e controllo della clientela. Riguarda tutte le persone fisiche e giuridiche con raccolta delle informazioni che vanno dai dati del soggetto a tutti i tipi di reddito, di capitale o finanziario, fino al saldo del conto. Deve essere poi individuato, identificato e comunicato il titolare effettivo del conto secondo le raccomandazioni antiriciclaggio GAFI.

Sarà posta altresì un'attività di adeguata verifica dei conti finanziari, nonché di

analoga due diligence con riferimento alla clientela preesistente ed effettuate ricerche negli archivi al fine di contestare o confermare il profilo del cliente e valutarne l'effettiva residenza. In tale ambito i clienti saranno distinti in high value account, caratterizzati da valori patrimoniali superiori ad un milione di dollari nei cui confronti verranno posti in essere verifiche rafforzate, nonché in lower value account nei cui confronti i controlli saranno limitati in presenza di residenza estera.

Queste informazioni, con cadenza annuale, saranno inoltrate alle amministrazioni fiscali di appartenenza dello Stato aderente che le trasmetterà

all'Autorità competente del singolo Stato partner.

1.3 ANTIRICICLAGGIO PER LA VALUTA VIRTUALE IN ALCUNI PAESI DEL MONDO

Come evidenziato la disciplina antiriciclaggio ormai è entrata, sulla spinta delle Raccomandazioni GAFI, a far parte di quasi la totalità dei Paesi del mondo. Tuttavia ogni ordinamento giuridico contiene delle variabili volte ad un adattamento alla situazione locale, ad una diversa criminalizzazione del riciclaggio ovvero a differenti procedure istruttorie. Va tenuto presente

che si sono formate nel tempo diverse organizzazioni tra Stati volte a monitorare il sistema finanziario per prevenire l'infiltrazione della criminalità nel settore economico-finanziario. In particolare abbiamo il Gulf Cooperation Council (GCC), unica organizzazione-membro del FATF/GAFI che, nato nel 1981 come mercato comune di alcuni paesi del Golfo Persico, aderisce alle raccomandazioni in materia di antiriciclaggio emanate dal FATF, nonché le associazioni affiliate al FATF/GAFI quali le:

- Asia/Pacific Group on Money Laudering (APG), le cui origini risalgono alle attività di

“sensibilizzazione” intraprese dal FATF nei primi anni '90 come parte della sua strategia per incoraggiare l'adozione di contro-misure al riciclaggio di denaro in tutto il mondo. Il primo accordo è stato raggiunto a Bangkok nel 1997 ove si è costituita l'APG. A seguito degli eventi USA dell'11 settembre 2001, l'APG ha ampliato il suo campo di applicazione includendo il tema del finanziamento al terrorismo. L'APG

effettua valutazioni sui propri membri e tiene un seminario periodico sui metodi e sulle tendenze del riciclaggio di valuta;

- Caribbean Financial Action Task Force (CFATF), è stata fondata come risultato di due incontri chiave effettuati ad Aruba ed in Giamaica nei primi anni '90. Nel 1996 è stato stipulato un memorandum d'intesa che ora funge da base per gli obiettivi e il lavoro del CFATF. In questo documento i membri del

CFATF accettano di adottare e attuare la Convenzione delle Nazioni Unite contro il traffico illecito di droga e sostanze psicotrope, hanno deciso di approvare ed attuare le Raccomandazioni del FATF e le raccomandazioni del Consiglio del CFATF, attuano qualsiasi altra misura per la prevenzione e il controllo del riciclaggio dei proventi dei "reati gravi definiti dalle leggi

di ciascun membro";

- Eurasian Group (EAG), istituito nel 2004 a Mosca su iniziativa della Federazione Russa, l'EAG è un organismo regionale simile al FATF. Gli obiettivi principali del EAG sono: facilitare l'attuazione delle norme internazionali in materia; condurre valutazioni sull'efficacia dei meccanismi antiriciclaggio esistenti; coordinare la cooperazione in materia

di assistenza tecnica; analizzare le tipologie di riciclaggio e scambiare esperienze nella lotta contro tali crimini;

- Eastern and Southern Africa Anti-Money Laudering Group (ESAAMLG), promosso in una riunione dei Ministri finanziari africani in Tanzania nel 1999, ove fu approvato un memorandum d'intesa (MoU) basato sull'esperienza del FATF. Tutti i membri si sono impegnati nel

recepimento delle Raccomandazioni FATF, tuttavia partecipano ad un processo di "autovalutazione" per verificare i progressi nell'attuazione delle stesse;

- Groupe d'Action contre le blanchiment d'Argent en Afrique Centrale (GABAC), task force sul riciclaggio di valuta in Africa Centrale, è un organismo della Comunità Economica e Monetaria dell'Africa Centrale. È stato istituito

nel 2000 con il mandato di combattere il riciclaggio di denaro e il finanziamento del terrorismo, valutare l'adesione dei suoi membri alle norme FATF, fornire assistenza tecnica ai suoi membri e facilitare la cooperazione internazionale;

- Financial Action Task Force of Latin America (GAFILAT), incoraggia la creazione nei singoli stati membri del reato di riciclaggio di denaro in relazione a reati gravi, lo

sviluppo di sistemi giuridici per un'efficace indagine e il perseguimento di tali reati, la creazione di sistemi per la segnalazione di transazioni sospette, la promozione dell'assistenza giudiziaria reciproca. GAFILAT tiene sotto osservazione tutti i fattori regionali sia nella individuazione sia nell'attuazione delle misure antiriciclaggio. Le origini di GAFILAT

risalgono al 2000 in seguito alla stipula a Cartagena, in Colombia, di un memorandum d'intesa da parte dei rappresentanti dei governi dei paesi del Sud America;

- Inter Governmental Action Group against Money Laudering in West Africa (GIABA), istituita nel 1999 con una decisione dei Capi di Stato e di Governo dell'ECOWAS . I membri del GIABA riconoscono che il riciclaggio di

denaro e il finanziamento del terrorismo sono questioni di fondamentale importanza per la comunità mondiale e che richiedono un'azione globale, nonché le economie e i sistemi finanziari dei paesi devono essere protetti dal denaro riciclato o proveniente da attività terroristiche;

- Middle East and North Africa Financial Action Task Force (MENAFATF), creato nel 2004. Gli obiettivi di

MENAFATF sono: l'attuazione delle raccomandazioni FATF e degli accordi dell'ONU; la collaborazione tra gli Stati membri e con altre organizzazioni, istituzioni e agenzie internazionali e regionali; l'attività congiunta per individuare le questioni regionali legate al riciclaggio di denaro e al finanziamento del terrorismo; l'adozione di misure nella regione per combattere efficacemente il riciclaggio di denaro e

il finanziamento del terrorismo “in un modo da non contraddire i valori culturali, i quadri costituzionali ed i sistemi giuridici dei paesi membri”.

Vediamo cosa succede in alcuni Paesi del mondo in materia di antiriciclaggio e valute virtuali.

AUSTRALIA

L’AUSTRAC è l’unità informativa antiriciclaggio centrale, molto simile alle strutture corrispondenti nell’Unione Europea. Già con il Financial Transaction Reports Act 1988 vigeva

una disciplina interna volta alla opportunità che particolari operazioni finanziarie fossero rese note agli organi inquirenti. Tale sistema, per quanto basato su alcuni principi chiave quali "privare le persone del denaro proveniente dalla commissione di reati", prevedeva la confisca dei beni connessi e dava specifici poteri di controllo alla Polizia, ma, non contemplando elementi procedurali di dettaglio, la normativa fu in parte facilmente superata dalle organizzazioni criminali con l'effettuazione di operazioni ad esempio sotto falso nome.

Soltanto nel 2006 con l'Anti-Money Laundering and Counter-Terrorism Financing Act il sistema antiriciclaggio

australiano ha avuto una più completa strutturazione alla stregua di quella vigente in Europa.

In un primo momento l'Australian Taxation Office (ATO) aveva considerato i Bitcoin come "bene intangibile", ma nel 2015 è stata ritenuta "moneta corrente", senza applicazione della relativa imposta sui servizi (IVA italiana). Nel corso del tempo il mercato delle criptovalute si è espanso al punto che Brisbane ha il primo terminal aeroportuale al mondo ove all'interno dell'area commerciale è possibile effettuare acquisti in valuta virtuale. Nel 2018 l'ATO ha affermato principi di compliance per tale settore entrato nel sistema finanziario australiano.

CANADA

Anche il Canada nel 1991 con il Proceeds of Crime (Money Laundering) Act ha dato una prima attuazione alle raccomandazioni GAFI. Successivamente nel 2001, con gli eventi terroristici negli USA, il sistema antiriciclaggio e di finanziamento al terrorismo si è ampliato prevedendo misure stringenti sull'identificazione del cliente, sulla tenuta dei registri con reporting periodici, sul segnalare operazioni sospette soprattutto rispetto ai trasferimenti elettronici di fondi internazionali in entrata ed in uscita, sull'effettuare valutazioni di rischio attraverso procedure codificate. In

Canada, i casinò, notai, commercialisti, banche, broker di titoli, agenzie di assicurazione sulla vita, i venditori immobiliari e commercianti in metalli preziosi sono soggetti agli obblighi antiriciclaggio.

Nel 2013 a Vancouver è stato aperto il primo sportello Bancomat al mondo di moneta virtuale, ma nel 2014 si formò un alone di diffidenza anche per effetto della chiusura della Banca canadese Flexcoin, in relazione ad un subito furto di quantità di Bitcoin. Tuttavia tale aspetto non ha influito nel tempo atteso che il mercato canadese è attualmente molto vivo in termini di transazioni finanziarie in criptovalute.

INDIA

Nel 2002 il Parlamento indiano ha approvato una legge sulla prevenzione del riciclaggio di denaro (Prevention of Money Laudering Act). Gli obiettivi principali di questa norma sono di impedire il riciclaggio di denaro, nonché di prevedere la confisca dei beni derivati da attività di riciclaggio. Descrive altresì gli obblighi che le banche, altre istituzioni finanziarie e gli intermediari devono avere. In particolare: mantenere i record che dettagliano la natura e il valore delle transazioni, soprattutto se tali operazioni avvengono entro un mese; fornire informazioni sulle operazioni entro un tempo prescritto, comprese le

registrazioni della identità di tutti i clienti; conservare le registrazioni per dieci anni. Il sistema antiriciclaggio è gestito dall'Income Tax Department, cioè direttamente dall'organizzazione impositiva fiscale indiana.

I Bitcoin hanno trovato diffusione con la creazione dell'exchange Unocoin, ma a luglio 2018 la Reserve Bank of India (RBI) ha vietato alle banche di fornire i propri servizi alle compagnie operanti in valuta virtuale.

STATI UNITI D'AMERICA

Nel tentativo di evitare che denaro "sporco", soprattutto derivante dal traffico di droga, entrasse nel sistema finanziario, il Congresso degli Stati

Uniti ha approvato una serie di leggi, a partire dal 1970, note come Bank Secrecy Act (BSA). Queste leggi richiedono alle istituzioni finanziarie, che sotto l'attuale definizione comprendono una vasta gamma di soggetti, tra cui banche, società di carte di credito, gli assicuratori sulla vita, le imprese di servizi monetari, broker/commercianti di valori mobiliari, di segnalare alcune operazioni al Dipartimento del Tesoro degli Stati Uniti. Le transazioni in contanti superiori a un certo importo devono essere riportate su un Currency Transaction Report (CTR), ove si identifica la persona che effettua l'operazione, così come la fonte della

valuta. La legge originariamente richiedeva la trascrizione di tutte le transazioni superiori ai US $ 5.000, ma a causa delle eccessive segnalazioni la soglia è stata elevata a US $ 10.000. Gli operatori finanziari devono riferire all'unità centrale antiriciclaggio (Financial Crimes Enforcement Network – FINCEN con sede in Virginia), mediante un documento chiamato Suspicious Activity Report (SAR), le operazioni finanziarie che ritengono "sospette", definite come un "conoscere o sospettare che i fondi provengano da attività illecita" o la "dissimulazione di fondi da attività illegali", ovvero che è "strutturata per eludere i requisiti della BSA o sembra servire nessuna azienda

conosciuta o avere uno scopo legale evidente". La BSA impone alle istituzioni finanziarie di impegnarsi nell'adeguata verifica della clientela, in modo soddisfacente con la garanzia che il conto è "veramente" in nome del cliente e non di terze parti. Ad un monitoraggio continuo, attraverso uno specifico database, sono sottoposti invece i conti stranieri considerati a maggiore rischio riciclaggio. Quest'ultimo è stato individuato come isolata ipotesi di reato già nel 1986 con il Money Laudering Control Act che vieta agli individui di impegnarsi in una operazione finanziaria con i ricavi generati da specifici crimini (specified unlawful activities - SUAs). Inoltre la

legge statunitense proibisce comunque di spendere più di US $ 10.000 se connesso ad una segnalazione sospetta, indipendentemente dal fatto che l'individuo lo voglia o meno nascondere. Sotto il profilo dei soggetti obbligati è interessante il fatto che sin dal 1988 con il Anti-Drug Abuse Act erano inclusi i commercianti di auto e le agenzie immobiliari. Infine sin dal 1998 i reati finanziari sono saldati con l'azione di contrasto al riciclaggio mediante il Money Laudering and Financial Crime Strategy Act, secondo cui l'attività investigativa è sviluppata a livello federale, statale e locale con analisi delle interconnessioni esistenti.

Gli USA sono il mercato più vasto di

valuta virtuale oggi esistente e nel 2018 Coinbase, la prima piattaforma exchange al mondo di valute virtuali, ha avuto l'approvazione della SEC, autorità di controllo dei mercati finanziari USA.

NIGERIA

L'Unità di Informazione Finanziaria è stata istituita nel 2004 e analizza e invia le informazioni finanziarie alla Polizia Locale. Il sistema è strutturato come quello europeo per cui i soggetti obbligati hanno il dovere di identificare i clienti prima di entrare in un rapporto di affari e aggiornare tutte le informazioni necessarie nel corso di simili relazioni finanziarie. Si prevede inoltre che, se un cliente non agisce per

proprio conto, devono usarsi tutti i mezzi ragionevoli per accertare chi possiede veramente il controllo dell'attività finanziaria. Se si sospetta o si ha motivo di sospettare che l'importo di una transazione è provento di un crimine o di qualsiasi atto illegale, l'operatore finanziario è tenuto a riferire il nome del cliente non importa quale è il valore della transazione in questione. Qualora una transazione supera il valore di 1.000 N (Naira) o il suo equivalente, il soggetto obbligato deve assicurare che il cliente compili un modulo standard di dati e confermi la propria identità presentando il passaporto internazionale, patente di guida, carta d'identità o altro documento contenente

la propria foto ed i dati personali. Gli obbligati devono controllare tutte le operazioni al fine di garantire che la transazione effettuata dal cliente è coerente con il profilo di rischio, nonché devono registrare tutte le transazioni in contanti in un ordine cronologico con indicazione del cognome di ogni cliente, del nome anteriore e l'indirizzo, in un registro numerato e trasmesso al Ministero del Commercio. I record devono essere conservati per almeno cinque anni. Gli obbligati devono riferire altresì entro 30 giorni qualsiasi presentazione o trasferimento superiore a N 5.000.000,00 (cinque milioni di Naira) da una persona fisica ovvero superiore a N 10.000.000,00, nel caso

di una persona giuridica. Infine i soggetti interessati hanno il dovere di sviluppare programmi per i loro dipendenti per creare "consapevolezza" nel combattere il riciclaggio dei proventi illeciti.

Per quanto utilizzata per operazioni finanziarie su piattaforme estere, la Banca Centrale e la Nigerian Deposit Insurance Corporation (NDIC), non riconoscono la legittimità delle criptovalute.

SUD AFRICA

Anche il Sud Africa, con la legge n. 38 del 2001, si è dotato di un sistema di prevenzione antiriciclaggio simile a quello esistente nei Paesi europei, dopo aver reso operativo il reato di

riciclaggio di valuta con la legge n. 121 del 1998 seppur conseguente a reati di criminalità organizzata. In particolare ogni organismo di settore economico e giuridico ivi esistente è stato designato a vigilare e sovrintendere alle operazioni dei propri aderenti, anche attraverso specifiche regole interne. D'interesse è il ruolo degli avvocati, sottoposti alla legge n. 33 del 2004 ed alle regole della Law Society of South Africa (LSSA), che criminalizzano gli atti commerciali che possono portare alla commissione di determinati reati tra cui il riciclaggio ed il finanziamento al terrorismo. Tuttavia sono esentati dall'obbligo di identificazione e registrazione nelle operazioni di acquisto e vendita di

immobili e/o imprese commerciali, nell'acquisizione/gestione di società fuori della Repubblica nonché rispetto alle operazioni dei clienti nell'ambito di un contenzioso.

Il mercato delle valute virtuali è aperto ed è consentita l'effettuazione di transazioni commerciali, tuttavia il Sud Africa non ha ancora una minima regolamentazione di settore.

RUSSIA

La legge primaria per la lotta al riciclaggio in Russia è la Legge Federale n. 115/FZ del 2001 che si applica alle cc.dd. "Persone Regolamentate" (banche, organizzazioni di credito, avvocati, notai, contabili,

partecipanti professionali nel mercato finanziario, compagnie di assicurazione, società di leasing e le poste federali). I soggetti "regolamentati" effettuano segnalazioni, previa analisi di rischio, al Servizio di monitoraggio della Federal Financial secondo le disposizioni emanate con Decreto del Presidente n. 808 del 2012. In particolare si fa leva sulle necessità di un forte controllo interno da parte di soggetti obbligati alla identificazione e registrazione dei clienti sospettati di riciclaggio e finanziamento al terrorismo, nonché di formazione del personale operante che deve essere in possesso di specifici requisiti. Registrazioni sono previste per le operazioni effettuate in contanti.

Ad una iniziale fase di divieto di eseguire operazioni finanziarie in criptovaluta, in Russia ne è seguita una seconda di generalizzato consenso. Tuttavia non è stata ancora definita una specifica regolamentazione interna di base.

CINA

Anche la Cina, con il Law Act penale del 2006, si è adeguata alle Raccomandazioni GAFI e rafforzato le misure di contrasto mediante l'inclusione, tra i soggetti obbligati, degli operatori del settore immobiliare. Tuttavia permangono aree "grigie" con riguardo alle attività dei legali che invero non sono obbligati ad effettuare

le segnalazioni per operazioni sospette per quanto sussistono due indirizzi generali in capo ad essi: di denuncia di sospetto di un qualsiasi crimine (facendo rientrare tra questi il riciclaggio di proventi illeciti) e di rivelazione di tutte le informazioni ricevute da un cliente quando possano mettere in pericolo la "statale pubblica sicurezza".

In Cina le transazioni in Bitcoin sono illegali per quanto si rilevano operazioni costanti con l'estero in valuta virtuale da parte di trader ed investitori, per cui il divieto riguarda le operazioni interne ed in particolar modo le offerte in Bitcoin (ICO).

GIAPPONE

Il riciclaggio di proventi illeciti è stato criminalizzato attraverso due leggi (Regole JFBA nn. 95 e 154) del 2003 che hanno riguardato il crimine organizzato ed il traffico di stupefacenti. Sotto il profilo preventivo la disciplina segue l'impostazione di tipo occidentale con disposizioni ad hoc per i consulenti e legali stranieri che operano in Giappone, mentre per le attività dei legali interni c'è particolare attenzione, anche di carattere fiscale, su alcune tipologie di operazioni economiche quali l'acquisto e la vendita di immobili, investire allo scopo di gestire una società, l'istituzione di una persona giuridica o di un ente simile, la

conclusione di un contratto di fiducia o l'acquisto e la vendita di una società.

In Giappone il mercato delle criptovalute è aperto e nel 2018 l'Agenzia per i Mercati Finanziari (FSA) ha approvato lo Japan Virtual Currency Exchange, un organismo composto dagli exchange nazionali al fine di realizzare un sistema di regole di settore secondo un modello di autoregolamentazione.

ARABIA SAUDITA

Il sistema preventivo antiriciclaggio si è strutturato con l'Anti Money Laudering Law di cui al Royal Decree n. M/39 del 2003. Tale disposizione prevede che nel momento in cui si raccolgono sufficienti

indizi e/o prove per quanto riguarda "insolitamente grandi, complesse o sospette" transazioni, le istituzioni finanziarie e non finanziarie devono informare immediatamente l'unità di informazione finanziaria e preparare un rapporto dettagliato con tutti i dati disponibili sulle parti coinvolte. Le stesse istituzioni non possono utilizzare il principio di "riservatezza dei conti" come pretesto per nascondere informazioni.

L'Arabia Saudita non riconosce le valute virtuali che ha considerato illegali.

2. 2. CRIPTOVALUTE E *DARK WEB*

a cura di Giovanni Reccia

(si ringrazia per la collaborazione prestata nella realizzazione del presente capitolo il dott. Giuliano Latini)

Sommario: 2.1 Il *dark web* e le reti decentralizzate – 2.2 Le criptovalute nel web "oscuro" – 2.3 L'operazione della Guardia di Finanza "Darknet Money"

13.

14.

1. 2.1 IL DARK WEB E LE RETI DECENTRALIZZATE

Il World Wide Web («ragnatela intorno al mondo») o semplicemente Web è un sistema che permette la condivisione di documenti ipertestuali e multimediali, costituiti cioè da un insieme di contenuti testuali, con eventuale aggiunta di immagini, audio o video, sfruttando l'infrastruttura di Internet. Per accedere al world wide web si utilizza un opportuno software detto browser. I documenti, chiamati genericamente pagine web, sono memorizzati in opportune porzioni della memoria dei

Server Web e sono tipicamente raggruppati in insiemi, detti Siti Web, più o meno uniformi per aspetto e contenuti e organizzati secondo una specifica struttura. Per essere accessibili, le pagine web vengono costruite mediante opportuni linguaggi descrittori, il più diffuso dei quali è l'HTML (HyperText Markup Language), che permette di specificare sia il contenuto delle pagine sia il loro formato di visualizzazione sul browser dell'utente. Tuttavia si tratta di un linguaggio poco flessibile e per superare tale limitazione si sono affermate nel tempo nuove metodologie e nuovi linguaggi per il Web, che hanno portato a quelle oggi note come pagine Web

dinamiche (contrapposte a quelle statiche scritte utilizzando solo l'HTML). Il contenuto e il layout di queste pagine dinamiche dipendono da una interpretazione operata dal browser o da una elaborazione da parte del Server, per cui il contenuto può cambiare in funzione dell'utente che richiede la pagina, al momento in cui lo fa e della navigazione precedentemente effettuata dall'utente stesso. Oggi la quasi totalità del Web è costituito da pagine dinamiche.

Il protocollo che regola le comunicazioni tra utente e fornitore (ossia tra client e server), nonché il trasferimento delle pagine web, è l'HTTP (HyperText Transfer Protocol)

o l'HTTPS nella sua versione "sicura". Le singole risorse disponibili sulla rete sono individuate univocamente da una serie di caratteri, denominata URI (Universal Resource Identifier) ad esempio www.gdf.it.

Esistono numerosi altri protocolli relativi ad altrettanti servizi presenti nel Web, di seguito se ne riportano i più comuni:

- DNS – per la traduzione da URL ad indirizzo IP;
- FTP – per il trasferimento di file;
- POP e SMTP – per la posta elettronica;
- RTP – RTSP – SIP per

la telefonia in Internet.

Nel 2011 Erich Shmidt, allora CEO di Google, ha stimato che l'intera dimensione di Internet fosse pari a circa 5.000.000 di terabyte ed ha inoltre osservato che, sino a quel momento, Google aveva indicizzato "solamente" 200 terabyte di dati. Tuttavia bisogna evidenziare che nella prima metà degli anni duemila vi è stata un'imponente crescita ed evoluzione dei contenuti della rete, dovuta alla nascita del Web 2.0. La peculiarità del Web è costituita dall'introduzione di plug-in che hanno consentito l'incremento dei c.d. Rich Internet Applications (RIA), applicazioni web che possiedono le

caratteristiche e le funzionalità delle applicazioni desktop senza però necessitare dell'installazione sul disco fisso. Si pensi agli attuali Social Network che, insieme alle App di messaggistica, hanno rivoluzionato l'utilizzo della rete Internet che in precedenza si limitava ad offrire più che altro servizi di tipo statico (consultazione motori di ricerca, navigazione tra le pagine, consultazione e-mail). Inoltre, con l'avvento dell'Internet of Things, unito alla sempre più larga diffusione a livello globale delle connessioni a banda larga, la crescita della rete si è ampliata in maniera esponenziale.

A riguardo, per avere contezza delle

dimensioni del Web conosciuto, vi sono alcuni servizi che offrono in tempo reale il numero di pagine indicizzate dai più comuni motori di ricerca. Tuttavia tale dato rappresenta solo una piccola porzione dell'intera rete Internet, comunemente denominata Clear Web, o Surface Web (Web "visibile"). Le stime ci dicono che la parte ancora sconosciuta del World Wide Web sia 10 volte più grande rispetto a quella attualmente indicizzata. Vi è, infatti, tutta una serie di contenuti che i motori di ricerca non indicizzano, il cosiddetto Deep Web.

L'indicizzazione è l'operazione che svolge un motore di ricerca, tramite l'utilizzo di appositi software chiamati

spider, i quali esplorano la rete Internet seguendo i link presenti sulle pagine e memorizzando i contenuti in un grande database che li associa al nome della relativa pagina (URL). La mancata indicizzazione di contenuti web può dipendere da fattori di policy o tecnologici: alcuni siti come ad esempio quelli delle testate giornalistiche, inseriscono nella directory principale del server un file di testo chiamato robots.txt contenente l'elenco di pagine e directory che gli spider dei motori di ricerca non possono prelevare. Quando una pagina viene pubblicata per la prima volta non sarà presente nei database di nessun motore di ricerca fino a quando non verrà visitata da uno spider, per cui

per questo lasso di tempo essa non farà parte del Clear Web così come è stato definito. Inoltre un'altra grande quantità di contenuti non possono essere visitati dai motori di ricerca perché non liberamente accessibili, si pensi a tutte quelle risorse la cui consultazione richiede un login con l'immissione di apposite credenziali. Tutti questi contenuti, insieme alle reti intranet, agli spazi di hosting condivisi tra scuole, università, uffici pubblici o aziende private costituiscono il Deep Web.

Essenzialmente, la Rete Profonda o Deep Web è quella porzione di Internet comunque accessibile tramite un tradizionale web browser, ma non indicizzata dai motori di ricerca.

Una particolare attenzione va rivolta al cosiddetto Dark Web, costituito a sua volta da diverse Dark Net. Secondo la più comune definizione il Dark Web è considerato un sottoinsieme del Deep Web. Questa affermazione può essere valida se si considera solo l'aspetto dell'indicizzazione, poiché effettivamente il contenuto del Dark Web non è indicizzato da alcun motore di ricerca. Tuttavia mentre il Clear ed il Deep utilizzano le stesse tecnologie, il Dark fa uso anche di altre, diverse ed esclusive. Una di queste tecniche è la Dark Net, ossia un tipo di Rete Privata Virtuale (VPN), che presenta misure idonee per oscurare gli indirizzi IP dei nodi della rete. In una rete di questo tipo

è difficile non solo risalire all'identità dell'emittente, ma persino sapere se un flusso di informazioni su un determinato protocollo è attualmente attivo. Esistono svariate tipologie di Dark Net, tecnicamente differenti tra loro, ma con uno scopo ben preciso: impedire il tracciamento del traffico al fine di occultare l'identità dei partecipanti ad una comunicazione digitale.

La Rete TOR rappresenta la più popolare via d'accesso al Dark Web, poiché mediante l'utilizzo dell'apposito client si possono raggiungere i Forum e Black Market. Il progetto TOR (acronimo di The Onion Router) è nato nel 1995 per merito della Marina Militare degli Stati Uniti allo scopo di

garantire che le conversazioni governative (ordini e disposizioni d'impiego) non fossero intercettate da entità nemiche o da servizi d'intelligence stranieri.

Sviluppato dal 2002 dalla Electronic Frontier Foundation è ora gestito da The Tor Project, un'associazione senza scopo di lucro. TOR, che utilizza il protocollo TCP, non solo permette di accedere ai servizi bloccati dagli Internet Service Provider svolgendo una funzione di proxy, ma ospita servizi che permettono agli utenti di pubblicare siti web senza dover rivelare il reale server su cui è ospitata la risorsa. Essi, infatti, sono protetti dall'analisi del traffico attraverso una rete di router (i c.d. onion

routers) che rendono la navigazione difficile da tracciare. Il funzionamento della rete Tor è concettualmente semplice: i dati che appartengono ad una qualsiasi comunicazione non transitano direttamente dal client al server (come invece avviene nel Clear e nel Deep Web), ma passano attraverso più nodi, detti anche relay, che costituiscono di fatto un circuito virtuale crittografato a strati (a cipolla). Infine, tramite il protocollo "onion" fornito da Tor, è possibile accedere ai cosiddetti domini ". onion", non accessibili dal Clear Web utilizzando i comuni browser. Si ritiene che ". onion" è uno pseudo-dominio di primo livello, cioè un dominio non tracciato dai server DNS tradizionali,

ma raggiungibile solo attraverso dei browser specifici, in questo caso Tor Browser.

Se si effettua una connessione attraverso la rete Tor il traffico in uscita viene cifrato e inviato verso un relay. Qualora si punti ad un dominio ". onion", tutta la comunicazione risulterà cifrata. Invece, se, tramite rete Tor, si volesse raggiungere un dominio tradizionale, il traffico verrà convogliato, completamente crittografato, verso degli exit node che si trovano in Paesi esteri dove la legislazione in materia di reati informatici è carente, riducendo il rischio di essere incriminati per il proprio traffico web.

Sicuramente la tipologia più diffusa di

servizi del Dark Web sono i Black Market, tuttavia esistono anche altri (pochi) tipi di applicazioni come Social Media. I più popolari sono Galaxy3 e Facebook. Facebook tende la mano agli utenti di TOR, noto sistema per la comunicazione anonima su Internet. Il social network utilizza gli stessi strumenti impiegati da coloro che condividono informazioni e risorse non passando attraverso il web tradizionale. È raggiungibile all'indirizzo https://facebookcorewwwi.onion dove gli utenti di TOR possono attivare una connessione cifrata end-to-end e mantenere il loro anonimato. Diversamente rispetto ad altre realtà, l'obiettivo di Facebook non è quello di

nascondersi né quello di creare una sua versione "parallela", inaccessibile ai motori di ricerca, ma la versione .onion di Facebook altro non è che una copia speculare del social network e di tutti i contenuti che sono quotidianamente veicolati attraverso di esso. L'obiettivo è quello di portare su Facebook ancora più utenti mettendo nelle loro mani uno strumento che permetta di partecipare "alla vita" del social network scavalcando ad esempio le misure censorie imposte da parte di governi antidemocratici.

I black Market operanti nella rete Dark hanno layout, funzioni e modalità di ricerca molto simili ai portali di e-commerce presenti nel Clear Web (tipo

e-bay). L'accesso avviene tramite registrazione: è sufficiente fornire un nome utente, una password, spesso senza la necessità di fornire un indirizzo e-mail, per usufruire di tutti i servizi offerti e raggiungibili dall'homepage. Bisogna evidenziare che i market si pongono come meri intermediari, essi infatti offrono lo spazio utile per la pubblicazione degli annunci dei vari venditori. Per ogni vendor è disponibile una pagina dedicata che offre, al pari di un qualsiasi altro portale legale di e-commerce, tutte quelle informazioni che ne formano il profilo pubblico e che contribuiscono ad aumentarne la "reputazione". Questa è ritenuta estremamente importante in una

compravendita anonima che, come quella che avviene nel Dark Web, è basata unicamente sulla fiducia che il venditore riesce ad ottenere dal cliente. Essa gli permetterà, tra l'altro, di ampliare la propria attività. La pagina offre informazioni dettagliate su: profilo del venditore, modalità di contatto, valutazioni di gradimento, oltre a "news" sui prodotti e a servizi offerti, spedizioni e pagamenti.

Gli annunci di vendita presenti nei Black Market sono suddivisi in diverse categorie di merci, beni e servizi di natura illecita. Generalmente, viene indicato il paese di spedizione ed il prezzo, espresso in euro e bitcoin. A tal proposito, occorre evidenziare che la

principale valuta di pagamento accettata sui Black Market operanti nel Dark Web, è il bitcoin. Una volta scelto e inserito il prodotto nel carrello personale, l'acquirente può passare al pagamento. La maggior parte dei Market adotta il metodo del deposito di garanzia, c.d. Escrow, con cui il cliente non paga direttamente il venditore, ma deposita la cifra stabilita presso l'operatore del mercato che, in tal modo, controlla tutte le transazioni, trattenendo la propria percentuale e risolvendo eventuali dispute. Non sono permessi pagamenti diretti, concordati in privato tra cliente ed acquirente, pena l'espulsione dal market place.

Gli annunci relativi alla vendita di

sostanze stupefacenti, solitamente, sono suddivisi in base alla tipologia di sostanza. Sono di facile reperibilità la maggior parte delle droghe, tra cui: cocaina, marijuana e hashish, nonché sostanze del tipo LSD e Ketamina, stupefacenti sintetici, principalmente MDMA (ecstasy) e altre anfetamine. I venditori sostengono di utilizzare precauzioni per il confezionamento e per la spedizione. In effetti nelle recensioni dei vari prodotti è possibile leggere i commenti degli acquirenti che si complimentano per lo Stealth utilizzato dal venditore, ovvero il metodo di camuffamento della sostanza inviata. Nella maggior parte dei Market, attraverso la visualizzazione delle

recensioni, è possibile stimare i volumi di vendita dei singoli venditori, almeno per l'ultimo mese.

Al fine di ostacolare le indagini di polizia giudiziaria molti venditori utilizzano un c.d. Drop. Si tratta di un vero e proprio intermediario che, in fase di spedizione, si interpone tra il cedente e l'acquirente, al fine di rendere difficoltoso il tracciamento di una spedizione da parte delle forze di polizia. Tale metodo viene utilizzato specialmente per la spedizione di droghe e armi, a volte inviate in più pezzi.

Oltre agli stupefacenti ed alle armi, tra i vari annunci è possibile rinvenire banconote, oro e documenti di identità

contraffatti. Il funzionamento di questi mercati è molto simile ai marketplace presenti sul Clear Web. Si cerca l'oggetto desiderato, si sceglie il venditore in base ai feedback ricevuti e si procede con l'ordine, fornendo, naturalmente, un indirizzo per la spedizione. Sono numerosi i venditori, verosimilmente anche italiani, che propongono in vendita documenti d'identità, nazionali ed esteri, e banconote contraffatte. Larga parte del commercio è costituito anche dalla vendita di carte di credito c.d. clonate. Il Ministero dell'Economia - Direzione V - Prevenzione dell'Utilizzo del Sistema Finanziario per Fini Illegali, si occupa, tra l'altro, dell'analisi e valutazione del

rischio e delle vulnerabilità del sistema finanziario e dell'elaborazione delle politiche di prevenzione di fenomeni criminali quali: riciclaggio del denaro, falsificazione dell'euro, finanziamento del terrorismo. Tale Dipartimento dirama, con cadenza quadrimestrale, la newsletter "Fraud: some facts" , mediante la quale pubblica i risultati del monitoraggio delle frodi nel panorama internazionale. Nella newsletter n. 15 vengono rilasciati i dati acquisiti dall'esplorazione dei Black Market, dai quali emerge come le banconote contraffatte rappresentano un commercio di primaria rilevanza in questa parte del Web.

Come abbiamo visto, la rete TOR,

finalizzata a garantire l'anonimato degli utenti che vi navigano, viene sfruttata per realizzare appositi siti simili ai comuni portali e-commerce, dove viene posta in vendita ogni sorta di merce illegale, tra cui, in particolare, droghe di ogni tipo, documenti falsi, valuta contraffatta, schede sim anonime e armi. Tutti gli utenti vengono identificati esclusivamente da un nickname, cui è legata tutta la loro attività online e la loro reputazione. I canali di comunicazione utilizzati sono: messaggistica interna dei siti di vendita, e-mail criptate, applicazioni per cellulare per messaggistica istantanea anonima, la chiave PGP.

La chiave PGP (acronimo di pretty good

privacy) viene utilizzata per cifrare il contenuto delle e-mail e rafforzare l'anonimato e la privacy delle comunicazioni. Il sistema PGP è un sistema definito "a doppia chiave", ovvero basato su due chiavi di cifratura. Delle due chiavi una è definita pubblica e l'altra è definita privata e sono necessarie entrambe per poter comunicare tramite messaggi criptati. La chiave pubblica serve per cifrare il contenuto dell'e-mail mentre la privata per decifrarlo. Qualora si intende mandare un messaggio a un determinato soggetto, se ne cifrerà il contenuto con la sua chiave pubblica cosicché solo il destinatario sarà in grado di leggerlo, decifrandolo grazie alla propria chiave

privata. All'atto di generare una coppia di chiavi da utilizzare per poter comunicare in maniera sicura, può essere comunicato anche un indirizzo e-mail da abbinare alla chiave pubblica, cosicché condividendo esclusivamente la propria chiave pubblica con eventuali soggetti che potrebbero avere la necessità di recapitare messaggi criptati, viene condiviso anche il contatto a cui inviare tali messaggi criptati. In tal modo può essere utilizzata sempre la stessa coppia di chiavi per ogni persona (o meglio per ogni indirizzo e-mail) e non è necessario generare e comunicare una nuova chiave per ogni messaggio. Tale indirizzo e-mail non viene verificato in alcun modo, quindi è

possibile abbinare anche indirizzi e-mail non validi o inesistenti. Tuttavia, nel caso dei vendors del Dark Web, essendo nel proprio interesse fornire un indirizzo valido per poter essere contattati dai potenziali clienti, è del tutto ragionevole ritenere validi gli indirizzi e-mail che vengono abbinati alle chiavi. Per generare, gestire e utilizzare la coppia di chiavi possono essere utilizzati appositi software, ad esempio GPG4Win, Enigmail o Kleopatra. Quando viene generata una coppia di chiavi, la chiave pubblica, abbinata all'indirizzo e-mail ed eventualmente ad altre informazioni facoltative, viene memorizzata su server appositamente predisposti, denominati

key-server. Invece la chiave privata viene custodita esclusivamente dal proprietario.

In questo settore, le investigazioni partono analizzando i profili, le attività e le discussioni nei forum dei vari vendor al fine di reperire il maggior numero di informazioni possibili. Una tecnica frequentemente utilizzata è quella di analizzare la chiave PGP per determinare l'indirizzo e-mail associato al venditore, per intraprendere successivamente un'attività di OSINT utile a verificare se tale indirizzo è stato utilizzato nel Clear Web (per registrazioni in Social Media, per partecipazioni a forum, inscrizioni a siti web ecc.). Va precisato infatti che il

monitoraggio del web può essere effettuato nel clear web ma è impossibile nel dark web atteso che in quest'ultimo vi sono venditori e compratori di prodotti illegali che pur celandosi sotto l'anonimato di fatto sono persone fisiche che devono essere individuate. Nel caso si riuscisse a trovare un riscontro positivo, si procederà con le classiche operazioni di Polizia Giudiziaria (acquisizione di log, risoluzione di indirizzi IP, operazioni sotto copertura, etc.).

Per quanto riguarda gli acquisti in ambiente Dark Web, come detto, questi vengono effettuati, nella quasi totalità dei casi, utilizzando la criptovaluta bitcoin. Possono essere concordati

tramite messaggi o portali di vendita, i quali gestiranno anche il trasferimento di bitcoin e lo scambio di dati, quale, ad esempio, l'indirizzo di consegna della merce. Come recapiti vengono utilizzati spesso i cosiddetti "punti di ritiro", ovvero servizi che si occupano di ricevere e custodire la corrispondenza che potrà essere ritirata in un secondo momento da parte dell'effettivo destinatario.

Oltre TOR vi sono poi altre reti analoghe definite di tipo decentralizzato. In sostanza una rete è centralizzata quando la sua integrità ed il suo funzionamento dipendono da un unico elemento principale, il server, senza il quale la rete non può funzionare. Tale

architettura ha un unico punto ove sono concentrate le risorse fruibili, offrendo semplicità di sviluppo e stabilità. L'amministratore del sistema dovrà gestire un unico nodo della rete, appunto il server, potrà osservare e analizzare il comportamento di tutti gli utenti ed avrà il controllo completo sul comportamento degli utenti e sulla loro privacy. Questa limitazione alla privacy ha portato al proliferare di nuove architetture di rete, cd. reti decentralizzate, che non prevedono un'unica entità centrale di gestione e offrono una maggiore libertà per il comportamento degli utenti e la loro privacy. Le tipologie decentralizzate, del tipo peer to peer (P2P), che hanno avuto maggior

successo negli anni, oltre a TOR, sono FreeNet, AnoNet e I2P, anche se con una sostanziale differenza. Difatti mentre TOR consente la navigazione web "classica" in modalità anonima, le altre sono da considerarsi come sotto reti chiuse, nel senso che non consentono di raggiungere risorse web allocate al di fuori di esse. Lo scopo di un sistema P2P è di permettere la condivisione, in modo non centralizzato, di risorse e servizi (es. scambio di informazioni, cicli di computazione, spazio su disco per i file). In tale sistema ciascun computer (detto nodo) è responsabile del passaggio dei dati alle altre macchine, svolgendo allo stesso tempo il ruolo sia di client che di server.

Freenet è un software gratuito che permette, in modo anonimo, di condividere file, chattare nei forum (privati) e navigare in particolari siti web accessibili solamente con tale software, i cosiddetti "freesites". Ha una topologia altamente decentralizzata il che lo rende un sistema resistente agli attacchi e alle intercettazioni, anche perché ogni nodo, ovviamente anonimo, conosce soltanto una ristretta cerchia di nodi ad esso direttamente collegati, ai quali gli è consentito connettersi. Dalla versione 7.0 (2008) Freenet offre una particolare modalità di utilizzo detta "darknet", che, al contrario della modalità classica OpenNet che permette di collegarsi a qualsiasi altro utente,

consente agli utenti di connettersi tra loro solo se "amici", ossia se già si conoscono e previa ricezione di inviti personali di connessione. Questa modalità di funzionamento è come un "circolo chiuso" praticamente impenetrabile e impossibile da rilevare. Dal punto di vista investigativo l'unico metodo per inserirsi in questa "darknet" è acquistare fiducia ricorrendo ad "operazioni sotto copertura" da parte della Polizia.

Le comunicazioni tra i nodi Freenet sono crittografate e vengono instradate attraverso percorsi che coinvolgono, in maniera casuale, altri nodi, rendendo così estremamente difficile sia determinare chi sta richiedendo le

informazioni sia il loro contenuto. A differenza delle altre reti P2P, Freenet, oltre a trasmettere i dati tra i nodi, li memorizza anche, lavorando come un enorme cache distribuita. Gli utenti contribuiscono alla rete fornendo sia larghezza di banda che una parte del loro disco rigido (chiamato “archivio dati”) per la memorizzazione dei file. I file vengono automaticamente mantenuti o eliminati a seconda di quanto sono popolari così che i meno popolari vengono eliminati per far posto a contenuti più recenti. Tutti i file archiviati sul disco rigido e condivisi con gli atri utenti sono cifrati, quindi l’utente non può scoprire cosa c’è nel proprio “archivio dati”. Questo

“archivio dati” contiene, in maniera cifrata, oltre ai file condivisi, anche le informazioni sui forum di chat e sui siti Web (freesites).

Un’importante differenza rispetto a TOR è che Freenet non fornisce un servizio di proxy, ossia non è possibile utilizzarlo per raggiungere in modo anonimo risorse web pubbliche, funzionalità invece offerta da TOR. Freenet consente solo connessioni tra gli utenti dello stesso software, è di fatto un “club chiuso”.

AnoNet è una rete decentralizzata peer to peer a cui possono collegarsi solo utenti che dispongono di una apposita chiave crittografica e che utilizzano un particolare software open source,

OpenVPN, molto diffuso per creare reti private virtuali VPN (Virtual Private Network). Quando due utenti decidono di mettersi in comunicazione via OpenVPN, devono scambiarsi le proprie chiavi pubbliche (generate dal software con algoritmo RSA). OpenVPN usa le chiavi per creare un "tunnel", ovvero un canale di comunicazione cifrato tra i nodi di AnoNet che protegge la comunicazione dall'analisi del traffico.

L'utilizzo del tunnel non garantisce l'anonimato limitandosi a proteggere il contenuto dei messaggi. Tuttavia AnoNet, per garantire l'anonimato degli utenti, svincola gli indirizzi IP che identificano i nodi della rete in quanto è di fatto una sottorete privata che utilizza

un particolare range di indirizzi IP (da 1.0.0.0 a 2.255.255.255) che non appartiene ai normali indirizzi IP usati in Internet. Inoltre è dotato di un proprio protocollo di routing detto "Quagga", sotto forma di software che deve essere installato su qualunque nodo della rete.

I2P nasce nel 2003 come proposta di modifica di Freenet originariamente chiamata Invisible Internet Project (IIP). Si tratta di un software Open Source per la realizzazione di una rete anonima. I2P è ancora in fase di sviluppo, quindi ritenuta non ancora idonea per usi che necessitano di un forte anonimato. La rete è costituita da un insieme di nodi (detti router) ognuno dei quali costruisce un certo numero di tunnel (canali virtuali

di comunicazione cifrata) unidirezionali in ingresso ed in uscita destinati al traffico cifrato. Ogni router (nodo della rete) è univocamente identificato all'interno della rete dal proprio ID (RouterIdentity), e comunica con altri router ed utilizzando protocolli standard può sfruttare l'infrastruttura Internet.

I client possono connettersi a qualsiasi router (gli altri client) ed autorizzare l'assegnazione temporanea di alcuni tunnel che saranno utilizzati per l'invio e la ricezione di messaggi attraverso la rete. Quando un client vuole inviare un messaggio ad un altro client, utilizza l'ID del destinatario per individuarlo nella rete. Il client che spedisce (mittente) invia il messaggio attraverso

uno dei suoi tunnel di uscita, e lo indirizza verso uno dei tunnel in entrata dell'altro client (destinatario). Ogni partecipante della rete decide la lunghezza di questi tunnel, ossia quanti altri client dovranno essere coinvolti per il rilancio dei messaggi in accordo alle proprie necessità, mantenendo un numero ridotto di nodi (client) per evitare la possibilità di intercettazioni.

2.2 LE CRIPTOVALUTE NEL WEB "OSCURO"

È attualmente crescente la consapevolezza che la criminalità è motivata soprattutto da logiche di

profitto e di potere, per cui è rilevante comprendere le dimensioni di tali profitti e in quali attività essi si concentrino. L'investimento criminale in aziende legali viene considerata la strategia di infiltrazione più pericolosa: la presenza sul mercato di imprese riconducibili alle organizzazioni criminali genera infatti delle distorsioni nella concorrenza che possono compromettere l'integrità del tessuto socio-economico di un territorio. L'uso di società o altri enti dotati di personalità giuridica (es. associazioni, cooperative, etc.) rende più difficile la tracciabilità dei beni al legittimo proprietario nonché di diversificare meglio l'investimento e quindi di

renderlo meno aggredibile dalle forze dell'ordine. La frammentazione del patrimonio in pacchetti azionari/quote di diverse società, magari anche intestati a prestanome, minimizza il rischio che possa venire sequestrato o confiscato nella sua interezza[38].

La scelta delle organizzazioni criminali di investire in aziende nasce da ragioni strategiche e funzionali legate in primo luogo all'occultamento delle attività criminali attraverso falsificazioni contabili o fatturazioni fittizie, ma può avere anche un obiettivo economico-sociale legato al rilevamento, paleso od occulto, di attività commerciali (favorito negli ultimi anni dalla crisi economica), che consente anche la realizzazione di un

profitto.

Dalle caratteristiche, entità e natura delle operazioni sospette (SOS), segnalate dai soggetti obbligati (intermediari finanziari, professionisti ed operatori non finanziari) alla Banca d'Italia e giunte per gli approfondimenti operativi ai reparti della Guardia di Finanza, le operazioni di riciclaggio sono state attuate nel tempo prevalentemente attraverso alcuni meccanismi diffusi nell'ambito delle condotte per evasione fiscale:

- da un lato il ricorso a fatture per operazioni inesistenti[39] (FOI) ovvero importazioni fittizie di beni che

consentono di giustificare una movimentazione finanziaria e/o il trasferimento di fondi a fornitori esteri (ad esempio un titolare di imprese operanti nel settore del commercio di auto, con particolare riguardo agli autoveicoli provenienti da paesi U.E., immessi nel mercato locale attraverso il sistema della cd. *frode carosello*[40], per mezzo delle quali clan camorristici hanno reimpiegato notevoli

disponibilità finanziarie di origine illecita);

- dall'altro ad operazioni realizzate mediante il meccanismo dell'*interposizione fittizia*[41], consistente nell'adozione di negozi giuridici simulati intestati a "prestanome" finalizzati ad occultare l'effettivo proprietario (ad esempio la ricchezza accumulata illecitamente nel periodo di massima operatività da clan dei cd. Casalesi e la successiva opera di

riutilizzo dei capitali, ha consentito ai familiari del citato gruppo di porre in essere una cospicua serie di compravendite di beni immobili, nonché l'avvio o il rilevamento di diverse attività commerciali controllate per interposta persona).

A queste due modalità illecite se ne è aggiunta una terza costituita sempre dall'interposizione fittizia di "prestanome", individuati dalle organizzazioni criminali e posti a capo di società che, dopo un periodo di avvio delle attività economiche non procedono

al versamento delle imposte, lasciando "morire" le stesse società e creando in tal modo una liquidità di denaro che si sposta in altre direzioni, paravento ad altre attività illecite o a forme di riciclaggio. Ormai la dimensione transnazionale dei fenomeni illeciti è la logica conseguenza dell'abbattimento dei confini e delle opportunità offerte dalla internazionalizzazione dei mercati, che se da un lato offrono prospettive di sviluppo alle iniziative economiche lecite, dall'altro consentono alle organizzazioni delinquenziali di ampliare lo spettro delle attività illecite proiettando i loro interessi su aree territoriali sempre più vaste. Nel quadro descritto, è evidente come il controllo

dei movimenti transfrontalieri di valuta, il contrasto all'evasione fiscale, insieme alla limitazione dell'uso del contante, alla canalizzazione dei flussi attraverso intermediari finanziari, rappresentino i cardini del sistema di prevenzione antiriciclaggio perché permettono di garantire il necessario monitoraggio sui trasferimenti di ricchezza tra soggetti diversi. È noto, infatti, che i proventi di natura illecita vengono realizzati e trasferiti evitando quanto più possibile forme di controllo disciplinate dalla normativa antiriciclaggio, utilizzando canali informali e rimesse dirette. Il denaro contante rimane il mezzo di pagamento a cui molto spesso le organizzazioni criminali ricorrono per

regolare i propri rapporti economici. Non a caso la Guardia di Finanza, lungo il confine, ai valichi e varchi portuali ed aeroportuali, nel solo 2016 ha individuato 11.280 soggetti che tentavano l'esportazione/importazione illegale di valuta con il sequestro di euro 81,5 milioni[42].

È evidente che tra riciclaggio ed evasione fiscale vi è uno stretto legame, tuttavia non tutte le evasioni fiscali configurano in automatico responsabilità per riciclaggio, per quanto però le frodi fiscali, l'emissione di fatture per operazioni inesistenti, la presenza di "prestanome" a capo di aziende che dopo pochi anni di attività spariscono senza versare le imposte dovute, sono

connessi al riciclaggio. In ogni caso è fondamentale approfondire i contesti investigativi in modo da affrontare in maniera trasversale tutte le possibili implicazioni d'ordine economico-finanziario, valorizzando nel modo più efficace gli strumenti normativi ed operativi di cui si dispone ed adottando le più appropriate tecniche investigative mediante un sistema che abbracci le funzioni di polizia economico-finanziaria (tributaria e valutaria) con quelle di polizia giudiziaria. È da ritenere che l'attività di prevenzione e repressione di tali fenomeni illegali vada svolta mediante quattro diverse tipologie:

- l'esecuzione di

controlli sulla movimentazione transfrontaliera di valuta;

- il monitoraggio dei flussi finanziari da e per l'estero, attraverso ispezioni e controlli antiriciclaggio;

- l'approfondimento delle segnalazioni di operazioni sospette, generate dal sistema di prevenzione antiriciclaggio[43];

- soprattutto, lo scambio di informazioni a livello internazionale, integranti dati aventi profili fiscali

e di antiriciclaggio (come il citato *Common Reporting Standard*).

Tale ultima azione è la più debole e, nello stesso tempo, la più importante nel complessivo sistema di prevenzione antiriciclaggio: anzi maggiori sono le restrizioni internazionali, maggiori sono le ricerche, da parte di gruppi criminali, di territori non cooperativi. È il caso della Corea del Nord e dell'Iran che sono individuati dal FATF/GAFI ancora come Paesi ove non sono stati fatti progressi in materia di antiriciclaggio. Possiamo affermare che tutti gli altri Paesi del mondo partecipano ai processi di cambiamento più sotto la spinta dei

timori connessi ad un riciclaggio di denaro che finanzi il terrorismo internazionale invece di un'adesione che limiti la criminalità economica. Difatti se guardiamo alla connessione Fisco/Riciclaggio notiamo che, oltre Bahrein, Cook, Nauru, Panama, Vanuatu che pur aderendo al CRS non hanno fornito indicazioni sull'effettivo termine di attuazione dello standard per l'inizio dello scambio obbligatorio di dati e notizie, vi sono molti altri Stati che non sembrano al momento volervi partecipare, lasciando quindi aperto il campo del riciclaggio di denaro proveniente da delitti tra cui lo stesso finanziamento al terrorismo, proprio per effetto della notata confusione esistente

tra reddito/patrimonio/provento illecito. Alle tre modalità illecite sopracitate si vanno aggiungendo le operazioni in valuta virtuale soprattutto nel Dark web. Come noto da tempo ormai, con appositi software e qualche competenza informatica è possibile navigare nel Dark Web e sfogliare "cataloghi digitali" di ogni sorta di materiale illegale, sia fisico che digitale. Navigando nel cosiddetto clear web, la parte di Internet normalmente indicizzata dai motori di ricerca, è semplice reperire informazioni su come raggiungere questi portali. Infatti, i siti del Dark Web non hanno nomi comuni e facilmente memorizzabili, bensì sono costituiti da stringhe alfanumeriche

pseudocasuali di 16 caratteri, che terminano con l'estensione ".onion". È possibile trovare sia informazioni provenienti da portali di informazione e forum, sia specifici siti web dedicati, come deepdotweb.com e darkwebnews.com.

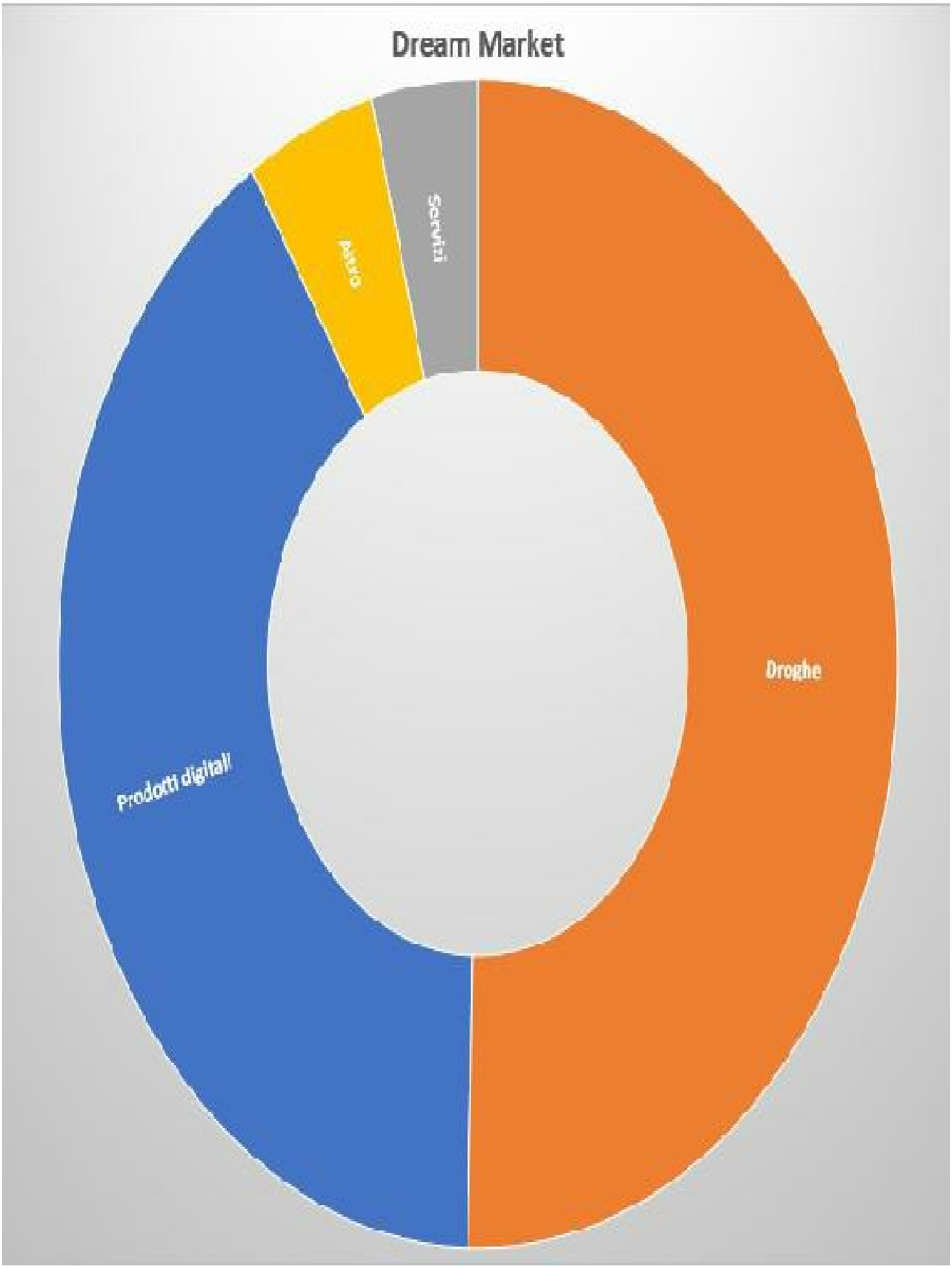
Consultando le risorse sopra citate e frequentando regolarmente ambienti virtuali dedicati al dark web, è molto semplice trovare una grande moltitudine di portali di vendita di merce illegale raggiungibili navigando nel Dark Web. Tra questi sono stati esaminati i seguenti, in quanto ritenuti essere i più frequentati e affidabili e per i quali non è prevista alcuna restrizione all'iscrizione:

- Dream Market (http://ptlsz6dxboul2u3z.c
- Wall Street Market (http://wallst4qihu6lvsa.o
- Point Tochka Free Market (http://pointgg344ghbo2s.
- Empire Market (http://empiremktxgjovhm

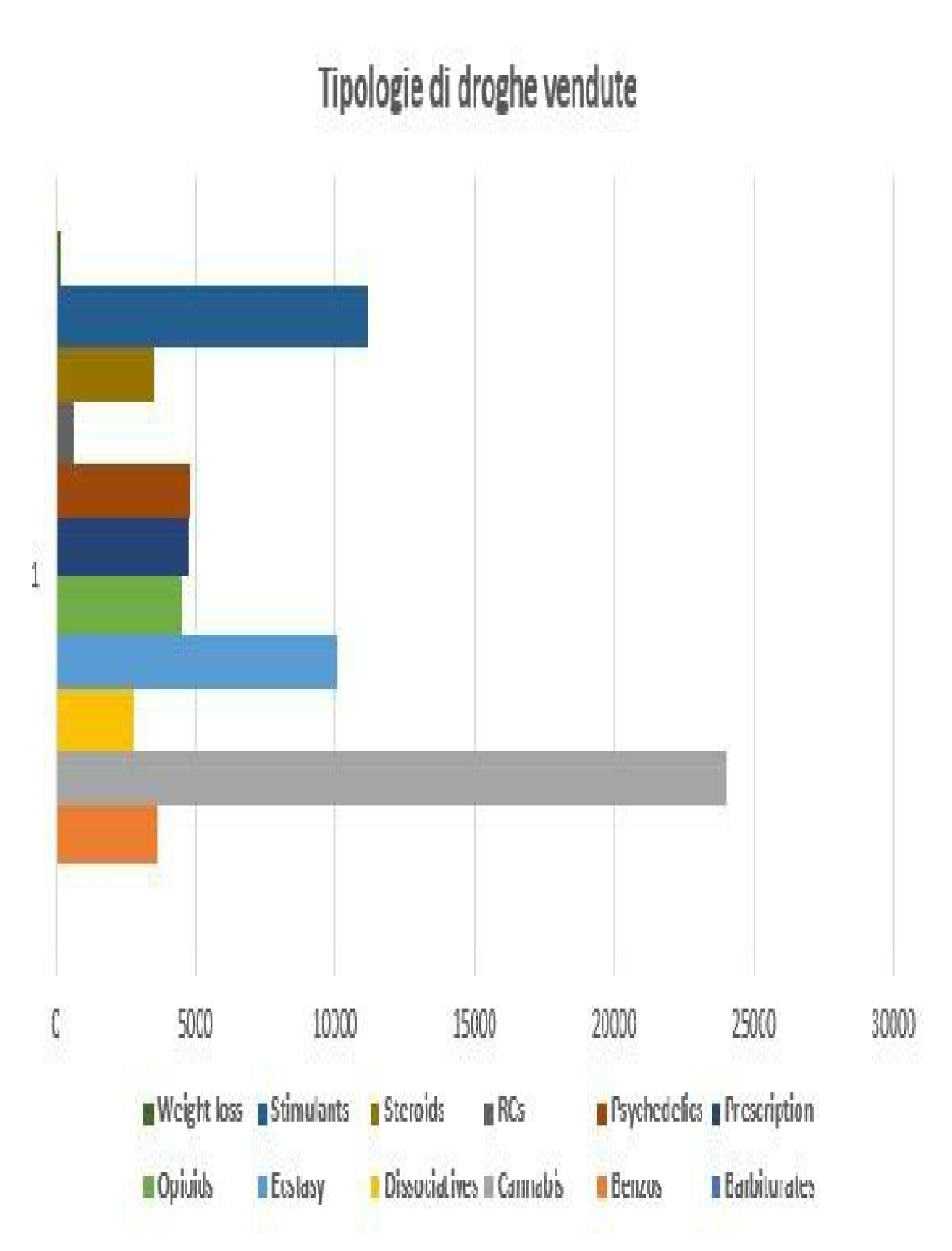
Il portale Dream Market è probabilmente quello più conosciuto e quello attivo da più tempo. È possibile trovarvi principalmente stupefacenti di ogni tipo, anche sintetici.

Di seguito una ripartizione delle categorie di merce venduta, basata sul numero di annunci presenti in ciascuna

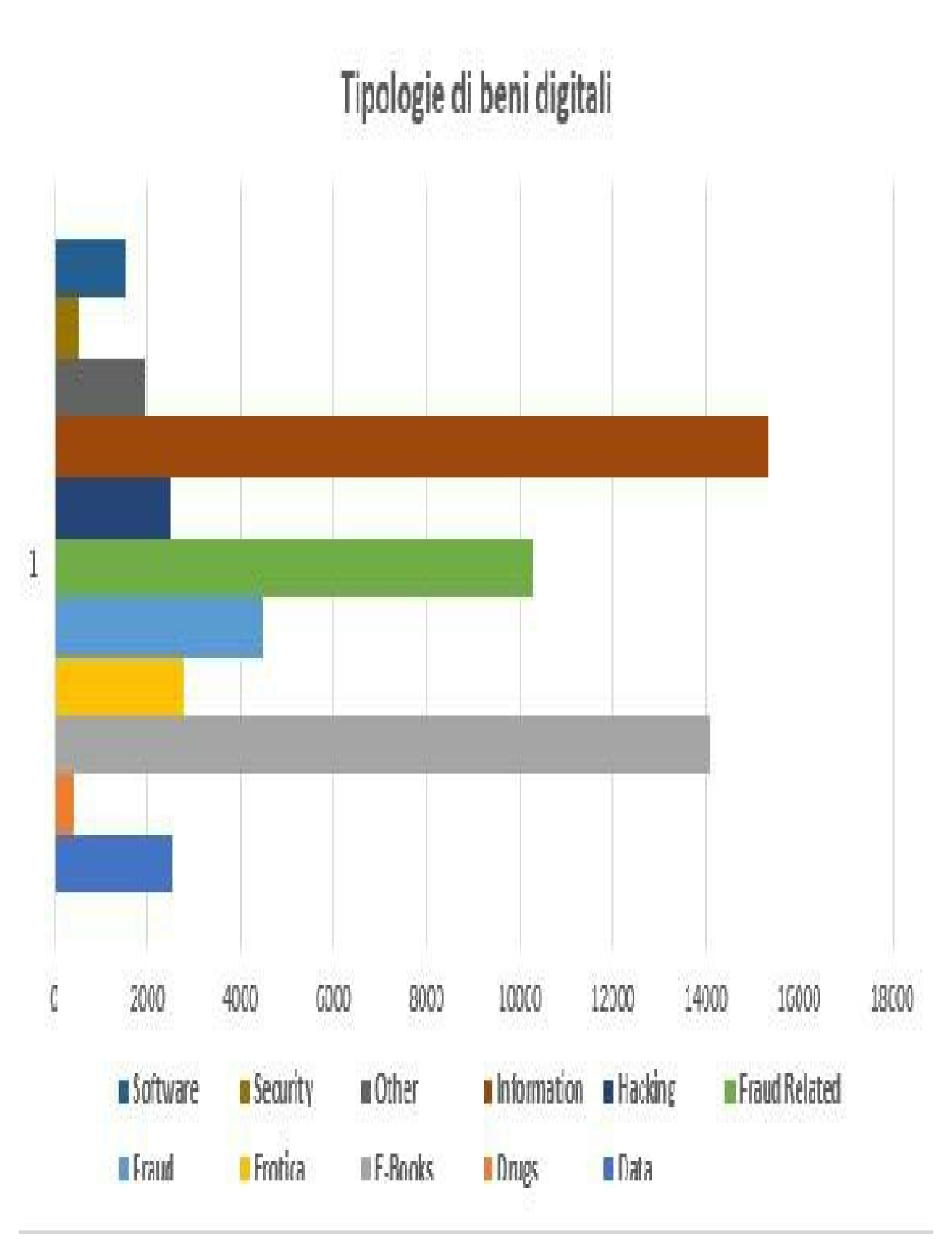
di esse.


Dream Market
Servizi
Altro
Prodotti digitali
Droghe

In particolare, all'interno della categoria droghe, sono presenti molte altre sottocategorie così ripartite.


Tipologie di droghe vendute
1
0
5000
10000
15000
20000
25000
30000
Weight loss
Stimulants
Steroids
RCs
Psychedelics
Prescription
Opioids
Ecstasy
Dissociatives
Cannabis
Benzos
Barbiturates

La categoria dove è possibile trovar più annunci è quella relativa alla Cannabis. Anche la categoria delle droghe stimolanti, tra le quali rientra la cocaina racchiude un gran numero di annunci. L'altra categoria rilevante, per quanto riguarda Dream Market, è quella dei cosiddetti beni digitali. È possibile acquistare tutti quei beni che non necessitano di essere spediti fisicamente ma che possono essere utilizzati per porre in essere attività illecite.


Tipologie di beni digitali
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
Software
Security
Other
Information
Hacking
Fraud Related
Fraud
Frnitica
F-Ronks
Drugs
Data

I prodotti più diffusi sono quelli relativi alla raccolta di informazioni. Infatti molti utenti si rivolgono ai black market per acquistare guide e informazioni condivise, dietro compenso, da altri criminali che possono così guadagnare vendendo la loro esperienza oltre che compiendo attività illecite.

Per poter effettuare acquisti su Dream Market è necessario prima di tutto aprire e ricaricare un proprio conto. Il market fornirà un indirizzo dedicato verso cui effettuare la transazione. Una volta completata la transazione, in alto a destra sarà visibile il saldo disponibile, che verrà stornato man mano che vengono effettuati acquisti.

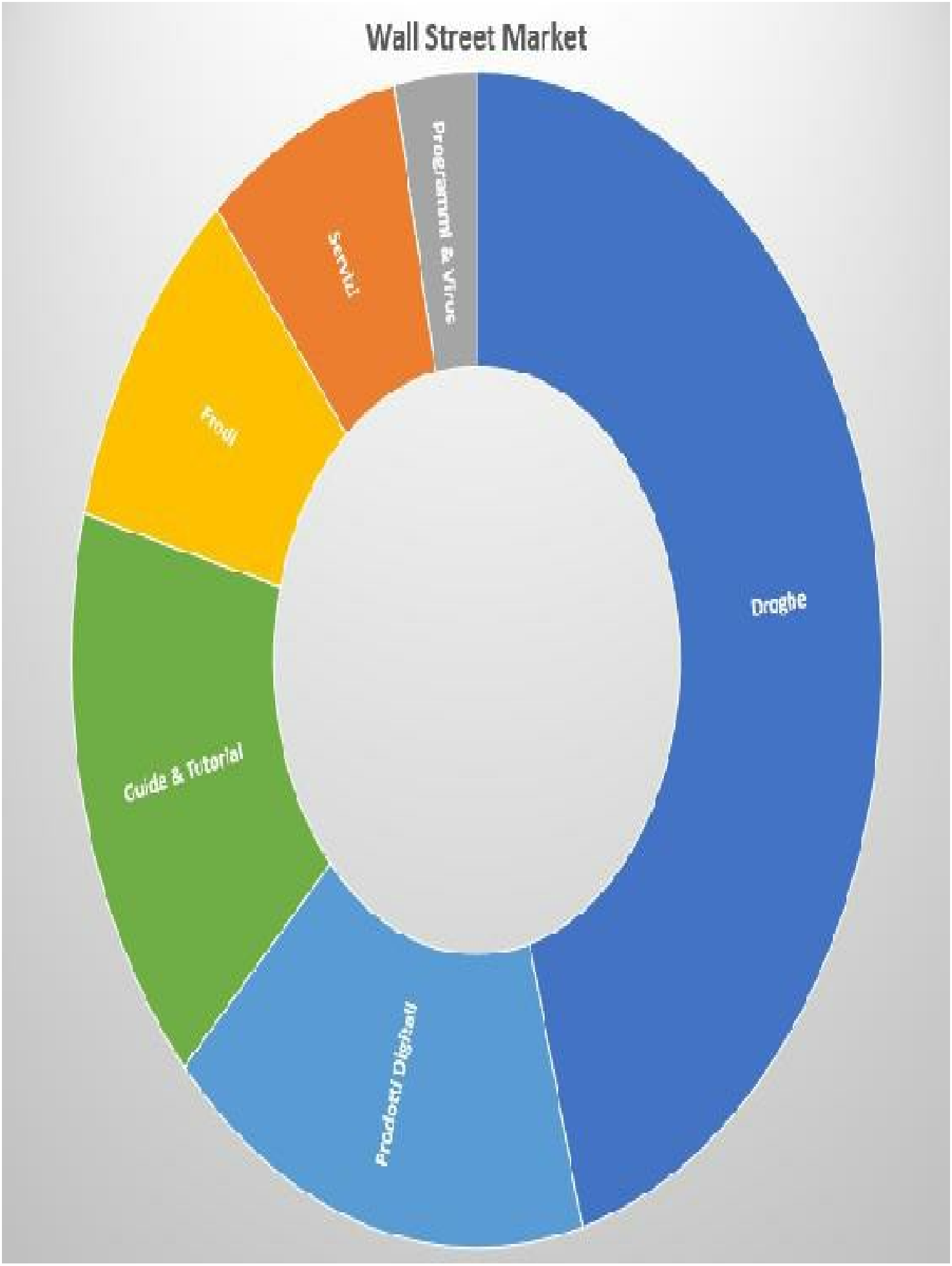
Il secondo portale esaminato, Wall Street Market, si presenta molto simile a Dream Market, sia per interfaccia grafica, sia per categorie merceologiche vendute.

Navigando sul lato sinistro dell'interfaccia è possibile visualizzare le seguenti categorie in cui sono suddivisi un totale di quasi 15.000 annunci.

Droghe	6.721
Servizi	1.149
Programmi & Virus	478

Frodi	1.455
Prodotti Digitali	2.498
Guide & Tutorial	2.374
TOTALE	14.675

Anche in questo caso la categoria più popolata di inserzioni di vendita è quella relativa agli stupefacenti, seguita dai prodotti digitali e dalle guide.


Wall Street Market
Droghe
Prodotti Digitali
Guide & Tutorial
Frodi
Servizi
Programmi & Virus

In questo caso, per effettuare i pagamenti non è necessario ricaricare il proprio saldo sul sito, affidando di fatto le proprie valute virtuali agli amministratori del portale. Infatti, una volta selezionato l'articolo desiderato ed aver indicato l'indirizzo dove si desidera ricevere la merce e gli altri dettagli richiesti, sarà generato un apposito indirizzo verso cui effettuare la transazione e perfezionare l'acquisto.

Order information

ID	#418133
Cryptocurrency	Bitcoin
Status	Waiting for deposit
Auto finalize	2d 23h 55m 14s
Trade address	3DefJnMYpiyooAVQJB2Jkxbg1dc24gdv41
	Open on block explorer
Price	**0.04779701** BTC (232,00€)
Received (confirmed)	0 BTC Nothing deposited

Un altro black market molto diffuso e attivo è Point Tochka Free Market. Si presenta con un'interfaccia diversa dal solito. Tutti i nickname sono preceduti dal carattere @, come accade su alcuni social network del clear web.

Sul lato destro dell'interfaccia sono presenti le seguenti categorie di prodotto acquistabili.

Droghe	5.283
Farmaci	2.952
Frodi bancarie	1.353
Documenti	

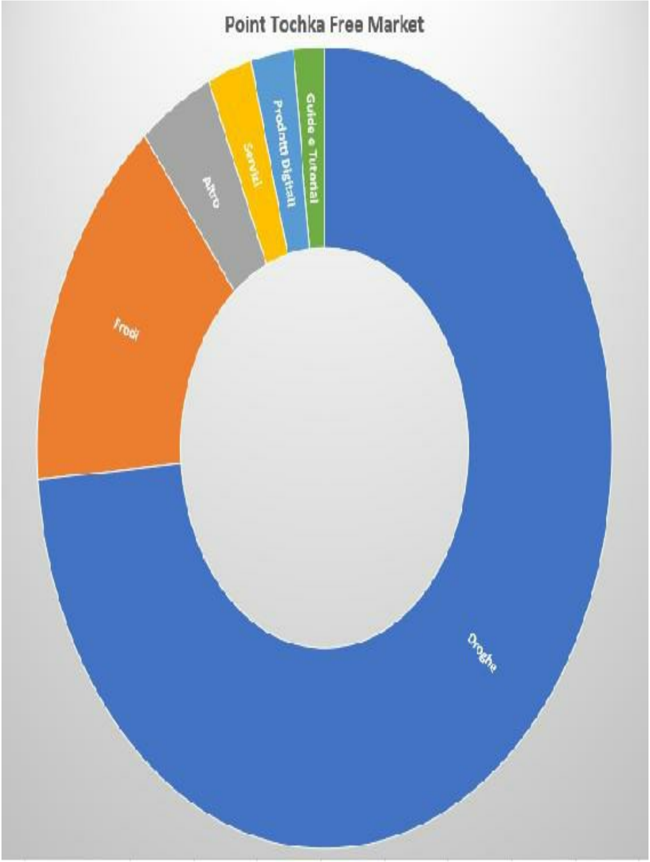
	423
Altro	406
Servizi	286
Steroidi	259
Prodotti Digitali	234
Guide e Tutorial	198
Software	44
Hardware	29
Luxury	23

Fashion	21
Biglietti	6
Alcohol	2

TOTALE	11.519

Raggruppando tra di loro categorie affini, è possibile vedere come anche in questo caso, la ripartizione degli annunci si presenti similare ai casi precedentemente esaminati, con una grande preponderanza di quelli relativi

agli stupefacenti.


Point Tochka Free Market
Guide e Tutorial
Prodotti Digitali
Servizi
Altro
Frodi
Droghe

Per effettuare un acquisto è necessario eseguire una transazione verso un indirizzo appositamente generato. Così facendo non ci si esporrà al rischio che gli amministratori del portale possano prendere il controllo delle somme depositate.

Altro market interessante che sta facendo molto parlare di sé è Empire Market. È nato dalle ceneri del portale Alphabay, sequestrato dal Federal Bureau of Investigation (FBI) nel luglio del 2017, e sembra conservarne e migliorarne le caratteristiche. Il market richiede di depositare le valute virtuali sul proprio account, così che l'utente possa avere un proprio saldo a cui

attingere per effettuare gli acquisti. È in più disponibile una sezione apposita dove acquistare codici di carte di credito indebitamente carpiti e credenziali di accesso per account di terzi, visibile cliccando in alto a destra sul tasto “My Autoshop”. Il venditore mette le informazioni vendute a disposizione del market. Quando l’utente ha effettuato e pagato un ordine, riceve in automatico le informazioni acquistate. Il market si occuperà di ricompensare il venditore. Praticamente questa parte del market è automatizzata, per questo viene chiamata autoshop.

Buy Cards | Buy Accounts | My Purchased Cards | My Purchased Accounts

BIN: [ ] City: [ ] State: [ ] Zip: [ ] Country: Italy Is Fullz (Any)

DOB (Any) SSN (Any) DOB Year 0000 to 9999 Price 0.01 to 999.99 Notes [ ] Rating (Any)

Bank (Any) Type (Any) Class (Any) Level (Any)

Search Clear All

Type	BIN	Exp.	Seller	Name	City	State	Zip	Country	Notes	DOB	SSN	Fullz	Price
VISA	471992	12/19	AMAZING (84.21%) (19)	Manue...	Monte Sabino	Rieti	02025	Italy	No	1973	Yes	Yes	$6.53
VISA	403293	03/19	AMAZING (84.21%) (19)	Roman...	Stagno Lombardo	Cremona	26049	Italy	No	1951	Yes	Yes	$6.53
VISA	471585	10/21	AMAZING (84.21%) (19)	Natal...	Lazzo Oro	Messina	98100	Italy	No	1986	Yes	Yes	$6.53
VISA	471591	04/21	AMAZING (84.21%) (19)	Ronca...	Collalbo	Bolzano	39043	Italy	No	1961	Yes	Yes	$6.53
VISA	[illegible]	[illegible]	[illegible]	Adele	[illegible]	[illegible]	[illegible]	Italy	No	1952	Yes	Yes	$6.53
VISA	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Italy	No	1940	Yes	Yes	$6.53

Per poter effettuare un acquisto, al pari di quanto accade con Dream Market e come accadeva con Alphabay, è necessario ricaricare il proprio saldo, che verrà stornato man mano che vengono effettuati gli acquisti. In ogni caso è possibile richiedere il rimborso delle somme depositate in qualsiasi momento. Il market effettuerà così una transazione per rimborsare i fondi richiesti.
È possibile visualizzare le varie categorie, di seguito elencate e a loro volta suddivise in sottocategorie maggiormente dettagliate.

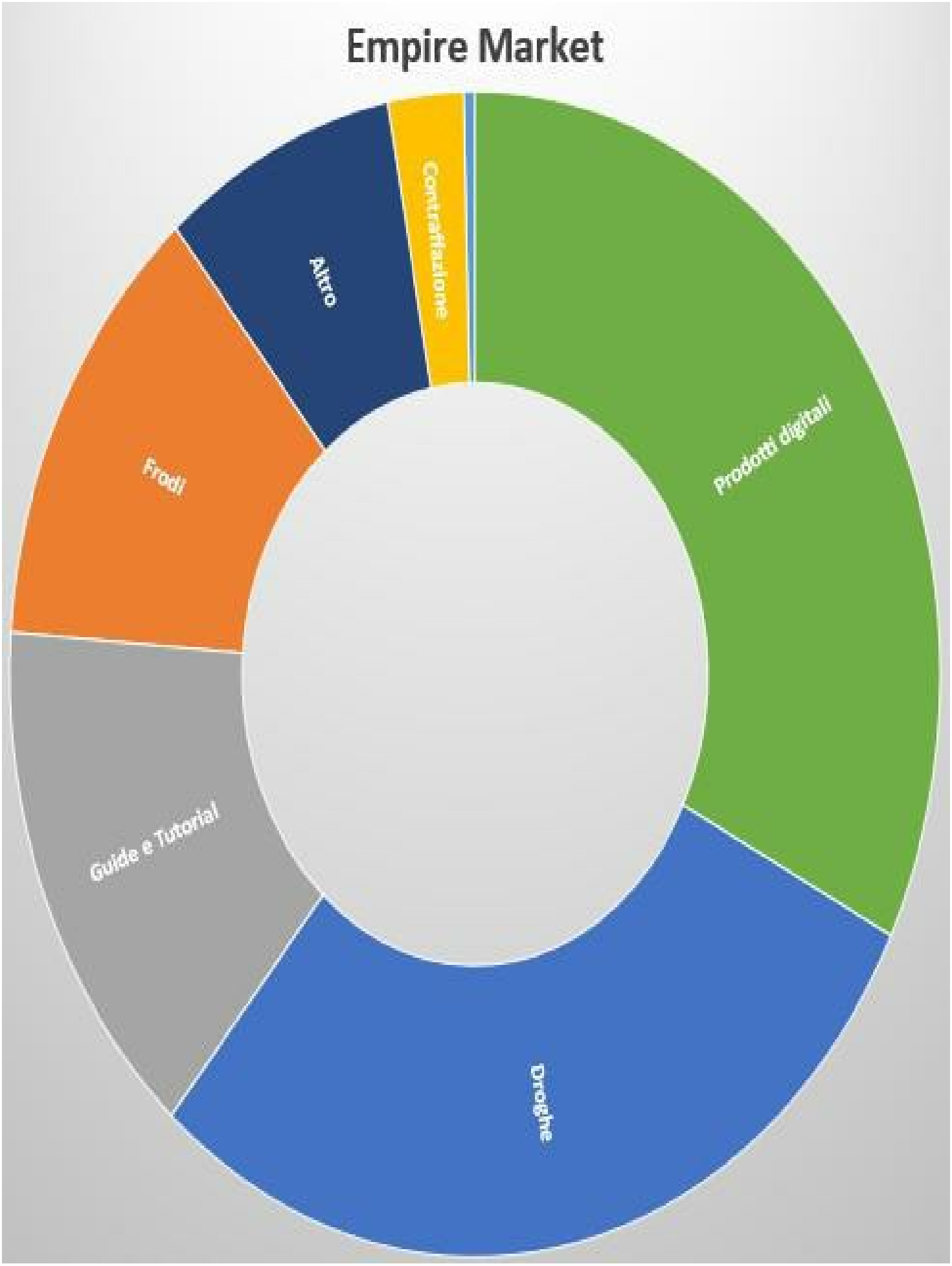
Frodi

Droghe	1044 2462
Guide&Tutorial	1263
Contraffazione	114
Prodotti Digitali	2758
Gioielleria	109
Armi	34
Oggetti Cardati	40
Servizi	166

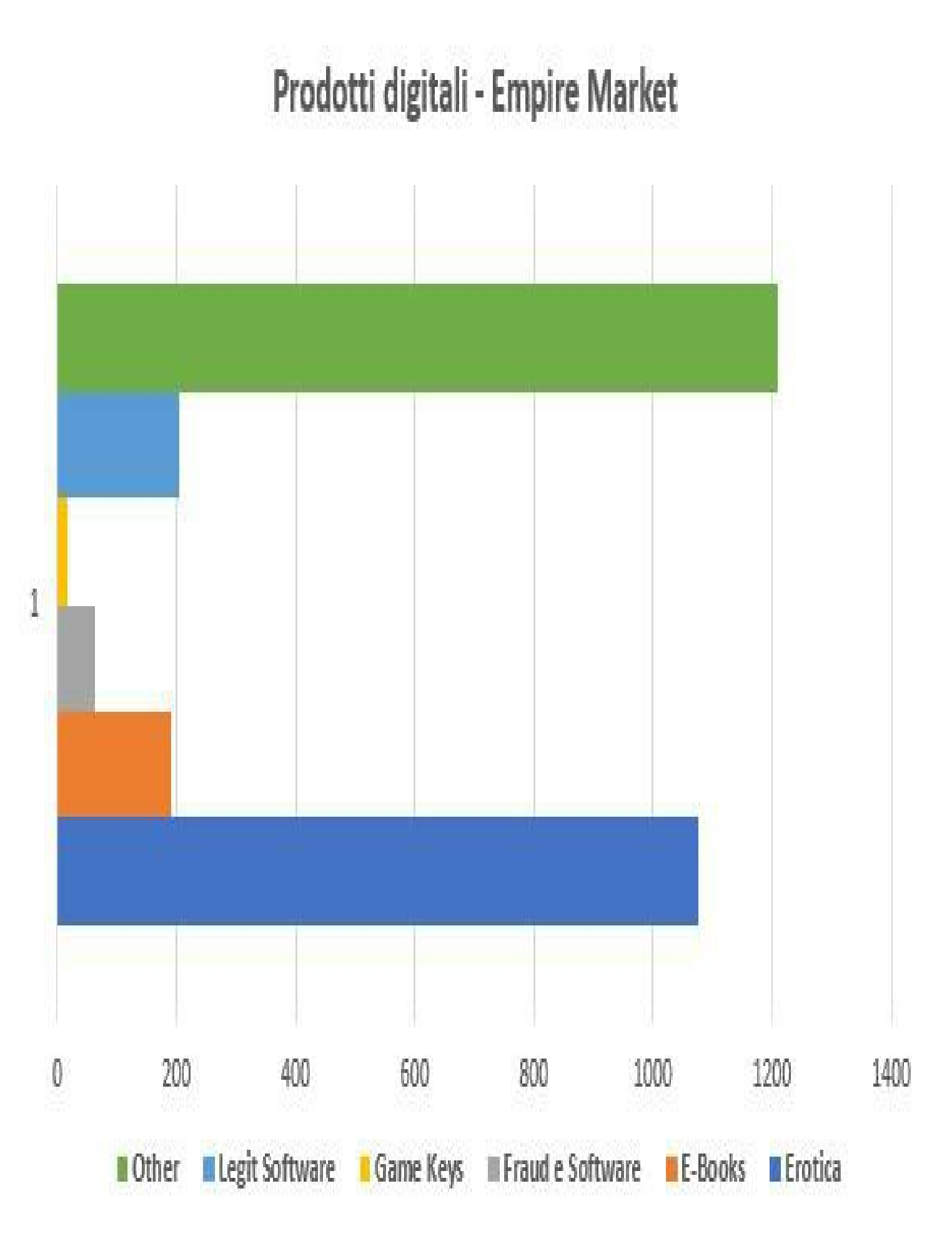
Altro	242
Software e Malware	214
Security e Hosting	68

TOTALE	8514

Raggruppando le categorie affini è possibile visualizzare la ripartizione delle categorie merceologiche.

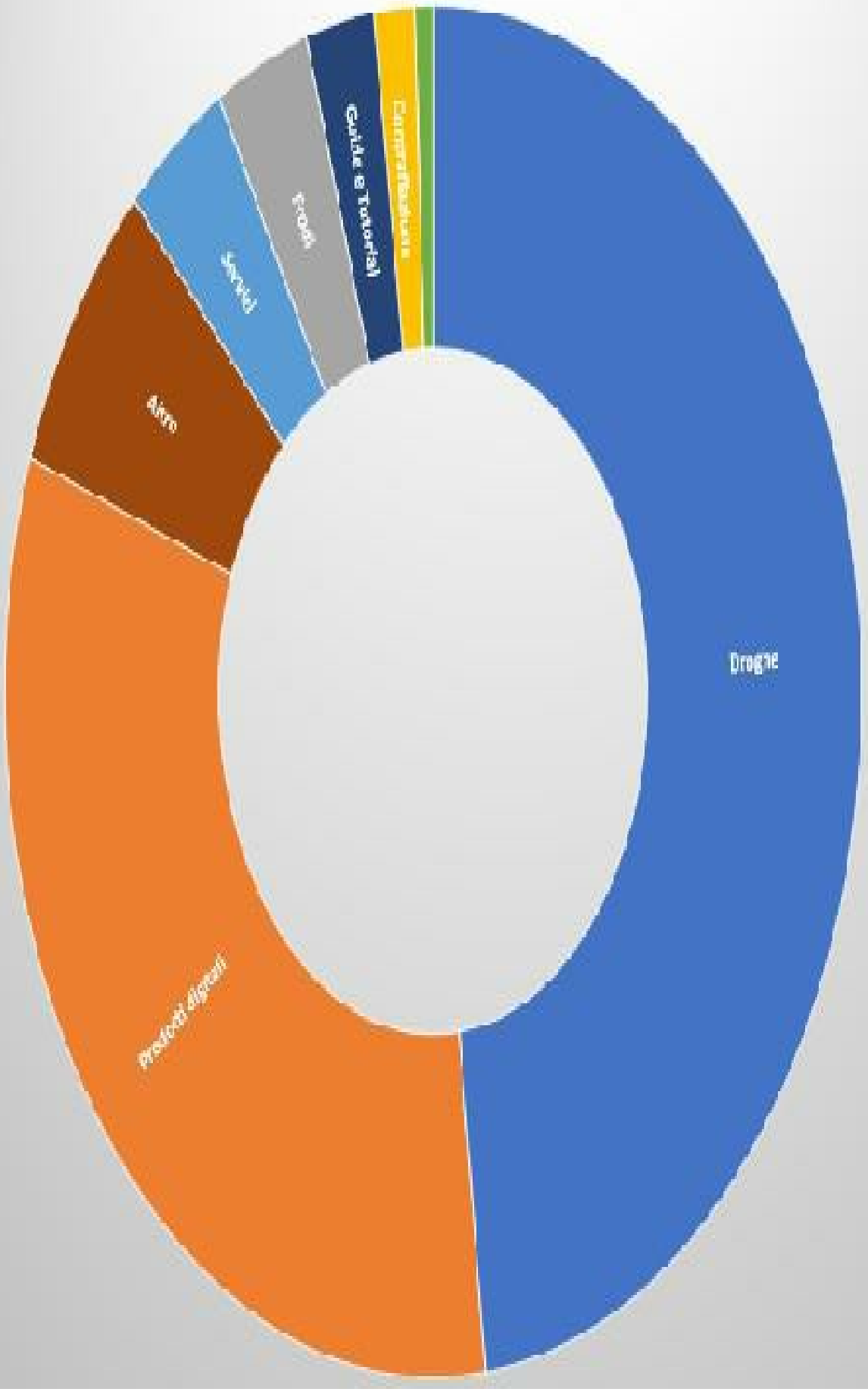

Empire Market
Prodotti digitali
Droghe
Guide e Tutorial
Frodi
Altro
Contraffazione

Diversamente dagli altri casi, in questo market vengono privilegiate le categorie legate ai prodotti digitali, così suddivisi.


Prodotti digitali - Empire Market
1
0
200
400
600
800
1000
1200
1400
Other
Legit Software
Game Keys
Fraud e Software
E-Books
Erotica

Prendendo come riferimento i black market sopra descritti, e raggruppando tra loro gli annunci di vendita riguardanti categorie affini, è possibile avere un'idea, da un punto di vista statistico, della ripartizione delle tipologie di merce che vengono poste in vendita nel dark web.

Prodotti venduti sui *Black Market*



La categoria che comprende più annunci è quella relativa alle droghe. Queste possono spaziare da ogni tipo di stupefacente e vengono ampiamente e dettagliatamente descritte nelle inserzioni di vendita.

0.50G PERUVIAN COCAINE - OFF THE BRICK

STRAIGHT FROM THE BRICK TO YOU! This will soon be known as the best cocaine on the market. Highest cla...

Sold by Cocainero - 0 sold since October 29, 2018 Vendor Level 1 Trust level 1

	Features		Features
Product Class	Physical Package	Origin Country	United States
Quantity Left	Unlimited	Ships to	United States
Ends In	Never	Payment	Escrow

First Class - No Tracking - 3 days - USD + 0.00 / order

Purchase price: USD 30.00

Qty 1 Buy Now Buy Now Buy Now Queue

0.005398 BTC / 0.709723 LTC / 0.343446 XMR

Description | Feedback | Refund policy

0.50G PERUVIAN COCAINE - OFF THE BRICK

STRAIGHT FROM THE BRICK TO YOU!

This will soon be known as the best cocaine on the market.

Highest class cocaine available anywhere.

Brilliant white shiny sparkling uncut fresh across the border.

Minimal drip, extremely pleasant experience from come up to comedown.

Guaranteed for shipping

Spesso ai market vengono affiancati dei forum specifici, dove i vari utenti possono recensire e descrivere i prodotti acquistati, cosicché gli altri utenti possano avere contezza del venditore e della qualità dei suoi prodotti.

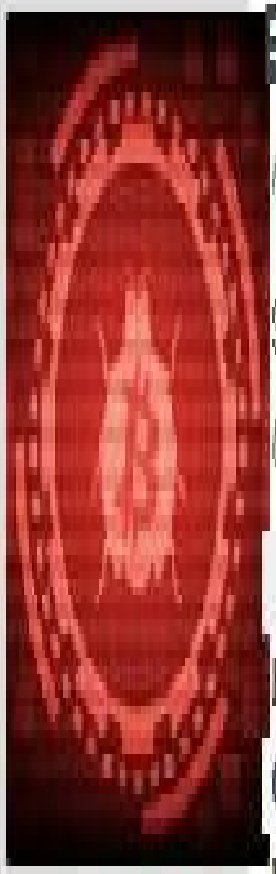
Home > Forums > LISTING REVIEWS > Drugs Sellers

Steroids / Stimulants

Page 1 of 2 | 1 | 2 | Next >

Title	Start Date	Replies	Views	Last Message
SAMPLE SALE 1 HALF GRAM of COKE 88-90% PURITY [illegible], Apr 8, 2018		Replies: 10	Views: 7,077	mrdollarsign Nov 15, 2018 at 1:11 AM
★★MerckGrade★★Review Section★★MerckGrade★★ MerckGrade, Nov 10, 2018		Replies: 0	Views: 87	MerckGrade Nov 10, 2018
Good Coke Vendor [illegible], Oct 27, 2018		Replies: 2	Views: 196	bdlb2 Nov 8, 2018
Why is adderall so goddamn expensive? [illegible], Oct 27, 2018		Replies: 27	Views: 420	J. Allen Nov 8, 2018
Great King is Back baby ! Best Snow and Ice on the market [illegible], Nov 5, 2018		Replies: 0	Views: 115	Hobsed Nov 6, 2018
[REVIEW] 20x Adderall 30mg IR [MULTISCROW] US 2 US [illegible], Nov 2, 2018		Replies: 1	Views: 161	OdysseyCorp Nov 2, 2018

Altre due categorie, strettamente correlate e molto diffuse, sono quelle relative ai prodotti digitale e alle guide e tutorial. Per prodotti digitali si intendono tutti quei beni che non richiedono una spedizione fisica. Sono, ad esempio, licenze per software, credenziali di accesso a siti di e-commerce o social network, libri, software particolari, programmi per hacking, ransomware, ecc.



Blackmail Bitcoin Ransomware (With Sourcecode) Easy-setup

ATTENTION: DO NOT BUY THIS UNLESS YOU KNOW HOW TO USE IT THE ORIGINAL SITE THAT HOSTED T...

Sold by motherfuckerOnes 25 sold since March 27, 2016 Vendor Level 1 Trust Level 1

Unlimited items available for auto-dispatch

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow, MultiSig

default - 1 day - USD 0.00

Purchase price: **USD 1.99**

Qty: 1 Buy Now Buy Now Buy Now Queue

0.000258 BTC / 0.047145 LTC / 0.072828 XMR

Per quanto riguarda le guide, molti utenti sono disposti a pagare per ricevere informazioni su come commettere illeciti nel miglior modo possibile. Si possono trovare manuali per l'anonimato online, sulla coltivazione di droghe, sull'utilizzo di soldi falsi, ecc.

How To Make $700 A Day (Very Easy)

How To Make $700 A Day (Very Easy) This guide will teach you how to make $700 a day Why buy from us: - We ...

Sold by DrunkDragon - 160 sold since February 08, 2018 Vendor Level 2 Trust Level 1

Unlimited items available for auto-dispatch

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

Default - 1 day - USD + 0.00

Purchase price: USD 0.99

Qty: 1

Buy Now Buy Now Buy Now Queue

0.00017000 BTC / 0.023404 LTC / 0.211362 XMR

Nella categoria dedicata alle frodi, è possibile trovare tutto il necessario per porre in essere attività fraudolente. Ad esempio è possibile trovare copie di documenti autentici, carte di credito intestate a terzi, documenti falsi, codici di carte di credito illegalmente carpiti. La categoria è molto simile a quella dei prodotti digitali. Spesso è possibile, a seconda del market, trovare prodotti similari in una categoria o nell'altra.

LUX QUALITY USA FULLZ SSN/DOB ANY STATE AVAILIABLE

2.41 EUR
0.000499

Buy Now
Currencies

SATAII [+1|-0]
Trusted

Escrow Type: Finalize Early

Sold: 0

UK bankstatement BARCLAYS (psd) + C56

12.95 EUR
0.002633

Buy Now
Currencies

BarryBusInc33 [+18 -0]

Escrow Type: Full Escrow

Sold: 0

Blanko Rezepte (Facharzt für Psychatrie Soltau)

10 EUR
0.002072

Buy Now
Currencies

Jimmy2018 [+28|-6]

Ships from: world

Escrow Type: Full Escrow

Sold: 0

Non è raro trovare la categoria dedicata alla contraffazione. Si tratta della categoria dove è possibile trovare beni come soldi falsi o documenti falsi, meno frequenti sono i prodotti di abbigliamento con marchi d'impresa contraffatti.

[RG] 1.500 x 50 EURO COUNTERFEIT MONEY - FREE SHIPPING

3910 EUR

0.810082

Buy Now

Currencies

Richtgang [+0|-0]

Ships from europe

Escrow Type Full Escrow

Sold 0

50€ euro notes 50€x500 (new product)

5500 EUR

1.139502

Buy Now

Currencies

lovistraues [+57|-4]

Ships from world

Escrow Type Full Escrow

Sold 0

Also available:

50€ euro notes 50€x200 (new product)

2600 EUR 0.517955

È possibile trovarvi anche prodotti più particolari, come oro falso, che è possibile vendere presso i cosiddetti compro oro ingannando i gestori, ovvero gioielli di moda recanti marchi contraffatti. In altri casi, è possibile trovare abbigliamento recante segni distintivi contraffatti, tuttavia si tratta di una nicchia di mercato del dark web. Non è questo il posto dove gli utenti sono soliti cercare merce di questo tipo. Infatti, i principali canali di vendita dove trovare tale merce sono i social network nel clear web, dove è molto più facile pubblicizzare i prodotti con le foto e interagire con i potenziali clienti. Basta considerare che, nonostante il

dark web sfrutti la rete Tor finalizzata all'anonimato degli utenti, al giorno d'oggi bastano poche accortezze e un minimo di cultura informatica per essere praticamente anonimi anche nel web comune.

Su alcuni black market è possibile trovare anche una categoria dedicata alle armi. Di solito le armi vengono vendute su portali appositi che funzionano con contatto diretto tra venditore e acquirente, senza procedure automatizzate e raccolta di recensioni e feedback.

Desert Eagle IMI, Kal.44

New and unused and unregistered!

Ammo can only be purchased if you also buy the gun.

Product	Price	Quantity
Desert Eagle IMI, Kal.44	1250 EUR = 0.254 Ƀ	1 X Buy now
Ammo, 50 Rounds	45 EUR = 0.009 Ƀ	1 X Buy now

Per l'effettuazione dei pagamenti, i black market sfruttano le valute virtuali. Questo perché le valute virtuali, con poche accortezze, sono in grado di fornire un buon livello di anonimato. Infatti le valute virtuali non sono necessariamente abbinate al soggetto utilizzatore e consentono trasferimenti non riconducibili direttamente ad alcun soggetto. Le transazioni, solitamente, sono pubbliche e consultabili da chiunque. L'anonimato risiede nel non poter ricondurre queste transazioni a chi le ha inviate e a chi le ha ricevute. La valuta più diffusamente accettata è il Bitcoin (BTC). Questo innanzitutto perché il Bitcoin è la prima valuta

virtuale creata e la maggiormente diffusa. Inoltre, altro punto di forza del Bitcoin è la facilità nel reperirli e nel venderli. Infatti esistono moltissime valute virtuali alternative, ma sono difficili da cambiare in poco tempo e a commissioni vantaggiose. Invece il Bitcoin ha un grande mercato e una grande platea di persone interessate ad acquistarli oppure a venderli. Altra valuta virtuale ora diffusa è Monero (XMR). È una criptovaluta nata dopo il Bitcoin ma che si propone di fornire agli utilizzatori un altissimo livello di anonimato. Infatti non è possibile consultare le transazioni effettuate da un indirizzo. Semplicemente, conoscendo l'identificativo di una transazione, è

possibile verificarne la sussistenza. Invece, conoscendo solo un indirizzo, non è possibile ricavare altre informazioni. Oltre a questi accorgimenti, il progetto si basa su una crittografia molto più complessa e articolata.

Altre due valute che è possibile incontrare nel dark web sono Litecoin (LTC) e Bitcoin Cash (BCH). Non esistono motivi particolari che rendano queste valute più indicate di altre. Si tratta di progetti molto simili al Bitcoin. Sono valute abbastanza facili da reperire e da rivendere per valuta corrente. Talvolta capita che la rete Bitcoin sia particolarmente intasata. Questo richiede tempi più lunghi per le

transazioni e costi di transazione (fee) più elevati. Per evitare queste problematiche alcuni utenti scelgono di utilizzare criptovalute alternative al BTC.

Ma come fare per poter scardinare tali complessi illegali?

Ovviamente l'anonimizzazione degli indirizzi IP, i segnali comunicativi crittografati, l'anonimato delle transazioni valutarie virtuali rendono complessi gli scenari investigativi e di difficile soluzione se non attraverso lo scambio di informazioni tra gli Stati mondiali. Quando anche un attacco informatico è condotto da server siti in Paesi esteri ovvero in essi sono allocati i server per le operazioni del

commercio illegale del darkweb, è impossibile procedere giudizialmente se non in presenza di collaborazioni con tali Paesi. Invero vige la cd. Convenzione di Budapest[44] che favorisce lo scambio di informazioni in materia di reati informatici ma molti sono gli Stati che non vi hanno aderito. Inoltre, come nel dark web, i reati di riferimento sono altri e diversificati per cui è necessario procedere con atti giudiziari (rogatorie) che hanno procedure amministrative più lunghe che non sono propriamente adatte alla volatilità ed alla velocità di cambiamento degli operatori informatici illegali. Molto spesso peraltro vi sono Governi esteri che favoriscono

l'allocazione sul proprio territorio di infrastrutture informatiche, con agevolazioni finanziare, fiscali, societarie, basata sul segreto nominativo al punto da creare veri e propri "Paradisi Informatici".

In sostanza da tale analisi emerge che soltanto un processo, fondato sulla continua combinazione "controllo del territorio economico – monitoraggio del web - analisi di rischio – scambio di informazioni", permette di ricostruire i flussi finanziari e le ricchezze accumulate, rilevandone gli illeciti e colpendo al cuore le organizzazioni criminali. Lo sforzo investigativo va infine orientato alla sistematica applicazione delle misure di aggressione

dei patrimoni illeciti accumulati, considerate uno strumento di primaria importanza per contrastare efficacemente ogni forma di crimine.

2.3 L'OPERAZIONE DELLA GUARDIA DI FINANZA "DARKNET.MONEY"

L'attività di indagine ha preso avvio dalla consapevolezza del fenomeno criminale crescente dell'offerta in vendita di documenti di identità sulle piattaforme informatiche e telematiche. Dalla ricerca è emersa la risorsa "italiandarknet.io" visibile solo mediante l'accesso al Dark Web. Si

premette che il dominio italiandarknet.io risulta registrato sul clear web e quindi indicizzato dai comuni motori di ricerca, avendo l'unica funzione di reindirizzare le connessioni verso il dominio dark web .onion. Per consentire tale operazione è necessario che il dominio venga registrato sui "pubblici registri dei domini" e allocato su un server i cui dati sono stati così estrapolati mediante ricerca whois (a. Indirizzo IP: --; b. Nazionalità: Stati Uniti; c. Data registrazione: --; e. Registrant:--).

Come detto, la rete TOR, anche chiamata Dark Wek è finalizzata a garantire l'anonimato degli utenti che vi navigano. Per fare ciò la connessione viene fatta "rimbalzare" tra più server

chiamati nodi, in modo da rendere pressoché impossibile rintracciare la sua reale origine. In più, i dati scambiati vengono criptati tra un nodo e l'altro, cosicché anche captando un flusso di dati relativo alla rete TOR, non sarà possibile ricavare le informazioni contenute al suo interno. In sostanza l'Onion routing è una tecnica di anonimizzazione delle comunicazioni in una rete di telecomunicazione.

Le attività investigative esperite sono state finalizzate alla captazione di ogni utile informazione ricavabile dall'analisi degli annunci di vendita presenti sui vari Market, i quali risultano strutturati secondo criteri e layout del tutto simili tra loro: l'accesso

non è libero ma ristretto agli utenti accreditati; i siti sono suddivisi in sezioni classificate in base alla tipologia dei prodotti compravenduti (es. Fraud, Drugs, Weapons, Counterfeit Items, Identity Data, Credit Cards, Knives, Guns and ammo, Explosives, IDs & Passports, etc.). Pertanto, sono state analizzate le chiavi pubbliche associate agli utenti ritenuti di maggior interesse investigativo. Attraverso mirate interrogazioni dei keyserver è stato possibile ricavare l'indirizzo di posta elettronica asservito alle chiavi di cifratura di un venditore che ha attirato l'attenzione investigativa del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza: Benz99.

Costui, in particolare, risultava attivo sul market di IDC reloaded e sul forum IDW. Si premette che l'attività dei vendors nel dark web è connotata da una rapidissima "mobilità", necessaria per garantire l'anonimato, talché gli annunci vengono rapidamente trasferiti su piattaforme e-commerce differenti. La varietà di prodotti offerti in vendita ha lasciato sin da subito intuire che dietro l'account Benz99 vi fosse un "vero" rivenditore, ed infatti, dall'esame del market IDC reloaded, attivo nel dark web, è stato possibile operare una stima del volume d'affari del venditore. L'operazione si è fondata sull'analisi dei feedback rilasciati dai clienti più o meno soddisfatti di quanto acquistato.

Tali feedback, anche se non paragonabili a vere e proprie scritture contabili, godono di adeguata attendibilità in quanto, per ogni vendita effettuata sul market è necessario corrispondere una percentuale agli amministratori. Va precisato inoltre che, il feedback non è obbligatorio e quindi i pubblicati non corrispondono esattamente a tutte le vendite perfezionate ma sono indicativi di un numero di transazioni certamente inferiore quantitativamente, talché la stima del volume di affari appare già di per sé intrinsecamente prudenziale.

In particolare, al mese di febbraio 2018, il venditore Benz99 aveva perfezionato, sulla sola piattaforma IDC, centinaia di

vendite, ed è stato indicato con grado di affidabilità pari a 5 (il massimo). Il venditore risultava aver ricevuto un totale di 94 feedback, i quali si presentano con un breve commento, la prima e l'ultima lettera del nickname relativo all'utente che ha effettuato l'acquisto, il prezzo espresso in euro e la data e l'ora dell'acquisto. In cinque mesi risultavano essere stati rilasciati feedback per acquisti per banconote false, sim telefoniche intestate a terzi, cessione di oro falso, per centinaio di transazioni bitcoin effettuate. Tramite l'analisi delle connessioni internet di una casella mail, ricollegata al venditore in quanto abbinata alla sua chiave pubblica, e delle connessioni al profilo

social registrato con tale mail, è stato possibile collegare al venditore alcune utenze mobili intestate a soggetti vari. Dall'esame dei tabulati telefonici delle utenze mobili è stato poi possibile appurare che queste sono state utilizzate tramite dispositivi per la connessione ad internet (IMEI riferito a chiavette internet ed a vari dispositivi). Dall'incrocio dei dati di traffico telefonico ottenuti dai vari gestori di telefonia attivi sul territorio nazionale, è stato possibile venire a conoscenza di ulteriori utenze mobili utilizzate in abbinamento ai citati dispositivi.

Sono stati esaminati i log di connessione a caselle di posta elettronica al fine di individuare ulteriori utenze in uso al

venditore oggetto di indagine, nonché ricerche su banche dati e fonti aperte per l'individuazione di persone, dati o numeri collegati, fino a giungere al confronto delle connessioni internet e ricondotte al venditore Benz99, sono stati richiesti i dati di connessione ad un profilo personale attivato su social network. A riscontro della individuazione di Benz99 con una specifica persona fisica sono intervenute le intercettazioni telefoniche e lo sfruttamento di celle telefoniche di tutte le utenze in una specifica area del territorio nazionale. Successivamente si è sviluppata una tradizionale attività di polizia giudiziaria con appostamenti, pedinamenti e riscontri in loco, fino alla

piena identificazione dell'autore dei reati avente il citato nickname.

Parte III

ANALISI DEI DATI DA *BLOCKCHAIN*

2. # 1. INTELLIGENCE SULLA BLOCKCHAIN

a cura di Marco Stella

Sommario: 1.1 Le informazioni ottenibili dalla *Blockchain* – 1.1.1 Blocchi, transazioni e indirizzi: definizioni – 1.2 Anonimizzazione e processamento dello streaming di dati dalla *Blockchain* – 1.2.1 Informazioni dal *clear web* – 1.2.2 Informazioni dal *dark web* – 1.3 Costruzione di un modello di rappresentazione relazionale delle transazioni – 1.3.1 Rappresentazione delle transazioni –

1.3.2. Ricostruzione del flusso di "denaro" virtuale – 1.4 Il problema dell'analisi dei dati relativi alle transazioni e agli indirizzi *Bitcoin* – 1.4.1 Tecniche di *tagging* – 1.4.2 Tecniche di *clustering* applicate all'analisi delle transazioni: introduzione – 1.4.3 Tecniche di *clustering* applicate all'analisi delle transazioni: le principali euristiche.

1.1 LE INFORMAZIONI OTTENIBILI DALLA BLOCKCHAIN

Le caratteristiche principali di una criptovaluta riguardano in sintesi

l'elevato grado di decentralizzazione, ovverosia il fatto che la stessa non è controllata da un'autorità centrale di vigilanza come accade per le monete tradizionali; è sì legata a costi di produzione ma questi sono riconducibili in termini di capacità di elaborazione di algoritmi di cifratura e relativa energia necessaria per le operazioni computazionali; può garantire, sotto certe condizioni, un elevato grado di anonimizzazione di coloro che intendono utilizzare tale strumento digitale per le più svariate ragioni e finalità.

In aggiunta può essere venduta, acquistata e generata senza incorrere in specifiche sanzioni. Tra gli ulteriori fattori che caratterizzano una

criptovaluta è possibile che diventi – anche se è molto probabile che lo sia già diventata – una forma di investimento, atteso il valore che viene continuamente attribuito alle stesse. È del tutto ovvio che le predette caratteristiche possono essere naturali e facili veicoli di attività illecite. Inoltre per chi ha interesse ad investire in questi "oggetti" innovativi, esiste comunque un significativo rischio derivante dalla estrema variabilità del suo valore e della non conoscibilità del rischio stesso. A ciò va aggiunta anche la limitata diffusione di tale strumento come forma di pagamento che non viene incentivata ed è appannaggio di relativamente pochi soggetti.

Per comprendere la filosofia sottostante

a questo tipo di “oggetti”, è possibile rifarsi all’idea presentata da Wei Dai [28], che ispirò fin dalla fine degli anni novanta la creazione delle prime “monete digitali”, sottratte alla dipendenza da un sistema centralizzato e autarchico, regolate da una “comunità” di utenti della stessa.

La maggior parte delle criptovalute sono state progettate e ne vengono prodotte continuamente di nuove e differenti tipologie per introdurre gradualmente nuove unità di valuta, ponendo un limite massimo alla quantità di “moneta” che va in circolazione. L’offerta di tali “oggetti” pertanto ha una sua rigidità intrinseca. Ciò viene fatto sia per imitare la scarsità (e il valore) dei

metalli preziosi, sia per evitare l'inflazione. Comparata con le valute ordinarie gestite dagli istituti finanziari o tenute come denaro contante, le criptovalute sono meno suscettibili a confische e favoriscono un elevato livello di privacy di coloro ne fanno uso e ne risultano in possesso.

Si può pertanto affermare che le caratteristiche di una criptovaluta sono riconducibili essenzialmente ad una serie di aspetti che coinvolgono l'anonimato delle transazioni, la velocità delle operazioni e l'elevata versatilità nelle modalità di trasferimento del credito, l'irreversibilità di una transazione, i limitati costi di transazione, una

inflazione molto ridotta (derivante – come detto – dal numero di monete spesso prestabilito), l'indipendenza del proprio valore da beni materiali, istituti finanziari o governi, l'elevata sicurezza e la possibilità di creare più copie del proprio credito, mettendolo così al sicuro, per esempio, da eventi accidentali e attività criminose. A queste si aggiungono la possibilità di "forgiare" la propria valuta senza dover investire obbligatoriamente in valute centralizzate, la facilità di conversione in altre valute digitali e non. Da ultimo, la connotazione sempre più vicina ad un mercato in espansione con un ruolo economico già riconosciuto in molti stati, quindi la possibilità di

investimento sia nel breve che nel lungo termine.

Sotto il profilo della sicurezza vi è l'impossibilità di duplicare o falsificare la moneta, nonché di essere intercettata come un normale pacchetto di dati, poiché essa rappresenta una variazione del credito, che viene pubblicata nella blockchain di riferimento. Detto questo la criptovaluta non esiste fisicamente né nel nostro mondo reale né in quello virtuale, quindi è più difficile da individuare e, di conseguenza, da sottrarre.

Ovviamente è d'obbligo precisare che il mercato delle criptovalute è influenzato da una molteplicità di fattori che non vengono considerati in questa trattazione

anche per ragioni di semplificazione dei concetti, ma è del tutto chiaro come tale "ricchezza" allo stato possa essere paragonata all'oro di un tempo ed alla sua ricerca. Le analogie sono molteplici. Per cominciare il limite massimo finito della quantità di oro presente nel mondo e, specularmente, la natura di moneta limitata del bitcoin; quest'ultimo infatti dovrebbe tendere ad un limite di ventuno milioni e per questo rappresenta una risorsa limitata, per quanto ampia essa possa oggi apparire.

Come si avrà modo di approfondire nei prossimi paragrafi, la tecnologia sottostante ad una criptovaluta si sostanzia nella blockchain ovvero nelle potenzialità di reti del tipo peer-to-peer.

La blockchain rappresenta, come già illustrato, il registro pubblico di tutte le transazioni avvenute in Bitcoin ed è la struttura fondamentale per poter garantire l'autenticità di una transazione e impedire che la stessa somma di denaro sia spesa più di una volta (il c.d. *double spending*).

La blockchain, come evoca la parola stessa, è costituita da una sequenza di blocchi concatenati. Ogni blocco contiene un insieme di transazioni. Le nuove transazioni che vengono generate dagli utenti sono raggruppate in un nuovo blocco. Per aggiungere il nuovo blocco alla catena è necessario creare il collegamento con l'ultimo blocco presente. Questa operazione consiste nel

calcolare, per tentativi successivi, un'impronta informatica (hash) avente determinate caratteristiche uniche.

Diversi utenti della rete Bitcoin, i cosiddetti miner, competono per risolvere questo problema matematico (*proof of work*). Il miner che risolve per primo il problema crea l'ultimo collegamento ed estende la blockchain aggiungendovi il nuovo blocco di transazioni. Di fatto, l'estensione della blockchain è una "prova di forza" tra miner ed è il meccanismo che impedisce ad un utente disonesto di violare l'integrità delle transazioni. Un nuovo blocco viene aggiunto ogni dieci minuti circa e contiene una speciale transazione, detta *coinbase*, che assegna

al miner vincitore una quantità predefinita, decrescente nel tempo, di bitcoin.

1.1.1 Blocchi, transazioni e indirizzi: definizioni

È noto che la Blockchain è una catena di blocchi che costituisce la "dorsale" di gran parte delle criptovalute, intesa come una struttura di dati di riferimento per la loro comprensione e la loro esistenza. In altri termini può essere considerata alla stregua di un database, una sorta di libro mastro digitale nel quale vengono registrate tutte le transazioni bitcoin. Una sorta di protocollo di comunicazione (una rete

diffusa in tutto il mondo), che risiede su migliaia di personal computer collegati tra loro chiamati nodi. In questo modo i dati non vengono memorizzati su un solo computer, ma su più macchine. Ed è proprio questo il suo punto di forza, perché chiunque può farne parte: è accessibile a tutti, essendo sufficiente scaricarla tramite un software specifico. Una logica di governance basata sul concetto di fiducia tra tutti i soggetti della rete, grazie alla quale nessuno ha la possibilità di prevalere e tutto passa rigorosamente attraverso la costruzione del consenso. Il problema che la Blockchain risolve è assicurare che colui che paga in criptovalute sia il vero proprietario della moneta, tramite la

ricostruzione di tutti i passaggi di quella moneta che si sta usando per quella specifica transazione. L'idea geniale alla base è questa: utilizzare un registro digitale pubblico (la Blockchain) per validare e verificare ogni singola transazione. Il pagamento deve essere in pratica certificato dalla maggioranza dell'intera rete. Qualsiasi transazione, quindi, viene documentata [29] [30].

La Blockchain è un protocollo 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 una serie di blocchi che

archiviano un insieme di transazioni validate e correlate da un marcatore temporale detto *timestamp*. Una delle caratteristiche più importanti della Blockchain è la sicurezza: la marcatura temporale impedisce anche che l'operazione, una volta eseguita, venga alterata o annullata. La caratteristica principale del modello, dunque, è che il funzionamento non è garantito da un ente centrale, ma ogni singola transazione è validata dall'interazione di tutti i nodi della rete. In ciò l'utilizzo di una marca temporale consente di associare una data e un'ora certe e legalmente valide a un documento informatico. In altre parole la marca temporale consente di definire una validazione temporale che può

essere opponibile a terzi. Essa è costituita da una sequenza specifica di caratteri che identificano in modo univoco, indelebile e immutabile una data e un orario per fissare e accertare l'effettivo avvenimento di un certo evento. La rappresentazione della data è sviluppata in un formato che ne permette la comparazione con altre date e permette di stabilire e definire un ordine temporale.

Ogni blocco include un valore di hash – da intendersi come una funzione algoritmica informatica non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita – che identifica il blocco in modo univoco e che permette il

collegamento con il blocco precedente tramite identificazione di quest'ultimo.

La Blockchain è costituita da una serie di componenti che le consentono di attribuire certezza e robustezza alla gestione di transazioni su reti di tipo *peer-to-peer*.

Uno dei componenti principali della Blockchain è rappresentato dai nodi che partecipano alla medesima catena di blocchi e sono costituiti fisicamente – come accennato – da macchine server di ciascun partecipante.

Altro elemento essenziale è costituito dalle transazioni che sono formate dai dati che rappresentano i valori oggetto di scambio e che necessitano di essere verificate, approvate e poi archiviate.

A seguire, ci sono i blocchi che rappresentano dei raggruppamenti di un insieme di transazioni che sono unite tra loro per essere verificate, approvate e poi archiviate dai partecipanti alla Blockchain.

Il *ledger* è il registro pubblico nel quale vengono opportunamente annotate con la massima trasparenza e in modo immutabile tutte le transazioni effettuate in modo ordinato e sequenziale. Esso è costituito dall'insieme dei blocchi che sono tra loro incatenati tramite una funzione crittografica e grazie all'utilizzo di funzioni di hash.

Di fondamentale importanza, all'interno della Blockchain, è l'operazione di hash, che va intesa come l'applicazione

di una funzione non invertibile che consente di mappare una stringa di testo e numerica di lunghezza variabile in una stringa unica ed univoca di lunghezza determinata; pertanto il valore di hash identifica in maniera univoca e sicura ciascun blocco ed essendo non invertibile, non consente di risalire al testo o alla stringa alfanumerica che lo ha generato.

Ciascun blocco contiene dunque diverse transazioni e dispone di un hash collocato nell'header. L'hash registra tutte le informazioni relative al blocco e un hash con le informazioni relative al blocco precedente che permette di creare la catena e di legare un blocco all'altro.

La transazione contiene invece informazioni relative all'indirizzo pubblico del ricevente, le caratteristiche della transazione e la firma crittografica che garantisce la sicurezza e l'autenticità della transazione.

La Blockchain è organizzata per aggiornarsi automaticamente su ciascuno dei client che partecipano al network. Ogni operazione effettuata deve essere confermata automaticamente da tutti i singoli nodi attraverso software di crittografia, che verificano un pacchetto di dati definiti a chiave privata, che viene utilizzata per firmare le transazioni, garantendo pertanto l'identità digitale di chi le ha autorizzate.

Come detto, la Blockchain è un database distribuito. Quindi, per capire bene il concetto di Blockchain, è necessario capire meglio le caratteristiche principali che identificano un database distribuito vale a dire una base di dati distribuita, ovvero condivisa tra più computer, chiamati nodi, connessi alla rete.

In altri termini può essere considerato come un database che non si trova fisicamente solo su un server, ma che si trova su più computer nello stesso momento, tutti perfettamente sincronizzati su tutti gli stessi documenti. Ad esempio, può trovarsi su tutti i computer che sono connessi alla rete. In questo modo l'informazione è reperibile

in maniera molto rapida, in quanto la potenza di calcolo sfrutta la potenza di tutti i computer connessi.
Ci sono fondamentalmente due processi che permettono ai database distribuiti di funzionare correttamente, e di non perdere dati. Uno di questi processi è la replica del database, ovvero un software è incaricato di analizzare il database per identificare cambiamenti. Una volta identificati questi cambiamenti, il software fa in modo che questi cambiamenti vengano replicati e che tutti i database siano identici. Altra soluzione è la duplicazione, come processo che assicura che tutti i database abbiano gli stessi dati. In pratica identifica un database master, che poi duplica su tutti

gli altri database, in modo da renderli uguali. Gli utenti possono modificare soltanto il database master, garantendo che i dati locali non vengano sovrascritti erroneamente.

La rete delle transazioni cresce in maniera molto rapida e fornisce una visione estremamente puntuale dei flussi di denaro che avvengono sulla blockchain.

Tuttavia potrebbe risultare più naturale ragionare in termini di utenti. Se nel mondo reale le indagini finanziarie devono fare i conti con i molteplici rapporti che un utente può attivare e con gli schermi posti in essere a scopo di riciclaggio o camuffamento delle operazioni, nel mondo virtuale tale

scenario è portato all'estremo.

Al limite, un utente potrebbe addirittura generare un nuovo indirizzo per ogni singola transazione. Praticamente è come se aprisse un nuovo conto in banca solo per fare un bonifico.

Questa prassi è addirittura consigliata agli utenti Bitcoin particolarmente attenti alla loro privacy ed è adottata, ad esempio, dall'attuale versione del portale Wikileaks, che riceve donazioni su indirizzi Bitcoin generati una tantum e che dichiara esplicitamente "*For a more private transaction, you can click on the refresh button above to generate a random Segwit (BIP-49) address*" [31].

Del resto, poiché gli indirizzi vengono agevolmente gestiti tramite i wallet, per

l'utente un'interazione con il sistema apparentemente complessa risulta, di fatto, quasi banale.

Premesso ciò, già da tempo alcuni ricercatori [32] *in primis* hanno proposto taluni criteri ("euristiche") che consentono di aggregare un insieme di indirizzi e di associarli ad un singolo utente.

In breve il primo criterio deriva dal funzionamento stesso delle transazioni, per come sono descritte nel prossimo paragrafo. Infatti, per poter creare una nuova transazione, l'utente deve aggregare fondi non spesi, contenuti nelle cosiddette UTXO (*Unspent Transaction Output*), che costituiranno l'input della nuova transazione.

Affinché la nuova transazione sia valida, tutti gli input devono essere firmati digitalmente dal medesimo utente. Da ciò si desume, pertanto, che le UTXO sono nella disponibilità della stessa persona.

Il secondo criterio consente di aggregare ulteriori indirizzi al cluster identificato con la prima euristica. Questo consiste nel riconoscere, tra gli indirizzi di output, quello utilizzato per veicolare il "resto" della transazione all'utente disponente. Si approfondiranno ulteriormente le caratteristiche di tali euristiche e di altre riconosciute come principali nel prosieguo del presente capitolo.

A questo punto occorre fare una

precisazione sul significato di "utente" nel particolare ambito che stiamo analizzando. Nello specifico, non va dimenticato che in Bitcoin gli indirizzi utilizzati nelle transazioni sono considerati pseudonimi dell'utente reale che le genera. Pertanto, anche un'aggregazione di pseudonimi non conduce direttamente all'identificazione, nel mondo reale, del relativo utente.

Il discorso cambia se si focalizza l'analisi sulle singole transazioni. Ogni transazione ha un insieme di input e di output. Unica eccezione è costituita dalla transazione coinbase che non ha input, ma solo l'output corrispondente al *miner*.

Per meglio comprendere la struttura

delle transazioni e i grafi che ne derivano, occorre introdurre alcuni concetti fondamentali che caratterizzano il sistema Bitcoin:

- ogni "moneta" non è intercambiabile con le altre, ma ha una sua propria storia. In altri termini, analizzando la blockchain, è possibile individuare tutti gli spostamenti di un bitcoin, dalla sua creazione alla sua posizione attuale, ossia all'indirizzo che la detiene;
- ogni utente può generare a piacimento

più indirizzi (per semplicità assimilabili agli IBAN dei conti correnti del sistema bancario reale). Gli indirizzi vengono gestiti, in forma aggregata, tramite un wallet, ossia mediante un software che consente, tra l'altro, di creare nuove transazioni;

- in una transazione, tramite l'opportuna configurazione degli output, si assegna una certa quantità di bitcoin ad un indirizzo. L'utente possessore di

quell'indirizzo, essendo a conoscenza della corrispondente "chiave", può svincolare i fondi ad esso associati e usarli in una nuova transazione; conseguentemente, il "saldo" di un indirizzo va ricalcolato sul momento sommando tutti i bitcoin trasferiti su quell'indirizzo tramite output di una transazione e non ancora spesi. Dovrebbe, dunque, risultare chiaro il motivo per cui il "saldo" di un indirizzo Bitcoin è più

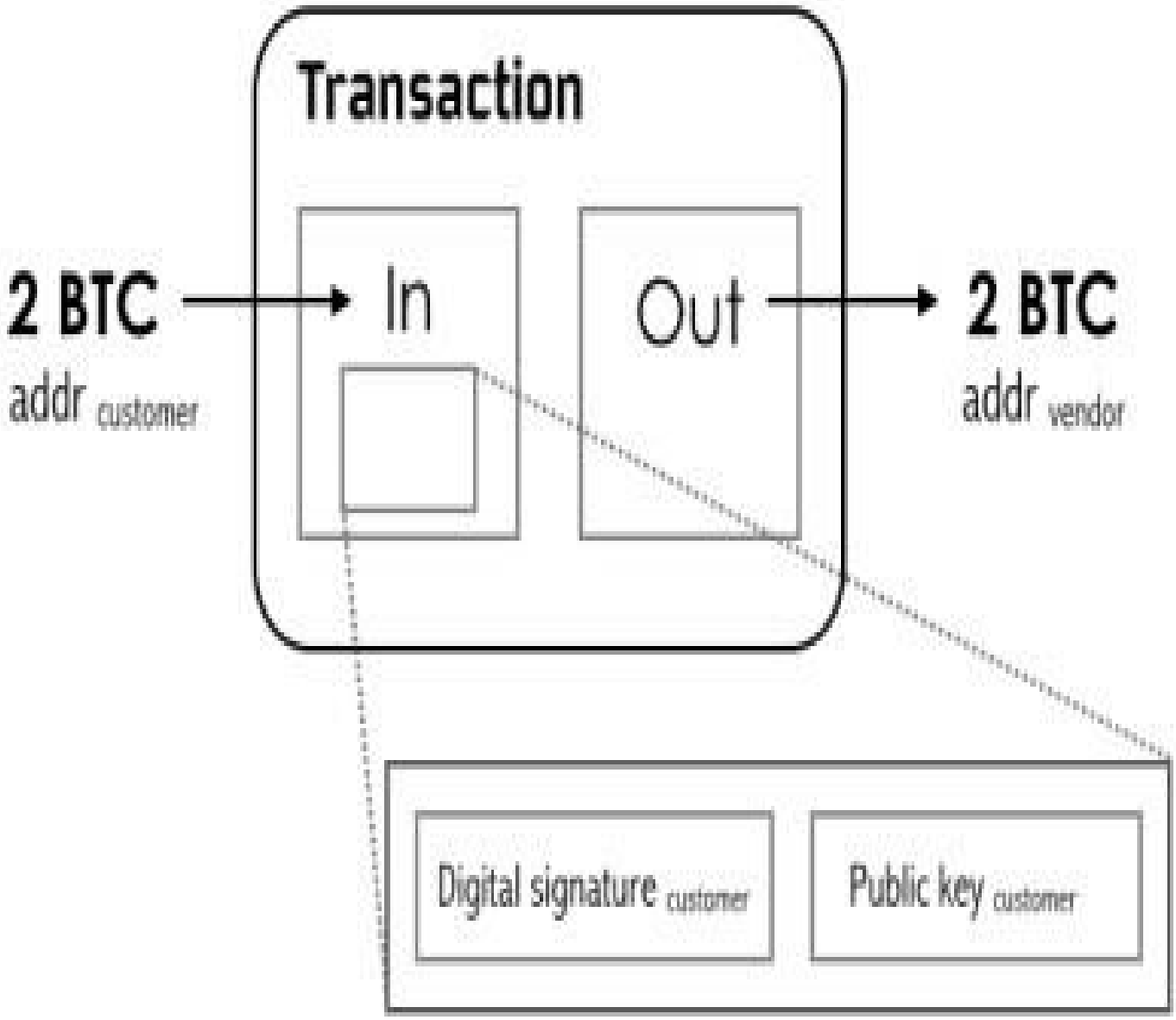
precisamente dato dalla somma degli UTXO;

- le transazioni sono conservative, ossia la somma algebrica degli input e degli output è nulla, a meno di un valore, detto *fee*, che viene incamerato dal *miner* che aggiunge la transazione al proprio blocco e che vince la *proof of work*.

Si osservi ora un possibile schema di una transazione in Bitcoin per comprendere meglio il potenziale delle informazioni che essa porta con sé

proprio con riferimento agli indirizzi coinvolti e ad altri interessanti dati.

In maniera molto esemplificata, una transazione Bitcoin è un insieme di dati che descrive il movimento dei bitcoin; essa accetta degli input e crea nuovi output. Come accennato in precedenza, Bitcoin non è un bene digitale tangibile, anzi, assume la forma di una transazione che viene registrata sulla Blockchain. Questa transazione contiene fondamentalmente l'origine dei fondi (input) come indirizzo Bitcoin e la destinazione (output) come un altro indirizzo.



Struttura semplificata di una transazione in Bitcoin

Per garantire la proprietà dei fondi,

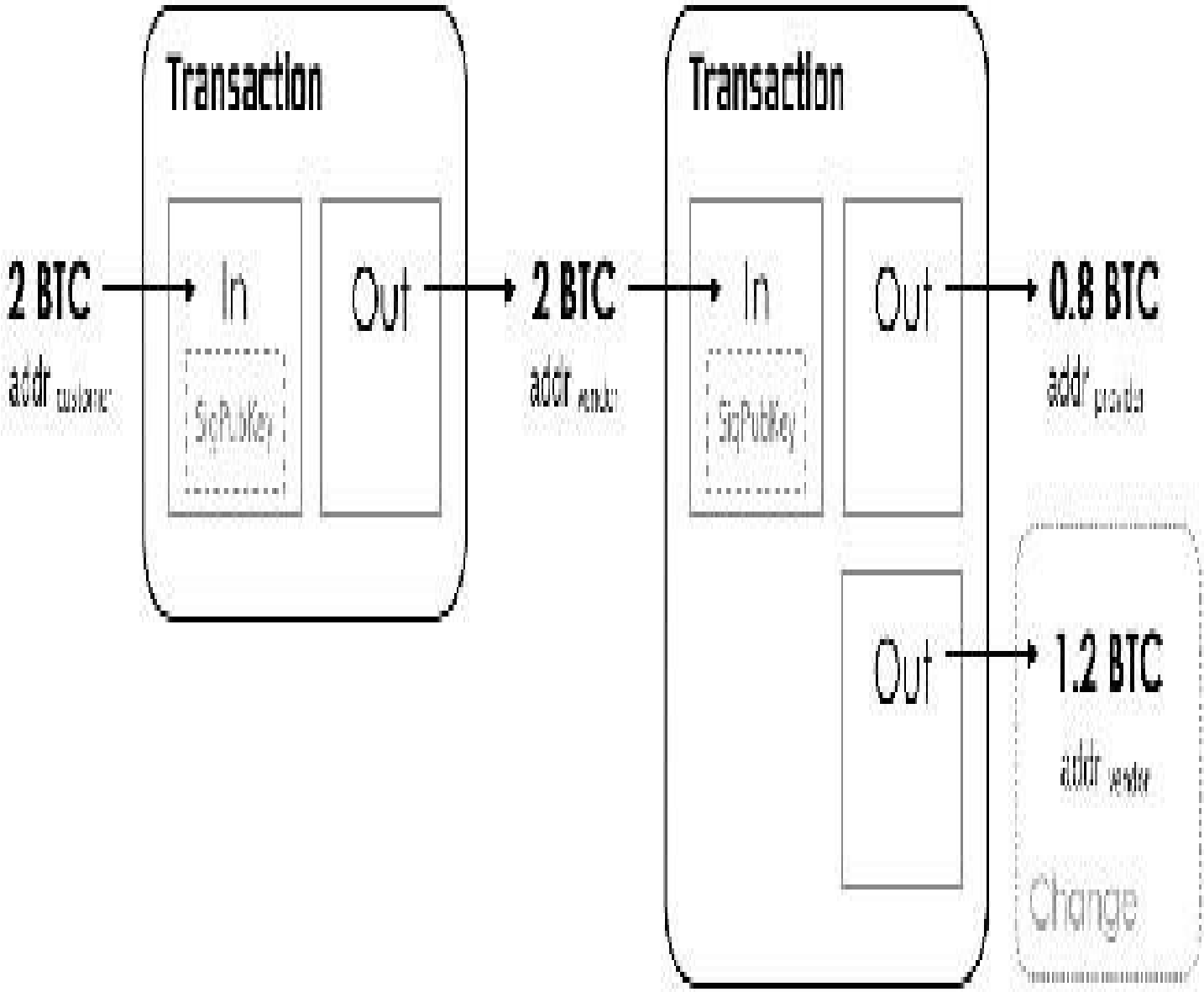
l’intero file delle transazioni è firmato digitalmente con una chiave privata dall’utente che invia i fondi. Quindi, la firma insieme alla chiave pubblica sono incluse nella transazione. Ciò consente a chiunque di convalidare i Bitcoin trasferiti che sono realmente di proprietà del mittente.

Sebbene l’origine dell’indirizzo dei fondi sia derivata dalla chiave pubblica inclusa, in teoria nessuno conosce la vera identità del proprietario di quella chiave pubblica. Lo stesso vale per la destinazione, che è rappresentata da un altro indirizzo Bitcoin, e non ha nemmeno una chiave pubblica da abbinare al proprietario.

Per semplificare, abbiamo mostrato il

punto di vista delle due parti coinvolte nella transazione. Se vedessimo questa transazione dall'esterno, vedremmo solo indirizzi casuali di Bitcoin e non avremmo idea di chi li possiede.

Le transazioni, tuttavia, non esistono da sole. Ogni input di transazione è un puntatore a una transazione precedente. In altre parole, l'input utilizzato in una transazione è stato l'output di una transazione precedente. Blockchain memorizza questo elenco di transazioni collegate in modo che qualsiasi Bitcoin possa effettivamente essere tracciato alla sua origine.



Struttura di due transazioni concatenate

Le transazioni Bitcoin memorizzate nella

Blockchain possono evidenziare una forma veramente semplificata ovvero essere molto complesse con l'evidenziazione di input e output molteplici.

Senza entrare nei meccanismi delle fee e di altri comportamenti esistenti nella rete Bitcoin, è possibile affrontare un approfondimento specifico della struttura di una transazione Bitcoin in maniera tale da comprenderne le potenzialità ove si intendesse operare in maniera quanto più automatizzata un'analisi dettagliata dei dati in essa contenuti. Nel prossimo Capitolo sarà descritta anche la struttura di una transazione di Bitcoin a basso livello in formato esadecimale, in maniera tale da

poter definire il modello di rappresentazione relazionale che potrà essere utile per il presente contributo.

1.2 ANONIMIZZAZIONE E PROCESSAMENTO DELLO STREAMING DI DATI DALLA BLOCKCHAIN

L'utilizzo di una criptovaluta, come ad esempio il Bitcoin, si può prestare anche ad ambiti non leciti. Ciò è incentivato in linea di principio dall'elevato livello di anonimizzazione – anche se più avanti questo aspetto verrà ulteriormente chiarito – che il paradigma delle criptovalute assicura ai loro utilizzatori.

Pertanto, nel verificare un flusso di transazioni presenti all'interno della Blockchain di riferimento per una criptovaluta non è possibile ottenere, in relazione alla peculiare struttura informatica delle transazioni e degli indirizzi di Bitcoin e più in generale delle criptovalute, informazioni relative ai portafogli e, men che meno, ai loro titolari.

Per esperire un'analogia con il mondo tradizionale bancario, conoscere un indirizzo Bitcoin con la possibilità di operare una transazione in modalità in o out è considerato alla stregua di sapere l'esistenza di un codice IBAN che individua uno specifico conto corrente bancario, sul quale è possibile ricevere

ovvero dal quale è possibile inviare del denaro, ma non se ne conosce né la banca o intermediario finanziario né tanto meno l'intestatario.

In tale scenario, si potrebbe ipotizzare di sviluppare un sistema informatico capace di analizzare il flusso di transazioni *real-time* pubblicato sulla Blockchain di riferimento, ad esempio, di Bitcoin con la consapevolezza che eventuali informazioni aggiuntive non possono prescindere dall'unica fonte disponibile, ovvero la Blockchain stessa, carpendone i meccanismi e gli algoritmi più nascosti che la governano.

Oltre alla fonte primaria delle transazioni e degli indirizzi (*rectius* catena di blocchi di transazioni, da cui

deriva il nome di Blockchain), occorre tenere in debita considerazione che le tecniche di deanonimizzazione delle transazioni di utilizzo di criptovalute come il Bitcoin impongono attività di *tagging* e di *clustering* nel Web proprio per far emergere una stretta connessione tra utenti della rete Internet e la pubblicazione di informazioni afferenti agli identificatori di indirizzi Bitcoin e, di conseguenza, delle connesse transazioni. In tale scenario, non si esclude – anzi è certo – l'utilizzo dei protocolli di comunicazione tipici delle c.d. *darknet*, reti in cui è possibile accedere mediante l'utilizzo di software specifici unite a particolari configurazioni di navigazione

anonimizzata o i cui canali di comunicazione sono protetti da robusti algoritmi crittografici. Tali reti – si ricorda – sono caratterizzate dai c.d. *hidden service*; in altri termini, sono caratterizzate da siti web che non vengono indicizzati dai tradizionali motori di ricerca. La più famosa delle *darknet* è individuabile nel progetto Tor [33] che, attraverso l'utilizzo di uno specifico software, abilita l'utente all'uso di un sistema di comunicazione sicuro e altamente anonimo attraverso una rete non raggiungibile tramite la normale connessione internet: occorre infatti installare uno specifico browser e il predetto software per la connessione alla rete Tor.

Senza entrare ulteriormente in dettagli tecnici circa la natura tecnologica della rete Tor, ai fini di delineare il perimetro di un possibile e realistico utilizzo di software di analisi visuale nello specifico settore per creare *intelligence*, è sufficiente evidenziare come l'anonimato garantito, ad esempio, da Tor, unito all'utilizzo dei Bitcoin o di altre criptovalute quale modalità di pagamento, abbia negli ultimi tempi incrementato la diffusione e la recrudescenza di traffici illeciti e attività malevole nel Dark web. Si pensi al recente fenomeno dei *cryptolocker* e, più in generale, dei *ransomware*, software malevoli che, a seguito della cifratura dei dati della vittima,

richiedono il pagamento di un riscatto per decifrare i file. Il pagamento del riscatto è rigorosamente richiesto in criptovaluta per ovvie ragioni.

1.2.1 Informazioni dal *clear web*

È utile comprendere a questo punto in quale spazio è possibile recuperare le informazioni afferenti agli indirizzi ed alle transazioni in criptovaluta. Spesso le informazioni sugli indirizzi Bitcoin e altre monete virtuali possono essere pubblicate e, di conseguenza, ottenute semplicemente mediante un'attenta analisi online. Gli indirizzi infatti possono essere trovati su siti web, forum, microblogging, social media e

siti di condivisione di software.

Occorre pertanto avere l'accortezza di valutare se la natura del sito, dei blog, dei forum o altro siano in ogni caso indicizzati dai motori di ricerca; in particolare, potrebbe capitare che un utente in un blog o in un forum richieda un pagamento in una determinata criptovaluta a fronte di un servizio reso pubblicando uno o più indirizzi in un determinato messaggio.

Sarebbe inoltre necessario, al fine di oltrepassare le logiche dei tradizionali motori di ricerca, di ipotizzare l'utilizzo di software che consentono attività di *crawling* di siti.

1.2.2 Informazioni dal *dark web*

Ci si può chiedere ora se il *dark web* sia veramente oscuro oppure esistano tecniche particolari per capire cosa accade in esso. In realtà sembrerebbe che il nome sia stato coniato da giornalisti a causa della sua natura misteriosa e pericolosa. Il *dark web* ha molti nomi anche se un po' imprecisi, come il *deep web*, *darknet* ovvero spesso identificato con Tor, che in realtà è il metodo principale per accedere e navigare in esso. I siti nel *dark web* sono semplicemente risorse basate su Internet come siti Web, forum, canali di chat IRC e altri tipi che non sono accessibili utilizzando un *browser* tradizionale; inoltre non può essere visto

e non si possono effettuare ricerche usando i normali motori di ricerca.

Essere in grado di accedere a quest'area di Internet è di vitale importanza per un investigatore perché, sebbene il *dark web* non sia interamente legato alla criminalità, molti siti che vendono servizi o prodotti che sono illegali o, nel migliore dei casi, non convenzionali, esistono proprio in questo spazio del Web. Molti di questi *trader* utilizzano Bitcoin e altre criptovalute per accettare pagamenti; pertanto è necessario essere in grado di conoscere tali oggetti per capire al meglio quali informazioni sono presenti in esso.

Seppur molto insidiosa, la navigazione nel *dark web* è possibile prendendo

precauzioni come, ad esempio, utilizzare una macchina virtuale per navigare e fare attenzione ai contenuti che si navigano ed ai relativi *download*.

Quando si tratta di indagare sui *trader*, l'investigatore cerca principalmente quali servizi o prodotti vengono offerti e, ovviamente, gli indirizzi di criptovaluta che vengono indicati per effettuare i pagamenti. In astratto sarebbe anche possibile, mediante meccanismi di acquisto tipici in Internet – come ad esempio il "carrello della spesa" – poter verificare mediante la Blockchain dove vanno a finire i valori di criptovaluta a seguito di ogni singolo acquisto.

Numerosi strumenti software possono

aiutare nella navigazione del *dark web*, ma probabilmente il metodo più semplice è dotarsi, ad esempio, di *Tor Browser* recuperabile da *torproject.org*. Una volta installato il *browser*, occorre eseguirlo e risulterà del tutto simile ad un browser web tipo Firefox.

La struttura del *dark web* è costituita da siti generalmente molto semplici nella struttura dinamica e non dissimili da Internet degli anni novanta. In esso è possibile trovare informazioni relative a indirizzi Bitcoin, pseudonimi, siti, forum, chat, blog e altro ancora.

Mediante l'utilizzo di tecniche di tipo *Open Source Intelligence* [34] è possibile individuare su Internet nomi e *alias* utilizzati dai venditori nel *dark*

web. Alcune operazioni importanti di polizia hanno dimostrato come gli stessi *alias* che si trovano nel *dark web* spesso affiorino sul Web in forum, siti di giochi d'azzardo e altre risorse web; in questi casi potrebbe risultare più agevole poter identificare una o più persone di interesse.

Altra modalità di interesse potrebbe essere quella di monitorare specifici indirizzi di criptovaluta che vengono pubblicati in determinati *hidden service* nel *dark web*. Pertanto taluni pagamenti reali che in esso vengono svolti unitamente a quelli effettuati per finalità anche legittime e legali, potrebbero disvelare la riferibilità degli indirizzi monitorati a soggetti realmente esistenti

con possibilità di identificarli nel mondo reale stesso.

In taluni casi ci si potrebbe imbattere nella presenza di informazioni afferenti al mondo reale pubblicate sui siti nel *dark web*, come ad esempio l'indicazione di indirizzi o altre informazioni che riconducono al mondo reale.

Ulteriori tecniche potrebbero riguardare l'attività di acquisire all'interno del *dark web* un certo livello di affidabilità che potrebbe portare anche alla condivisione di dati e informazioni afferenti al mondo reale.

1.3 COSTRUZIONE DI UN

MODELLO DI RAPPRESENTAZIONE RELAZIONALE DELLE TRANSAZIONI

Giunti a questo punto della trattazione, appare opportuno comprendere se vi sia la possibilità di immaginare le transazioni e gli indirizzi Bitcoin in esse coinvolti come una rete e, di conseguenza, valutare di sfruttare i principi della teoria dei grafi per rappresentare e recuperare nuova "conoscenza" dalla loro applicazione allo specifico contesto delle criptovalute, in particolare al Bitcoin. Una rete di transazioni di criptovalute e dei relativi indirizzi in esse coinvolti, a

prima vista, può essere ricondotta nell'alveo dei cd. sistemi complessi e, come tali, rappresentabili con l'utilizzo di grafi [35].

Senza entrare nel merito di dissertazioni di natura metodologico-matematica, si può affermare che un modo efficiente per lo studio di un sistema complesso è quello di scomporlo in parti più semplici, comprenderne il funzionamento e, di conseguenza, cercare di ricomporre il sistema originale; molti sistemi complessi possono essere rappresentati in termini di reti o *network* di elementi o entità di vario genere che interagiscono tra loro.

Essenzialmente ciascuna rete è caratterizzata sempre da due componenti

fondamentali, senza le quali non si potrebbe pensare al concetto che essa esprime nel suo insieme: un insieme di nodi e un insieme di connessioni e relazioni tra i predetti nodi.

Un nodo può essere visto come un'entità computazionale: riceve, ad esempio, un input e lo elabora per fornire un output. Tale processo potrebbe assumere connotazioni estremamente semplificate, persino nulle, o parimenti complesse per le implicazioni che ha sull'intera rete. Le connessioni, di contro, determinano un flusso tra i nodi, come per esempio una serie di informazioni, potendo essere unidirezionale o bidirezionale.

Pertanto, le interazioni tra i nodi attraverso le connessioni portano a

determinare un comportamento globale del sistema, che non può essere osservato nelle sole singole componenti. Ciò fa emergere le peculiari capacità di una rete che possono superare, per gli effetti che determinano, quelle dei singoli comportamenti ovvero quelle della loro semplice somma.

Se si affronta il tema della Blockchain e delle transazioni Bitcoin con questo tipo di strumento, è possibile creare nuova "conoscenza" nello studio e negli approfondimenti del fenomeno, tenendo in considerazione come può influire nel complesso la singola transazione ed i relativi indirizzi coinvolti [36].

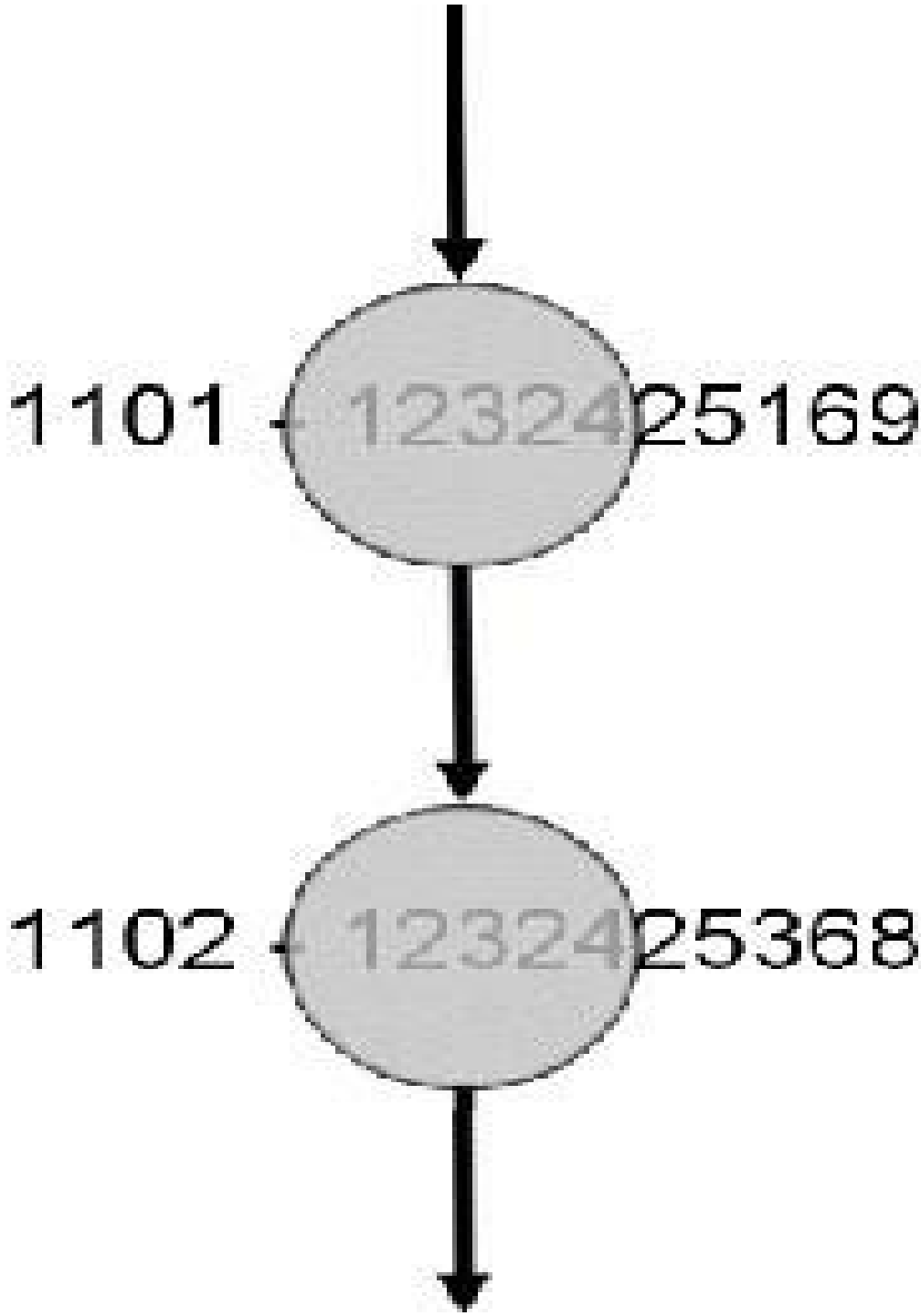
Il modello che qui si vuole proporre, in un'ottica poi di creazione di un metodo

dedicato alla ricerca di informazioni utili ad una più approfondita conoscenza del Bitcoin, deve essere costituito da nodi e da connessioni ben chiare che potranno essere opportunamente interpretate ed elaborate per essere rappresentate secondo un reticolo relazionale ben definito.

Le componenti del modello che vengono prese in considerazione sono le transazioni e gli indirizzi Bitcoin. Le relazioni e le connessioni tra di loro sono recuperabili dalla struttura medesima della Blockchain che unisce, in un reticolo lineare, tutte le transazioni in blocchi.

Tutti i nodi di blocco sono collegati da archi orientati che puntano al loro

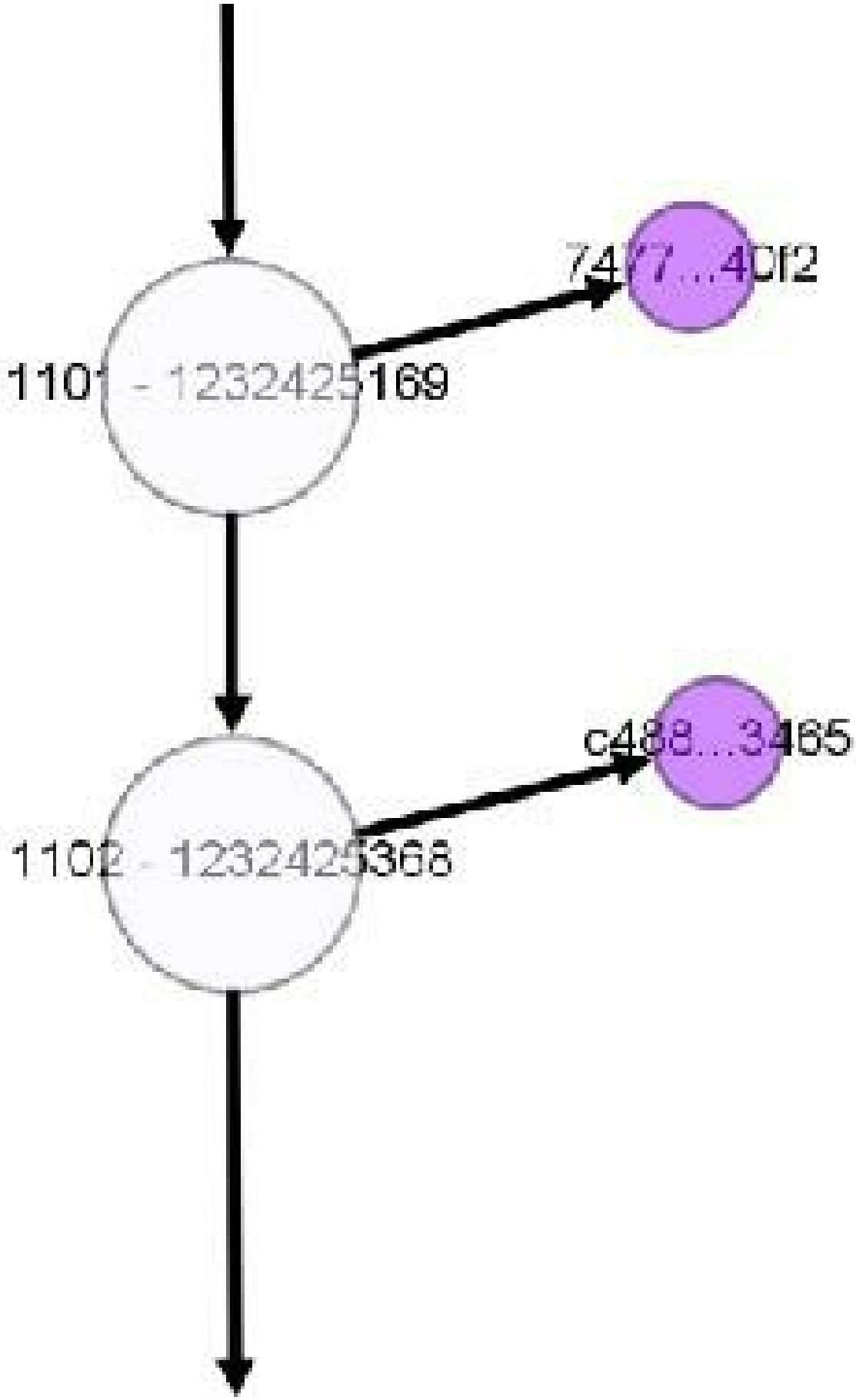
successore. Il nodo che rappresenta un blocco contiene un'*altezza* del blocco, memorizzata come numero intero, e un *tempo* di blocco memorizzato nel formato orario Unix come numero intero. Di seguito la possibile schematizzazione di due blocchi successivi.



Modello visuale di due blocchi di transazioni

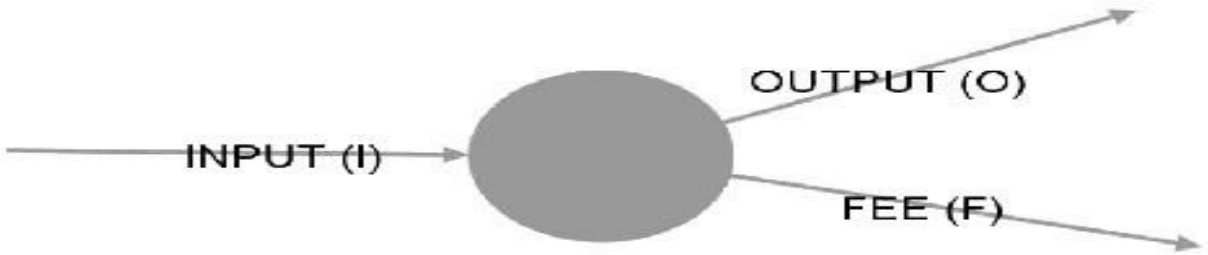
I nodi di ciascun blocco hanno i

collegamenti orientati che puntano a tutte le transazioni contenute nei blocchi rappresentati. Il nodo di transazione contiene un valore di hash della transazione memorizzato come stringa ed una commissione di transazione memorizzata come numero intero.


7477...4012
1101 - 1232425169
c488...3465
1102 - 1232425368

Modello visuale di due blocchi con le relative transazioni

Sotto il profilo grafico è possibile costruire il modello visuale che rappresenta una transazione in Bitcoin.



Modello visuale di una transazione

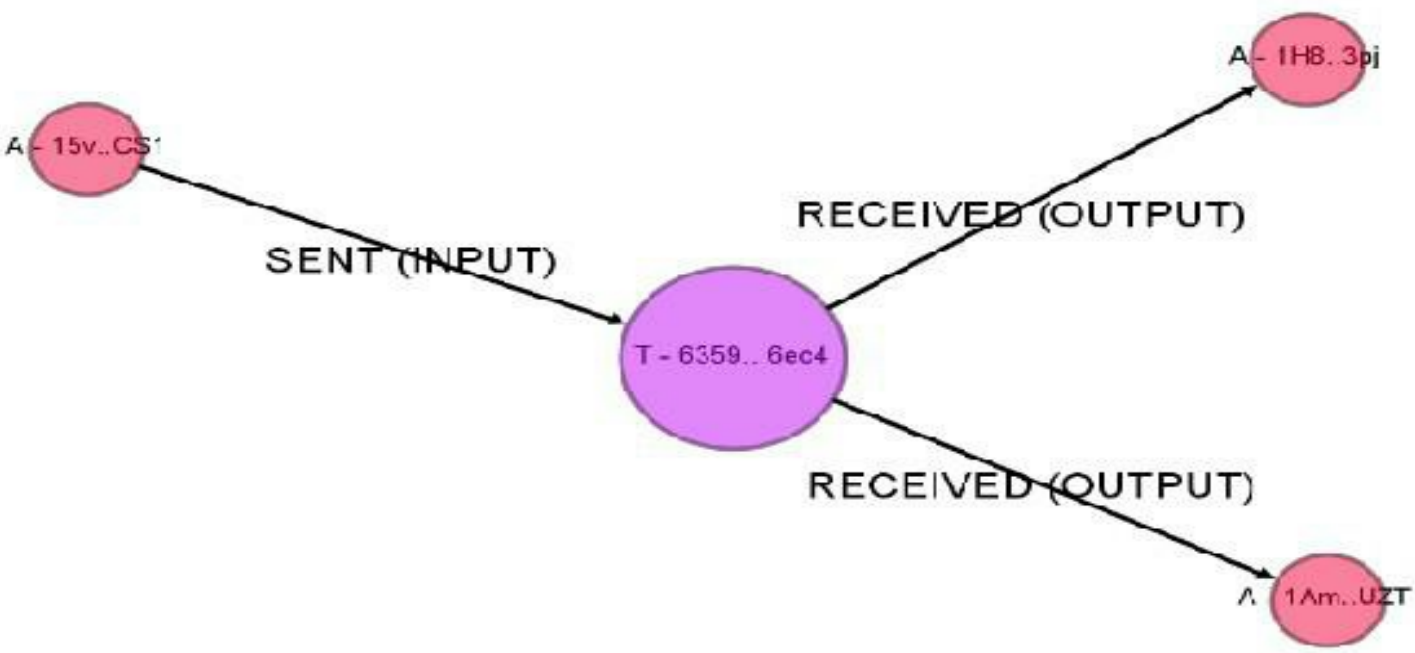
Data la conservazione delle transazioni, risulta sempre verificata la uguaglianza:

$$I - O - F = 0 \leftrightarrow I = O + F$$

ossia la somma algebrica degli input e degli output è nulla, a meno di un valore, detto *fee*, che viene incamerato dal *miner* che aggiunge la transazione al proprio blocco e che vince la *proof of work*.

In altri termini, esistono due tipi di connessioni tra ciascun indirizzo interessato e, quindi, coinvolto in una transazione. Ciascun indirizzo con un collegamento orientato di tipo *sent*

rappresenta un input della transazione medesima. Di contro, i nodi che rappresentano indirizzi con collegamenti orientati di tipo *received* si identificano con gli output della transazione in esame. Gli archi stanno a rappresentare il flusso di valuta virtuale che è stato inviato o ricevuto nell'ambito della transazione. Di seguito una possibile rappresentazione grafica di quanto sopra specificato.



Modello visuale di una transazione reale Bitcoin

1.3.1 Rappresentazione delle transazioni

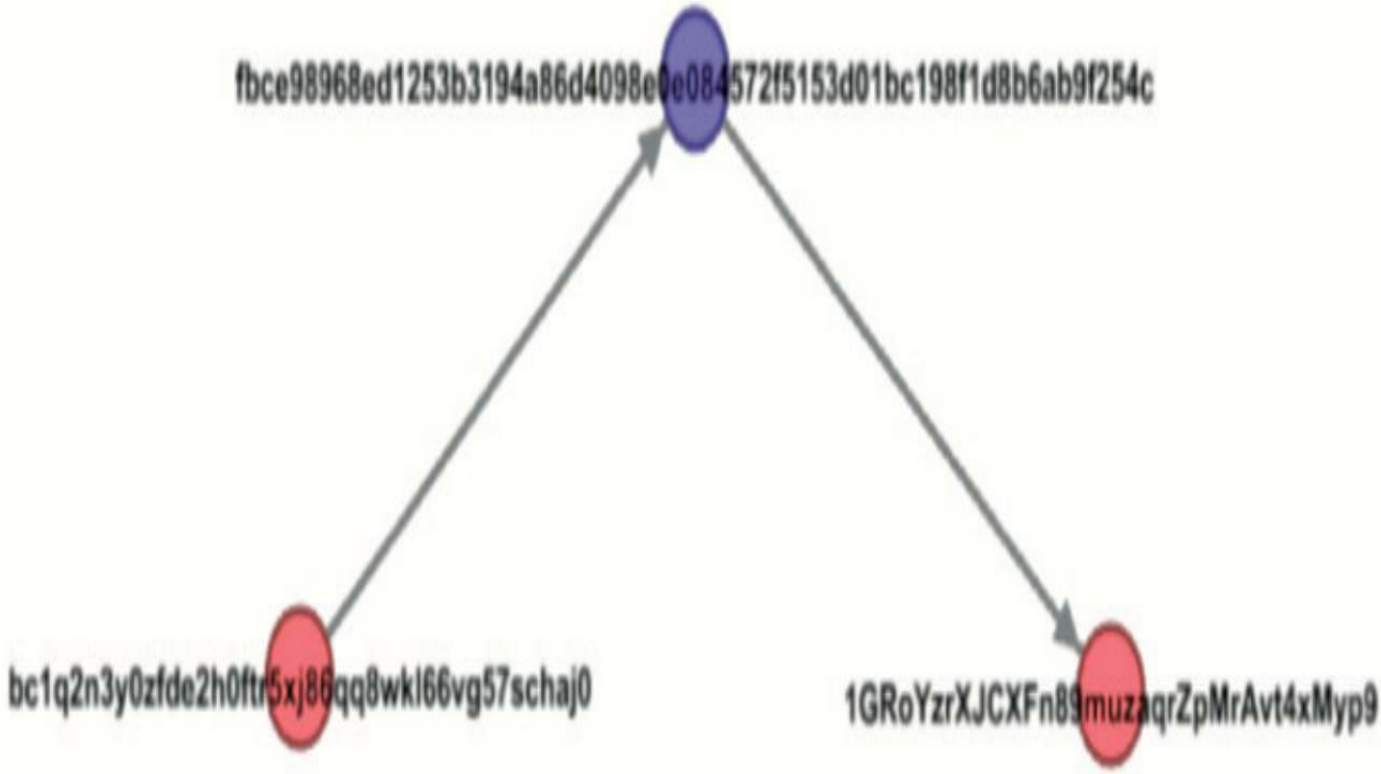
Prendendo le mosse da tale struttura concettuale, è possibile modellare ciò che accade normalmente nell'osservare in tempo reale l'evoluzione della Blockchain di Bitcoin. In altre parole, si potranno osservare le transazioni che, istante dopo istante, collegano – secondo la logica sottesa dalla loro struttura computazionale per come affrontata nei precedenti paragrafi – due o più indirizzi Bitcoin.

Le figure che seguono mostrano possibili schematizzazioni della rete di transazioni e di indirizzi Bitcoin mentre si osserva l'evoluzione, per un determinato intervallo di tempo, della Blockchain di riferimento. I nodi di

colore rosso rappresentano gli indirizzi Bitcoin mentre quelli di colore viola raffigurano le transazioni che li coinvolgono. Il meccanismo di modellazione può essere rappresentato in maniera estremamente semplificata nel modo che segue: si parta ad esempio dalla seguente transazione che vede un indirizzo Bitcoin in input e uno in output come meglio specificato di seguito.

Da un punto di vista visuale e relazionale, la transazione in esame può essere rappresentata con un grafo

orientato come quello che segue.



Transazione rappresentata secondo il modello proposto

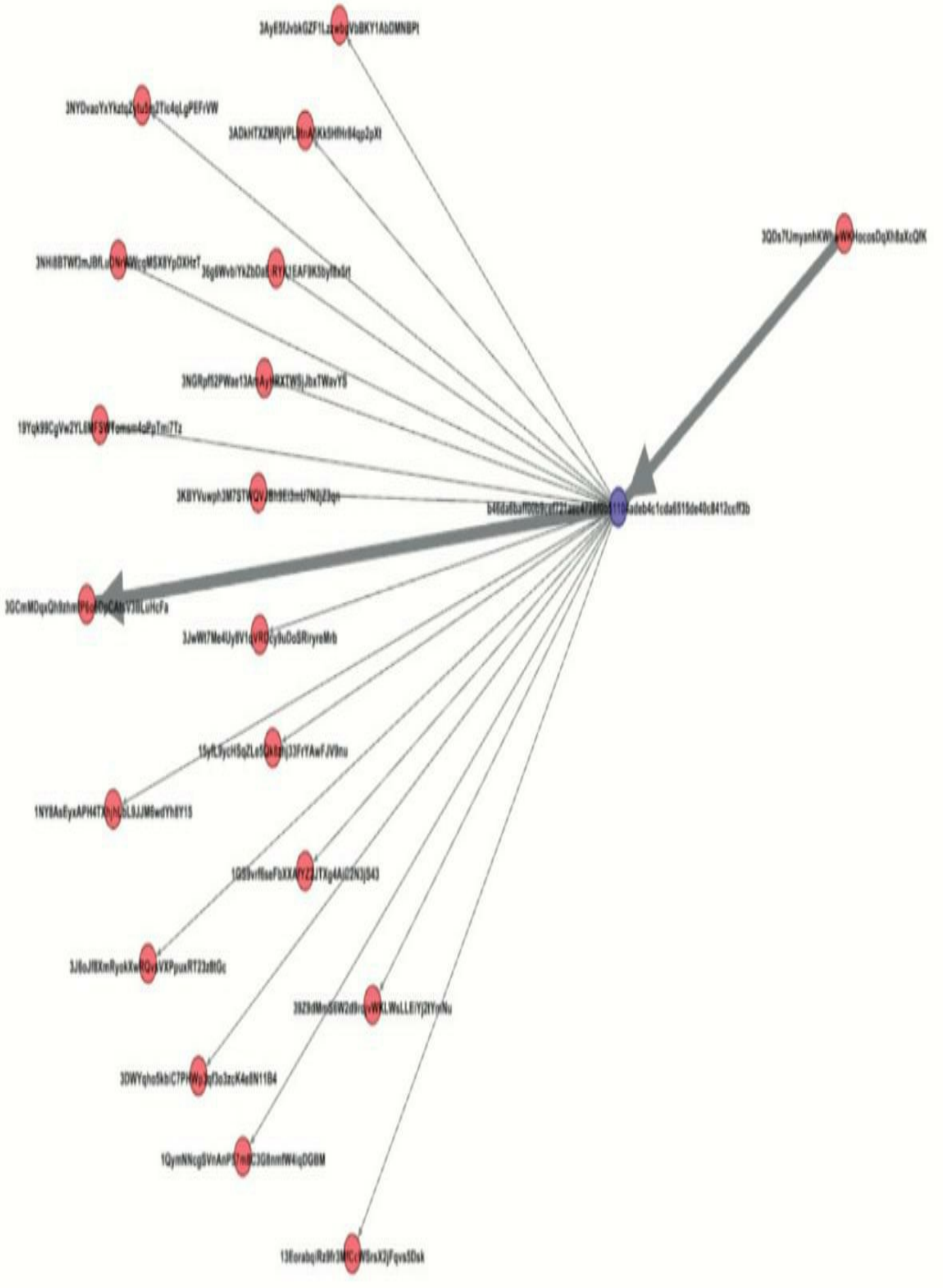
Ovviamente è possibile recuperare strutture relazionali molto più complesse come quelle che rappresentano il

seguente scenario.

b46da6baff00b9cef721aec4726f0b51104adeb4c1cda6515de40c8412ccff3b

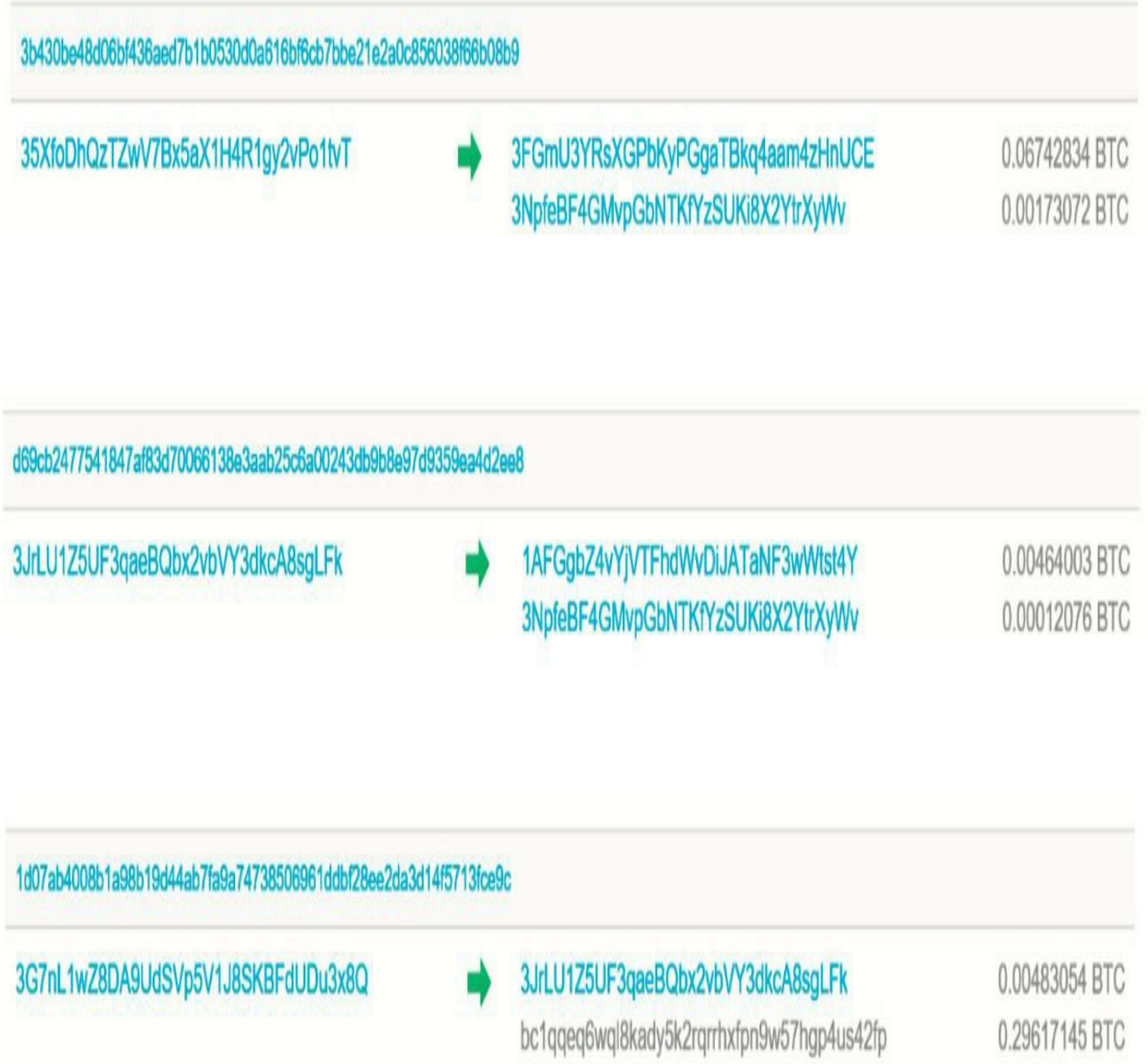
3QDs7fJmyanhKWhwWKHocosDqXh8aXcQfK	→	3NYDvaoYxYkztqZytu5m2Tic4qLgPEFrVW	0.00311588 BTC
		3DWYqho5kbiC7PHWp3qf3o3zcK4e8N11B4	0.00283247 BTC
		39Z9dMmS6W2d9rojvWKLWsLLEiYj2tYmNu	0.00924998 BTC
		36g6WvbiYkZbDaEiRYK1EAF9K5byf8x5rt	0.0031836 BTC
		3KBYVuwph3M7STWQVJBh9Ei3mU7N2jZ3qn	0.0059982 BTC
		3ADkHTXZMRjVPL9tnA5Kk5HfHr84qp2pXt	0.002281 BTC
		3NHi8BTWf3mJBfLuDNrWWcqMSX8YpDXHzT	0.0034 BTC
		13EorabqiRz9fr3MfCcWSrsX2jFqvs5Dsk	0.03928628 BTC
		19Yqk99CgVw2YL6MFSWTomsm4oPpTmi7Tz	0.01093959 BTC
		15yfL9ycHSqZLe5Qk8zhj33FrYAwFJV9nu	0.0025 BTC
		3GCmMDqxQh9zhmfP6o6DpCAtsV3BLuHcFa	27.14517462 BTC
		1GS9vrf6seFbXXAfYZ2JTXg4AiC2N3jS43	0.00576957 BTC
		3NGRpf52PWae13AmAyHRXTWSjJbxTWavYS	0.00395659 BTC
		1QymNNcgSVnAnP57m8C3G8nmfW4iqDGBM	0.07812354 BTC
		3AyE5fJvbkGZF1LzzwbqVbBKY1AbDMNBPt	0.0016956 BTC
		3J6oJf8XmRyokXwRQvsVXPpuxRT23z8tGc	0.0041458 BTC
		1NY8AsEyxAPH4TXhjhLbL9JJM6wdYh8Y15	0.00105619 BTC
		3JwWt7Me4Uy8V1qVRDcy9uDoSRiryreMrb	0.00320734 BTC

In tal senso si potrà ottenere una struttura relazionale come quella che segue, capace di far percepire *ictu oculi* quali sono i nodi sui quali è possibile osservare il maggiore flusso di criptovaluta, grazie alla possibilità di rappresentare le connessioni tra i nodi con uno spessore proporzionale alla dimensione di valori di Bitcoin che ciascun indirizzo movimenta sia in ingresso che in uscita.


3AyE5fJvbkGZF1LzzwbqVbBKY1AbDMNBPt
3NYDvaoYxYkztqZ1tu3e2Tic4qLgPEFrVW
3ADkHTXZMRjVPL9tnA2KkShfHr84qp2pXt
3QDs7fJmyanhKWhaWKHocosDqXh8aXcQfK
3NH8BTWf3mJBfLuDNrAWcgMSXBYpDXHrT
36g9Wvb/YkZbDaERYA1EAF9K3byfbx8rt
3NGRpf52PWae13Ar4AyHRXTW5jJbxTWavY5
19Yqk99CgVw2YL6MF3Wfomsm4qPpTmi7Tz
3KBYVuwph3M7STNQVJBh9Eh3mU7N3jZ3qn
b46da6baff00b9cdf221aaa4728f0b5119dadeb4c1cda6515de40c8412ccff3b
3GCmMDqxQh9zhmPfbdMDpCAtkV3BLuHcFa
3JeWt7Me4Uy8V1qVRQCy9uDoSRiryreMrb
15yfL5ycH5qZLe5Qk8hj33FrYAwFJV9nu
1NY8AaEyxAPH4TXhjhLbLSJJM6wdYh8Y15
1Gt59vrf6aeFbXXAfYZ2JTXg4AJ2N3jb43
3J8oJfBXmRyokXwRQvaVXPpuxRT22zBtGc
39Z9dMmS6W2d9rqvWKLWsLLEiYj2tYrwNu
3DWYqhe5kbiC7PHWp3qf3o3zcK4e8N11B4
1QymNNcgSVnAnP17mBC3G8nmfW4qDGBM
13EorabqiRz9h3MKCvW9rsX2jFqvs5Dsk

Transazione rappresentata secondo il modello proposto

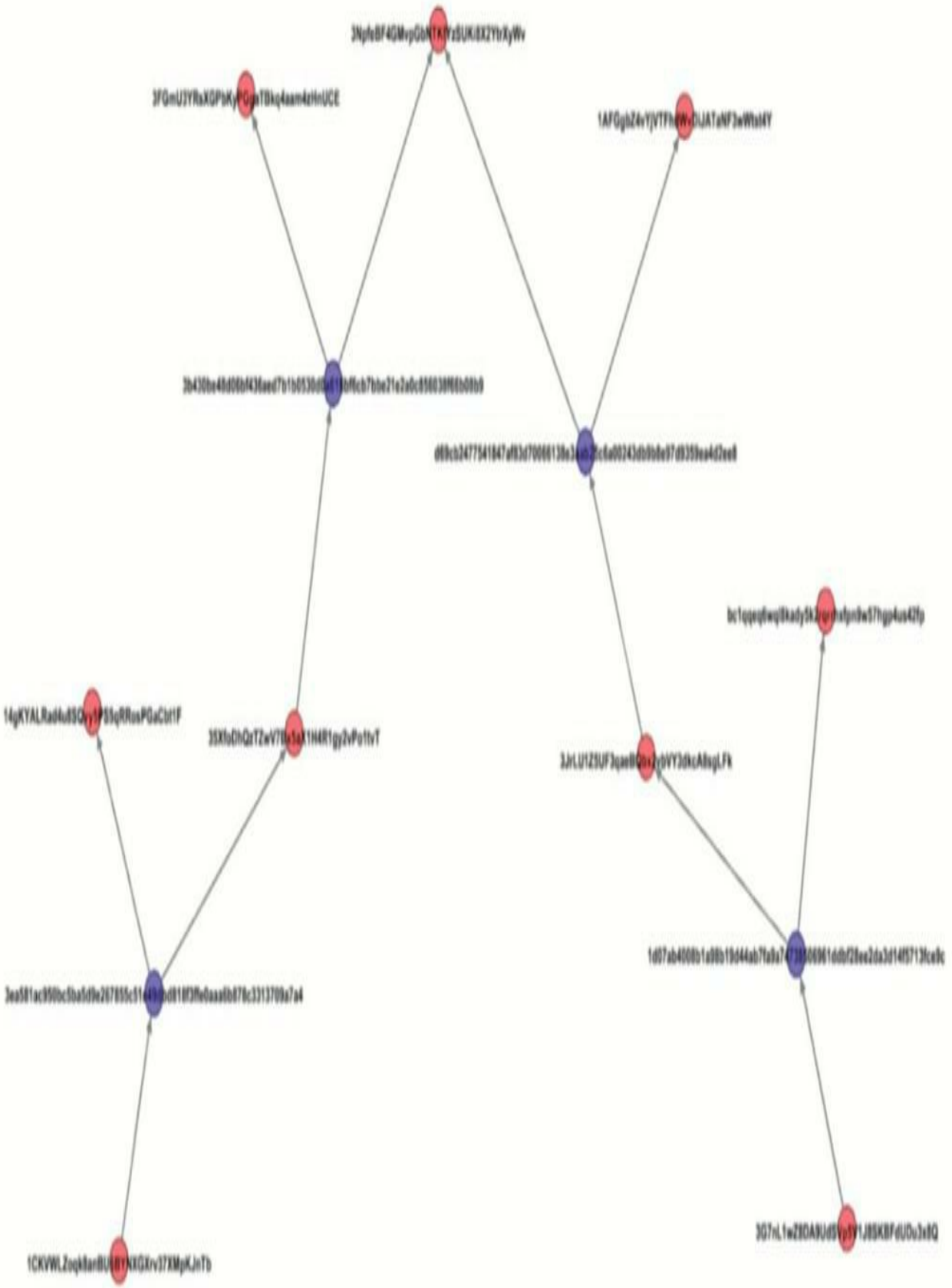
Ulteriori casistiche interessanti che sono applicabili al modello così descritto possono consentire di recuperare una concatenazione di transazioni, permettendo di seguire in astratto il flusso di criptovaluta attraverso la rete di indirizzi in cui sono coinvolti.



Dati di più transazioni collegate

Le transazioni sopra individuate ed i

relativi indirizzi Bitcoin possono essere agevolmente rappresentati in maniera visuale e relazionale in modo tale da far comprendere ancora una volta in maniera rapida ed intuitiva la dinamica dei flussi di criptovaluta attraverso i vari nodi di interesse.



Rappresentazione della rete di transazioni e indirizzi collegati

Come è facile notare, anche se fortemente semplificata nel numero di entità presenti in ordine al relativamente breve lasso temporale osservato, la rete evidenzia una sua complessità intrinseca con specifico riferimento alle relazioni che la stessa fa emergere, anche in maniera indiretta, tra i singoli nodi. In teoria, potendo osservare senza soluzione di continuità – sia in termini temporali che computazionali – le informazioni pubblicate nella Blockchain, sarebbe possibile ottenere una visione complessiva della rete di

transazioni e di indirizzi Bitcoin, potendone calcolare agevolmente il diametro complessivo, eventuali cluster e altre statistiche utili ad una comprensione più profonda del fenomeno che andrebbe oltre il classico approccio circoscritto e puntuale ovvero di natura economico-finanziaria e meramente computazionale.

1.3.2 Ricostruzione del flusso di "denaro" virtuale

Un'attività molto interessante sotto il profilo tecnico ed investigativo è senza dubbio il tentativo di ricostruire i flussi di criptovaluta e le dinamiche sottostanti al loro utilizzo.

Mediante la struttura della Blockchain e delle informazioni connesse a ciascun blocco di transazioni, è in astratto possibile poter recuperare il flusso di criptovaluta che attraversa, sia in input che come output, uno o più indirizzi. Se ricostruire il flusso è teoricamente possibile, meno agevole risulterà determinare la riconducibilità di un determinato importo di criptovaluta ad un ben identificato soggetto.

Nel prosieguo della presente trattazione saranno forniti alcuni esempi di tecniche che, ove condotte con particolare attenzione e perizia, potrebbero rilevarsi molto interessanti e utili a comprendere in maniera più ampia l'utilizzo di criptovalute da parte di soggetti ben

determinati.

1.4 IL PROBLEMA DELL'ANALISI DEI DATI RELATIVI ALLE TRANSAZIONI E AGLI INDIRIZZI BITCOIN

In questo paragrafo si fa cenno alle tecniche di deanonimizzazione di base per le reti di transazioni in Bitcoin, in considerazione del fatto che un utente può autonomamente generare più di un indirizzo, fino ad uno per singola transazione.

Appare utile ricordare che gli indirizzi Bitcoin sono dei "codici" simili agli identificativi IBAN (*International Bank*

Account Number) bancari e possono essere utilizzati per ricevere della moneta e da essi si può attingere, come se fossero dei conti correnti, per disporre dei versamenti.

La vera differenza rispetto al modo bancario è che in ambito Bitcoin nessuno è tenuto a comunicare il possesso di uno o più particolari indirizzi. Se da un lato vi è quindi una percezione di anonimato, dall'altro è possibile osservare come di contro ogni aspetto del Bitcoin è pubblico: per questo motivo è tendenzialmente più corretto, come accennato, definire il Bitcoin come "pseudonimo" piuttosto che "anonimo".

1.4.1 Tecniche di *tagging*

Una prima tecnica di deanonimizzazione che può essere utilizzata è il *tagging*, ossia l'associazione a un indirizzo e, conseguentemente, all'interno *cluster* di indirizzi collegati, di una sorta di etichetta che ne identifica, anche in via indiretta, il detentore [37].

Tale attività può utilizzare un motore di web *crawling* e di *scraping*: con il processo di *crawling* si analizzano interi siti web e se ne indicizzano tutti i contenuti.

Un *crawler* è un software specializzato per prelevare tutto il contenuto di una pagina web e seguirne i vari *link* per analizzare siti web collegati o pagine

secondarie. Una volta raccolte tutte le pagine, queste vengono analizzate con il processo di *scraping*.

Il processo di *web scraping*, noto anche come *web data extraction*, è una tecnica, di solito automatizzata, che consiste nel prelevare singoli dati da un insieme di pagine web, per collezionarli all'interno di database o file per essere poi sottoposti ad analisi future. Nel contesto di studio, si procede con la ricerca all'interno delle pagine web tramite *match* del testo della pagina con una espressione regolare, le stringhe che possono rappresentare indirizzi Bitcoin.

Vengono essenzialmente ricercate stringhe lunghe da 26 a 35 caratteri, con il primo carattere rappresentato dal

carattere 1 o 3, che non contengono all'interno caratteri ambigui (del tipo O, 0, I, l) nella nota codifica *base58* utilizzata per tale ambito. Viene quindi utilizzato un algoritmo di validazione per verificare l'esatta corrispondenza della stringa candidata con un indirizzo bitcoin. All'indirizzo trovato viene quindi associata la pagina web in cui è presente ed ogni indirizzo e-mail, *nickname* o pseudonimo, in modo da poter, usando questi dati, risalire all'identità dei possessori dell'indirizzo Bitcoin stesso.

Un limite di tale tecnica riguarda il fatto che il numero di indirizzi etichettabili in questo modo è di molto inferiore dell'intero numero di indirizzi esistenti.

Per tale ragione è necessario abbinare a questa tecnica l'attività di *clustering*.

1.4.2 Tecniche di *clustering* applicate all'analisi delle transazioni: introduzione

Il *clustering* degli indirizzi bitcoin è un processo che tenta di de-anonimizzare gli utenti bitcoin attraverso la scoperta di tutti gli indirizzi generati da un singolo utente, grazie l'analisi delle informazioni derivate dalla blockchain. Osservare la rete *peer-to-peer* (abbrev. P2P) rappresenta anche un'altra fonte di informazioni che aiuta nella deanonimizzazione degli utenti di Bitcoin. La combinazione di Blockchain

e informazioni da una rete P2P può promuovere il processo di *clustering* degli indirizzi Bitcoin.

Precedenti studi di ricerca [32] hanno presentato l'euristica per il *clustering* degli indirizzi bitcoin e hanno dimostrato che è possibile, sotto certe condizioni e assunzioni, collegare più indirizzi a un singolo *wallet* ovvero ad un singolo utente. Inoltre, è stato dimostrato che in molti casi è possibile collegare l'indirizzo bitcoin di un utente a informazioni derivate da fonti aggiuntive che aiutano nella rivelazione dell'identità dell'utente. Nello scenario peggiore, questa informazione può essere utilizzata per correlare tutte le transazioni di un utente identificato.

Prima di essere archiviate sulla Blockchain, le transazioni vengono trasmesse attraverso una rete P2P decentralizzata. Tramite la connessione e il monitoraggio della rete, è possibile ottenere ulteriori informazioni relative al mittente di una transazione. Ciononostante, con gli utenti bitcoin che utilizzano *virtual private network* (abbrev. VPN), *server proxy* o servizi di portafoglio *online*, non è certo se le informazioni ottenute, attraverso l'adesione alla rete e il monitoraggio del normale flusso di messaggi, possano essere utilizzate per deanonimizzare gli utenti di Bitcoin.

Tutte le transazioni confermate formano un grafico noto come *grafico delle*

transazioni, che viene tracciato utilizzando tutte le transazioni confermate come vertici e aggiungendo un singolo fronte da ogni uscita all'input di spesa. Il grafico della transazione è rappresentato un grafo aciclico, diretto e orientato che riflette i passaggi della proprietà del Bitcoin. Se si è in possesso di alcuni Bitcoin, si ha il diritto di spendere queste monete virtuali. In pratica, la proprietà dei Bitcoin equivale al possesso di una particolare chiave privata che corrisponde alla chiave pubblica trasmessa insieme all'output della transazione che ha dato la proprietà a queste monete. Di conseguenza, per emettere una transazione valida, il

proprietario delle monete deve firmare l'input di spendita della transazione utilizzando la chiave privata specifica che corrisponde alla chiave pubblica delle monete che è stata trasmessa insieme all'output della transazione procedurale.

La sfida principale è che, anche con la presenza di *cluster* di indirizzi basati su blockchain e di informazioni derivate dalla rete, non vi è alcuna garanzia che la tracciabilità di un utente bitcoin sulla propria identità del mondo reale possa avere successo nella totalità dei casi.

In altri termini, è possibile tentare di utilizzare le relazioni e i corrispondenti dati pubblicati su Blockchain per raggruppare, anche parzialmente, gli

indirizzi di criptovaluta in maniera tale da poterli ricondurre ad un preciso *wallet* o portafoglio. Riuscire in questo intento potrebbe consentire di analizzare i l *background* finanziario di un determinato soggetto.

Il protocollo si fonda, come sopra accennato, sulla crittografia asimmetrica e offre una copertura dell'identità del possessore della moneta limitata alla pseudonimia: ogni indirizzo è provvisto di una chiave privata (che il proprietario usa per confermare e autorizzare le transazioni) e di una chiave pubblica (che poi viene tradotta in un "indirizzo" bitcoin). Un utente può avere infiniti indirizzi (e quindi infinite coppie di chiavi privata e pubblica) che di solito

vengono raccolti e gestiti in wallet ("portafogli") ma nessuno è obbligato né a richiedere a terzi l'autorizzazione a utilizzare indirizzi o *wallet* né a comunicare il loro possesso.

Gli indirizzi Bitcoin si possono generare autonomamente, anche su un personal computer, in numero potenzialmente infinito. Questo aspetto ha nel tempo portato a credere che le transazioni potessero essere irrintracciabili e che non si potessero ricostruire i *wallet* e le proprietà degli indirizzi tramite l'analisi della Blockchain.

Una delle principali tecniche di base che possono essere utilizzate per cercare di individuare dei collegamenti tra soggetti e indirizzi Bitcoin è detta *clustering*,

ossia il raggruppamento di più indirizzi e la loro attribuzione ad un unico utente. Ciò è possibile applicando delle logiche, cd. euristiche, alle transazioni contenute nella Blockchain.

Questa tecnica consiste nel trovare e raggruppare gli indirizzi in wallet, cioè in gruppi d'indirizzi appartenenti presumibilmente a un singolo soggetto (che può poi essere riconducibile ad un individuo, un negozio, un *exchange*, un *mixer* o altro). Il *clustering* avviene tramite un'analisi della Blockchain e l'utilizzo di alcuni approcci euristici, descritti efficacemente da Jonas David Nick [38]. Sostanzialmente, tramite il *clustering* è possibile, dato un indirizzo Bitcoin appartenente a un'entità,

identificare eventuali altri indirizzi facenti parte del suo stesso wallet. Trasponendo l'esempio teorico nella realtà, sarebbe come riuscire a identificare tutti i conti correnti di proprietà di un soggetto – anche quelli che questi sta tentando di mantenere segreti – conoscendone soltanto uno tramite il quale, ad esempio, sono stati commessi degli illeciti.

Le euristiche sono misurazioni basate sull'analisi del protocollo Blockchain e sull'esperienza; tali misurazioni non sono sempre valide ma se correttamente pesate possono consentire di indicare un elevato livello di attendibilità delle risultanze dell'analisi.

Più in dettaglio, nel prossimo paragrafo

sono descritti i principi su cui si basa il *clustering*, così come abilmente raccolti e documentati da Jonas David Nick nel suo lavoro sulla deanonimizzazione del Bitcoin [38].

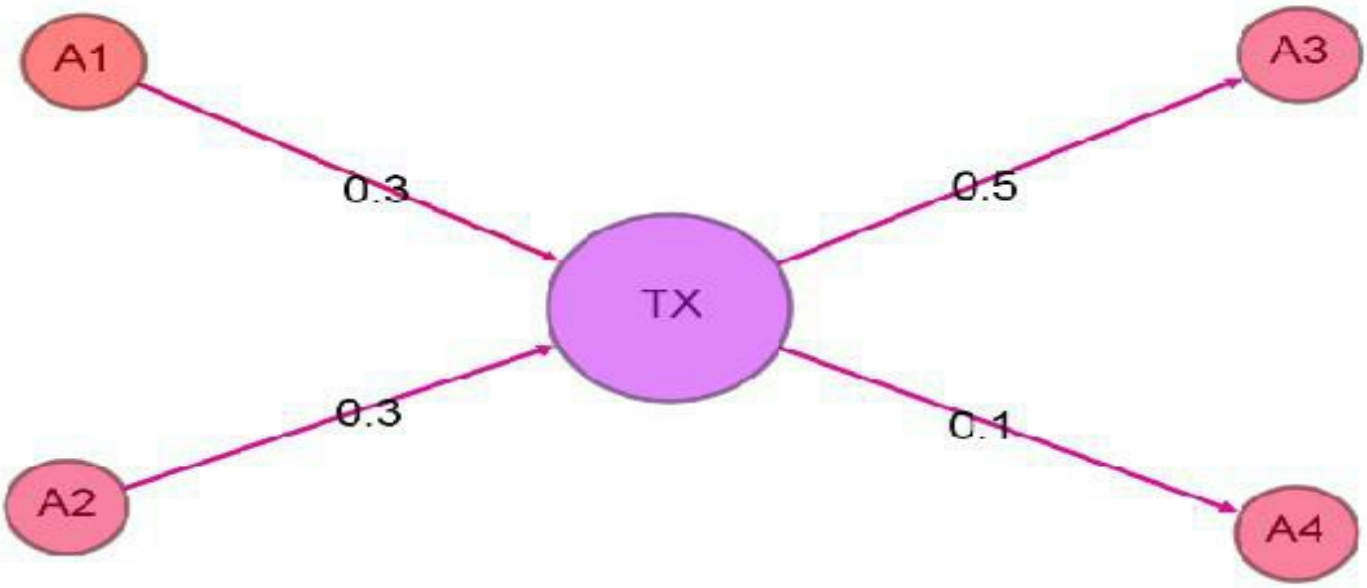
1.4.3 Tecniche di *clustering* applicate all'analisi delle transazioni: le principali euristiche

La prima euristica ipotizzata viene definita "*Multi-Input Heuristic*". La stessa venne già accennata dal presunto creatore del protocollo, noto come Satoshi Nakamoto [39]; questa regola mostra come tutti gli indirizzi in input di una transazione provengano dallo stesso *wallet*, principio questo valido sempre,

nel senso che l'autore della transazione possiede le chiavi private di tutti gli indirizzi in input. Ciò su cui vanno fatte le giuste premesse è cosa si deve intendere con "autore" o "soggetto": non sempre infatti si tratta di una persona, potrebbe essere infatti un *exchange*, un *mixer*, un *wallet online*. Tale approccio è basato sul fatto che solitamente i *wallet* sono i soli responsabili della generazione delle transazioni di un utente e che quindi, se si è a conoscenza del fatto che, in una transazione definita come *multi-input*, un indirizzo sia di proprietà dell'utente, anche tutti gli altri indirizzi in input apparterranno allo stesso.

Pertanto, potendo supporre che tutti gli

indirizzi di input siano associati al medesimo wallet, si può presentare il seguente schema in cui un preciso *client wallet* sta inviando 0,5 Bitcoin, utilizzando due indirizzi come input per la transazione in esame; ciò sta a significare che tutti gli input provengono dal medesimo portafoglio.



Più in generale, l'euristica *multi-input* di un determinato indirizzo A_n consente pertanto di ricercare tutte le transazioni che hanno più di un input, in cui uno di essi è proprio A_n e, di conseguenza, restituisce tutti gli indirizzi che sono

input della transazione. Nel caso sopra esposto, se si considera l'indirizzo A1, l'euristica *multi-input* ad esso applicata restituirà la coppia di indirizzi (A1, A2).

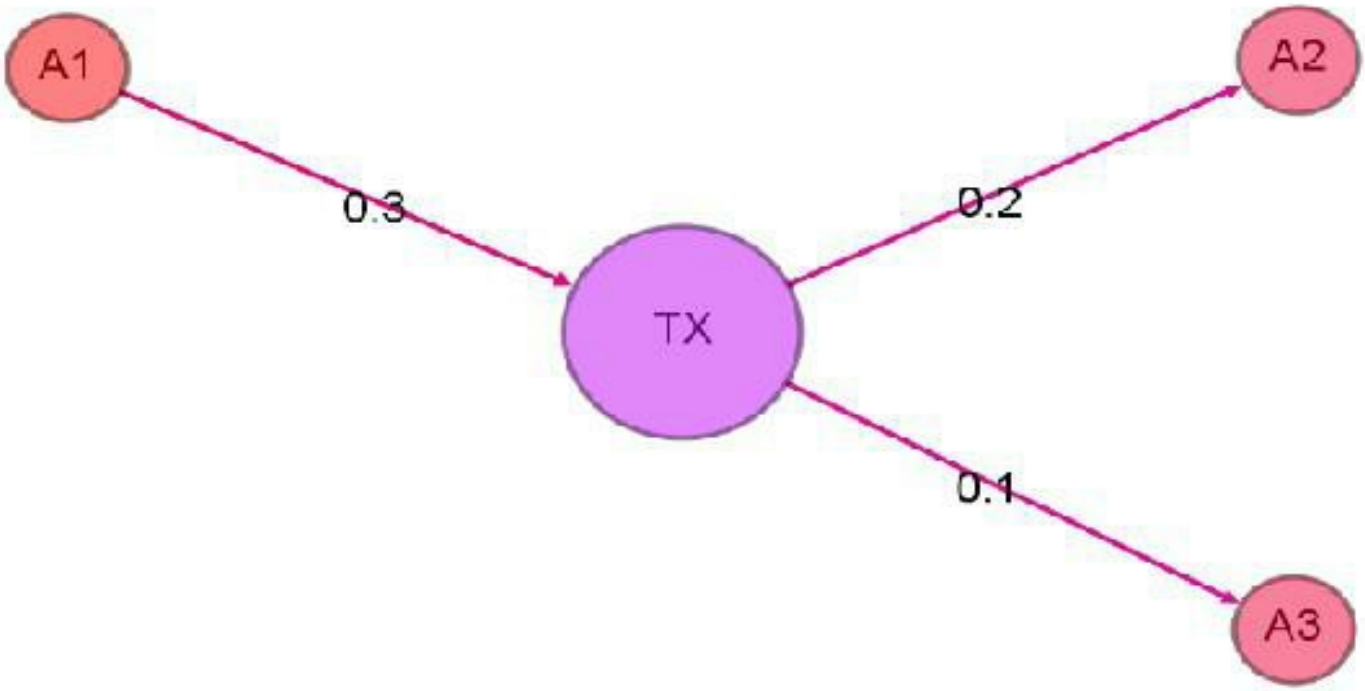
La secondo euristica nota come "*Shadow Heuristic*", letteralmente l'"*euristica ombra*", è invece sviluppata tenendo in considerazione come i *wallet* gestiscono le transazioni con il resto. La quasi totalità dei *wallet* cerca di tutelare la *privacy* del proprio utente generando una nuova coppia di chiavi per ogni output di resto che viene generato in una transazione. Se quindi vi è una transazione con un input e due output, si può supporre che uno sia l'indirizzo di destinazione e l'altro sia il resto.

Supponiamo che la destinazione sia la chiave pubblica di un commerciante, questo indirizzo si presume rimanere costante in ogni transazione; l'altro input variabile sarà quindi l'indirizzo generato dal wallet per la ricezione del resto della transazione.

Da qui si evince che le chiavi pubbliche di invio e del resto siano nello stesso *wallet*. Un indirizzo che può essere un potenziale resto è uno che viene usato per massimo due transazioni: uno in entrata e uno in uscita.

Si può rappresentare con tale scenario la logica di tale euristica: l'euristica "ombra" di un indirizzo A_n cerca le transazioni che ricevono da A_n ed evidenziano due o più nodi in output,

restituendo l'indirizzo di output che appare per la prima volta nella cronologia della Blockchain.



Di conseguenza, capita spesso che gli

indirizzi A1 e A2 appartengono al medesimo *wallet*.

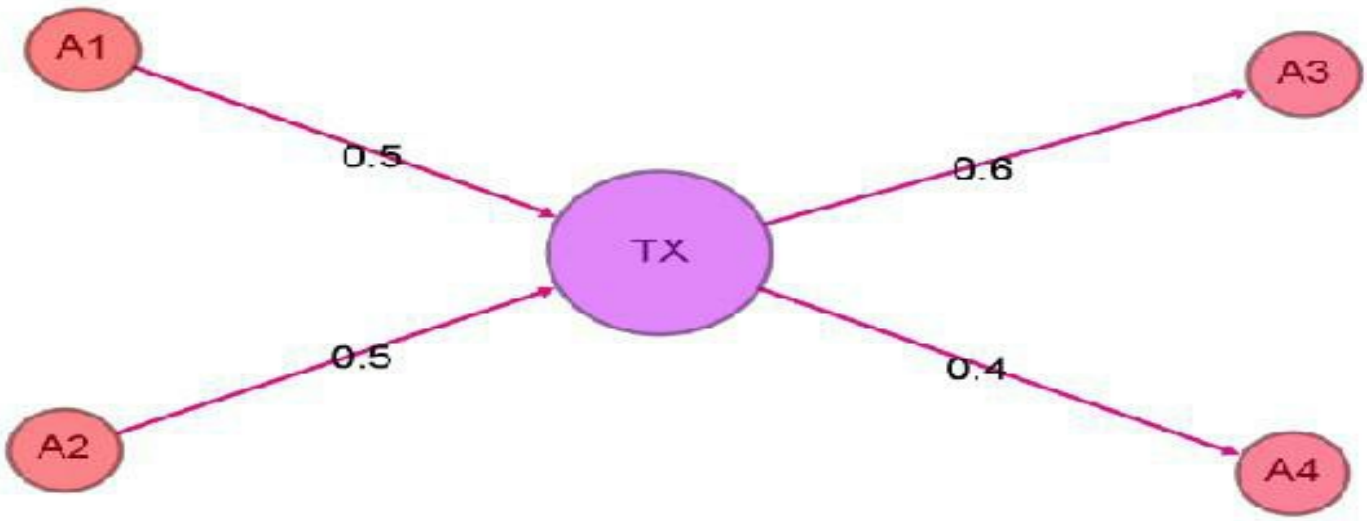
Il terzo tipo di euristica è detta "*Consumer Heuristic*" ed è applicabile nel caso di *wallet* gestiti da utenti privati (*consumer*), cosa che avviene nella maggior parte dei casi. Questo fa sì che le transazioni abbiano massimo due output, di cui uno è il resto; solitamente un privato non invia denaro a più entità diverse. Questa caratteristica diventa importante quando sorge il dubbio di quale, tra due transazioni, sia quella che porta i fondi verso il destinatario e quale il resto. Se, al secondo livello, una delle due transazioni dubbie riversa denaro su più output (magari prendendolo da più

input), significa che quella è la transazione di resto, l'altra quella da seguire per ricercare i dettagli del destinatario della moneta.

L'ultima euristica presentata è chiamata "*Optimal Change Heuristic*", che intuitivamente spiega come i *wallet* cerchino di ottimizzare la gestione del resto andando a cercare i migliori output da spendere. Ad esempio, se in una transazione si trovano due input da 0,5 bitcoin ciascuno e due output rispettivamente da 0,6 bitcoin e da 0,.4 bitcoin, allora si otterrà con certezza che quest'ultimo è il resto. Non avrebbe senso il contrario: infatti non sarebbe conveniente se gli 0,4 bitcoin fossero il trasferimento principale, in quanto per

sostenerlo sarebbe stato sufficiente un solo input da 0,5 bitcoin, con un avanzo di 0,1 bitcoin. La situazione opposta risulterebbe fortemente pleonastica e comporterebbe solamente lo svantaggio di incrementare le dimensioni della transazione e, di conseguenza, le commissioni a carico dell'utente.

Tale algoritmo fa in modo di restituire l'elenco degli indirizzi in output che hanno utilizzato l'euristica Multi-Input sopra descritta. Più in dettaglio esso utilizza due specifiche funzioni; la prima restituisce la somma dei valori degli indirizzi mentre la seconda fornisce il valore più basso che deriva dagli indirizzi.



Nel caso in esame, l'euristica restituirebbe l'unico indirizzo A4, che costituisce il resto della transazione in esame. Pertanto gli indirizzi A1, A2 e A4 nella maggior parte di casi appartengono al medesimo *wallet*.

3. 2. ANALISI VISUALE DEI DATI DI BLOCKCHAIN

a cura di Marco Stella

Sommario: 2.1 Analisi delle transazioni di Bitcoin a basso livello – 2.1.1. Possibili visualizzazioni dei flussi di criptovalute – 2.1.2. Utilizzo di tecniche di Social Network Analysis (SNA) per capire i flussi – 2.2 Modalità di visualizzazione dei flussi di criptovalute utili alle investigazioni – 2.2.1 Metriche e statistiche tipiche della rete di transazioni – 2.2.2. Metriche di rete

avanzate per comprendere le criptovalute – 2.3 Strumenti di analisi visuale real time della Blockchain – 2.3.1 Costruire una piattaforma di analisi visuale integrata – 2.3.2 Risultati ottenuti su casi reali – 2.4 Tagging e clustering: tecniche analitiche a contrasto del cybercrime – 2.5 Applicazione delle funzionalità del framework ad un caso reale – 2.5.1. Interesse della criminalità alle criptovalute – 2.5.2. Capacità di contrasto e analisi delle reti di transazioni.

2.1 ANALISI DELLE TRANSAZIONI DI BITCOIN A BASSO LIVELLO

La prima e più diffusa valuta virtuale, Bitcoin, è stata da sempre associata, in maniera spesso imprecisa, al concetto di anonimato e, pertanto, è stata spesso rappresentata come uno strumento che si può prestare a supportare traffici illeciti come, ad esempio, il riciclaggio e il finanziamento del terrorismo.

Senza entrare nel merito dell'utilizzo per fini più o meno leciti, è pacifico che in Bitcoin vi è il problema dell'associazione di indirizzi (che possono essere assimilati al concetto di pseudonimo) a soggetti reali. È come se a partire da un codice IBAN, non si fosse in grado di conoscere il nome del correntista poiché non vi è alcuna banca a cui poter chiedere. Inoltre, un utente

può autonomamente generare più di un indirizzo Bitcoin, anche per una singola transazione.

Per comprendere meglio tale aspetto, è possibile esperire un breve ma significativo approfondimento della struttura di una transazione a basso livello, analizzandone la sua struttura, ad esempio, esadecimale.

Le transazioni sono molto complesse da interpretare manualmente perché possono avere più ingressi e uscite, di contro il numero di campi che le compongono è abbastanza agevole da individuare nella struttura esadecimale.

Si parta con un esempio reale [40], mediante l'utilizzo di un servizio presente in blockchain.info che consente

di recuperare i dati di una specifica transazione in formato esadecimale, mediante il seguente *Uniform Resource Locator* (URL):

https://blockchain.info/rawtx/**<TXID>**?format=hex

in cui TXID (*Transaction ID*) è rappresentato dal codice di una transazione. Si consideri pertanto la transazione avente quale identificativo univoco:

61635d927796c87164fa919ac21367fd7b

che, inserita nel URL, restituisce il seguente risultato raffigurante la struttura

della transazione in formato esadecimale:

0200000000108ea335579f6ee3

Si parta da un'analisi speditiva all'interno dei servizi offerti dal sito blockchain.com, che evidenziano la struttura della transazione in esame costituita da un indirizzo in input e due in output.

Dati della transazione in esame in blockchain.info

In particolare, dalla struttura esadecimale della transazione, è possibile individuare i seguenti campi con le relative informazioni di interesse.

Versione software utilizzata nella transazione (*Little Endian*): nel caso di specie trattasi della Versione 2.

02000000108ea335579f6ee3a4e46319

Numero di input per una transazione (*Big Endian*): il risultato è un solo input.

0200000001**08ea335579f6ee3a4e463192**

Hash della precedente transazione (*Internal Byte Order*): è interessante notare che, sebbene tutti i visualizzatori blockchain mostrino i valori di input e output, i valori di input non esistono nel formato esadecimale della transazione reale, ma solo il collegamento alla transazione precedente in cui l'importo esisterà negli output.

0200000001**08ea335579f6ee3a4e4631**

Numero di indice di output (*Little Endian*): il valore successivo è il numero di indice di output della transazione precedente. In questo

esempio, è 6, il che significa che era il sesto risultato della transazione precedente.

020000000108ea335579f6ee3a4e463192

Valori di uscita (*Internal Byte Order*): il prossimo valore che è possibile osservare riguarda il valore totale del primo output della transazione. Questo valore viene decodificato come valore in satoshi. Nella transazione in esame, il valore è 16992362 satoshi. Il valore è di 16 cifre esadecimali o 8 byte ed è possibile iniziare dallo zero finale e tornare indietro, in questo esempio da 00 a 6a. Quindi, 6a48030100000000 in Byte Order si traduce in 16992362

satoshi. Gli zeri non saranno mai usati poiché il valore corrispondente sarebbe maggiore di tutti i bitcoin che possono mai essere estratti.

020000000108ea335579f6ee3

Vi è un secondo valore di uscita in questa transazione, come si evince dai valori indicati a seguire della sequenza UTXO riportante feffffff, che indicata 02. Ancora una volta, se si osserva quanto indicato nei dati grezzi, si può trovare un altro valore di 16 cifre esadecimali che include una stringa di zeri. La stringa è 548ff90000000000. Se si converte questo valore in decimale, è possibile ottenere un valore totale della

seconda uscita di 16355156 satoshi.

020000000108ea335579f6ee3

LockTime (*Internal Byte Order*): questo valore definisce l'istante in cui deve essere attivata la transazione. Può essere un valore temporale UNIX o un'altezza del blocco. In questo caso, l'altezza del blocco è 489344. Il valore è codificato come segue:

020000000108ea335579f6ee3

Pertanto la struttura di una transazione consente di ricostruire con estrema precisione i vari passaggi di valore.
Si approfondiscano ora le ulteriori parti

della transazione. In particolare si vuole indagare se la struttura della transazione ricomprende in maniera chiara la struttura degli indirizzi coinvolti in essa.

Riprendendo la struttura indicata nella figura che rappresenta il modello di transazione in modalità visuale, è possibile recuperare ulteriori informazioni sugli indirizzi coinvolti nella transazione in esame, ed in particolare come riportate nella seguente tabella.

Tipo nodo	**Indirizzo**
In	**1PDz8qLjADAmZqPAkARLQw**

Out 1	**19T36T98L4gao3RxrY5g3cX**
Out 2	**1N1Q9oYiJt946KhTnQE6dkez**

Di seguito si riportano le stringhe recuperabili dalla struttura *raw* della transazione in approfondimento che, come detto, evidenzia soltanto due output.

0200000001**08ea335579f6ee3a4e46319**

Mentre per quanto attiene l'indirizzo in input, occorre fare riferimento alla transazione precedente che riporta, alla

posizione di indice 6 dei suoi output, l'indirizzo Bitcoin che costituisce l'input della transazione in esame.

Dati della transazione precedente a quella in esame in blockchain.info

Pertanto è del tutto evidente come sia possibile ricostruire in ogni caso la struttura delle transazioni e degli indirizzi Bitcoin in esse coinvolti. Di contro, non è mai possibile recuperare dalla Blockchain e dall'approfondimento di ciascuna transazione dati ed informazioni afferenti alla titolarità degli indirizzi Bitcoin in essa eventualmente coinvolti sia in input che in output.

2.1.1 Possibili visualizzazioni dei flussi di criptovalute

Le criptovalute e le transazioni stanno diventando sempre più di utilizzo comune. Sistemi come quello della

criptovaluta digitale Bitcoin, funzionano su transazioni monetarie puramente digitali che sono verificate tecnicamente per correttezza e validità, ma non vengono né regolamentate né tantomeno controllate al fine di scongiurare utilizzi fraudolenti. In generale, quando si ha a che fare con reti molto articolate ed estese, come potrebbe essere quella delle transazioni Bitcoin, migliaia di aggiornamenti della topologia della rete stessa e delle transazioni avvengono in pochissimi secondi, e diventa fondamentale poter riuscire ad analizzare un volume elevato di transazioni in modo da rilevare comportamenti e attività di utilizzo del circuito *real time*.

Dato che le transazioni Bitcoin evidenziano un elevato grado di anonimato, gli algoritmi di rilevamento che devono essere implementati per poter analizzare la rete nella sua vastità richiedono che gran parte dei sistemi funzionino su procedure *batch*, informazioni *offline* o grafi di dimensioni minori rispetto all'ampiezza della rete Bitcoin, con evidenti limiti di *discovery* di contesti caratterizzati da una così elevata dinamicità. L'idea che ha portato fin qui sta nella possibilità di implementazione di un sistema di analisi visuale modulare, che sia capace di condurre un approfondimento delle transazioni Bitcoin in tempo reale con la possibilità di creare nuova conoscenza.

Si ritiene possibile un tale approccio al tema del monitoraggio e della rappresentazione visuale della rete di transazioni Bitcoin grazie anche allo sfruttamento di alcune *Application Programming Interface* (in breve API) rese disponibili dal portale della Blockchain (https://www.blockchain.com/it/api) per sviluppatori in ambito Bitcoin.

Tali servizi possono agevolare la definizione di un approccio orientato all'analisi di numerosi flussi di dati e non direttamente intellegibili, come potrebbero essere quelli derivanti da un approfondimento specifico sulle transazioni e sugli indirizzi Bitcoin.

2.1.2 Utilizzo di tecniche di *social network analysis* (SNA) per capire i flussi

In questa fase della trattazione è possibile fare riferimento alle tecniche d i *social network analysis* [35] per studiare in dettaglio la struttura delle transazioni ed il coinvolgimento di tutti quegli indirizzi che cedono e ricevono valori in valuta virtuale.

A tal proposito, è utile considerare lo schema relazionale e visuale che vede collegare gli indirizzi in input, la transazione e gli indirizzi in output mediante uno schema riconducibile ad un grafo orientato; il verso dei collegamenti consente di descrivere in

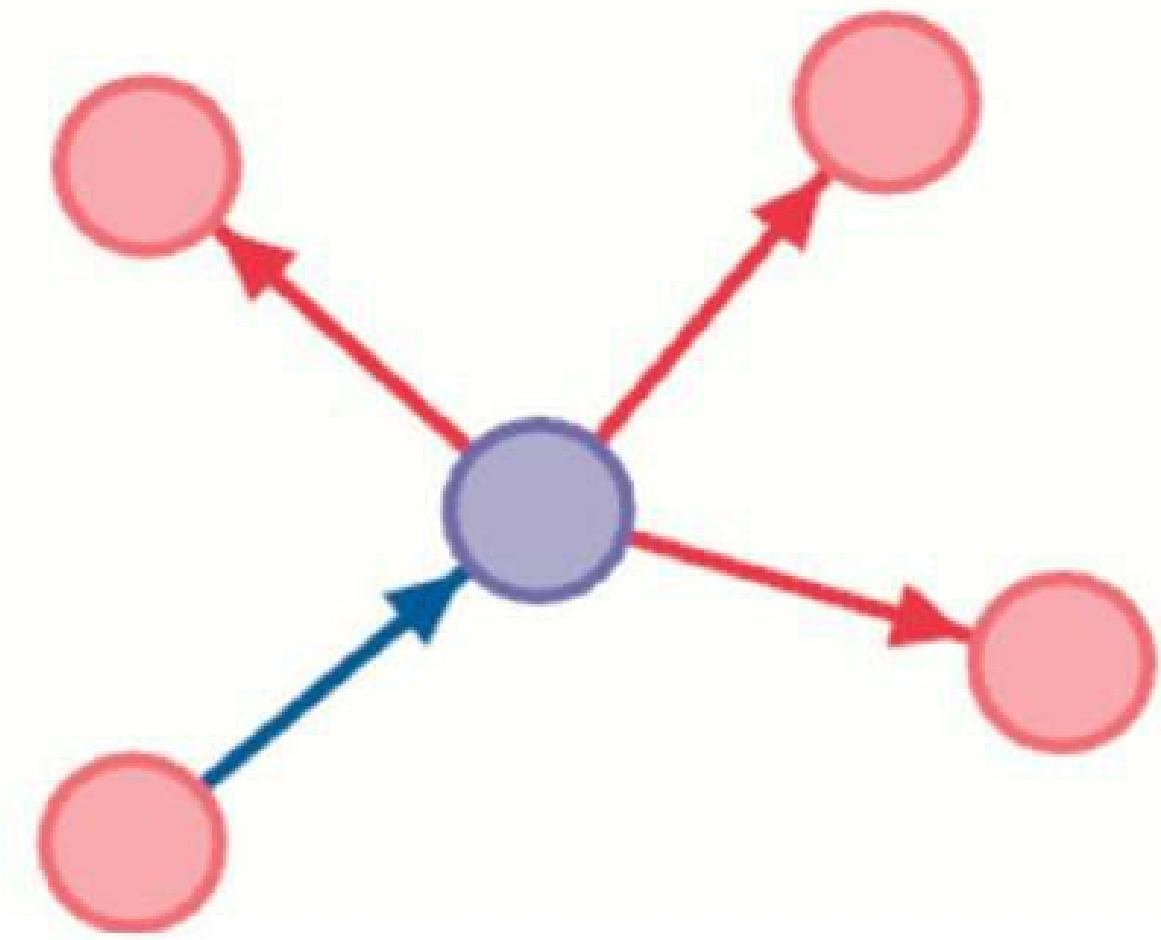
maniera efficace e visuale il flusso di valuta virtuale che fluisce mediante la transazione in esame. È inoltre possibile ipotizzare di utilizzare lo spessore delle linee di connessione per rappresentare differenti importi di valuta che sottostanno alla transazione medesima.

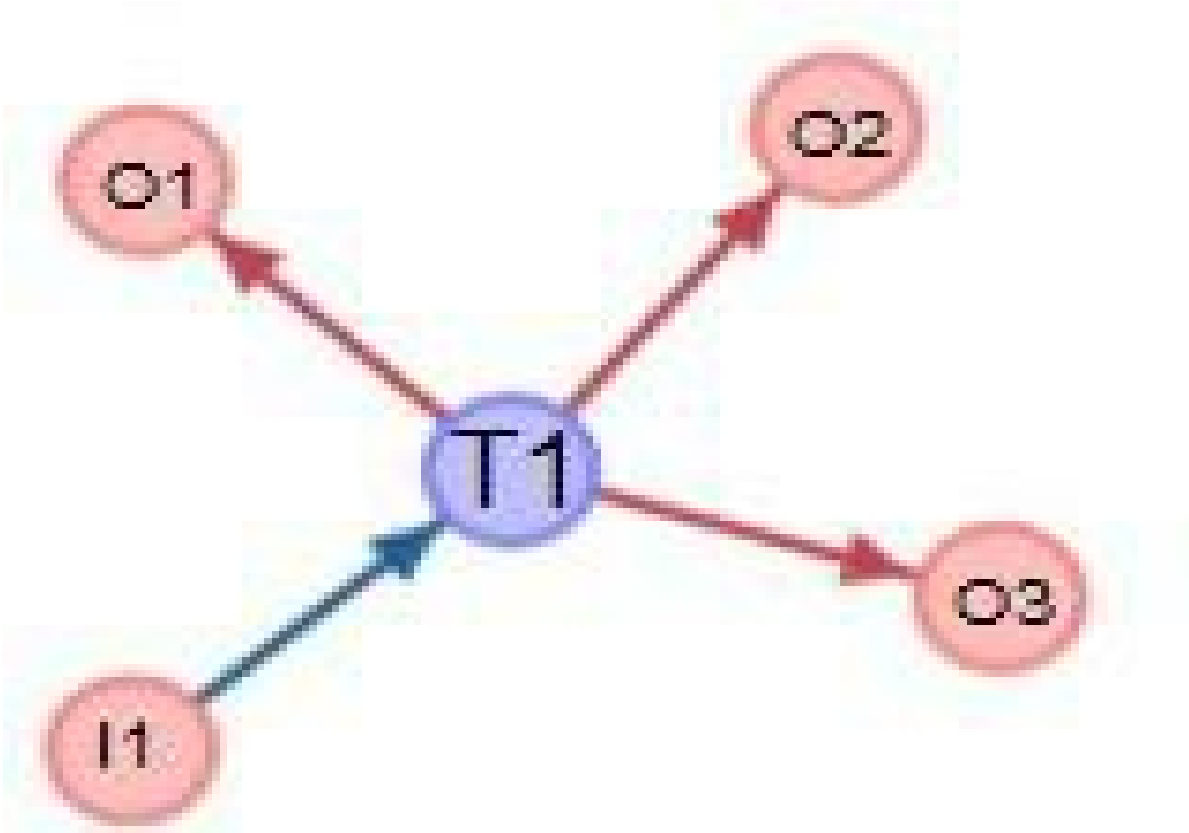
Per poter utilizzare alcune tecniche di SNA nell'analisi dei flussi e delle strutture relazionali delle transazioni, occorre definire un modello visuale costituito da nodi e connessioni. In particolare è possibile e pressoché intuitivo, data la struttura della blockchain, dei blocchi e soprattutto di ogni singola transazione di Bitcoin, poter individuare nodi di tipo *transazione* e nodi di tipo *indirizzo*

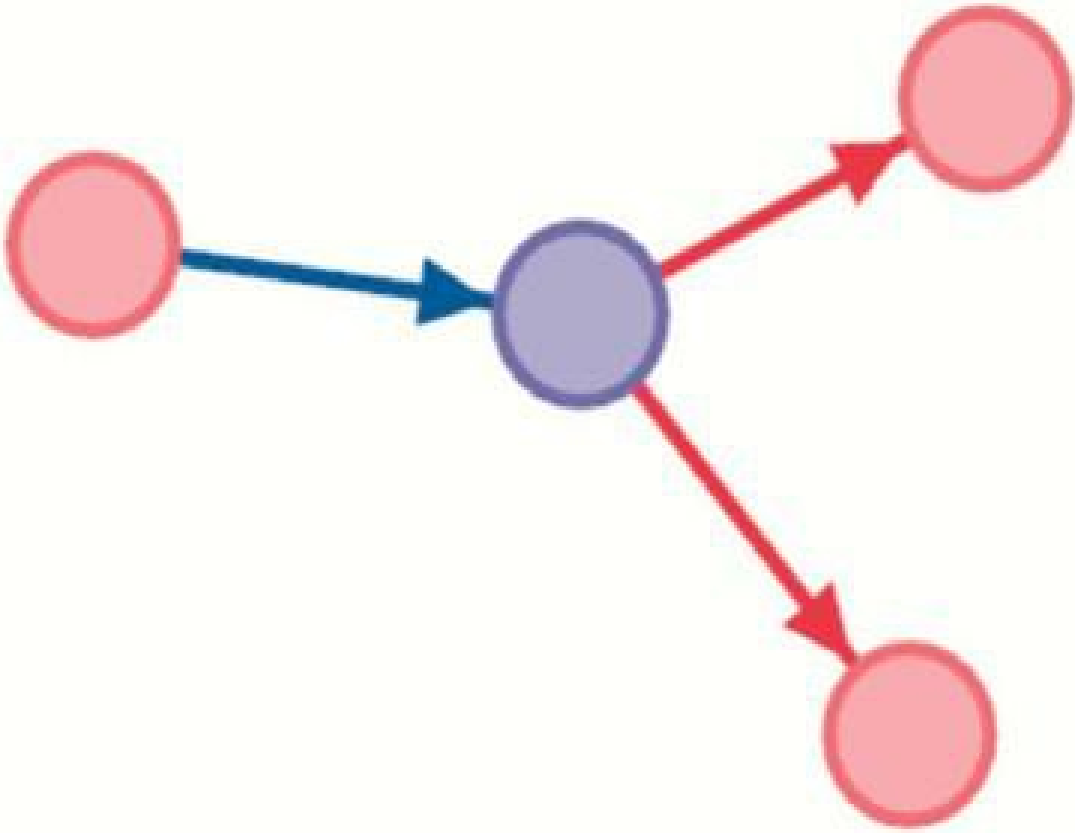
Bitcoin. Le connessioni tra i nodi, orientate con uno specifico verso, rappresentano il flusso di criptovaluta che riguarda una transazione; esso ha origine dai nodi di tipo *indirizzo Bitcoin* che evidenziano connessioni in uscita verso un nodo di tipo *transazione* e termina nei nodi *indirizzi* che evidenziano un verso di connessione in entrata.

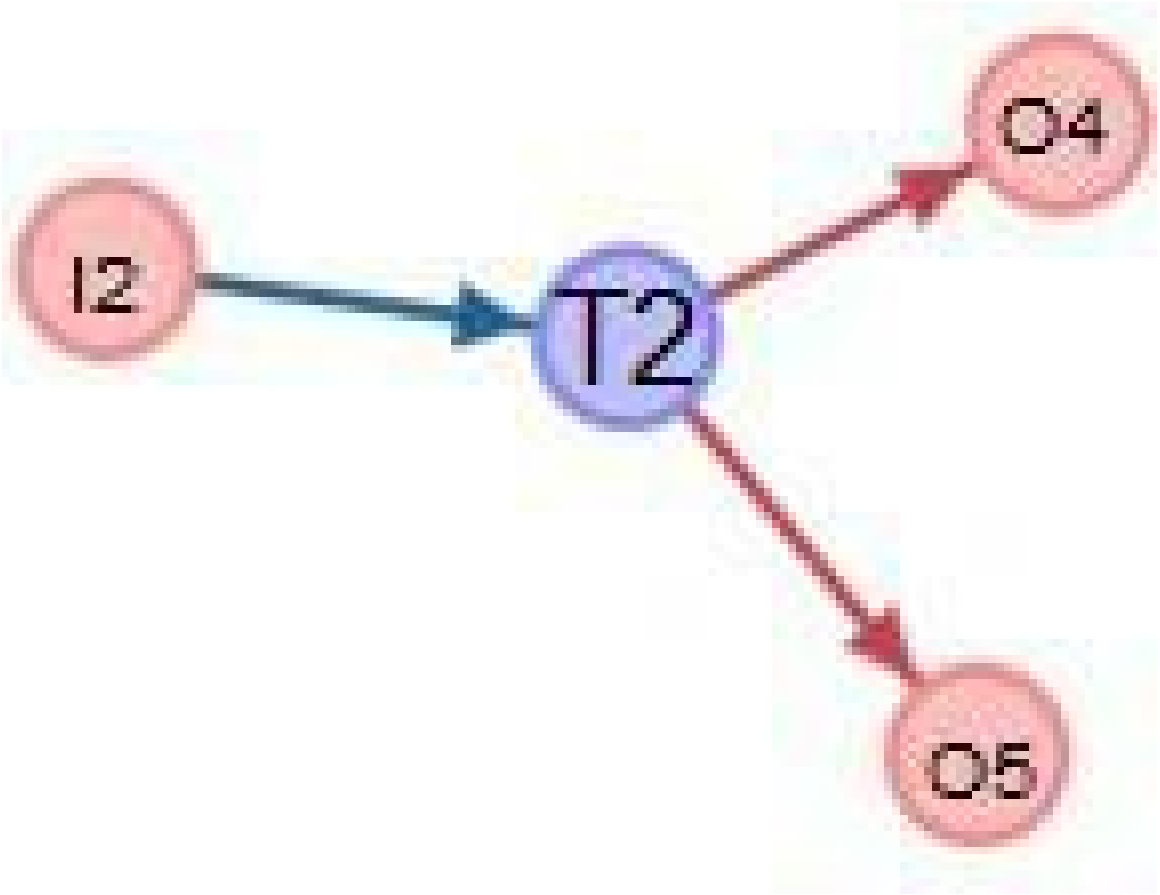
Di seguito sono riportati semplici esempi della schematizzazione del predetto modello che consentono di individuare con estrema facilità, mediante specifiche cromie, i nodi *indirizzi* (di colore rosso) differenziandoli da quelli di tipo *transazione* (di colore viola); inoltre il

verso delle frecce che collegano i predetti nodi conferisce estrema intuitività nella interpretazione dei flussi di criptovalute sottostanti all'analisi.




O1
O2
T1
O3
I1





Schematizzazione di transazioni in criptovaluta

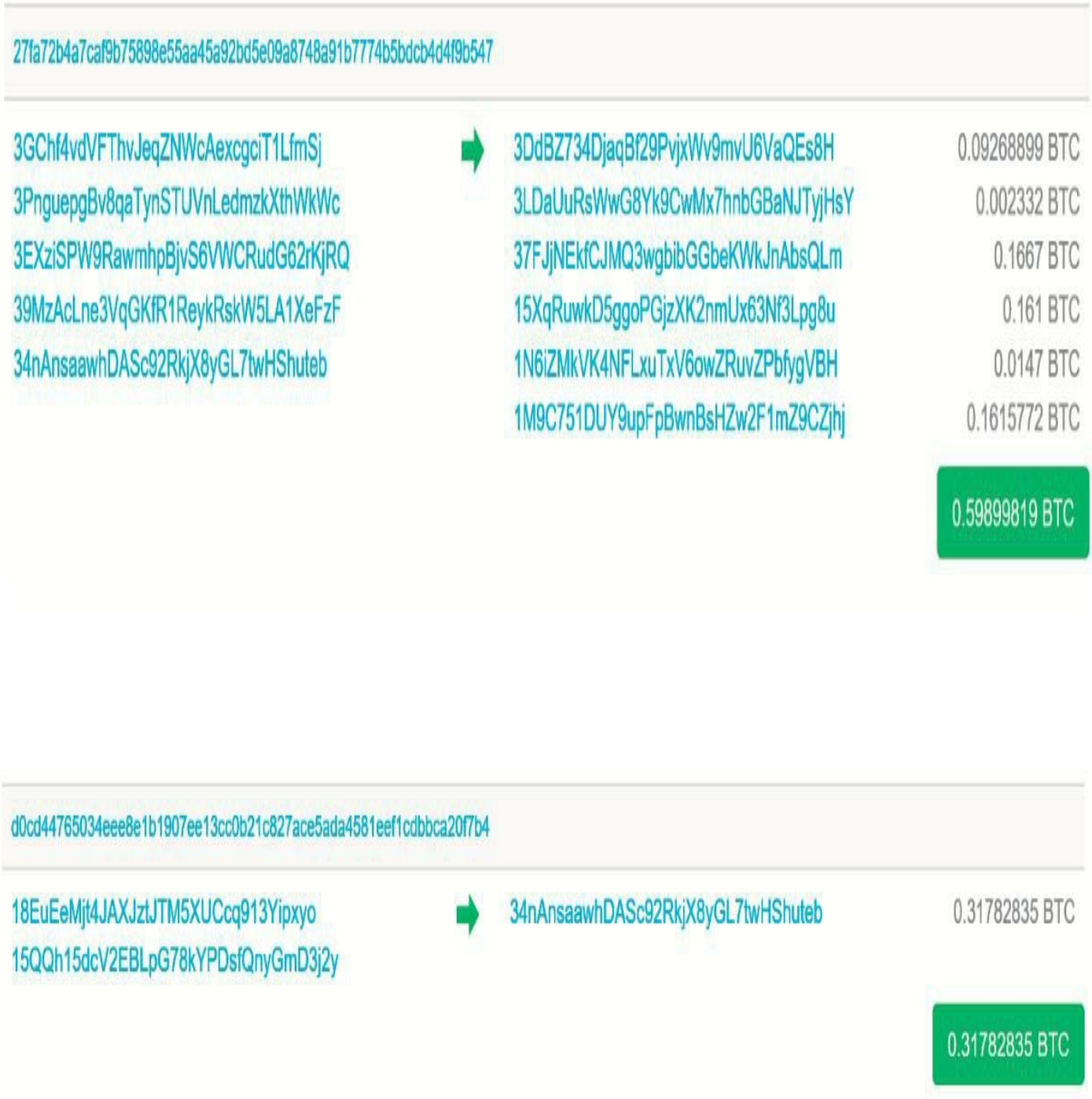
In queste due configurazioni, così descritte, è agevole comprendere che il flusso di criptovaluta defluisce, in un caso da uno (I1) a tre specifici indirizzi (O1, O2, O3) e nell'altro da uno (I2) a

due indirizzi (O4, O5); in entrambi i casi esiste un nodo transazione, rispettivamente T1 e T2, che riunisce gli indirizzi, secondo la logica dell'algoritmo e della struttura dati della stessa come in precedenza approfondita a basso livello.

A questo punto, il modello si presta in maniera efficace a descrivere configurazioni di flussi di criptovaluta ben più complessi e, più in generale, capaci di coinvolgere numerosi indirizzi in diverse transazioni.

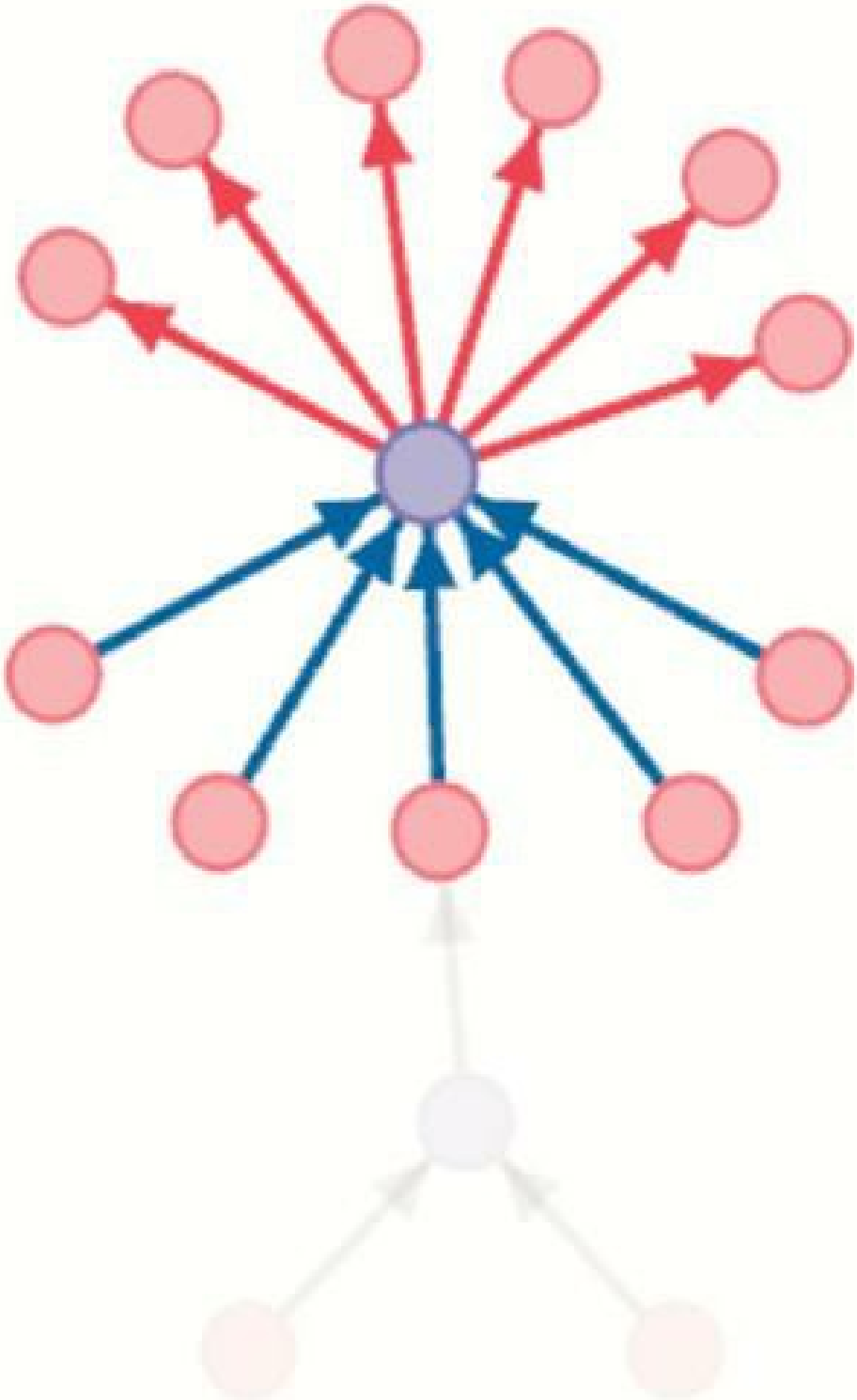
Si parta da un esempio reale, procedendo con una ricerca di due transazioni sul registro Blockchain pubblico che risultano essere collegate tra loro mediante uno o più indirizzi

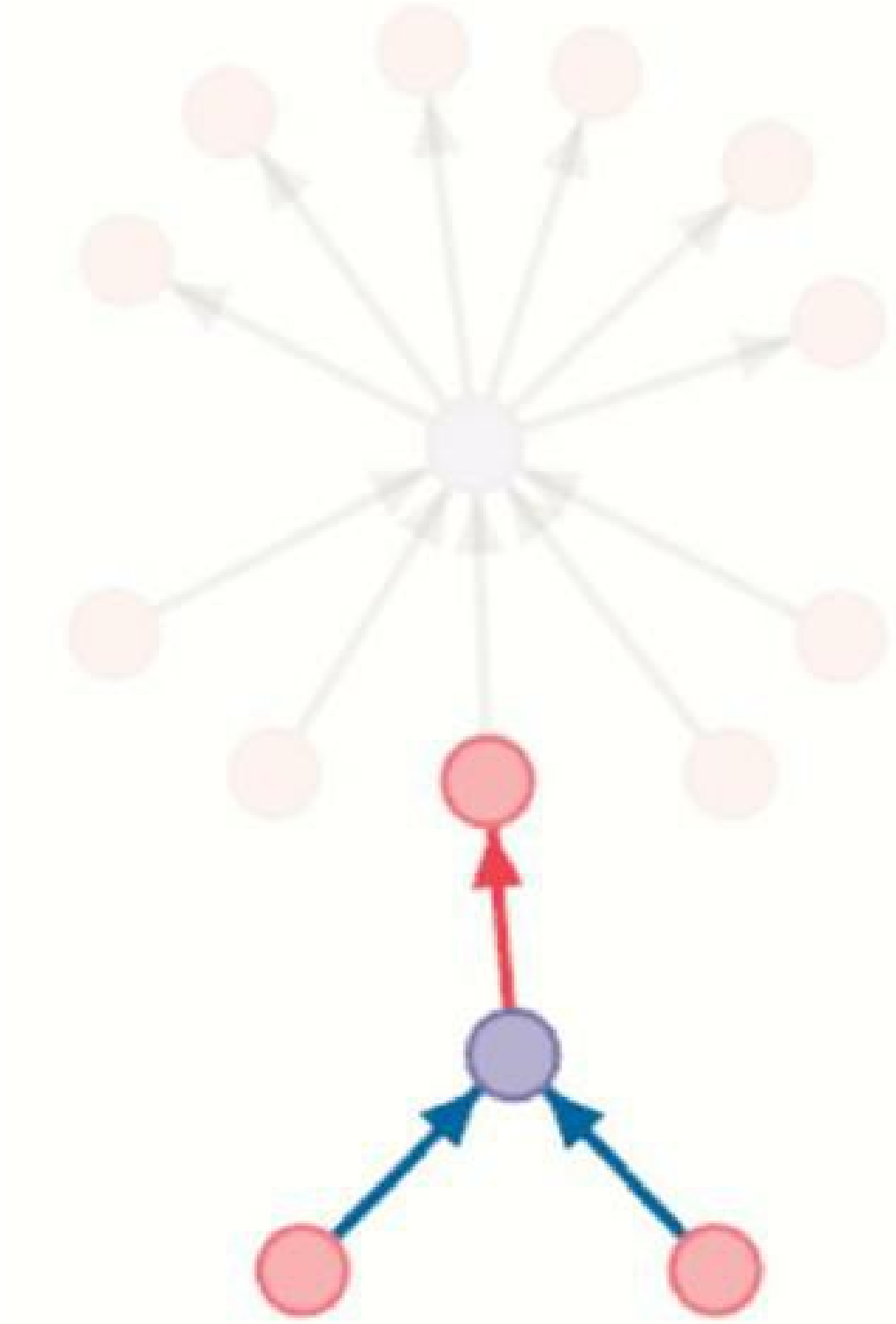
Bitcoin. Di seguito ciò che viene visualizzato sul sito di riferimento *www.blockchain.com*:



Due transazioni dalla Blockchain di Bitcoin

Se si vuole esplorare la rete di transazioni, navigando mediante gli *hyperlink* disponibili da una transazione all'altra, non risulta molto agevole comprendere la struttura del flusso nel suo complesso; pertanto, schematizzando tali tabelle secondo il modello visuale testé proposto, è possibile recuperare una struttura delle singole transazioni come segue.

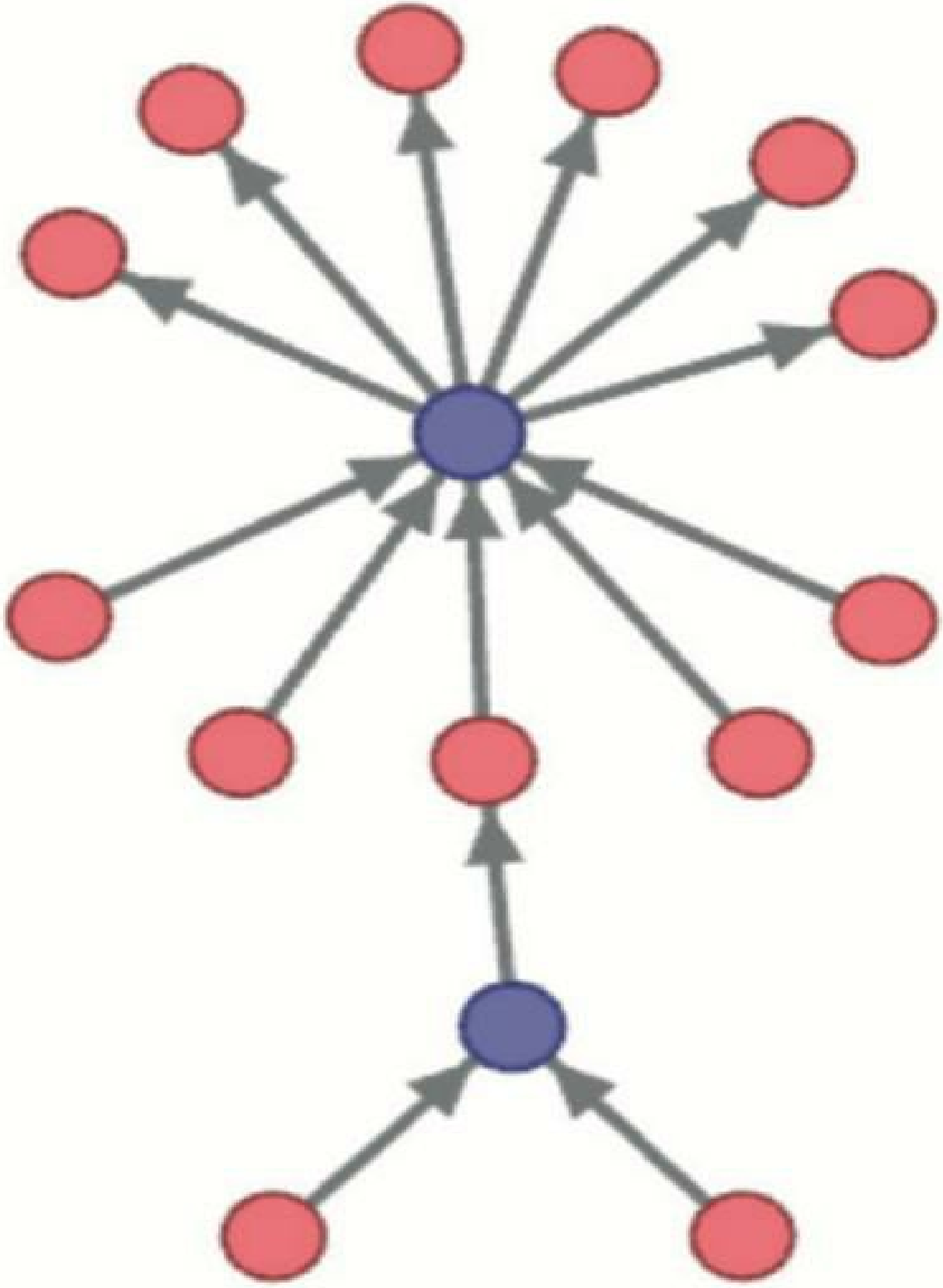




Struttura di singole transazioni in

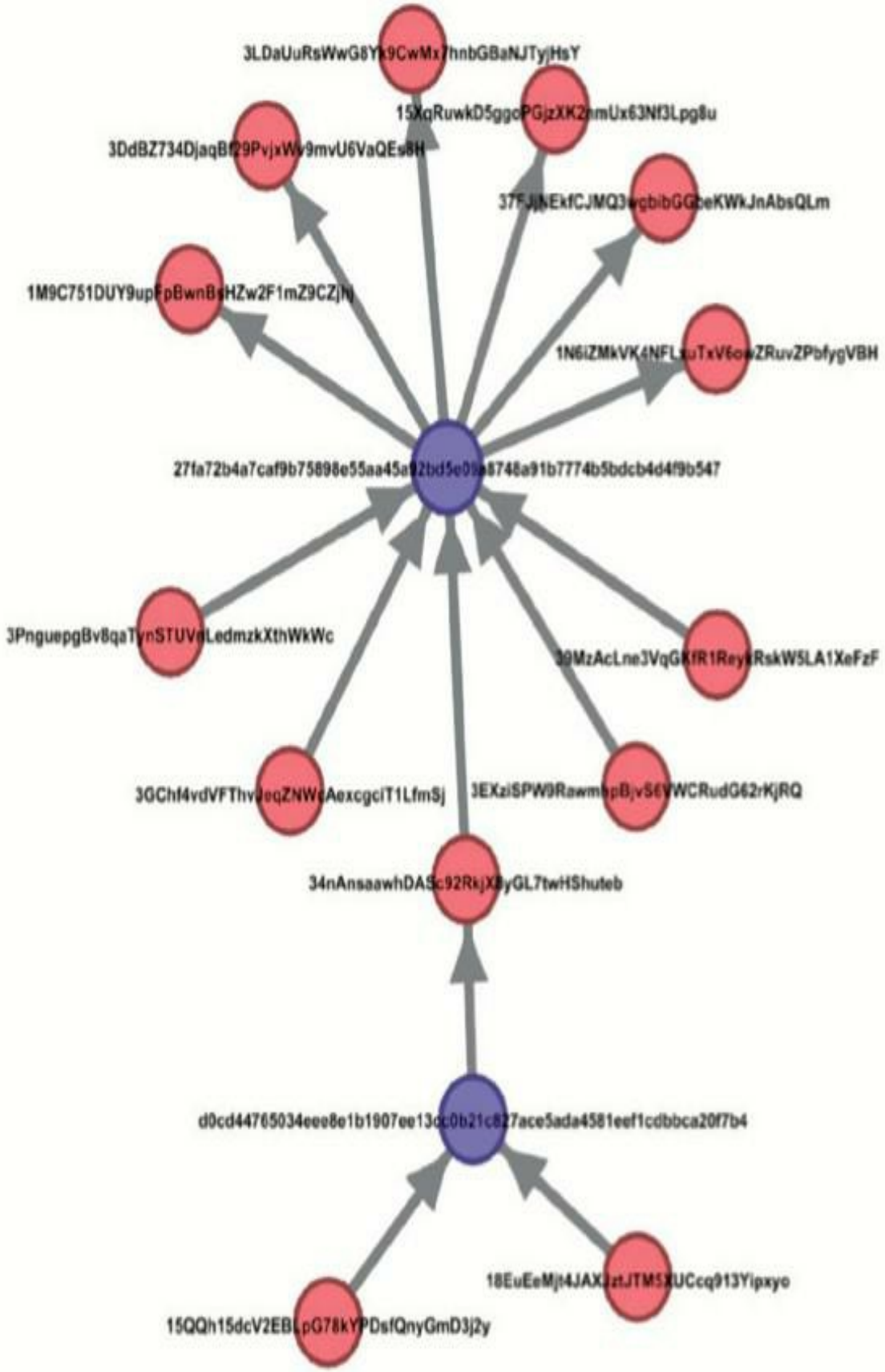
criptovaluta

Nella prima transazione sono presenti cinque indirizzi in input e sei in output; nella seconda, due indirizzi in input ed uno in output. Ciò rende estremamente efficace la ricostruzione del flusso di criptovaluta risultante con la precisa individuazione *ictu oculi* di uno specifico nodo di tipo *indirizzo* che, nella prima transazione è un input e nella seconda rappresenta un output.



Modello di transazioni applicato

I software di analisi visuale – come nel caso di Gephi [41], che è stato efficacemente utilizzato in questa trattazione – consentono generalmente di mostrare specifiche *l a b e l* per una precisa individuazione dei nodi, come di seguito riportato.


3LDaUuRsWwG8Yk9CwMx7hnbGBaNJTyjHsY
15XqRuwkD5ggcPGjzXK2nmUx63Nf3Lpg8u
3DdBZ734DjaqBf29PvjxWv9mvU6VaQEs8H
37FJjNEkfCJMQ3eqbibGGbeKWkJnAbsQLm
1M9C751DUY9upFpBwnBsHZw2F1mZ9CZjNj
1N6iZMkVK4NFLxuTxV6ewZRuvZPbfygVBH
27fa72b4a7caf9b75898e55aa45a92bd5e0ba8748a91b7774b5bdcb4d4f9b547
3PnguepgBv8qaTynSTUVgLedmzkXthWkWc
39MzAcLne3VqGKfR1ReykRskW5LA1XeFzF
3GChf4vdVFThvJeqZNWcAexcgciT1LfmSj
3EXziSPW9RawmspBjvS6YWCRudG62rKjRQ
34nAnsaawhDASc92RkjXByGL7twHShuteb
d0cd44765034eee8e1b1907ee13dc0b21c827ace5ada4581eef1cdbbca20f7b4
18EuEeMjt4JAXJztJTM5XUCcq913Yipxyo
15QQh15dcV2EBLpG78kYPDsfQnyGmD3j2y

Modello di transazioni con etichette

I predetti software consentono inoltre di rappresentare, anche in modalità *data streaming*, le transazioni e tutti gli indirizzi che in esse sono coinvolti sia come loro *input* che come *output*. Pertanto i reticoli relazioni che possono essere rappresentati e visualizzati, oltre che nelle semplici transazioni, potrebbero riguardare contesti estremamente complicati, soprattutto in presenza di servizi di *mixing* che, più in dettaglio, hanno la capacità di aumentare il livello di anonimizzazione delle transazioni consentendo di scambiare criptovaluta con altri nodi della rete

senza per questo essere associati ad un proprietario originale.

In particolare i servizi di *mixing* sono utilizzati per "mescolare" diversi fondi con quelli altrui, con il preciso (e presunto) scopo di confondere il recupero di informazioni relative al percorso che porta alla reale fonte originaria dei fondi. Al di là delle implicazioni giuridiche di attività che potrebbero in qualche misura ostacolare la riconducibilità ovvero la liceità di una o più fonti di finanziamento, l'utilizzo di criptovalute su reti anonime per di più con servizi di *mixing* rende molto complicato e non sempre certo il recupero di informazioni precise circa il proprietario originario ed il destinatario

di uno specifico ammontare di valore in criptovaluta.

In questo senso, basta osservare le transazioni in tempo reale mediante specifici *script*, in linguaggio Python [42], unitamente ad una piattaforma di analisi visuale per recuperare in pochissimi minuti strutture relazionali, modellate come sopra in termini di rappresentazione delle transazioni ed indirizzi di criptovaluta in esse coinvolti, per capire quanto complesso sia il meccanismo di recupero di informazioni utili da essi, anche soltanto per comprendere se esiste o esistono nodi di tipo *indirizzo* su cui confluisce gran parte del flusso della criptovaluta coinvolta nelle transazioni oggetto di

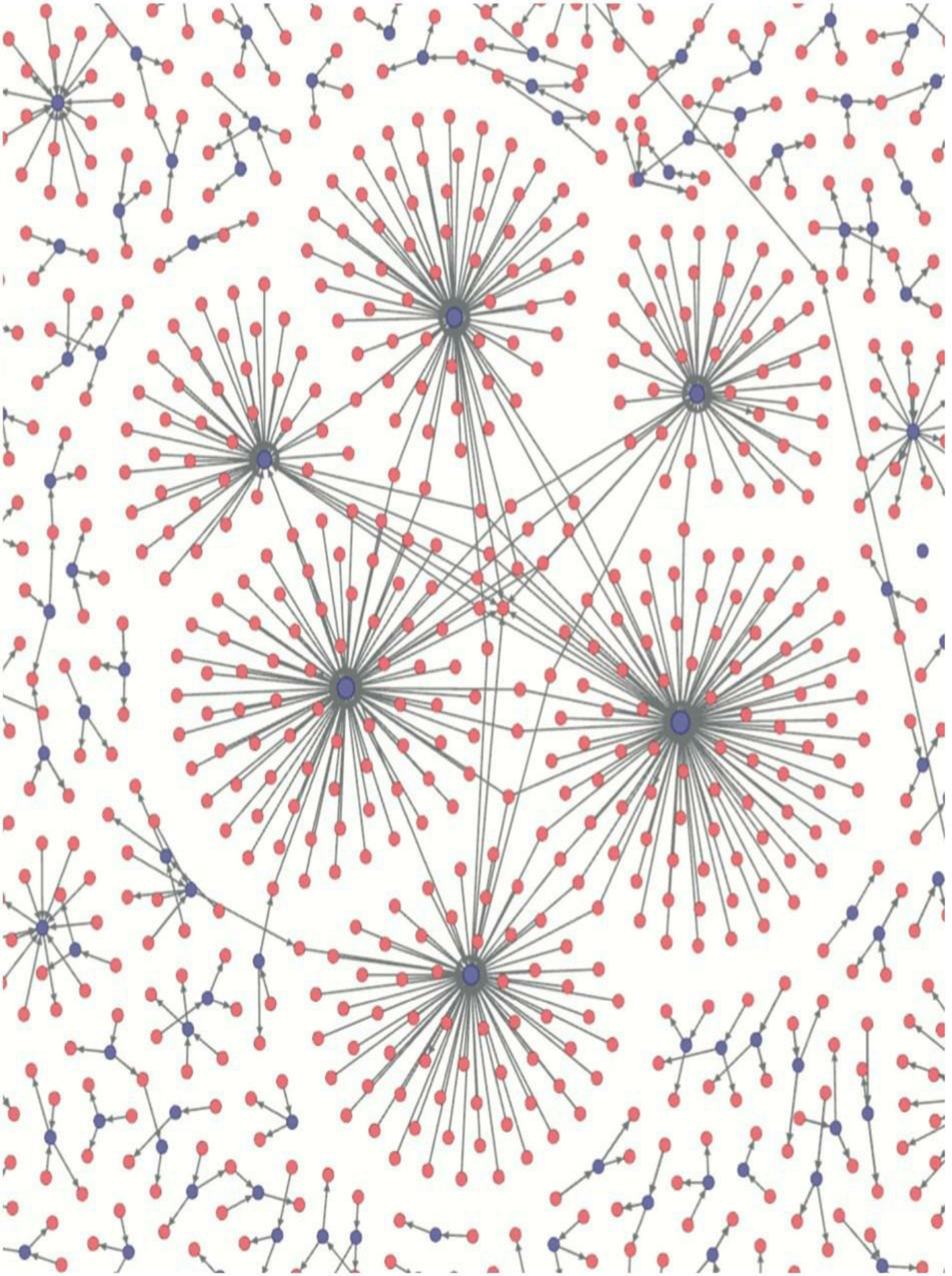
analisi.

2.2 MODALITÀ DI VISUALIZZAZIONE DEI FLUSSI DI CRIPTOVALUTE UTILI ALLE INVESTIGAZIONI

Dopo aver affrontato, nel precedente paragrafo, la costruzione del modello visuale da poter applicare ad un dominio complesso come lo è quello delle criptovalute, si può ora approfondire un possibile metodo di applicazione delle tecniche di SNA al dominio in esame.

Si consideri pertanto il contesto di seguito riportato in cui molteplici sono

gli indirizzi coinvolti in transazioni di criptovaluta.

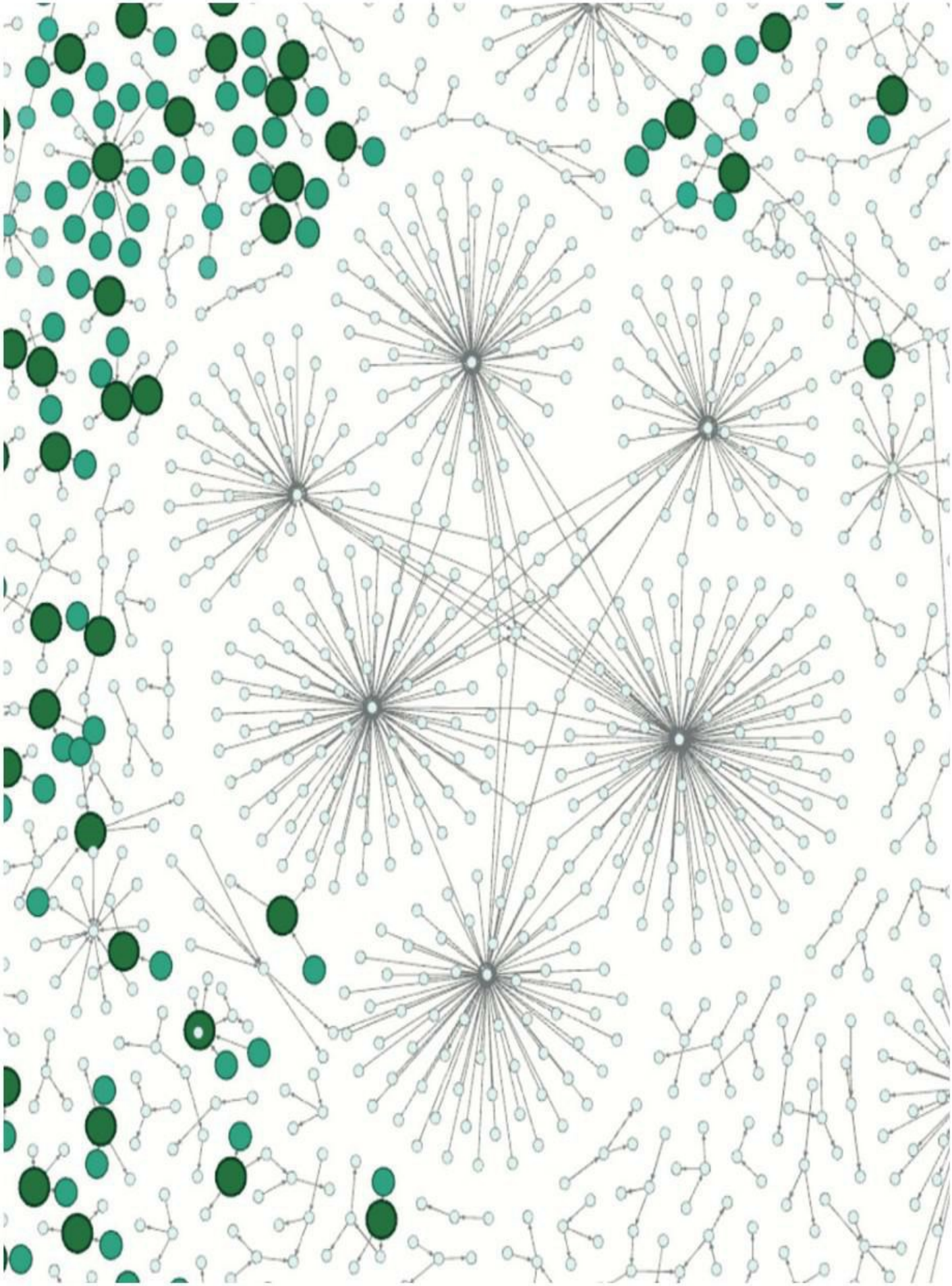


Rete di transazioni e indirizzi complessa

Da una prima sommaria analisi visuale è del tutto chiara ed evidente la difficoltà di comprendere quali siano i nodi di maggiore interesse per comprendere il flusso, in particolar modo quali siano gli indirizzi maggiormente interessanti.

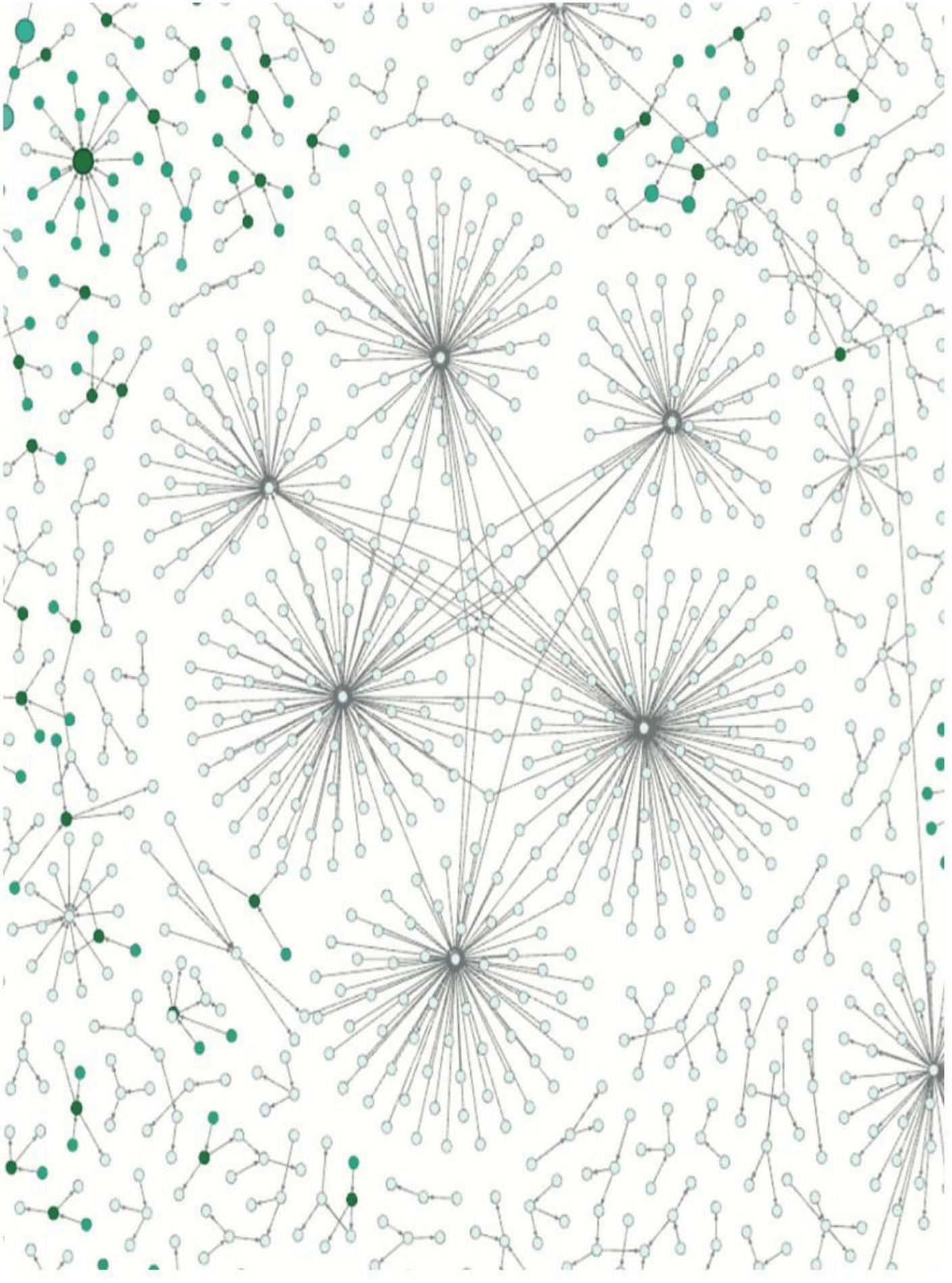
A questo punto se si è interessati a verificare quali nodi sono di maggiore interesse, è sorprendente come strutture particolarmente complesse, mediante l'applicazione di metriche relative ai nodi tipo quella della *closeness* [43] o della *betweenness* [44], facciano emergere la tipica struttura

decentralizzata e distribuita costruita sulla rete delle transazioni e degli indirizzi di criptovaluta come desumibile da un'analisi della blockchain. Di seguito è possibile osservare la porzione di rete sopra recuperata con un'applicazione del filtro della *closeness*, in cui gran parte dei nodi sfuggono a tale filtro, essendo tutti parimenti del medesimo colore e grandezza.



Rete complessa di transazioni e indirizzi con nodi a maggiore valore di closeness

Vediamo ancora il medesimo contesto reticolare dopo aver applicato un filtro relativo a far emergere i nodi con più elevata *betweenness*.



Rete complessa di transazioni e indirizzi con nodi a maggiore valore di betweenness

Anche in quest'ultimo caso, non emergono particolari posizioni significative con riguardo alla struttura centrale distribuita.

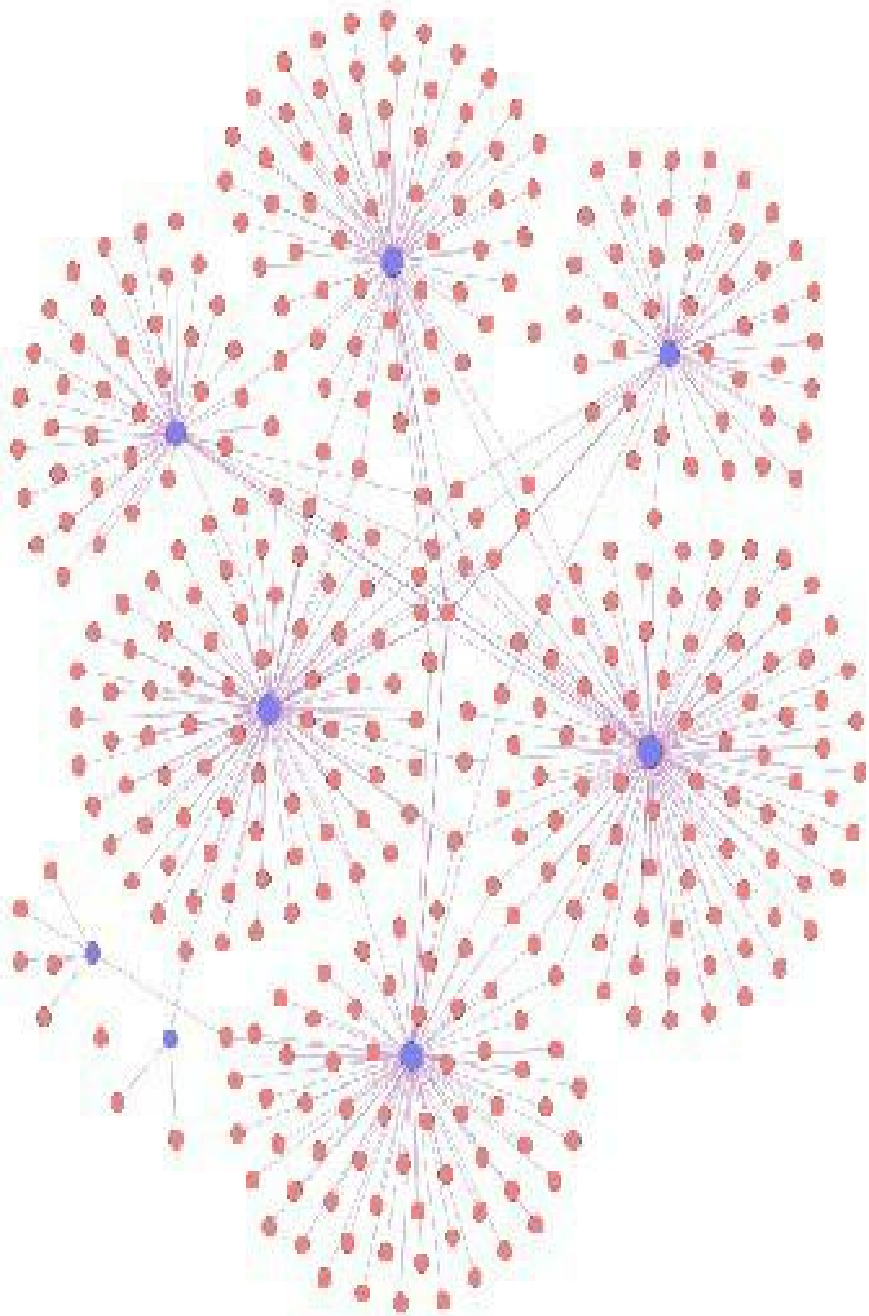
2.2.1 Metriche statistiche tipiche della rete di transazioni

A questo punto vale la pena soffermarsi sui possibili approcci di analisi di una siffatta struttura decentralizzata che, vale la pena ricordare, è stata recuperata mediante l'osservazione di qualche

minuto del flusso di transazioni e degli indirizzi Bitcoin in esse coinvolti presente nella struttura della blockchain.

Attraverso i software di analisi visuale, agendo opportunamente su alcune semplici funzionalità di selezione dei nodi rappresentati, è possibile isolare la struttura relazionale da sottoporre ad un'analisi più completa e approfondita.

Nel caso di specie si procede con l'isolamento della struttura di interesse come segue.



Componente maggiormente connessa isolata

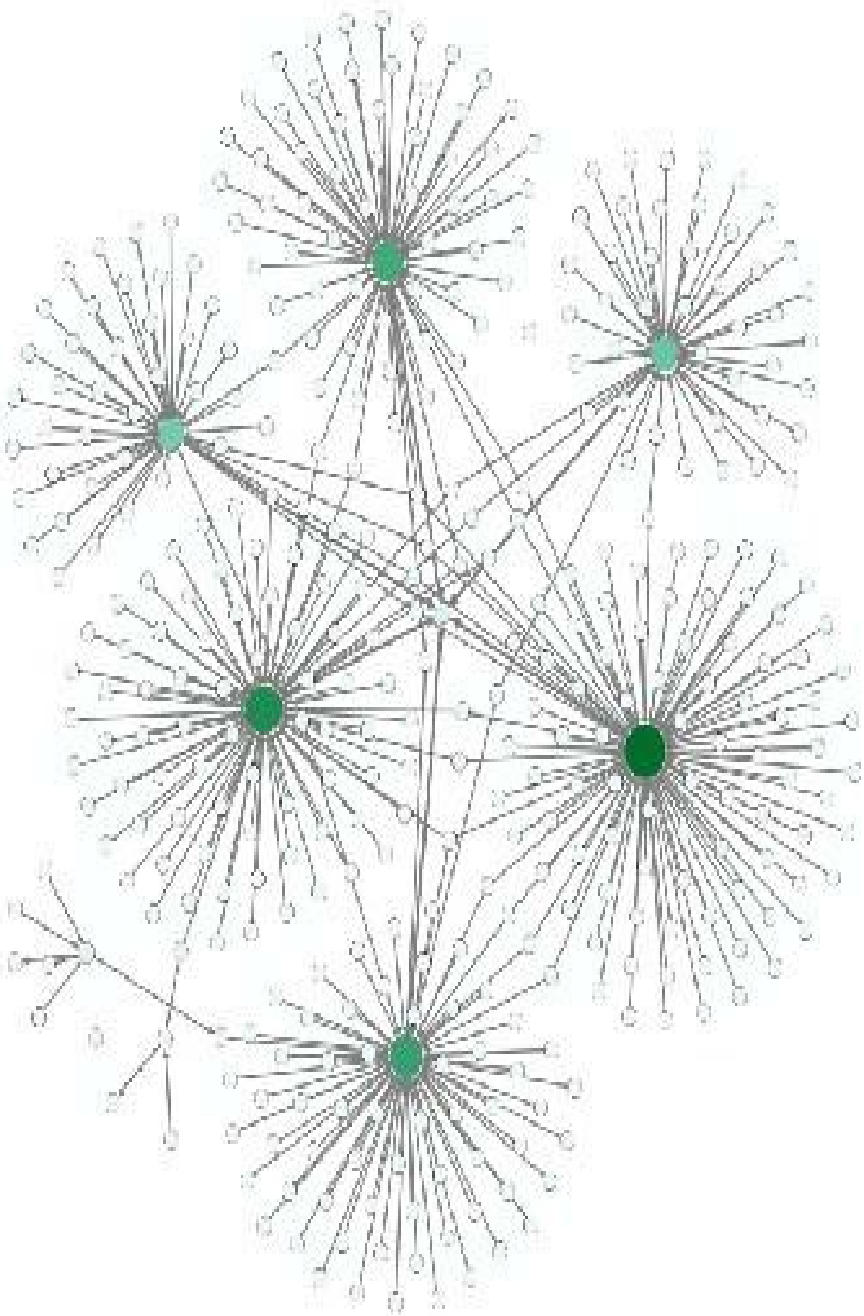
Ricordiamo che gli *indirizzi* di criptovaluta Bitcoin sono rappresentati con colore rosso e le *transazioni* con quelli di colore viola. Nello specifico la rete in esame è costituita da 8 transazioni e da 394 indirizzi in esse coinvolti. I collegamenti presenti sono 427.

Se consideriamo il grafo risultante come non orientato, la sua densità è pari 0,005 mentre per il medesimo grafo di tipo orientato scende a 0,003. Ciò fa capire che siamo di fronte ad un grafo casuale ove non dovrebbero emergere nodi

particolari rispetto ad altri e tutti hanno la medesima probabilità di essere collegati agli altri.

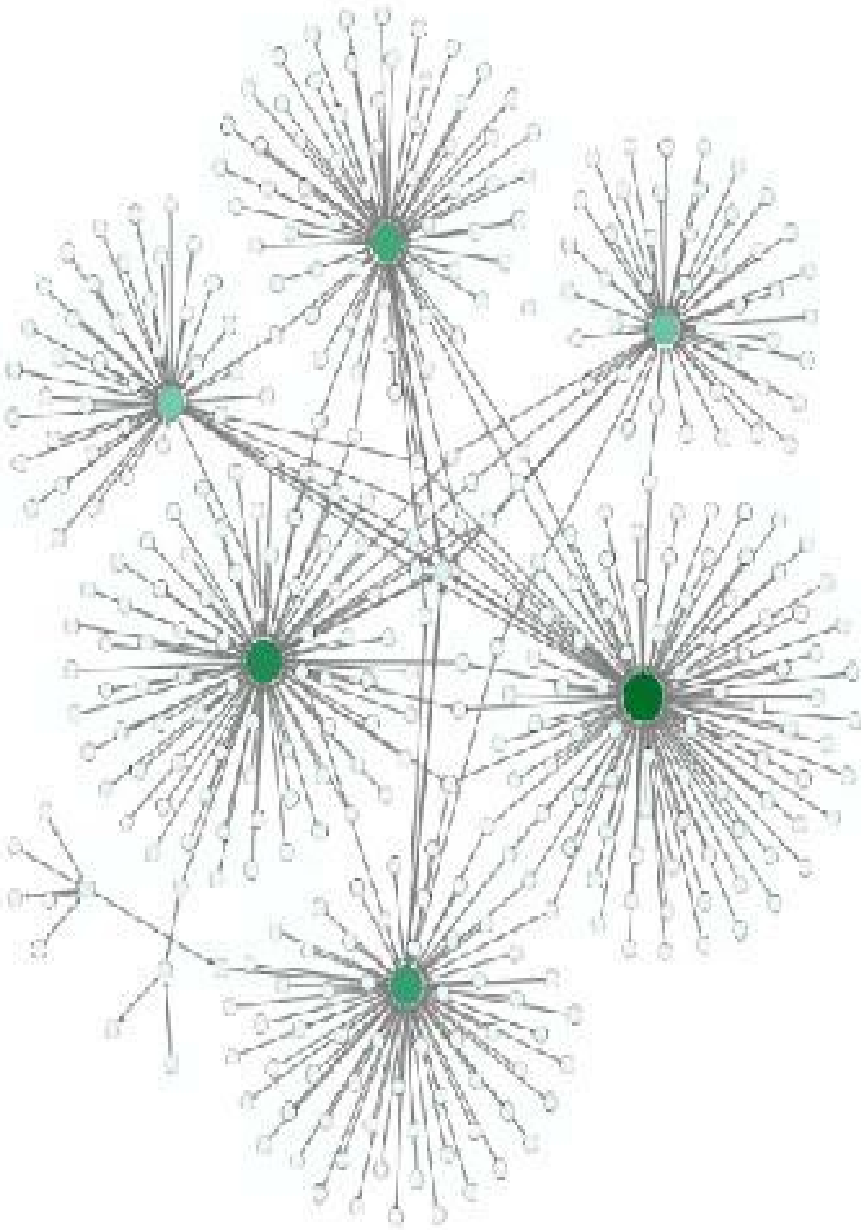
È possibile da subito, quindi, comprendere se il sistema così come costruito è di tipo casuale ovvero assume altre strutture caratteristiche calcolandone la densità.

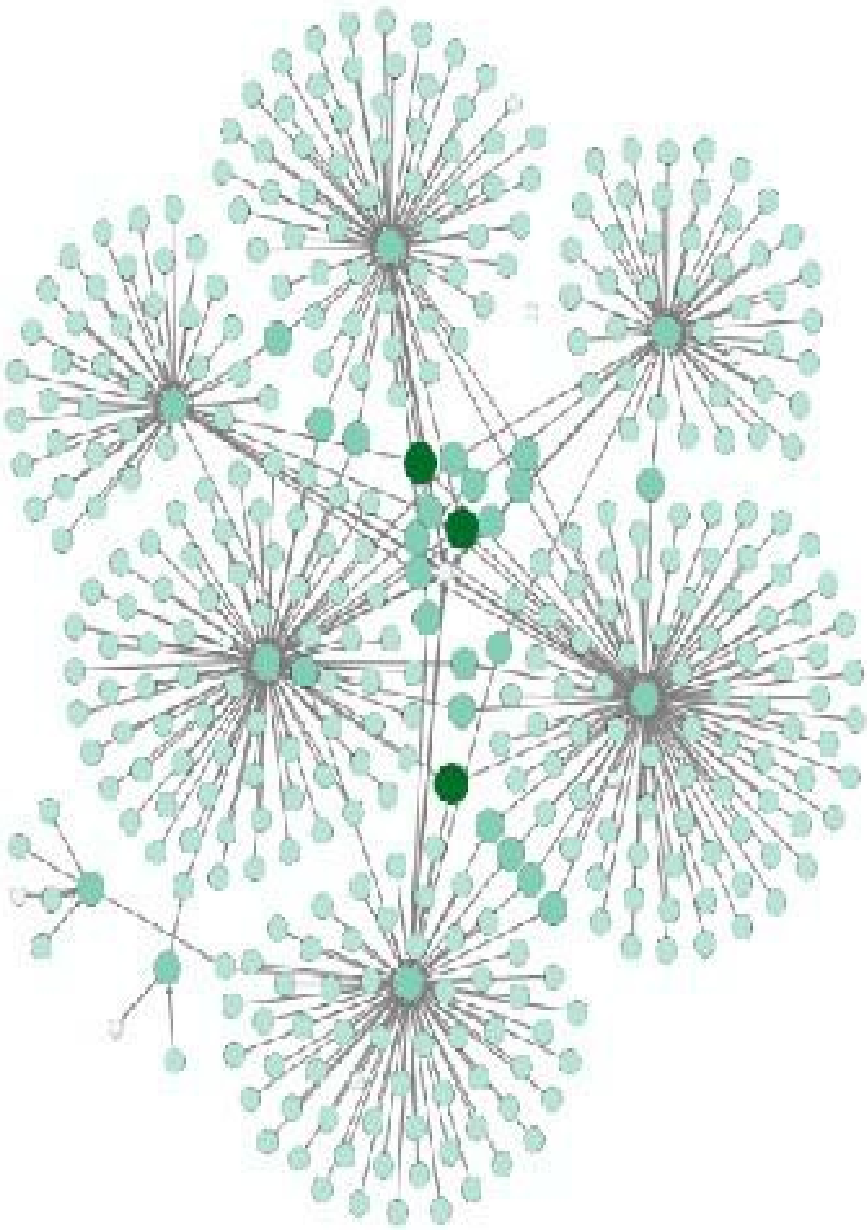
Alla predetta rete di transazioni, è possibile applicare un'analisi connessa a far emergere i nodi che evidenziano il più elevato valore di *degree* ovvero quei nodi che evidenziano maggiori collegamenti con altri nodi della rete medesima. Pertanto il risultato è del tutto evidente e semplice in termini di visualizzazione attesa.



Componente maggiormente connessa isolata con nodi a maggiore valore di degree

I nodi maggiormente connessi, che fanno emergere un più elevato *degree*, sono proprio le transazioni della rete distribuita, a eccezione delle due transazioni periferiche alla rete. A questo punto si può applicare una ulteriore vista della rete selezionando le due metriche *in-degree* e *out-degree* che non fanno altro che far emergere, rispettivamente, i nodi della rete in esame con maggiori connessi entranti in ovvero uscenti da un determinato nodo.





Confronto tra componente maggiormente connessa isolata con nodi a maggiore valore di in-degree (a sinistra) e out-degree (a destra)

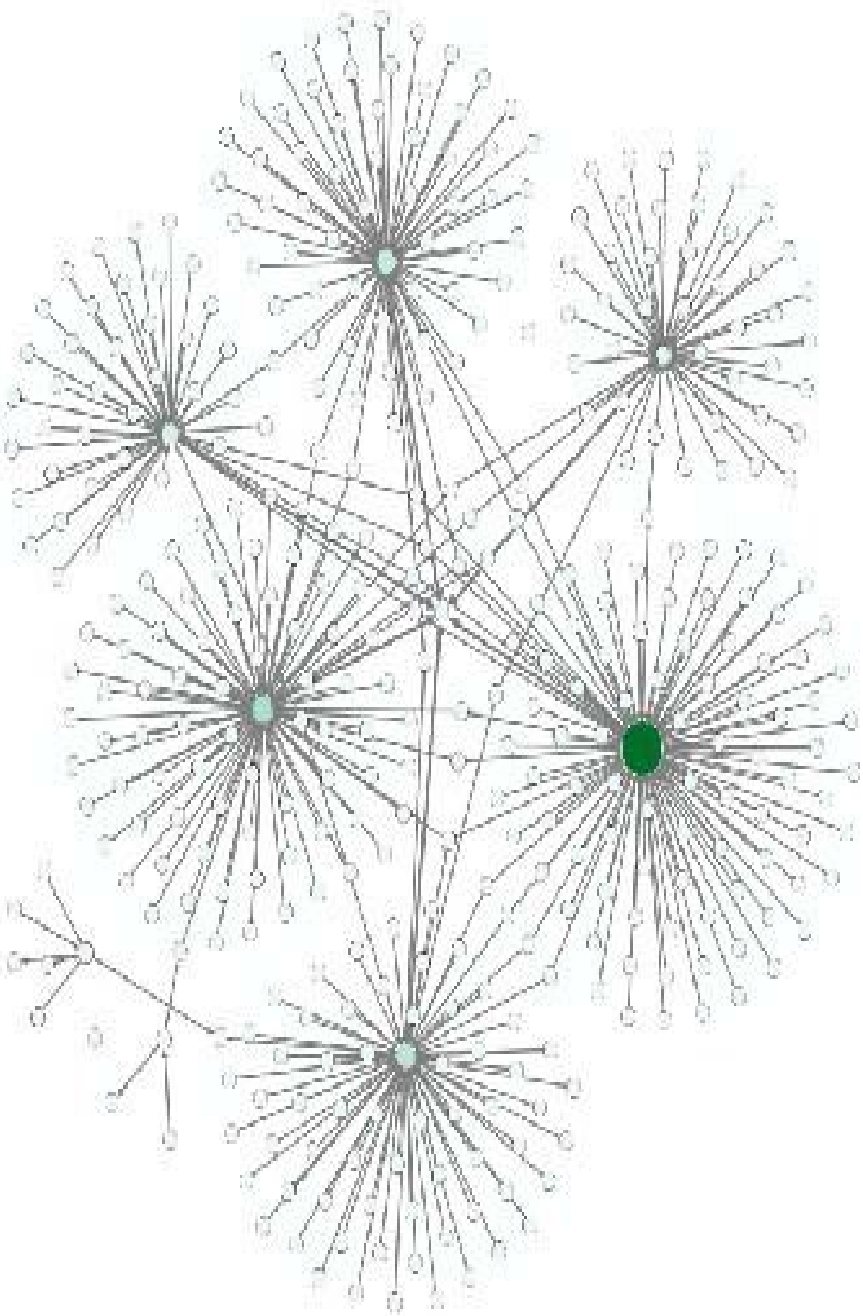
Il risultato che emerge è relativo alla possibilità di capire quali delle transazioni ricevono maggiori frammentazioni di criptovaluta (*in-degree*) e quali indirizzi sono maggiormente operativi nella rete (*out-degree*); in quest'ultimo caso, è agevole osservare i nodi con un colore verde più deciso ed un diametro più ampio rispetto a tutti gli altri.

Pertanto, volendo tirare le prime conclusioni avendo semplicemente operato sulla sola metrica del *degree*,

l'analisi condotta ha consentito di focalizzare l'attenzione su sei transazioni e su tre indirizzi bitcoin. Il tutto con pochissime azioni sul sistema di visualizzazione utilizzato.

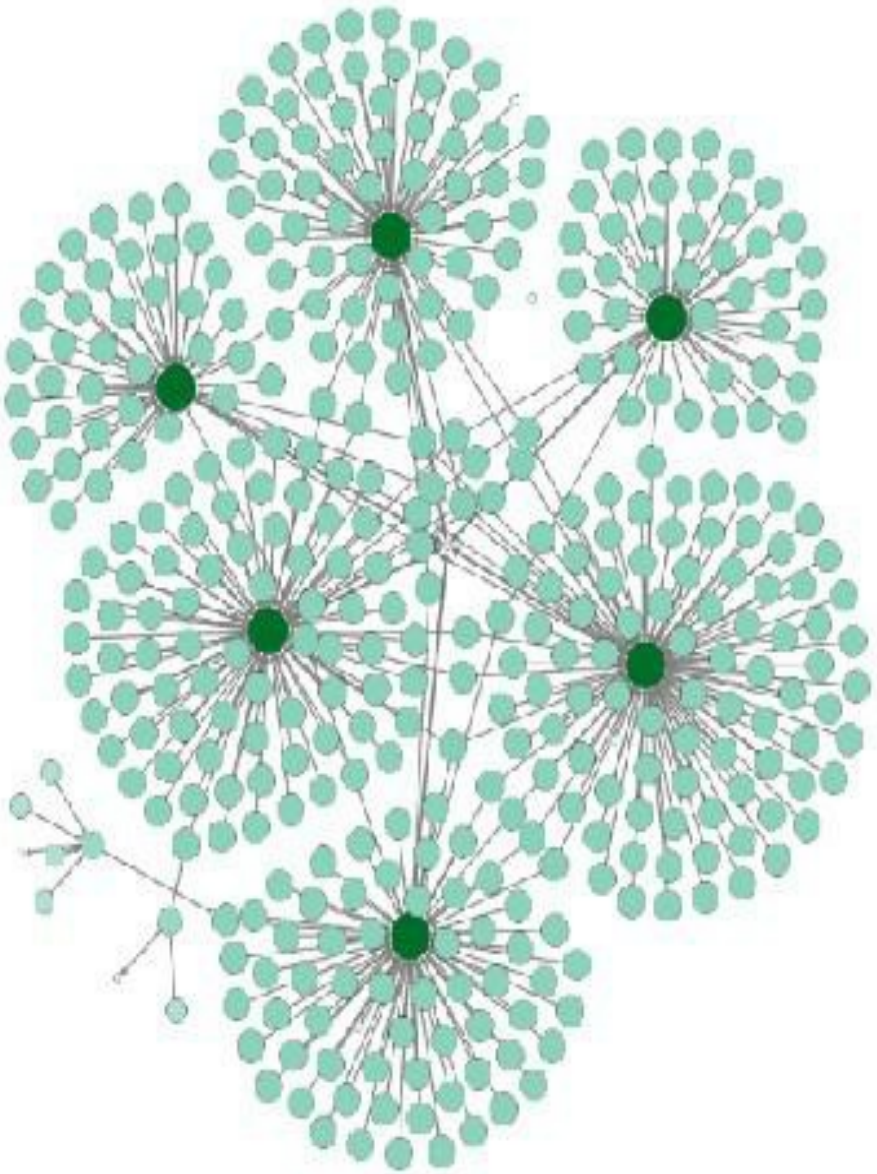
2.2.2 Metriche di rete avanzate per comprendere le criptovalute

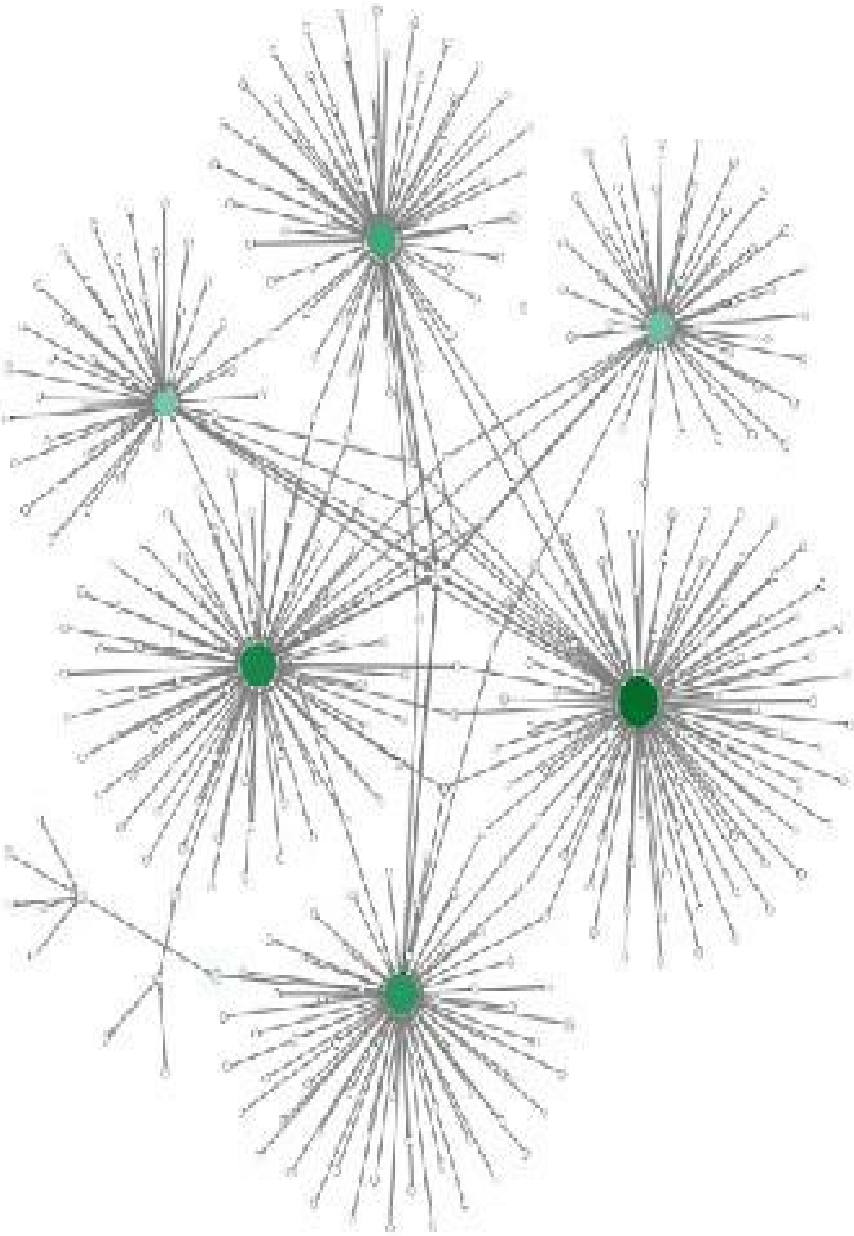
È possibile ora estremizzare l'analisi verificando se tra i nodi maggiormente connessi e centrali per la rete in esame vi siano le cosiddette *Authority* [45]. Attraverso il filtro opportunamente specificato sulla piattaforma di visualizzazione ne emerge uno in particolare di tipo *transazione*.



Componente maggiormente connessa isolata con nodi a maggiore valore di authority

Se si approfondiscono le ulteriori misure si ottengono conferme circa la struttura decentralizzata e distribuita delle transazioni e degli indirizzi della criptovaluta. Di seguito, in ordine, il grafo rielaborato secondo il valore di *closeness* e di *betweenness*. In dettaglio emergono in ogni caso, anche se con sfumature differenti, le sei transazioni che hanno lo scopo di attrarre su di sé l'attenzione della rete.



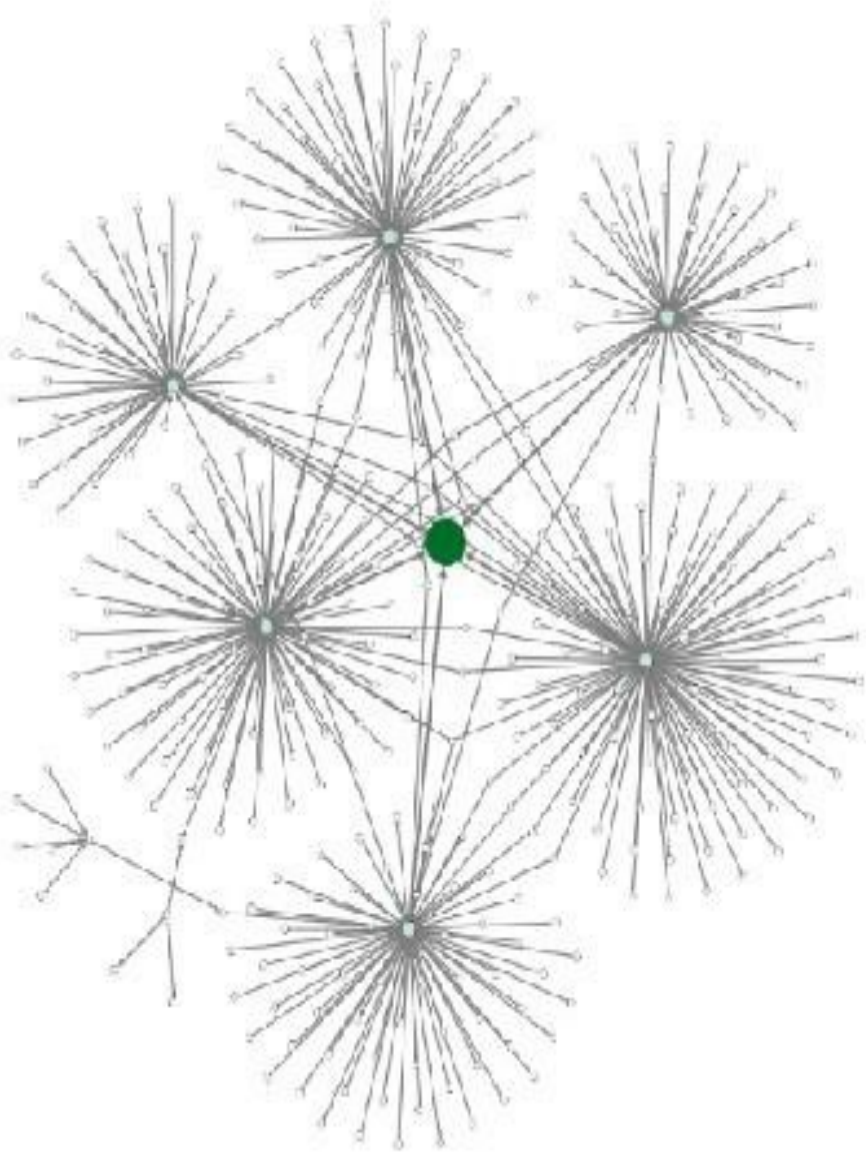


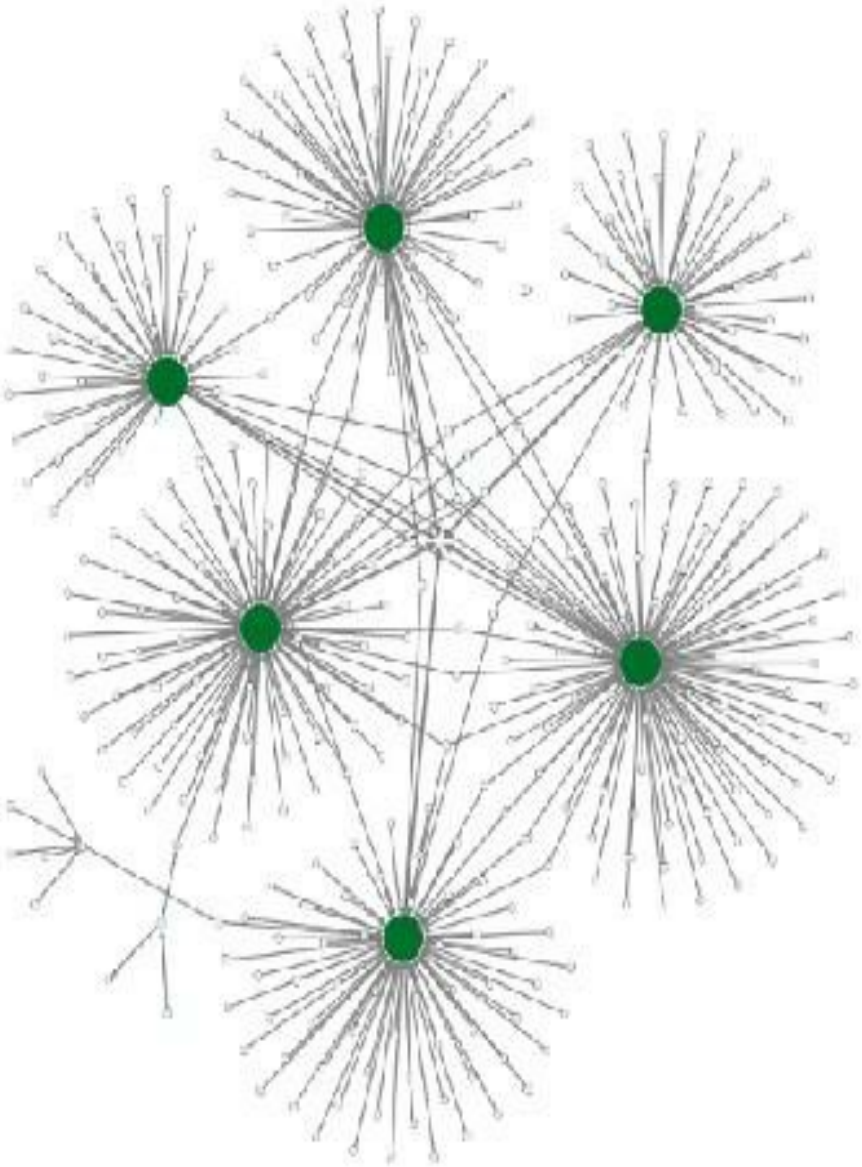
Confronto tra componente maggiormente connessa isolata con nodi a maggiore valore di closeness (a sinistra) e betweenness (a destra)

Osservando con maggiore attenzione la rete si può comprendere come in realtà possano esistere uno o più nodi destinatari dell'intero flusso di criptovaluta come intercettato dallo *streaming* della blockchain.

Nello specifico è possibile ulteriormente filtrare il grafo secondo il peso delle connessioni sia in ingresso che in uscita da ciascun nodo. Il software consente infatti di recuperare le metriche rispettivamente come *weigthed in-degree* e *weigthed out-*

degree.





Confronto tra componente

maggiormente connessa isolata con nodi a maggiore valore di weigthed in-degree (a sinistra) e weigthed out-degree (a destra)

Il risultato interessante per questa rete di transazioni e indirizzi molto estesa è che si riesce ad individuare, con estrema agevolezza mediante talune metriche, l'indirizzo di criptovaluta che, nella circostanza, ha ricevuto l'intero flusso di criptovaluta rappresentato. Ciò, nonostante l'estesa ed enorme complessità di presenza di numerosi nodi di tipo transazioni e indirizzi in esse coinvolti.

Ovviamente le predette tecniche di analisi sono utilizzabili ed applicabili a

contesti più semplici ovvero più complessi rispetto a quello sopra affrontato e descritto. Ciò che deve far riflettere il lettore è il fatto che è proprio grazie alla elevata capacità di elaborazione e visualizzazione dei risultati offerta da software specifici, come Gephi [41], che si può analizzare in maniera rapida ed efficace il flusso e le dinamiche dei pagamenti effettuati in criptovalute.

Ciò a totale vantaggio delle investigazioni e della chiarezza degli esiti oggettivi a cui si è giunti mediante l'applicazione di un metodo in ogni caso scientifico, come quello rinvenibile nella teoria dei grafi e della *social network analysis*, all'analisi dei flussi

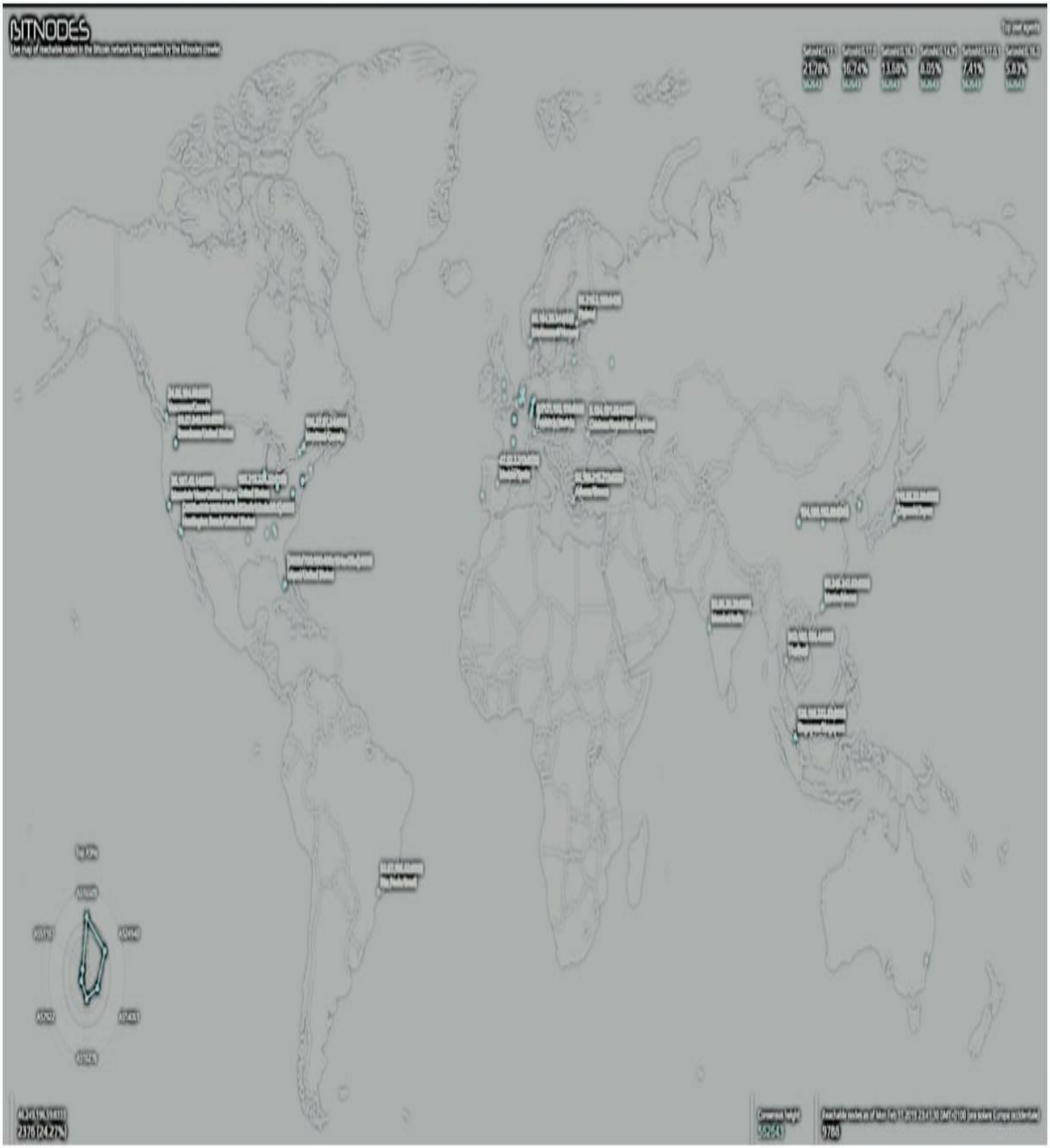
che interessano una rete come quella di Bitcoin.

2.3 STRUMENTI DI ANALISI VISUALE *REAL TIME* DELLA BLOCKCHAIN

Dopo aver trattato, seppur sinteticamente, di possibili applicazioni delle tecniche di SNA alla *blockchain intelligence* di Bitcoin, è opportuno affrontare il tema della ricerca di strumenti di analisi visuale della Blockchain che, in tempo reale, sfruttano l o *streaming* di dati da essa recuperabile attraverso l'utilizzo delle *Application Programming Interface*

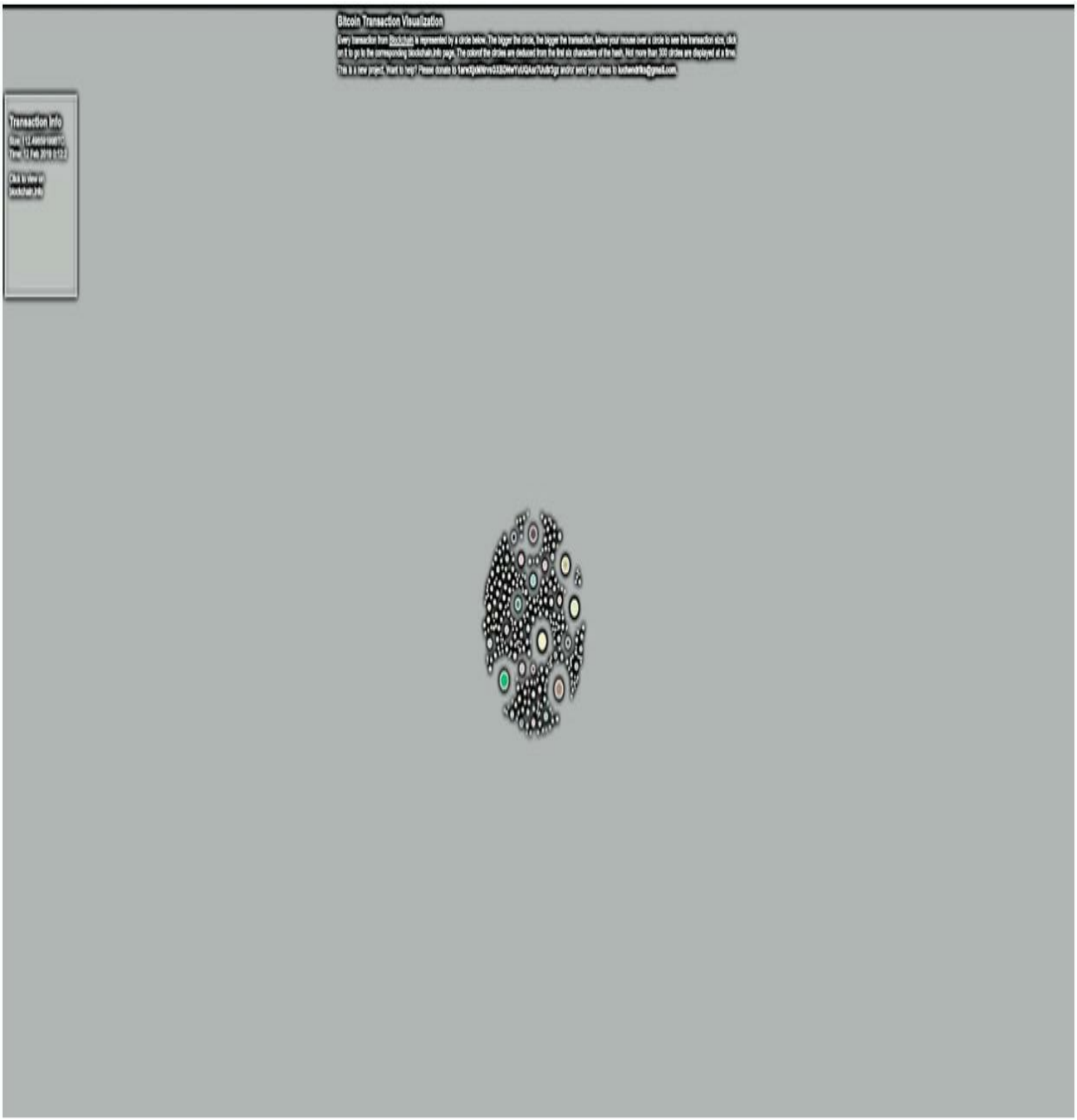
(API) attualmente esistenti.

Occorre rappresentare preliminarmente che esistono diverse piattaforme *on-line* che consentono di osservare il flusso di dati recuperabili da Blockchain di Bitcoin. Un interessante esempio è la piattaforma di *Bitnodes* (https://bitnodes.earn.com/nodes/live-map/) che offre, tra i diversi servizi, una mappa in tempo reale dei nodi raggiungibili nella rete Bitcoin derivante da attività di *crawling* di Bitnode.



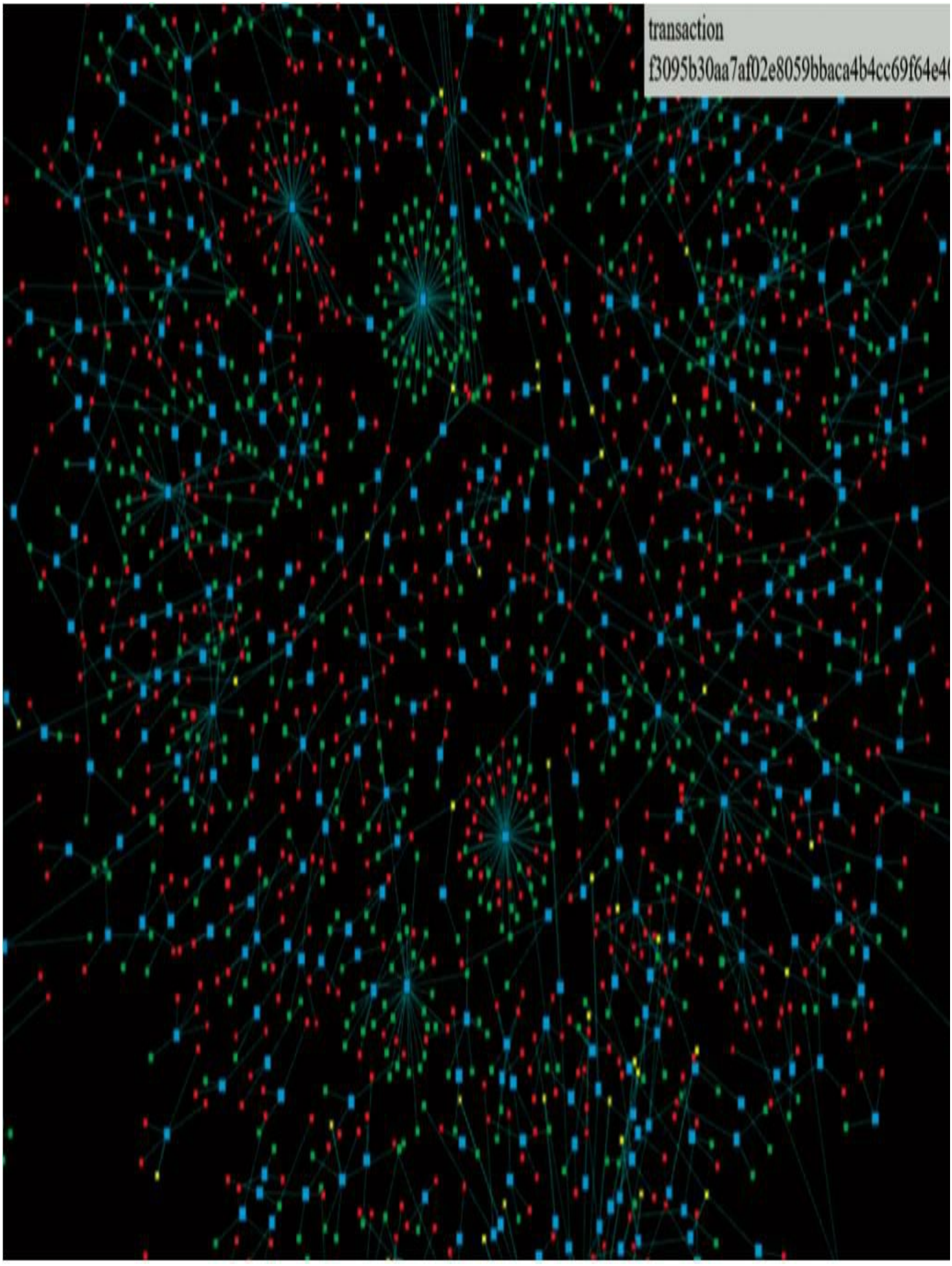
Piattaforma Bitnodes

Senza soffermarsi su ulteriori caratteristiche del sito che si lascia al lettore per gli opportuni approfondimenti ed utilizzi, è possibile trovare ulteriori piattaforme che consentono tale tipologia di analisi, come ad esempio *Bitcoin Transaction Visualization* (http://bitcoin.interaqt.nl/). In questa piattaforma ogni transazione derivata dalla Blockchain di Bitcoin è rappresentata da un cerchio. Più grande è il cerchio, maggiore sarà la transazione sottostante. È possibile passare con il mouse sopra un cerchio per vedere la dimensione della transazione, ovvero per andare alla pagina blockchain.info corrispondente.



Piattaforma Bitcoin Transaction Visualization

Altra piattaforma interessante è realizzabile mediante l'utilizzo congiunto delle API di blockchain.info e della *vivagraph.js library* [46]; in questo caso i diversi colori utilizzati per i nodi rappresentano gli indirizzi input, gli indirizzi output e le transazioni (https://www.infodata.ilsole24ore.com/2 transazioni-si-accettano-pagamenti-bitcoin-le-mappe-della-criptovaluta/).


transaction
f3095b30aa7af02e8059bbaca4b4cc69f64e4

Piattaforma realizzata con vivagraph.js library

Gli esempi sopra riportati testimoniano la crescente necessità di comprendere il meccanismo di funzionamento delle criptovalute non semplicemente verificando le singole transazioni di interesse eventuale, ma cercando di comprendere l'evoluzione della Blockchain in tempo reale e in maniera visuale per far emergere eventuali comportamenti anomali o di interesse che dovessero mai verificarsi.

2.3.1 Costruire una piattaforma di analisi visuale integrata

Un interessante strumento *open source* per l'analisi dello streaming della Blockchain di Bitcoin è rappresentato dallo script *gephi-bitcoin* di Matthieu Totet [42].

Esso consente di utilizzare le elevate capacità del noto linguaggio di programmazione Python per attività di *parsing* sulla Blockchain *real time*.

Oltre al *parser*, lo script, se opportunamente eseguito con specifiche configurazione della piattaforma di analisi visuale Gephi, consente di ottenere il grafo delle transazioni che il citato *parser* garantisce nell'estrazione.

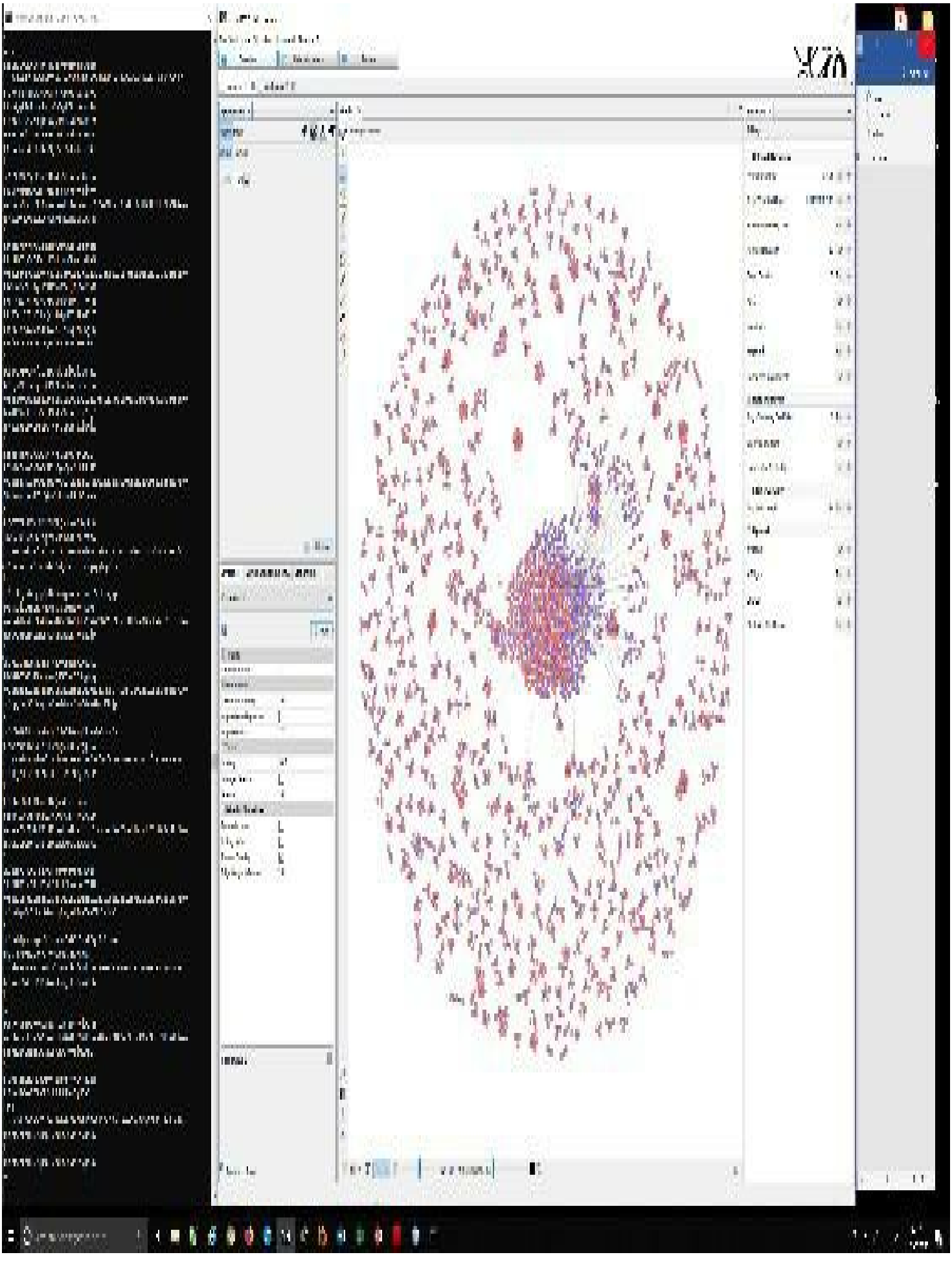
Il risultato che si ottiene è estremamente efficace e soprattutto molto performante se si considera l'enorme mole di dati e

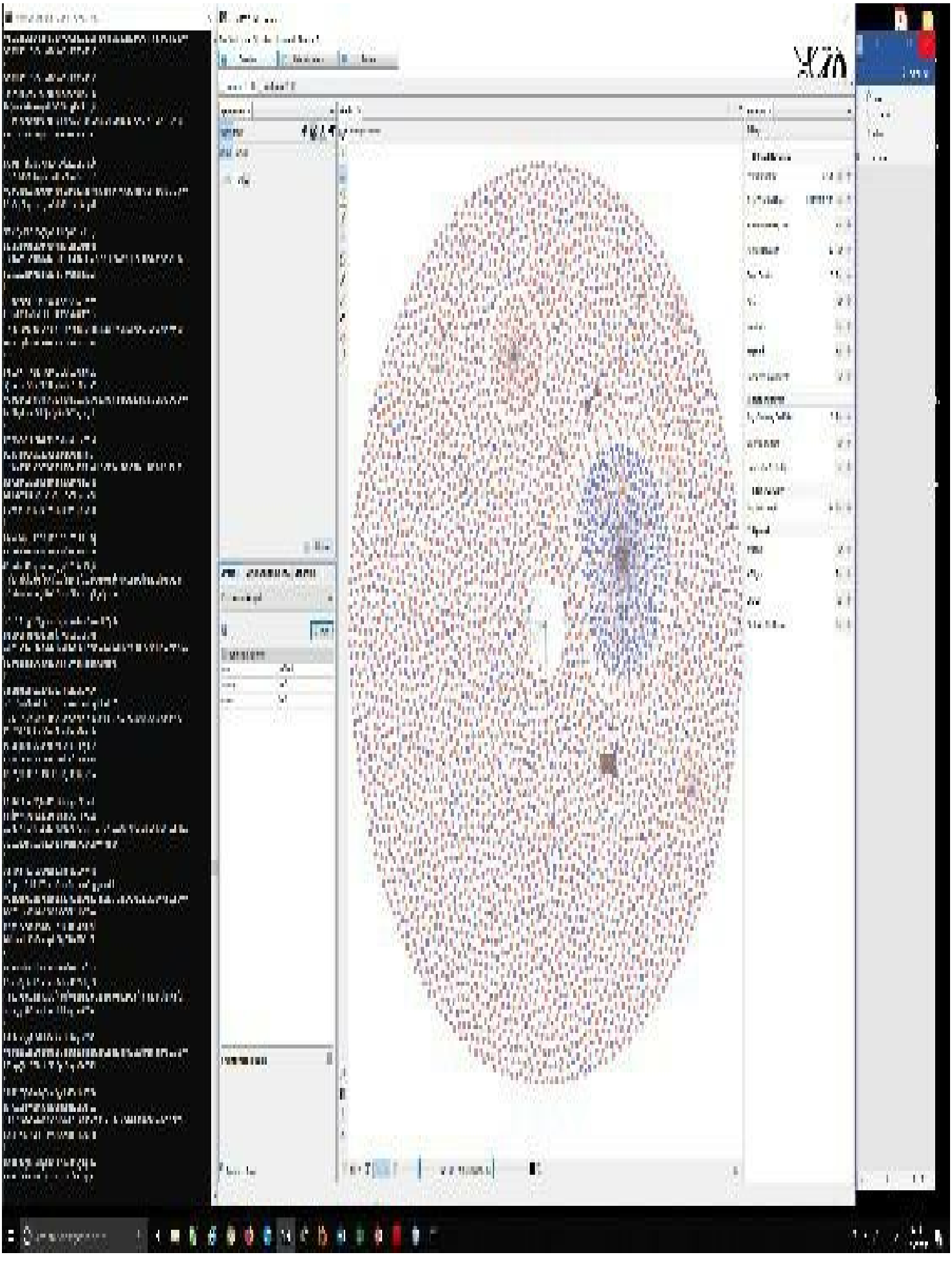
di informazioni che sono pubblicate giornalmente sulla stessa Blockchain in termini di numero di transazioni e indirizzi in esse coinvolti.

2.3.2 Risultati ottenuti su casi reali

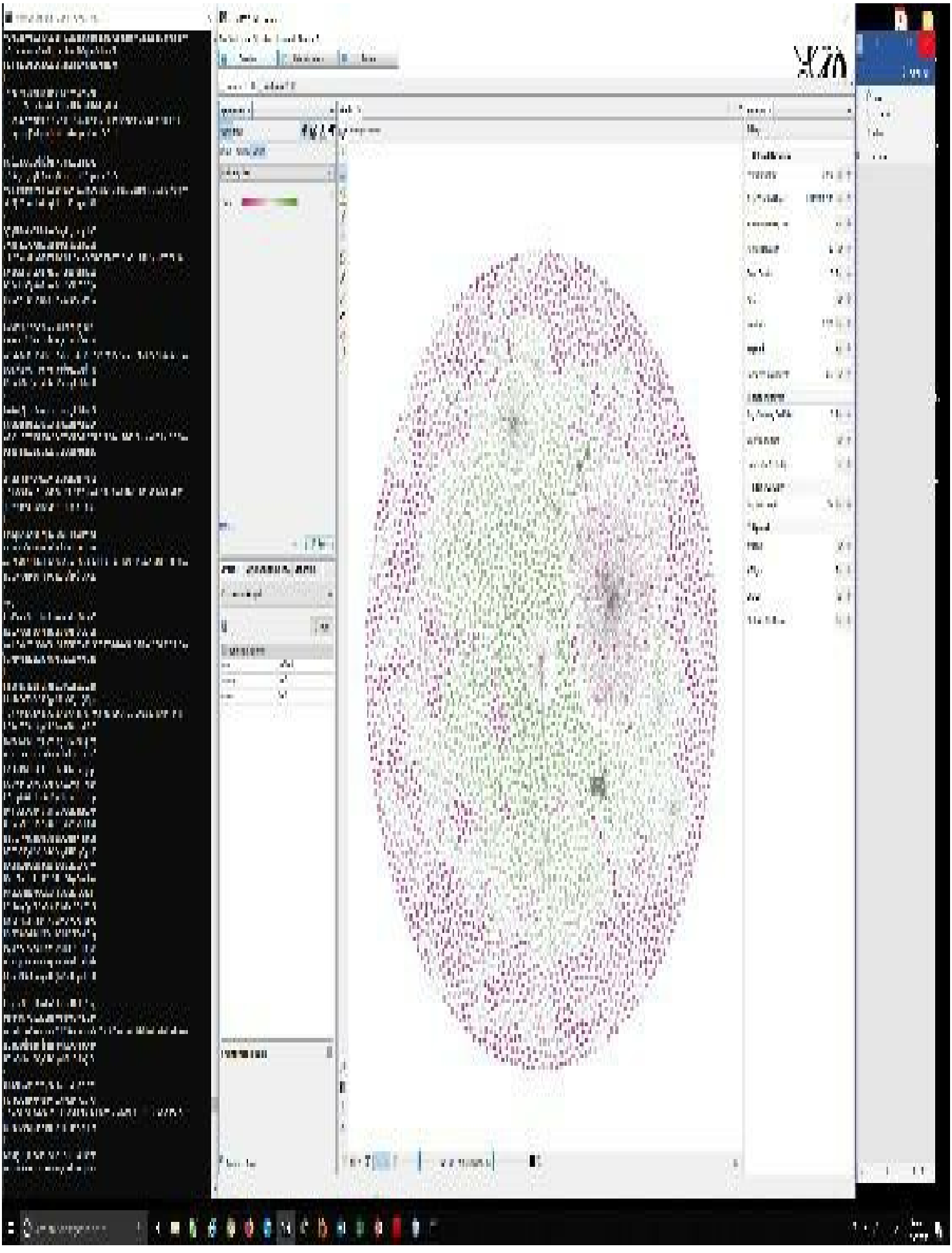
Si osservi come l'esecuzione dello script consenta di disporre delle transazioni e degli indirizzi in esse coinvolti, sia in input che in output, secondo un grafo orientato. Di seguito due immagini che raffigurano la medesima osservazione della Blockchain mediante due differenti layout disponibili in Gephi. Il primo utilizza il *layout ForceAtlas2* [47], simulando attrazione dei nodi

maggiormente collegati, e il secondo *Fruchterman Reingold* [48], che organizza i nodi con equidistanza tra di loro.

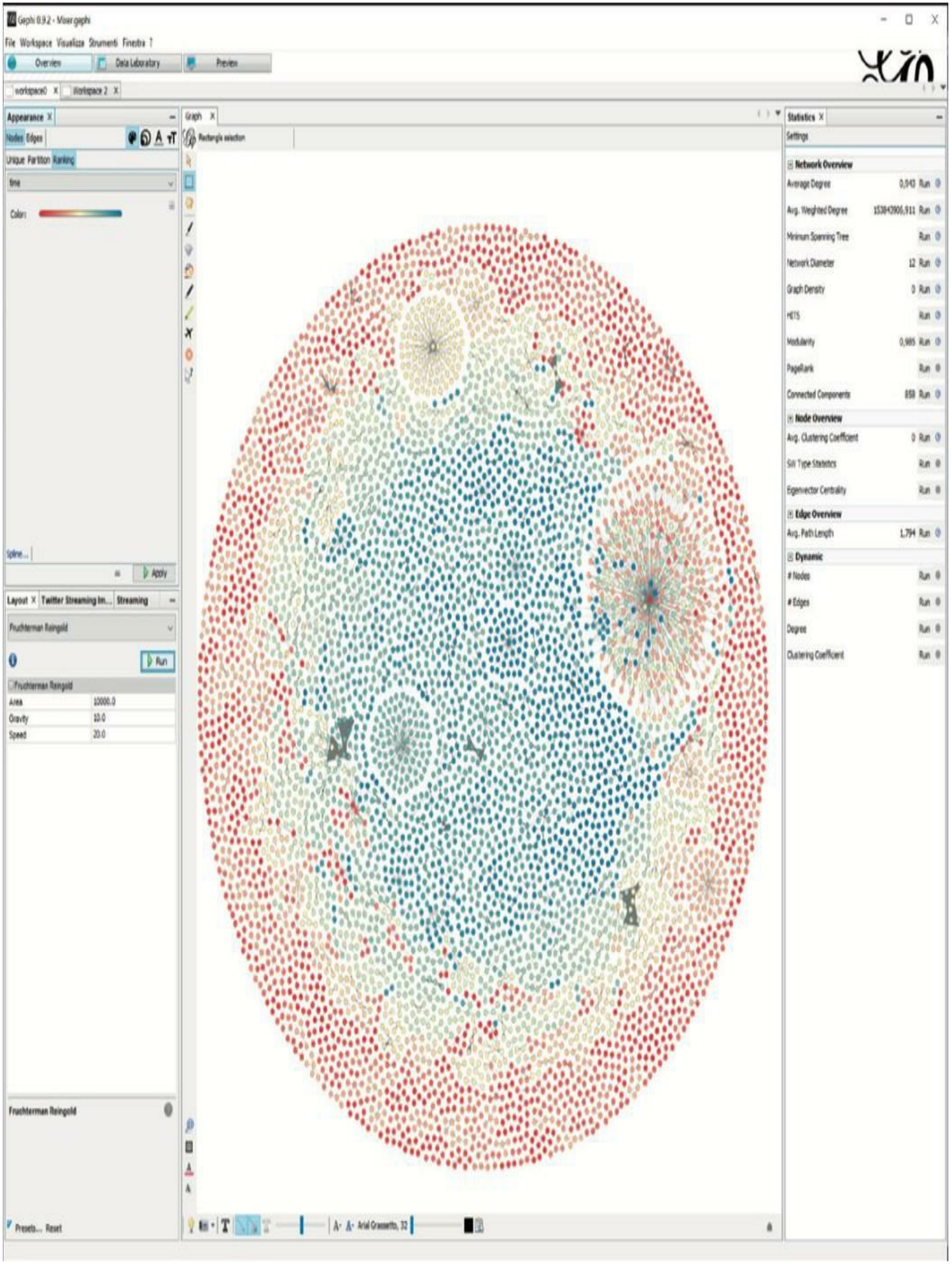




Ulteriore apprezzata funzione di analisi della rete così raffigurata, è il filtro che evidenzia la ricorrenza di moduli all'interno della rete, in modo da far emergere *pattern* ricorrenti. Nel caso in esame è evidente la presenza di due tipologie di pattern. Ciò consente di capire rapidamente che la rete che si viene a formare ha specifiche strutture relazionali che ricorrono anche su larga scala.



Altra visualizzazione molto utile ed interessante sotto il profilo dell'analisi, è data dalla possibilità di ricercare, secondo una scala temporale – modulata con una scala cromatica che va dal rosso (nodi più datati) al blu (nodi più recenti) – che rende semplice comprendere ed individuare l'evoluzione temporale delle transazioni. Tale cromia può consentire, sotto certi aspetti, di capire se taluni indirizzi sono maggiormente utilizzati nel tempo rispetto ad altri ovvero se vi sono transazioni che utilizzano indirizzi nuovi ovvero altri più datati.


Gephi 0.9.2 - Mixergephi
File Workspace Visualize Strumenti Finestra ?
Overview
Data Laboratory
Preview
workspace0
Workspace 2
Appearance
Nodes Edges
Unique Partition Ranking
time
Color:
Spline...
Apply
Layout
Twitter Streaming Im...
Streaming
Fruchterman Reingold
Run
Fruchterman Reingold
Area 10000.0
Gravity 10.0
Speed 20.0
Fruchterman Reingold
Presets... Reset
Graph
Rectangle selection
Arial Grassetto, 32
Statistics
Settings
Network Overview
Average Degree 0,943 Run
Avg. Weighted Degree 153843906,911 Run
Minimum Spanning Tree Run
Network Diameter 12 Run
Graph Density 0 Run
HITS Run
Modularity 0,985 Run
PageRank Run
Connected Components 859 Run
Node Overview
Avg. Clustering Coefficient 0 Run
SNA Type Statistics Run
Eigenvector Centrality Run
Edge Overview
Avg. Path Length 1,794 Run
Dynamic
Nodes Run
Edges Run
Degree Run
Clustering Coefficient Run

2.4 *TAGGING* E *CLUSTERING*: TECNICHE ANALITICHE A CONTRASTO DEL CYBERCRIME

Giunti a questo punto della trattazione, è opportuno spingersi ulteriormente in avanti con le tecniche di analisi della Blockchain. L'utilizzo di una criptovaluta, come ad esempio il Bitcoin, si può prestare anche ad ambiti non leciti. Ciò è incentivato, come detto, in linea di principio dall'elevato livello di anonimizzazione che il paradigma delle criptovalute assicura ai loro utilizzatori. Pertanto, nel verificare un flusso di transazioni presenti all'interno

della Blockchain di riferimento per una criptovaluta non è possibile ottenere, in relazione alla peculiare struttura informatica delle transazioni e degli indirizzi di Bitcoin, più in generale delle criptovalute, informazioni relative ai portafogli e, men che meno, ai loro titolari.

Per riprendere un'analogia con il mondo tradizionale bancario, conoscere un indirizzo Bitcoin con la possibilità di operare una transazione in modalità *in* o *out* è considerato alla stregua di conoscere dell'esistenza di un codice IBAN che individua uno specifico conto corrente bancario, sul quale è possibile ricevere ovvero dal quale è possibile inviare del denaro, ma non se ne

conosce né la banca o intermediario finanziario né tanto meno l'intestatario.

Si può pertanto ipotizzare la necessità, in determinate condizioni, di cercare di identificare un utente specifico utilizzando le tracce presenti sia nel *Clear web* che nel *Dark web* correlate agli elementi identificativi dell'utilizzo di moneta virtuale; in altri termini, attesa la natura del Bitcoin, si potrebbe ipotizzare di recuperare le informazioni relative agli indirizzi Bitcoin pubblicati in rete e, di conseguenza, recuperare le relazioni indirette con altri indirizzi Bitcoin mediante l'analisi delle transazioni presenti e validate sulla Blockchain.

I dati relativi agli indirizzi Bitcoin

possono provenire da molteplici fonti, come per esempio, da social network, forum, testi di e-mail pubblicate in rete ovvero ricevute sul proprio account, oltre che dai *post* e dai siti presenti nelle *darknet* in cui vengono indicate le modalità di pagamento di specifici beni o servizi in esse venduti.

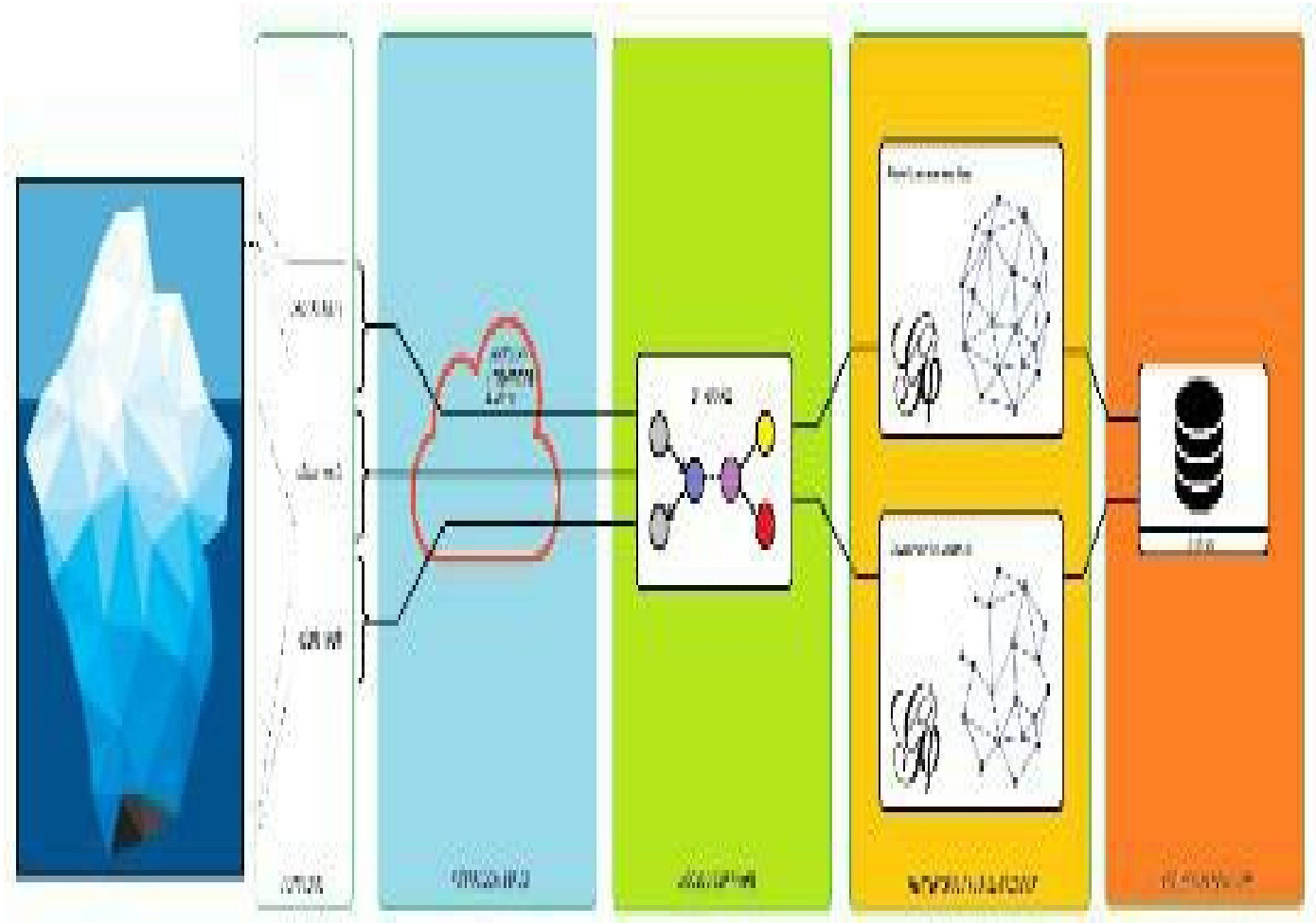
Detto ciò, è del tutto evidente che l'attività di analisi che viene richiesta al software ha diversi fattori di complessità derivanti dal fatto di poter attingere, gestire, processare e visualizzare enormi quantità di informazioni. Pertanto, è possibile immaginare un *framework* a moduli in cui siano contenuti i dati e le funzioni specifiche per rendere possibile

l'analisi dei dati.

Uno dei principali obiettivi del predetto *framework* dovrebbe essere quello di recuperare, mediante un'analisi della Blockchain, i possibili domini che hanno pubblicato uno o più indirizzi di criptovaluta nel *clear web* ovvero gli *hidden service* nel *dark web* al cui interno sono presenti. Per poter assicurare ciò, è necessario disporre di fonti di dati che interagiscono con un modulo software di analisi mediante una interfaccia di servizi opportunamente configurata su talune API (*Application Programming Interface*).

Il modulo software centrale consente di recuperare tutte le informazioni dalle fonti dati; inoltre viene inserito un

modulo di visualizzazione relazionale e visuale dei risultati oltre che un modulo di archiviazione degli stessi.



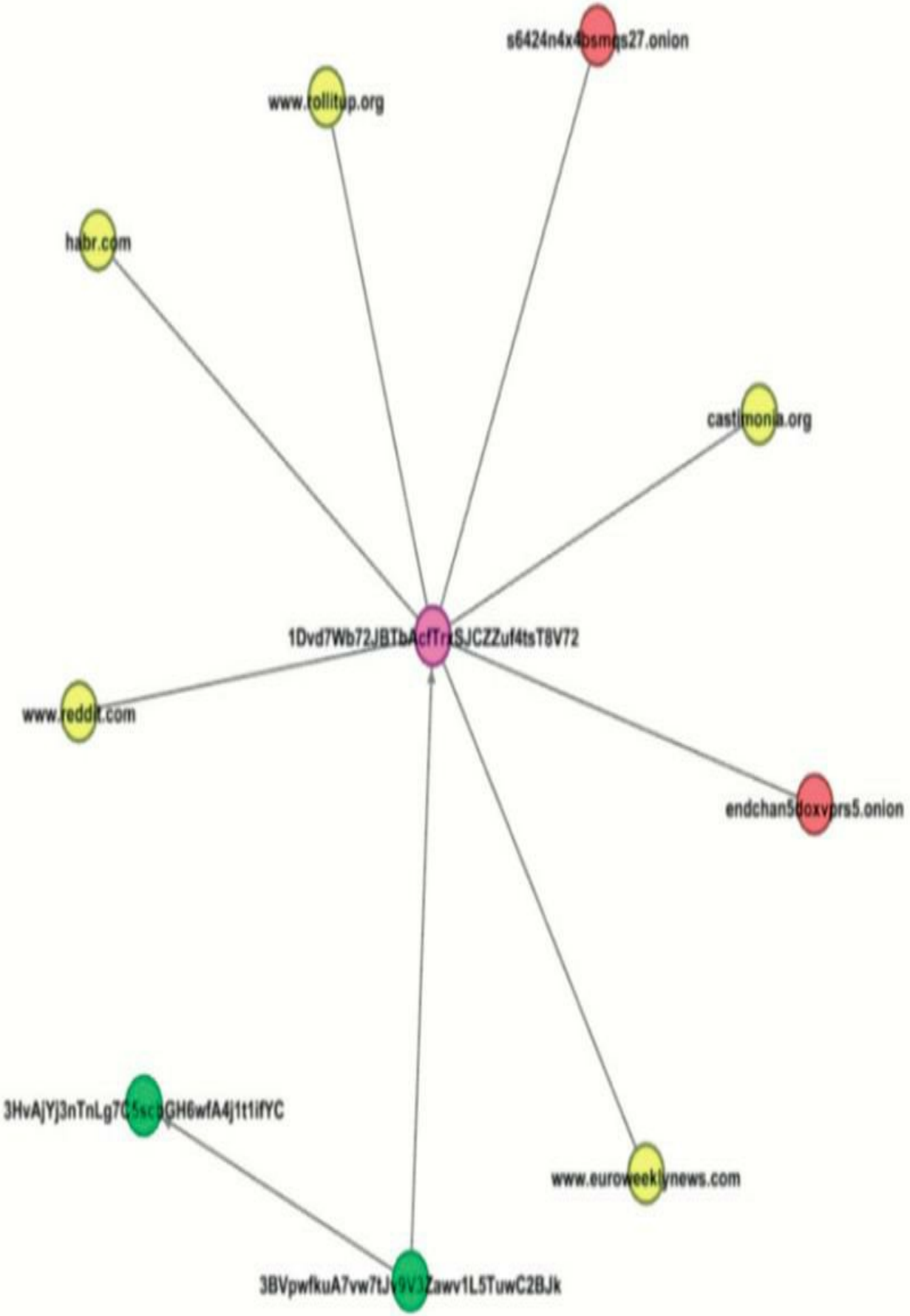
Schema di un possibile framework per l'analisi della blockchain di Bitcoin

Il predetto framework potrebbe operare secondo due modalità:

- specificando un indirizzo Bitcoin: in questo caso l'analisi verrebbe condotta a partire dal singolo indirizzo, ossia estraendo le transazioni ad esso collegate e gli indirizzi univoci in esse coinvolti;
- senza argomenti: in questo modo opererebbe in *real time* estraendo le ultime transazioni disponibili sulla *blockchain*.

2.5 APPLICAZIONE DELLE FUNZIONALITÀ DEL *FRAMEWORK* AD UN CASO REALE

A scopo dimostrativo, si può effettuare un approfondimento sull'indirizzo BTC 1Dvd7Wb72JBTbAcfTrxSJCZZuf4tsT8V utilizzato in un'attività di presunta estorsione sessuale recentemente apparsa sul Web, sul quale può essere interessante recuperare utili informazioni. Il *framework* in esame potrebbe recuperare la seguente rete di informazioni.


s6424n4x4bsmqs27.onion
www.tollitup.org
habr.com
castlmonia.org
1Dvd7Wb72JBTbAcfTrtSJCZZuf4tsT8V72
www.reddit.com
endchan5doxvprs5.onion
3HvAjYj3nTnLg7C5scpGH6wfA4j1t1ifYC
www.euroweeklynews.com
3BVpwfkuA7vw7tJv9V3Zawv1L5TuwC2BJk

Pertanto, è possibile analizzare – oltre che la struttura relazionale delle transazioni che utilizzano il citato indirizzo – informazioni con particolare riguardo ai seguenti siti nel *Clear web:*

- castimonia.org

Phishing scam known as 'sextortion' is using people's real passwords to blackmail them for supposedly watching porn

- www.euroweeklynews.c

EMAIL SCAM: Police in Spain warn of porn site 'sextortion' blackmail campaign

- habr.com
В США набирает обороты секс-фишинг (Negli Stati Uniti sta guadagnando slancio sex phishing)

Inoltre è possibile ottenere le seguenti informazioni individuate attraverso attività di crawling nel Dark web sui due hidden service s6424n4x4bsmqs27.onion e endchan5doxvprs5.onion.
In uno dei due *hidden service* si recupera un interessante dettaglio: "*è probabile che questo tentativo di sextortion migliorato sia almeno semi-automatizzato: la mia ipotesi è che il*

perpetratore abbia creato una sorta di script che attinge direttamente dai nomi utente e password da una data violazione in un sito Web popolare avvenuto più di un decennio fa, e che ogni vittima che ha avuto la sua password compromessa come parte di quella violazione sta ricevendo la stessa e-mail all'indirizzo utilizzato per registrarsi a quel servizio che venne hackerato".

In questo caso, il recupero di informazioni consente di esperire ipotesi concrete circa la modalità di attacco che è stata utilizzata.

2.5.1 Interesse della criminalità alle criptovalute

La complessità del mercato delle criptovalute, con particolare riguardo al bitcoin, si estrinseca – si ricorda – nella considerazione che l'offerta è praticamente rigida o quantomeno tendente ad una rigidità, laddove sia effettivamente riconosciuto che il numero di bitcoin è comunque finito e non può essere aumentato. Pertanto il valore unitario e di cambio che viene attribuito alla specifica criptovaluta risente in maniera ampia della domanda presente nello specifico mercato.

In questo senso appare non peregrina l'ipotesi che gruppi di cyber criminali possano orientare la domanda di tali "oggetti", ovviamente in aumento,

attraverso la richiesta di bitcoin per essere utilizzati, ad esempio, nel pagamento di un riscatto a seguito di infezione di un *ransomware*, come i recenti noti casi di cronaca mondiale.

Tale meccanismo appare estremamente efficace quanto redditizio e genera speculazione su "oggetti" che possono essere utilizzati ineludibilmente anche per scopi non leciti. Si pensi al comportamento della vittima di un ransomware che pur di rientrare – anche se, è bene sempre ribadirlo, non vi è certezza o garanzia alcuna sul buon esito – in possesso dei propri dati presenti sull'host colpito, sarebbe disposta a cambiare un valore equivalente di moneta corrente in criptovaluta.

Ovviamente la complessità dell'"oggetto" è tale che la vittima inizia ad orientarsi, magari attraverso i motori di ricerca tradizionali presenti sul Web e, di conseguenza, a cercare di conoscere meglio le modalità di "cambio" della valuta.

La combinazione di servizi che garantiscono l'anonimato, come il network TOR, delle criptovalute e del *Dark web* crea un universo parallelo che fornisce ai cyber criminali sia un vero e proprio arsenale digitale che un luogo sacro.

Dal punto di vista del cybercrime, ad esempio, l'ultimo biennio è stato caratterizzato dalla diffusione esponenziale dei *ransomware*, mediante

alcuni attacchi su scala globale come, tra i primi comparsi, WannaCry e Petya.
Gli attacchi *ransomware* – si ricorda – sono quelli che cifrano i dati del computer infettato, al fine di ottenere un riscatto per la loro decrittazione.
Negli ultimi mesi tuttavia il fenomeno appare essere in calo, a causa di numerosi fattori. Prima di tutto in seguito agli attacchi su scala globale utenti e aziende hanno imparato a difendersi in una maniera più efficace tramite *policy* di backup, opportune difese informatiche e formazione più approfondita. Inoltre il metodo del riscatto tramite bitcoin ha mostrato grossi limiti in quanto molte vittime di attacchi *ransomware* non hanno voluto o potuto pagare, magari

perché non hanno mai avuto a che fare con bitcoin o criptovalute.

Se da un lato la diffusione dei *ransomware* ha subìto una forte battuta d'arresto, dall'altro si è diffuso un nuovo e ancor più insidioso tipo di *cybercrime*: il *cryptomining*. In questo caso i computer infettati, con i soliti mezzi, ad esempio allegati di mail apparentemente innocue, cominciano a lavorare in *background* per generare criptovalute inviate automaticamente ai cybercriminali. In pratica il computer infettato arricchisce i pirati informatici senza che il legittimo possessore della macchina possa notare molto più di rallentamenti e picchi di consumo di energia. La vittima di *cryptomining*

quindi paga direttamente sul proprio conto energetico il lavoro di *cryptomining* di cui beneficiano i cybercriminali.

2.5.2 Capacità di contrasto e analisi delle reti di transazioni

Essere in grado di analizzare in dettaglio le criptovalute, con specifico riferimento alla loro struttura tecnologica, il loro funzionamento a basso livello e le modalità di creazione delle stesse potrebbe consentire di far evolvere gli attuali scenari di indagine tecnica che, oggi più che mai, è richiesta per poter affrontare in maniera seria e competente il tema delle criptovalute.

Ciò è ancor più importante se si considerano i molteplici e versatili utilizzi che tali "oggetti" di nuova generazione consentono di portare avanti.

Un approccio serio e determinato all'analisi di una criptovaluta richiede una conoscenza scientifica e tecnica estremamente precisa, che deve andare oltre le oramai diffuse questioni di natura giuridica e finanziaria. Pertanto deve essere del tutto chiaro il ruolo che Blockchain ha nell'esistenza e nella vita di una criptovaluta unitamente ai meccanismi che consentono di affermare che una transazione è tale e universalmente riconosciuta se e solo se essa è confermata nella stessa

Blockchain.

Parimenti deve essere chiaro il concetto che nell'utilizzo di una criptovaluta, come ad esempio Bitcoin, non si deve pensare che i reali titolari dei portafogli o wallet possano essere totalmente schermati e protetti nella loro *privacy* dalla robustezza dell'algoritmo posto alla base del funzionamento della stessa moneta virtuale.

È per questo che, in talune condizioni e per specifiche finalità non proprio trasparenti, gli utilizzatori di criptovalute tendono ad associare diversi mezzi tecnologici che innalzano il livello di anonimato. In altri termini, non si deve condannare ad ogni costo colui che investe in monete virtuali per

mere speculazioni finanziarie; di contro possono esistere soggetti che utilizzano lo strumento della criptovaluta per evitare che uno o più pagamenti possano essere riconducibili ad un rapporto di natura più o meno lecita tra due o più soggetti; il caso dei *ransomware* ne è un esempio. In altri casi il loro utilizzo, come si faceva cenno, è abbinato all'utilizzo di *darknet* e a particolari *browser*, tipo TOR, che consentono di mascherare la reale identità digitale di uno o più utenti che operano nella rete, pur lasciando in ogni caso tracce più o meno indirette.

In un tale contesto, il ruolo di analista, di consulente o di investigatore resta pertanto imprescindibile e fondamentale

per garantire un approccio di successo nella complessa attività di deanonimizzazione delle transazioni in criptovalute.

PARTE IV

SEQUESTRO E CONFISCA DI BITCOIN E CRIPTOVALUTE

4. 1. DAL SEQUESTRO TRADIZIONALE A QUELLO VIRTUALE

a cura di Paolo Dal Checco

Sommario: 1.1 Inquadramento Generale – 1.2 Tipologie e finalità di sequestro – 1.3 Come approcciarsi al mondo virtuale.

1.1 INQUADRAMENTO GENERALE

Dal punto di vista del protocollo, della

tecnologia e degli strumenti i bitcoin, e diverse criptomonete, sono ormai diventate quasi di uso comune, in certi ambienti, o comunque argomento noto anche da parte degli operatori di Forze dell'Ordine e Autorità Giudiziaria. Grazie ai notevoli vantaggi conferiti dalla possibilità di mantenere un certo grado di anonimato, sono però diventate un mezzo piuttosto diffuso per commettere reati o godere dei proventi degli stessi. Si pensi, ad esempio, alle estorsioni, ricatti, furti di criptomoneta o truffe che grazie ai Bitcoin e alle monete matematiche hanno avuto un rilancio soprattutto in ambito cosiddetto "cyber", dove la localizzazione fisica o il contatto diretto non sono più un vincolo

ma, anzi, permettono nuove forme d'illegalità e nello stesso tempo garantiscono livelli di protezione un tempo impensati.

Proprio per questi motivi, sono sempre più frequenti i casi nei quali si arriva a identificare wallet, indirizzi o transazioni sospette e talvolta si entra in possesso di portafogli utilizzati per commettere o godere dei frutti di reati: si rende quindi necessario predisporre modalità creazione di wallet e trasferimento sicuro da utilizzare nel momento in cui vengono richiesti dall'Autorità Giudiziaria il sequestro o la confisca del contenuto di tali portafogli.

Le Forze dell'Ordine hanno ormai

procedure consolidate per il sequestro di beni anche pericolosi come armi o prodotti chimici, metalli preziosi o diamanti, contanti, titoli al portatore o conti correnti. In base alla tipologia di bene da sequestrare, vengono predisposti conti intestati al Tribunale, caveau, depositi sicuri ove stoccare quanto sequestrato tramite protocolli e metodologie ormai condivise e considerate "standard" sia tecnicamente sia giuridicamente.

Persino i sequestri di siti internet, account su portali web o comunque scenari online sono stati sdoganati al punto che l'Autorità Giudiziaria è in grado di gestire con facilità attività di sequestro su server, hosting, DNS, nomi

di dominio e sequestrare o impedire l'accesso a siti anche esteri o ospitati presso paesi poco collaborativi.

Nel mondo delle criptomonete, lo scenario cambia pesantemente: vi sono nuove sfide, nuove incognite, una realtà decentralizzata dove l'unico elemento comune è la blockchain - ampiamente illustrata in questo testo - con la quale si può interagire in diversi modi e che richiede particolari cautele, proprio per la novità che rappresenta.

Il presente capitolo non vuole essere un manuale onnicomprensivo o una guida pratica passo passo al sequestro di bitcoin e criptomonete ma ha la pretesa - o quantomeno la speranza - di fornire alcune basi che si ritengono essenziali e

mostrare scenari che devono guidare l'operatore nelle scelte cui si troverà di fronte durante una eventuale attività di sequestro.

Premessa essenziale quindi è avere massima cautela nelle decisioni che vanno sempre, ove possibile, condivise anticipatamente con l'Ente per il quale si sta operando, i superiori, colui o coloro che hanno affidato l'incarico e i colleghi. L'assenza di schemi consolidati, la novità delle metodologie (non dei protocolli, che ormai hanno compiuto 10 anni) e le variabili che spesso cambiano le carte in tavola fanno sì che ciò che può andare bene in un caso possa essere rischioso in un altro e viceversa.

L’esperienza in ambito di sequestri di criptomonete è infatti molto frammentata, spesso parziale, poco condivisa e chi ha operato spesso purtroppo lo ha fatto improvvisando in base a qualche nozione acquisita dal web o dai colleghi, con il rischio quindi di creare precedenti magari anche errati che poi vengono riproposti da chi seguirà.

Per questo motivo, è importante che si scriva, si discuta, si condivida l’informazione così da validarla prima in ambito della comunità e poi in ambito scientifico, magari con pubblicazioni che, certamente, non tarderanno a venire.

1.2 TIPOLOGIE E FINALITÀ DI SEQUESTRO

Partiamo dall'ottima analisi[45] sulle tipologie di sequestro presentata presso l'Università di Pavia da Davide Gabrini, per mostrare come i requisiti di un'attività di questo genere siano quelli di togliere i beni dalla disponibilità di un indagato e porli a disposizione dell'Autorità Giudiziaria. Due vincoli che sembrano in sé scontati, ma parlando di criptomonete, potrebbero non essere semplici da realizzare, come si vedrà più avanti.

Le finalità di un sequestro "tradizionale" sono diverse – probatorio, preventivo o conservativo – e con il protocollo

bitcoin vanno rielaborate nell'ottica di un diverso approccio orientato in alcuni casi ai "wallet", in altri ai Bitcoin stessi. Il sequestro probatorio è finalizzato ad acquisire potenziali fonti di prova e l'attenzione, in tale contesto, andrebbe posta sui wallet e sulle tracce lasciate da tali sistemi su PC, smartphone o rete Internet. Il possesso dei Bitcoin in sé da parte degli inquirenti, dal punto di vista probatorio, non ha impatto mentre contano invece le evidenze digitali a corredo. La blockchain, per il resto, tiene traccia indelebile e già "cristallizzata" dei dati potenzialmente utili a provare eventuali illeciti o coinvolgimenti di soggetti in attività oggetto d'indagine.

Nel sequestro preventivo, la finalità è quella di impedire la prosecuzione di un reato e di goderne i frutti. Ha senso, in questo caso, agire direttamente sui bitcoin, quindi sulla moneta digitale, togliendola dalla disponibilità del soggetto per evitare che la possa ancora utilizzare. Detenere il wallet originale - ad esempio acquisendo il PC o lo smartphone in maniera forense - con le chiavi private ed eventualmente le tracce di accesso e utilizzo locale, non ha impatto dal punto di vista preventivo anzi, tendenzialmente risulta piuttosto ininfluente dal punto di vista del soggetto che potrebbe facilmente avere copia delle chiavi e utilizzarle anche successivamente al sequestro.

Il sequestro conservativo, similmente a quello preventivo, ha la finalità di togliere i beni nella disponibilità del soggetto per mantenerli disponibili nel tempo. Anche in questo caso, ha poco senso occuparsi del wallet - inteso come "contenitore" portafoglio sia esso software o hardware - ma è necessario orientarsi alla gestione della moneta stessa.

Si osserva quindi come, nei vari casi proposti, a differenza dei sequestri e confische tradizionali, esiste uno "sdoppiamento" che porta talvolta a concentrarsi sulla moneta in sé, talvolta sul sistema utilizzato dai soggetti per gestirla.

1.3 COME APPROCCIARSI AL MONDO VIRTUALE

Il passaggio dal sequestro tradizionale a quello virtuale, legato alla criptomoneta, non è in realtà netto come può sembrare a un primo approccio. Gli elementi che godono di fisicità, anche in ambito di cripotomonete, continuano ad avere importanza e anzi non vanno sottovalutati durante le fasi di perquisizione.

Poniamoci infatti nell'ottica di trovarci in un contesto di perquisizione e sequestro tradizionali, ad esempio presso il domicilio di un soggetto, per attività legate o meno alle criptomonete.

Se l'interesse è già fin dalle prime fasi quello di ricercare potenziali wallet, ovviamente pare scontato dedicarsi al rinvenimento di elementi che possano portare all'identificazione e accesso a portafogli elettronici. Non va però sottovalutato il caso – sempre più frequente – di sequestri e perquisizioni nei quali non è chiaro fin dall'inizio che vi potrà essere coinvolgimento e utilizzo di cripotomonete.

Vi sono elementi che vanno cercati e tenuti presenti in entrambi i casi durante la perquisizione e il sequestro presso i locali, che permetteranno poi nella fase successiva di sequestro "digitale" di agevolare le operazioni o anche di conoscere dettagli utili per esplorare gli

aspetti legati alle monete matematiche in possesso dei soggetti. In primis, andrà ricercato tutto ciò che può identificare o contenere un wallet, siano esse chiavi private, paper wallet, QR Code, seed, mnemonic o dispositivi hardware.

Uno dei metodi più diffusi per mettere da parte criptomoneta ed eventualmente nasconderla, soprattutto in passato, era quello di stampare una chiave privata su foglio di carta e ove possibile plastificare il tutto. Questo rende il pezzo una sorta di "banconota", con la differenza che rispetto al contante, chiunque ha avuto accesso alla chiave o lo ha avuto in passato (copiandola o alternativamente ricordandola a memoria) può spenderne i bitcoin

contenuti sull'indirizzo corrispondente. La comodità di un tale approccio è il fatto che non sono richiesti particolari algoritmi di generazione (vedremo in seguito i vari BIP 32, 39, 44, etc.) ma la codifica è insita nella chiave stessa, che può essere importata su qualunque wallet e i fondi prelevati, trasferiti o spesi.

Paper Wallet

Rispetto a un wallet composto da più chiavi, una singola chiave non permette la suddivisione di fondi su più indirizzi,

con riduzione quindi delle potenzialità di anonimato dei portafogli. Va comunque tenuto presente che è frequente l'utilizzo di paper wallet, soprattutto quando il soggetto intende avere massima compatibilità e garanzia di poter recuperare i propri fondi senza dover ricorrere a wallet o protocolli particolari.


Load & Verify
bitcoin

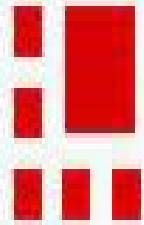
Esempio di paper wallet contenuti in un cassetto

Da non sottovalutare i wallet hardware, che hanno parvenza di periferiche USB (assomigliando spesso a pendrive o portachiavi) ma che invece possono contenere interi portafogli di numerose criptomonete, non soltanto Bitcoin.

Wallet hardware "Ledger Nano S"

Spesso, associati alla presenza di wallet hardware, si riscontrano fogli di carta contenenti le 24 parole che compongono la "mnemonic" delle master key dei vari

portafogli generati dal dispositivo.



Recovery Sheet

Confidiential document

store this document in a safe place

My recovery phrase

Write down your recovery phrase on this sheet.

24 words will be displayed on your device when it is initialized.Make sure to copy each word below,it is a full backup your account and configuration.

1.	13.
2.	14.
3.	15.
4.	16.
5.	17.
6.	18.
7.	19.
8.	20.
9.	21.
10.	22.
11.	23.
12.	24.

“Recovery sheet” contenente le 24 parole di “mnemonic”

I fogli di carta contenenti le mnemonic sono indispensabili se non è possibile ottenere il PIN di sblocco dei dispositivi hardware, in particolare perché dopo alcuni tentativi questi potrebbero resettare completamente il loro contenuto. A parte il nuovissimo Model T del wallet Ledger (che può suddividere il recovery sheet tra più fogli in modo che uno soltanto non sia sufficiente) è sufficiente trovare un foglio per ricostruire l’intero wallet e, tipicamente, chi inizializza un portafoglio hardware ne scrive i codici

di ripristino nascondendoli poi da qualche parte, in un cassetto o magari fotografandoli con lo smartphone.

Tramite le 24 parole scritte sui fogli denominati “Recovery Sheet” è infatti possibile sia rigenerare i dispositivi corrispondenti, sia creare una copia speculare del wallet in essi contenuti senza dover necessariamente disporre di un dispositivo hardware. La modalità con la quale questi portafogli generano le chiavi è definita “gerarchica deterministica” e permette di costruire un insieme di indirizzi bitcoin potenzialmente infinito a partire da un’unica master key, che gli utenti possono ricordare perché viene codificata in un insieme di parole, dette

“mnemonic”. Tramite protocolli tra i quali spiccano quelli denominati BIP 32, BIP 39 e BIP 44 che insieme ad alcuni algoritmi crittografici permettono di racchiudere in un numero prefissato di parole (in genere i wallet hardware ne richiedono 24) il “segreto” tramite il quale è possibile ricostruire un intero portafoglio, partendo da un elenco di parole.

Per fare un esempio pratico, un elenco di 24 parole come quello che segue indica – secondo il protocollo BIP 39 – un insieme di chiavi private corrispondenti a indirizzi Bitcoin sui quali potrebbero potenzialmente essere memorizzati anche milioni di dollari:

crane giant smoke enrich suspect thing trade turn media lake lemon creek engine load valid key bless bridge violin double armed arctic negative copper

Esempio di mnemonic con protocollo BIP 39

Le 24 parole sopra riportate possono essere ricordate a memoria, con non troppa difficoltà, o essere scritte appunto su foglietti o pezzi di carta. Dal punto di vista matematico, il passo successivo è la generazione del seed (il cosiddetto “seme”) derivato dalla “mnemonic”, dal quale vengono poi

generati diversi wallet per diverse criptomonete.

26bbb8cf1448986ada04e5111

Seed generato tramite protocollo BIP 39

In sostanza, un unico seed (ricavato a partire dalle 24 parole “mnemonic”) permette di generare wallet per ogni criptomoneta contemplata nel protocollo, convertendo il seed in una master key che verrà poi utilizzata per produrre le infinite chiavi che saranno parte del wallet. Infatti, volendo generare un wallet Bitcoin a partire

dalla mnemonic utilizzata nell'esempio, otterremmo una root key dalla quale poi generare migliaia di indirizzi controllabili tutti da un unico wallet.

xprv9s21ZrQH143K2eSugajrI

Root key per wallet BTC Bitcoin generato a partire dal seed BIP 39

Esistono numerose implementazioni dei protocolli di generazione wallet gerarchici deterministici, una delle più note è quella di Ian Coleman, a codice aperto e disponibile[46] gratuitamente per il download su GitHub. Per l'utilizzo, si raccomanda lo scaricamento in locale

dello script e l'avvio offline su un browser, poiché esiste sempre il rischio che vi possano essere su PC, browser o nello script stesso codici che inviino in remoto le 24 parole o le chiavi tramite esso generate. Rimane in ogni caso, per ogni software relativo alle criptomonete, il rischio che l'algoritmo di generazione sia compromesso e che quindi generi indirizzi con chiavi note o poco casuali: per questo motivo è importante verificare sempre su GitHub se ci sono stati aggiornamenti recenti al codice oppure se la versione scaricabile è datata e quindi "consolidata". Può anche essere utile cercare in rete se compaiono notizie di attacchi avvenuti al codice, al sito dello sviluppatore o all'account

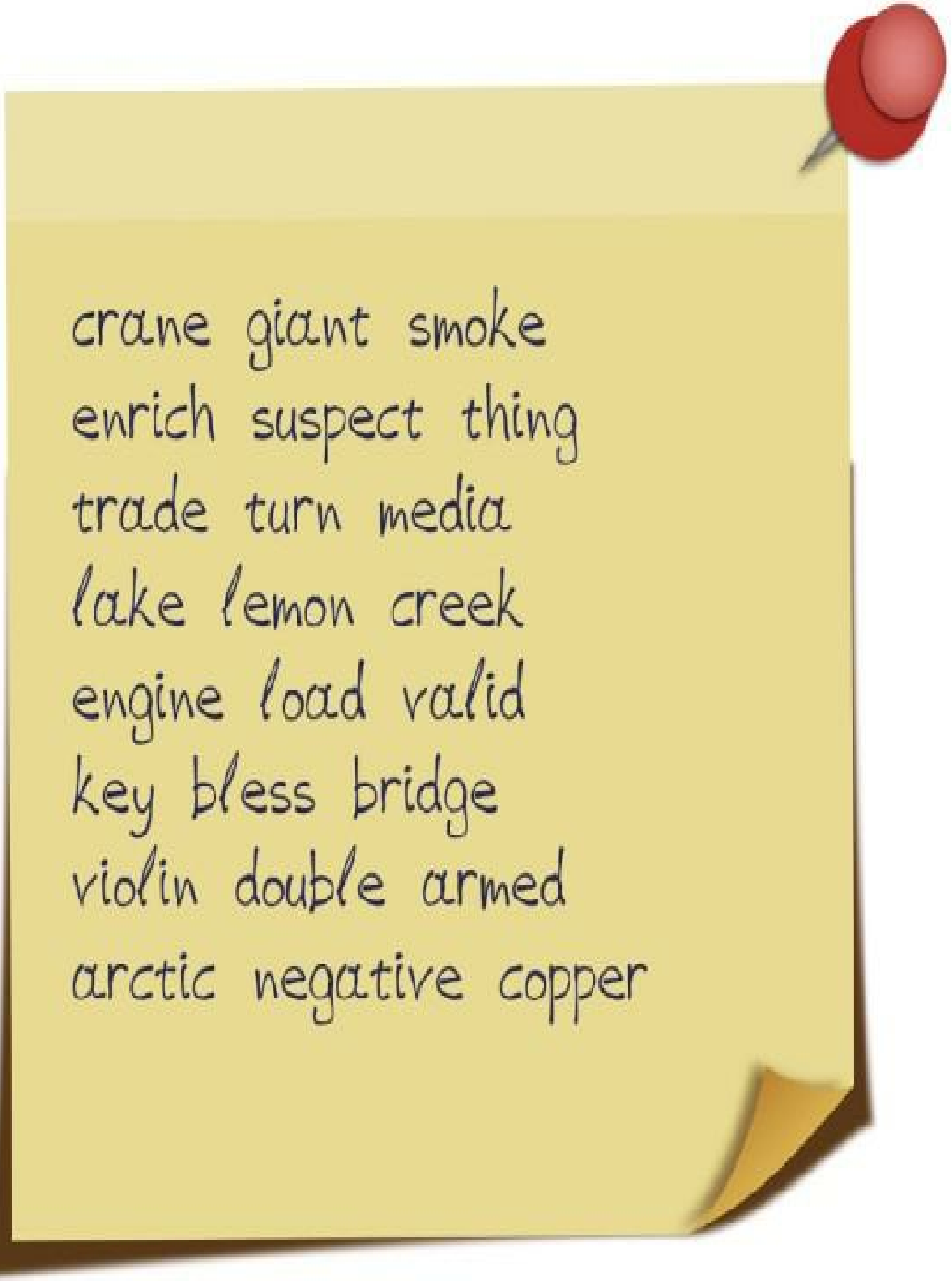
GitHub. Quando l'autore mette a disposizione la possibilità di verificare la firma del codice tramite una propria chiave PGP, è consigliabile perdere qualche minuto per accertarsi che sia tutto corretto: non è raro trovare wallet o script di generazione di chiavi e indirizzi alterati da criminali che, una volta creato il wallet e versati i fondi, procedono senza indugio a sottrarli al proprietario.

Si ricordi che le parole componenti la mnemonic sono indispensabili anche quando si ha a che fare con wallet software, dato che ormai la maggior parte dei sistemi utilizza la tecnologia gerarchica deterministica per generare i portafogli. Ad esempio, i wallet

hardware Ledger Nano S supportano seed BIP39 e BIP44, così come anche il wallet hardware Trezor. MultiBit supporta sia il BIP32 che BIP44, mentre Eidoo supporta il BIP39 e il wallet software Electrum solamente il BIP32. L'implementazione del protocollo BIP32 in base alle diverse monete è illustrata in modo tabellare su GitHub[47] mentre un ottimo schema delle compatibilità tra protocollo BIP e wallet è presente sul sito BlockPlate[48].

Ribadita l'importanza delle mnemonic, risulterà chiaro il motivo per il quale è essenziale - durante le operazioni di sequestro e perquisizione - ricercare qualunque tipo di appunto, post-it, scritto a mano o stampato, che sia a

disposizione del soggetto. La differenza rispetto a una comune password, per la quale è necessario conoscere dove possa essere impiegata, è che la "mnemonic" costituisce integralmente il wallet, non è una chiave di accesso a qualcosa di esterno (un file, un sito web, un dispositivo hardware). Importante ricordare che il numero di parole utilizzato, in base ai diversi wallet, varia in genere da 12 a 24, quindi un post-it con 12 parole potenzialmente senza senso, può con buona probabilità trattarsi di un wallet.


crane giant smoke
enrich suspect thing
trade turn media
lake lemon creek
engine load valid
key bless bridge
violin double armed
arctic negative copper

Esempio di mnemonic scritta su un post-it

Nel caso in cui vengano trovati PC o smartphone, diventa essenziale l'attività di digital forensics con la quale si procede alla ricerca di wallet software o tracce di essi, indirizzi o chiavi private. Alcuni software aiutano l'operatore nella ricerca, come ad esempio Axiom della società Magnet Forensics, con ottime funzionalità di rilevamento e velocità di analisi oppure Bulk Extractor che può essere opportunamente programmato per la ricerca tramite espressioni regolari.

Un indirizzo Bitcoin, ad esempio, può essere identificato tramite l'espressione

regolare "^[13][a-km-zA-HJ-NP-Z1-9]{25,34}$", con una ricerca tramite software basilari come "grep" oppure con strumenti avanzati come Bulk Extractor (che deve essere opportunamente configurato) o Axiom (che all'interno possiede già le espressioni regolari e le regole di carving della maggior parte dei wallet, indirizzi e chiavi). I risultati di una tale ricerca saranno tutti gli indirizzi bitcoin ancora recuperabili dalle aree del disco, anche quelle non allocate, con eventualmente tracce delle transazioni, chiavi private o wallet utilizzati dal soggetto proprietario del PC o dello smartphone.

In entrambi i casi, ma soprattutto su PC,

se possibile è consigliabile in fase di acquisizione procedere anche alla copia della memoria volatile, prima di spegnere il sistema. Si può procedere ad esempio tramite software gratuiti come FTK Imager, che permette di salvare su di un file la RAM così da poterla esaminare in seguito e da lì recuperare eventuali artefatti riguardanti attività su criptomonete.

2. STRUMENTI E METODOLOGIE PER IL SEQUESTRO DI CRIPTOMONETE

a cura di Paolo Dal Checco

Sommario: 2.1 Errori tipici – 2.2 Metodologie e strumenti suggeriti – 2.3 Creazione del Wallet – 2.4 Trasferimento della criptomoneta – 2.5 Dissequestro – 2.6 Riepilogo e sviluppi futuri.

1.1 ERRORI TIPICI

Apriamo la trattazione sugli strumenti e le metodologie consigliate per il sequestro di criptomonete con indicazioni su cosa non fare o non utilizzare in un tale contesto operativo, per evitare errori tipici in particolare di chi si approccia alla materia. Uno degli errori più banali ma anche frequenti - soprattutto fra i novizi - in ambito di attività investigativa sulle criptomonete è pensare che il possesso delle chiavi private degli indirizzi Bitcoin o del wallet (o la privazione degli stessi da parte dell'individuo oggetto d'indagine) sia sufficiente per poter configurare un sequestro e confisca.

È necessario tenere ben presente il fatto - ampiamente illustrato nel presente scritto - che chiunque possiede una copia delle chiavi private di indirizzi Bitcoin è in grado di movimentare i fondi in essi contenuti. Sequestrare quindi una copia, lasciando eventuali duplicati al soggetto sul quale è in corso una indagine, è non soltanto inutile, ma anche controproducente e persino rischioso.

Inutile perché è sufficiente che il soggetto, una volta terminato il sequestro, recuperi una copia delle chiavi da lui memorizzata in aree delle quali ha ancora disponibilità e le utilizzi per rientrare in possesso dei fondi attestati sugli indirizzi Bitcoin ad esse

corrispondenti. Lo stesso vale, ovviamente, anche per wallet gerarchici deterministici, dove invece delle chiavi private l'oggetto del sequestro sarebbe il wallet installato sul PC del soggetto oppure la mnemonic del portafoglio. Colui che ha operato il sequestro si ritroverebbe quindi con una copia delle chiavi ma nessun bitcoin presente sugli indirizzi, poiché potrebbero essere stati spostati dal soggetto successivamente al sequestro.

Non soltanto quindi il processo diventerebbe inutile, ma persino controproducente e rischioso, dato che gli operanti potrebbero essere persino accusati dall'indagato di aver in qualche modo disposto dei fondi sequestrati

essendo - a parte lui - gli unici in grado di movimentare i bitcoin gestiti tramite chiavi private o i wallet sequestrati. Questa problematica va tenuta, tra l'altro, presente anche quando il sequestro viene eseguito nella maniera corretta, che vedremo qui in seguito, poiché rimane valido l'assioma che chiunque possiede una copia delle chiavi private o della frase mnemonic è in grado di movimentare i fondi.

Altrettanto banale, ma forse talvolta meno evidente agli occhi dei novizi, è l'errore che si compie nel limitarsi a sequestrare il PC, lo smartphone o comunque il wallet del soggetto, oppure di cambiarne la password. Anche in questo caso, l'operatività del soggetto

non verrebbe pregiudicata, con il rischio di vedere svuotato un wallet prima di poter disporre dei contenuti ai fini di un potenziale sequestro di criptomoneta.

L'unico caso in cui un cambio password (attività che, talvolta, la Polizia Giudiziaria esegue in ambito di profili social network o account di posta elettronica) può essere efficace è quello di un web wallet che non permetta l'esportazione delle chiavi private. In tal caso, impedire l'accesso all'account al soggetto sarebbe equivalente a impedirgli la spendita dei fondi in esso contenuti. Ovviamente, non deve essere possibile per il soggetto eseguire un reset della password per ottenere nuovamente accesso all'account web.

In tutti gli altri casi, un cambio di password del wallet, del PC o smartphone o anche dell'accesso al web wallet sarebbe inutile perché è presumibile che chi detiene quantità rilevanti di criptomoneta abbia anche, da qualche parte, un backup delle chiavi private o quanto meno delle parole che compongono lo mnemonic del wallet. Osserviamo infatti come la totalità dei portafogli, software o hardware, nel momento in cui generano il wallet richiedono all'utente di salvare le parole componenti la mnemonic e di scriverle nuovamente, magari soltanto un sottoinsieme a campione, per dimostrare di averle effettivamente memorizzate da qualche parte. Per questo motivo,

quando si rileva la presenza di wallet hardware come il Ledger Nano o il Trezor, è altamente probabile trovare anche i fogli di carta con la "Recovery Phrase" scritta a mano dal proprietario del dispositivo oppure nello smartphone fotografie delle parole, scritte ad esempio su di un foglio poi successivamente stracciato.

L'unico caso in cui è sufficiente un sequestro "fisico" del dispositivo, per togliere al soggetto che ne è proprietario la disponibilità dei fondi, è quello in cui questi non ha memorizzato le parole delle mnemonic da nessuna parte, lasciandole quindi esclusivamente nel dispositivo. Caso piuttosto inusuale e poco probabile, poiché il rischio di

danneggiamento o perdita del dispositivo è debitamente tenuto in considerazione da chi ne fa uso e che quindi tende la quasi totalità delle volte a salvare in uno o più posti diversi le parole di mnemonic.

Riassumendo, è ora chiaro che non è sufficiente anzi è persino rischioso – per operare un sequestro di criptomoneta – limitarsi a eseguire una copia delle chiavi private, così come è inutile procedere esclusivamente tramite sequestro del PC o dello smartphone anche tramite copia forense dei sistemi. Vediamo quindi una possibile linea di condotta, con i suoi limiti ma anche con evidenti vantaggi in termini di sicurezza, responsabilità ed efficienza.

1.2 METODOLOGIE E STRUMENTI SUGGERITI

Dovrebbe essere ovvio, arrivati a questo punto, come l'unica modalità per eseguire un sequestro o confisca di criptomoneta è quella di eseguire uno spostamento di moneta, dal wallet (o dall'indirizzo) del soggetto a un wallet (oppure un indirizzo) generato ad hoc e messo successivamente in disponibilità dell'Autorità Giudiziaria. In caso di trasferimento verso exchange, ovviamente, il portafoglio potrebbe essere intestato direttamente alla Procura o al Tribunale.

Suddividiamo quindi la questione del sequestro o confisca di criptomonete in due problemi distinti: il primo è stabilire verso quale destinazione spostare la moneta (cioè creare un "portafoglio" per il deposito) mentre il secondo è quello di gestire l'attività vera e propria di trasferimento delle criptomonete. Nessuno dei due quesiti è banale e ognuno implica rischi e difficoltà che possono essere superati – o per lo meno minimizzati – attenendosi a rigidi protocolli che possono talvolta sembrare eccessivamente restrittivi ma sono in realtà cautelativi per tutte le parti in causa.

La prima possibilità, per la scelta del portafoglio, è quella di procedere con un

sequestro per equivalente, con conversione quindi delle criptomonete in moneta FIAT (euro, dollari, etc.) e trasferimento presso un conto corrente bancario intestato a Procura o Tribunale.
Passando per ora oltre questa alternativa più "semplice" (perché si esce dall'ambito della criptomoneta) affrontiamo la questione partendo dallo stabilire dove trasferire la criptomoneta che verrà sequestrata, contemplando innanzitutto la possibilità più immediata, cioè quella di depositare la criptomoneta presso un Exchange.
Va ricordato che gli Exchange non sono – per l'ordinamento giuridico italiano – equiparabili a banche, quindi gli accordi di apertura conti intestati a Procure o

Tribunali non sono ancora consolidati così come – a meno di accordi specifici – non vi è alcuna garanzia circa le somme depositate. Negli ultimi anni si sta assistendo a una regolamentazione degli Exchange che sono soggetti – come le banche – a verificare i propri clienti, a mantenere storico di quanto accade all'interno, a comunicare con le Autorità e presto, probabilmente, potranno anche fornire garanzie sui fondi. Questo significa che, in futuro, potrebbero nascere accordi specifici o, comunque, potrebbe diventare più facile gestire un conto intestato al Tribunale presso un Exchange: al momento è una soluzione con innegabili vantaggi ma anche evidenti rischi.

È comunque possibile, con l'autorizzazione dell'Autorità Giudiziaria, intestare un conto presso un exchange e trasferirvi le somme sequestrate, ma è necessario, caso per caso, valutare la disponibilità del servizio, la responsabilità di colui che viene identificato come titolare del conto, la solidità della struttura presso la quale si deposita la somma oggetto del sequestro.

La comodità, nel caso di conto aperto presso un Exchange, va infatti controbilanciata con i rischi che si corrono nel lasciare a un'azienda, sostanzialmente privata, la disponibilità di denaro e la responsabilità della conservazione delle criptomonete

sequestrate. Sono frequenti le notizie di Exchange che subiscono attacchi, furti, ammanchi o più semplicemente scompaiono chiudendo i battenti. In un caso simile, sarebbe certamente poco avveduto aver depositato le somme sequestrate presso uno di tali Exchange. Ovviamente avere un terzo "fidato" che può autorizzare la Procura o il Tribunale ad accedere ai fondi può avere vantaggi in merito alle questioni autorizzative e di accesso, ad esempio, permettendo al Tribunale di accedere senza dover dimostrare di avere le credenziali ma basandosi sulla titolarità del conto (così come può fare un privato che apre un conto in banca o persino su un Exchange) con minori rischi di perdita

credenziali e chiavi di accesso.
Contempliamo, invece, ora il caso - più comune - in cui si ritiene conveniente o comunque preferibile rimanere direttamente in ambito di criptomoneta, sequestrando quindi i Bitcoin o le monete matematiche in possesso del soggetto e trasferendole su di un wallet creato ad hoc, non presso un Exchange ma direttamente dagli operatori, che operano il sequestro, al fine di conservazione in luogo sicuro.

1.3 CREAZIONE DEL WALLET

Più complicato rispetto a utilizzare un Exchange, ma anche più sicuro, è creare

un wallet o un indirizzo Bitcoin in autonomia, così da poterne gestire il contenuto con le modalità tipiche di sequestro ormai consolidate presso l'Autorità e la Polizia Giudiziaria. Un wallet può, infatti, presentarsi in diverse forme: da foglio di carta a software; su supporto di memorizzazione o su smartphone; memorizzato su un dispositivo hardware o persino inciso su materiale ignifugo a lunga durata.

Per la creazione di un indirizzo singolo su cui versare i fondi, vi sono diverse alternative: la più immediata è quella di creare un indirizzo bitcoin tramite codice javascript, come quelli forniti dal software presente sul sito "bitaddress.org", utilizzabile online

(seppur altamente sconsigliato) oppure scaricabile in locale dal repository “github.com/pointbiz/bitaddress.org” e utilizzabile su di un PC offline. Tale script, che per essere eseguito deve essere aperto da un browser, richiede all’utente di generare “entropia” muovendo il mouse e scrivendo caratteri casuali nella textbox messa a disposizione per poter aumentare il grado di “casualità” della chiave generata.

English | Español | Français | Italiano | Deutsch
Česky | Magyar | 日本語 | 简体中文 | Русский | português

bitaddress.org

Open Source JavaScript Client-Side Bitcoin Wallet Generator

43%	43%	43%	Brain Wallet
43%	43%	Wallet Details	

Generating Bitcoin Address...
MOVE your mouse around to add some extra randomness... 134
OR type some random characters into this textbox

d9e414c81dbc28ffb1263751feea57d7b393a80da1e12949296[illegible]20dfa98b6a36
bcf819839aaaa5b36a5b7e61c00e18235d7f3a109d3300d77e26[illegible]7124ad5dc28
45d219c3ab5d101c9c069e08036ad6705d839635dfca924c4998[illegible]9d412ae7b2fc
c1caaa67dd6f309a3cbb74d66dbc9ff46a9b1d881b39f3a77ad74c295394230ea
4388119dbb15b562baa52840988148bbcd899b7[illegible]2ca8d194c14c0cfdbb1f8d6d
ce962701f9ceb8d9878731bb628560921d934a7d015[illegible]46c3541c2eda073328611d
8f39cf9c99f3b7c0642[illegible]dd002e782a28dd[illegible]2259c12b6af29[illegible]70f8c2cf693c0
2067cf3cad46c0677727a62c0bc0926cd6524a[illegible]930eebdcf228d4ee5e

⚠ ✔ … =

Donations: 1NiNja[illegible]bUnhSnTXnzRRBFIR8 nF9TGb7BN
GitHub Repository (zip)

Version History (3.3.0)
5270 5C82 B1F6 B2DB 72A0
ECBF 8749 7B9[illegible] 6597 4F5A
(PGP) (sig)

Creazione di un indirizzo tramite script BitAddress.org

Al termine della raccolta di entropia – cioè di "casualità" prodotta dagli spostamenti del mouse e dalla tastiera – il software genera una chiave privata e il relativo indirizzo bitcoin, che potrà essere utilizzato per ricevere i fondi oggetto del sequestro. La chiave privata va, ovviamente, mantenuta segreta perché è l'elemento che permette a chiunque di disporre della criptomoneta contenuta all'interno dell'indirizzo.

bitaddress.org

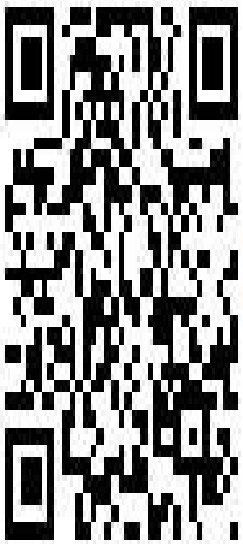
Open Source JavaScript Client-Side Bitcoin Wallet Generator

Single Wallet | Paper Wallet | Bulk Wallet | Brain Wallet

Vanity Wallet | Split Wallet | Wallet Details

Generate New Address | Print

Bitcoin Address



SHARE

1Cd7iPuQqfyNk1aPaPkWAr7s3vqncMQvCL

Private Key

SECRET

KwJmuQgUAu1gKiXnKJu4WD7Jbcj JUkImspmnypahgbtiKiaupQAQ

Chiave pubblica e privata generata tramite BitAddress

L'indirizzo generato si può stampare, scrivere, salvare in un file o PDF e la chiave privata si può cifrare così da non correre rischi che qualcuno, leggendo il paper wallet, sia in grado di spendere i fondi che verranno ivi trasferiti. In sostanza, la destinazione del versamento di criptomoneta sarà l'indirizzo che compare nel campo "SHARE", mentre ciò che dovrà essere mantenuto nascosto è la componente "SECRET" del foglio, corrispondente alla chiave privata.

È consigliabile, in ogni caso, prima di versarvi dei fondi ingenti, fare due

verifiche: la prima, di versamento di una piccola somma, per accertarsi che non venga sottratta a causa di generazione di indirizzo con poca entropia o "bachi" dovuti a errori/alterazioni nel codice; la seconda, è quella di verificare che effettivamente, dalla chiave privata generata, si ottenga l'indirizzo bitcoin sul quale si andranno a versare i fondi posti sotto sequestro. Uno dei metodi per accertare velocemente che la chiave privata sia in grado di generare autonomamente l'indirizzo bitcoin corrispondente è quello di utilizzare l'opzione "New → Transaction" del codice visionabile sul sito "coinb.in", anche in questo caso scaricando da Github su

“https://github.com/OutCast3k/coinbin/” il codice sorgente ed eseguendolo in locale su di un PC fuori dalla rete Internet. Digitando la chiave privata, si ottiene la generazione dell’indirizzo Bitcoin corrispondente e, ovviamente, tale indirizzo deve essere quello generato tramite il codice BitAddress.

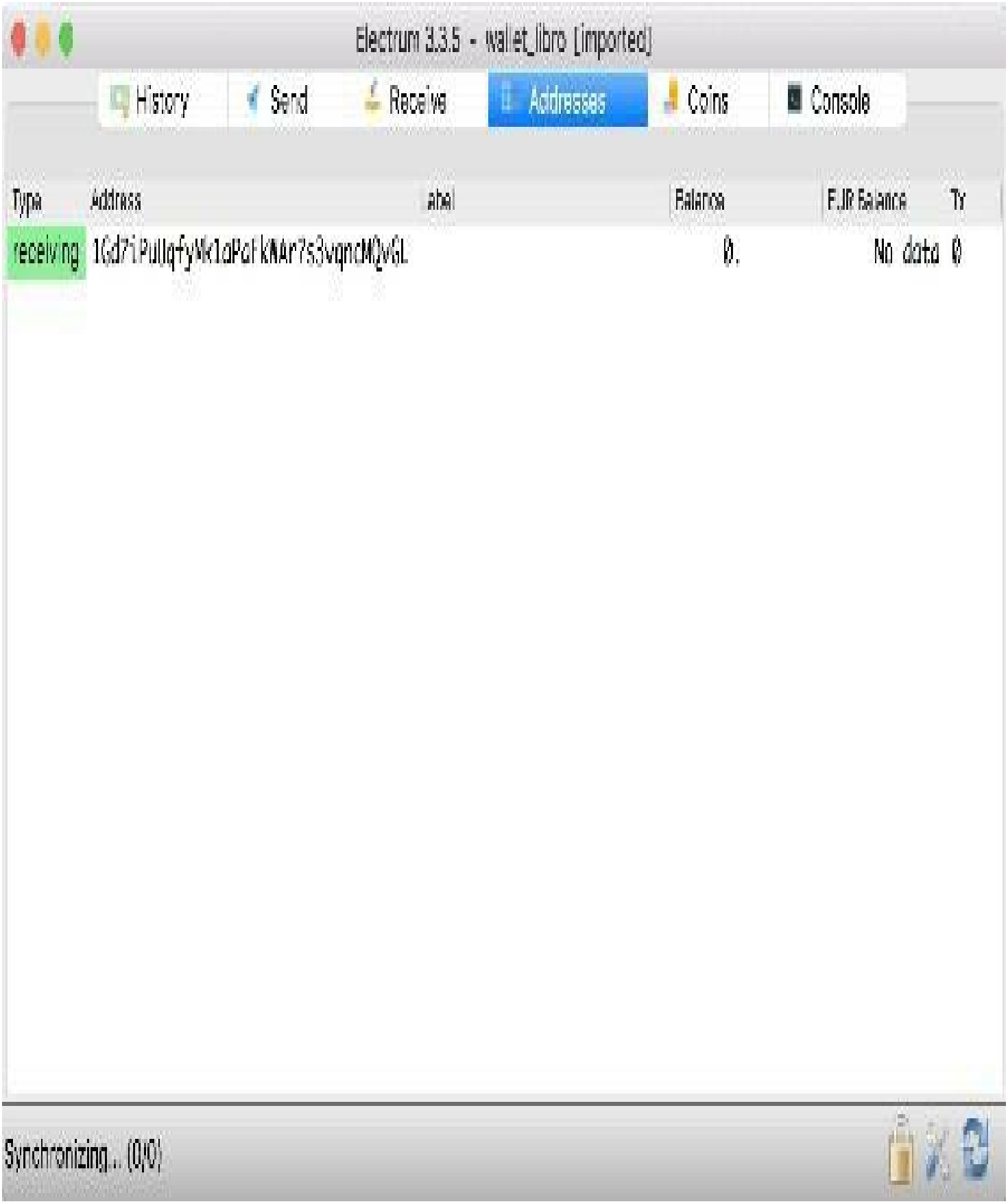
Verifica tramite Coinb.in dell'indirizzo generato tramite BitAddress

Come si può osservare dalla figura qui sopra, inserendo la chiave privata nel campo “Address, WIF Key or Redeem Script”, anche offline e senza connessione a Internet, si ottiene la conversione della stessa nell’indirizzo Bitcoin corrispondente, così da verificarne la correttezza. In alternativa, è anche possibile avviare una sessione di un client locale di wallet Bitcoin (es. Electrum) e creare un nuovo wallet con modalità “Import Bitcoin addresses or private keys” e incollare nel campo disponibile la chiave privata generata tramite BitAddress.


Electrum - Install Wizard
nport Bitcoin Addresses
Enter a list of Bitcoin addresses (this will create a watching-only wallet), or a list of private keys.
Info
KwJmuHqUAu1gKfXnKJu4WB7TbcjJUkLnapmnypahqbtEXfsupBAQ
Back
Next

Importazione su Electrum dell'indirizzo generato tramite BitAddress

Ciò che deve comparire è il wallet con l'indirizzo bitcoin, creato nella fase precedente, mostrato all'interno. Non è essenziale che Electrum sia online anzi è meglio che questo test venga fatto sempre su un sistema live (es. una distribuzione forense come Tsurugi Linux, che ha il client Electrum preinstallato) e allo spegnimento della macchina non rimanga traccia delle informazioni visualizzate durante la sessione.



Verifica tramite Electrum

dell'indirizzo generato mediante BitAddress

La presenza dell'indirizzo "1Gd7iPuUqfyMk1aPaFkWAr7s3vqncM a seguito dell'inserimento della chiave privata generata al passo precedente "KwJmuHqUAu1gKfXnKJu4WB7TbcjJ indica che l'indirizzo creato è formalmente corretto e può ricevere fondi che l'operatore sarà in grado di movimentare, ad esempio in caso di dissequestro, confisca o vendita dei beni.

Creare un singolo indirizzo, con una singola chiave privata visibile dagli operatori, può però essere un problema in caso di sequestro di somme molto

ingenti e rischio quindi di alta responsabilità data dal fatto che, in caso di fuoriuscita dei fondi sequestrati, è facile accusare chi ha avuto la possibilità di vedere (ed eventualmente appuntare, lasciare su un dispositivo, ricordare) una singola chiave privata o un singolo mnemonic.

Un rischio da non sottovalutare, infatti, per chi esegue sequestri di criptomoneta è la possibilità di poter essere, in seguito, ritenuto responsabile in eventuali episodi come la sparizione delle somme depositate. Questo può avvenire, ovviamente, soltanto se in qualche modo l'autore del sequestro è stato in grado di vedere la o le chiavi private, la mnemonic, la master key o

avere in disponibilità il wallet. Immaginiamo il caso di un operatore che crea un wallet o una chiave sul suo PC, depositando poi milioni di euro di equivalente in bitcoin su tale destinazione. Una volta stampata la mnemonic, o la chiave privata, ed esportato il wallet con la relativa password al fine del deposito degli stessi in un caveau o all'ufficio reperti del Tribunale, pur cancellando i dati dal PC, rimane sempre il dubbio che qualcosa possa essere rimasto visibile o utilizzabile.

Per questo motivo, esistono due accorgimenti per limitare la responsabilità degli operatori: uno in fase di creazione del wallet, l'altro in

fase di trasferimento. Per quanto riguarda la fase di trasferimento, la approfondiremo più avanti, ma uno dei primi consigli per limitare la responsabilità dell'operatore che esegue materialmente la creazione del wallet (non il trasferimento della moneta) è quello di non farsi fornire le chiavi private degli indirizzi, le mnemonic o master private key di generazione dei wallet deterministici o le credenziali di accesso ai wallet. Vedremo come è possibile operare come se le transazioni fossero assegni bancari: prepararli, verificarli, farli firmare al soggetto e riprenderli, mettendoli poi sul mercato senza mai dover fare la firma.

Il secondo accorgimento per limitare la

responsabilità degli operatori verte sulla scelta del wallet e sulla tipologia di protezione delle chiavi o dei segreti che proteggono i fondi. Le scelte sul tipo di wallet, nel momento in cui si decide di operare un sequestro di criptomonete, sono diverse. E' possibile riversare i fondi su wallet hardware, come le chiavette USB Ledger Nano oppure le Trezor, che hanno il vantaggio di permettere all'utilizzatore la creazione di un "backup" delle chiavi e della mnemonic, così come è possibile utilizzare wallet software, con i quali è possibile, oltre che eseguire backup, anche suddividere le chiavi tra più utenti.

La possibilità di condividere le chiavi

con altri utenti, in modo che per spendere i fondi di un wallet sia necessario mettere insieme n chiavi su un insieme massimo di k, è essenziale per la riduzione della responsabilità degli operatori. Il motivo è che questa modalità di creazione di wallet - chiamati "multisig" perché le transazioni richiedono firme multiple per poter essere valide - garantiscono che una persona da sola non possa essere decidere di (o essere costretta a) mantenere una copia della chiave utilizzata per la creazione del wallet del sequestro e utilizzarla per appropriarsi, successivamente, dei fondi. Tramite il protocollo definito "Secret Sharing", teorizzato per la prima volta nel 1979

dal ricercatore Adi Shamir, è possibile, agevolmente e con sicurezza garantita dalla matematica, condividere un segreto con più persone in modo che siano necessarie almeno n persone su k per poter svelare il segreto. Se come segreto immaginiamo un generatore di wallet deterministico, possiamo immaginare che con lo schema di Shamir - che tra l'altro è uno dei tre autori anche dell'algoritmo di cifratura asimmetrica RSA - è possibile proteggere un wallet con segreti condivisi tra più persone.

I dispositivi hardware stanno adeguandosi e tentando di supportare lo schema di suddivisione dei segreti di Shamir ma al momento si tratta di

esperimenti non ancora consolidati. Suddividere le 24 parole della frase mnemonic tra due o tre utenti non è raccomandabile (a meno che non vengano depositate le parole di tutti i gruppi) perché non garantisce la sovrapposizione di utenti che, nel modello di Shamir, possono, invece, eventualmente mancare lasciando intatto e ricostruibile il segreto.

I software di gestione dei wallet, invece, sono ormai giunti a uno stadio maturo dell'utilizzo di schemi n su k di gestione dei portafogli multisig tramite lo schema di Shamir. Ad esempio, Electrum è un ottimo wallet con cui creare un portafoglio multi signature, condividendo la responsabilità delle

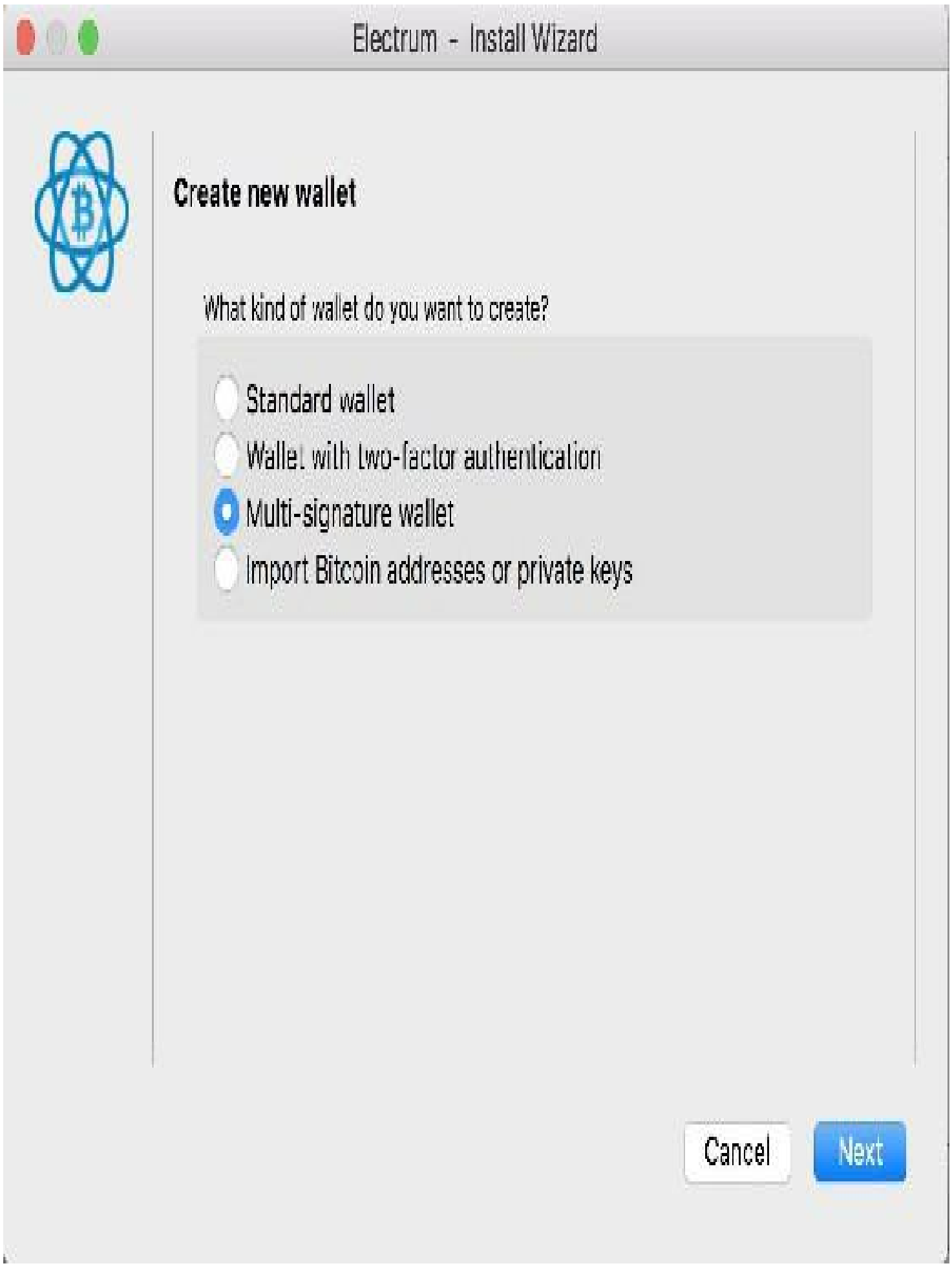
chiavi tra più soggetti. Ogni soggetto conserverà (o depositerà, in base alla scelta strategica) un foglio contenente l'elenco delle parole che compongono la frase "mnemonic", che singolarmente sono inutili ma, raggiunta la soglia minima stabilita in fase di creazione del wallet, permettono di movimentare i fondi.

È possibile sperimentare la creazione di un wallet multisig scaricando il software Electrum dal sito "electrum.org", avendo l'accortezza di verificare che il dominio digitato sia quello corretto ma, soprattutto, che il programma scaricato sia quello ufficiale firmato con le chiavi degli sviluppatori. La firma si può controllare tramite il software PGP

oppure GPG scaricando la chiave pubblica degli sviluppatori di Electrum dal sito.

Ulteriore consiglio è quello di non utilizzare un PC già inizializzato – ad esempio quello in uso quotidiano agli operatori che gestiranno il sequestro – né connesso in rete: esistono distribuzioni "live" che permettono di avviare su di un PC un sistema operativo "pulito" e che a ogni riavvio viene sostanzialmente reinizializzato, impedendo così la conservazione di malware. In ambito criptomonete, Tsurugi Linux è certamente, tra le live disponibili, una delle migliori scelte perché contiene, preinstallati, già diversi strumenti per bitcoin forensics o

gestione di wallet e indirizzi. Electrum, ad esempio, è pre-installato e funzionante sulla distribuzione Tsurugi Linux e può essere utilizzato, senza bisogno d'installazione, su di un sistema neutro e privo di malware. Ovviamente, va ricordato che allo spegnimento del PC viene perso tutto quanto è stato realizzato tramite la distribuzione, quindi è necessario salvare i wallet, stampare i codici o scrivere le mnemonic su carta per poter poi recuperare, in futuro, quanto sequestrato. Una volta installato il software, sarà sufficiente creare un nuovo wallet e impostare come tipo "Multi-signature wallet".

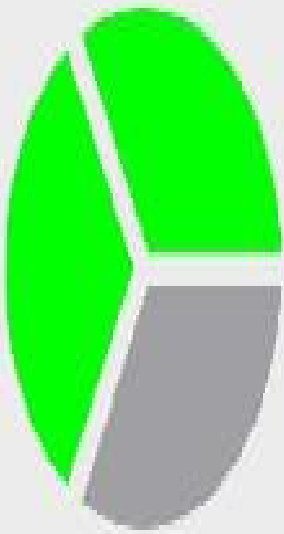

Electrum - Install Wizard
Create new wallet
What kind of wallet do you want to create?
Standard wallet
Wallet with two-factor authentication
Multi-signature wallet
Import Bitcoin addresses or private keys
Cancel
Next

Generazione di un wallet multi signature con Electrum

Per semplificare, scegliamo tre firmatari tra i quali è sufficiente la presenza di due per poter firmare, e quindi attivare, una transazione. Questo significa che un soggetto, da solo, non sarà in grado di prelevare fondi dal wallet ma, nello stesso tempo, la scomparsa di un soggetto (o la perdita delle chiavi) non impedirà ai due rimanenti di poter accedere ai bitcoin.

Electrum - Install Wizard

Multi-Signature Wallet



Choose the number of signatures needed to unlock funds in your wallet:

From 3 cosigners

Require 2 signatures

Back Next

Generazione di un wallet multi signature 3 su 2 con Electrum

A questo punto, ogni firmatario deve creare un nuovo “seed” ottenendo così una “Master public key” da condividere con i firmatari. Si può condividere anche il seed, ma diventa più complicato, in tale maniera, fare in modo che nessun utente entri in contatto con più di una chiave, così da non poter essere in grado di firmare transazioni.

In sostanza, ogni firmatario deve conservare un elenco di parole come questo: “edit lunar final harbor right brief guess angle term mention reason expect”. Le parole possono andare da un

minimo di 12 a un massimo a piacere: in genere si ritiene che 24 parole rappresentino un alto grado di sicurezza. Mentre normalmente queste 12/24 parole rappresentano un wallet, in questo caso rappresentano una componente necessaria per poter ricostruire il wallet e firmare le transazioni per portare verso l'esterno i fondi ivi attestati, ma singolarmente risultano inutili, al punto che ogni firmatario non può essere ritenuto responsabile se non insieme agli altri.

Un accorgimento che sembra banale, ma che può sollevare ulteriormente da rischi e responsabilità, è quello di creare il wallet e depositarlo in un posto sicuro prima di operare il sequestro.

Caratteristica peculiare delle criptomonete è il fatto che per depositare valori all'interno di un wallet non è necessario avere con sé il wallet, sia esso hardware, software o chiavi/mnemonic scritte su un foglio. Il rischio di furto e "intercettazione" del vettore che deposita fisicamente il wallet in location sicura viene altamente ridotto se questa operazione viene fatta prima del sequestro perché, in caso di furto, il sequestro ovviamente non verrà disposto sull'indirizzo le cui chiavi private siano state sottratte. In sostanza, nel momento del sequestro, gli operatori avranno a disposizione gli indirizzi su cui depositare o eventualmente anche un intero wallet, composto da più indirizzi,

ma creato caricando indirizzi pubblici oppure a partire da XPUB e contenente solamente indirizzi pubblici, nessuna chiave. In questo modo si divide anche "fisicamente" la fase di creazione dei wallet, con il deposito in luogo sicuro, dalla fase di trasferimento della criptomoneta che, quindi, può avvenire con la massima sicurezza.

Una nota di colore: è capitato in diverse occasioni che tale procedimento non venisse opportunamente compreso e fosse considerato "anomalo" poiché si ha la tendenza a credere che un wallet chiuso in una cassaforte nel caveau di una banca non possa ricevere fondi. E' sufficiente, in tal caso, chiarire come una volta creato il wallet, l'elemento

essenziale è poter disporre degli indirizzi su cui versare la somma sequestrata e il saldo non viene inserito "fisicamente" nel wallet ma il tutto viene scritto - come più volte ribadito nel corso del presente lavoro - nella blockchain, che è accessibile da ovunque e da chiunque. Ovviamente, per la spendita dei fondi sequestrati (o l'eventuale dissequestro) diventa sì necessario accedere fisicamente al wallet (se si tratta di hardware) o ai fogli di carta o documenti informatici su cui sono state scritte le chiavi private, le mnemonic o le credenziali di accesso ai portafogli.

Vediamo, quindi, la fase altrettanto delicata del trasferimento della

criptomoneta che, come accennato poc'anzi, suggeriamo di operare successivamente al deposito del wallet in luogo sicuro, dopo averne opportunamente testato la sicurezza, il funzionamento e la disponibilità delle chiavi.

1.4 TRASFERIMENTO DELLA CRIPTOMONETA

Il trasferimento della criptomoneta verso il wallet del sequestro è un altro argomento molto complesso, con rischi e conseguenze per tutto il procedimento, se non viene gestito con la dovuta attenzione.

Come anticipato, la prima raccomandazione per gli operatori è quella di non entrare in contatto con le chiavi private del soggetto al quale dovranno essere sequestrate o confiscate le criptomonete. Il motivo è sottile: nel momento in cui un operatore viene ad avere a disposizione le chiavi private di un wallet, è in grado di spostare i fondi ivi contenuti ma lo è anche il proprietario, o terzi che eventualmente avessero a disposizione le chiavi. Se successivamente alla consegna delle chiavi agli operatori - ma prima delle operazioni di effettivo spostamento dei fondi - qualcuno dovesse svuotare il portafoglio, è chiaro il rischio che la responsabilità venga estesa anche agli

operatori stessi. Essi, infatti, avrebbero potuto - mettendosi nei panni di una eventuale accusa da parte del proprietario del wallet - comunicare le chiavi a terzi e sottrarre così le somme depositate nei portafogli prima del sequestro. Poiché per spostare criptomonete non è necessario essere in una precisa sede o posizione geografica né avere una "password" di un account con accesso controllato e univoco (come può avvenire, però, per i web wallet custodian che non forniscono backup delle chiavi) è chiaro che chiunque può svuotare un portafoglio o un indirizzo del suo contenuto di criptomonete in qualunque momento e ovunque si trovi, a patto ovviamente che abbia una copia

delle chiavi.

Ci sono ovviamente situazioni nelle quali gli operatori devono per forza entrare in contatto con le chiavi, le credenziali o wallet fisici o software e in tal caso vanno comunque presi tutti gli accorgimenti possibili per proteggere il contenuto di quanto acquisito, almeno fino al momento del sequestro.

Nel caso, invece, in cui fosse possibile ottenere la collaborazione del soggetto che detiene la criptomoneta che sarà oggetto di sequestro, è di strategica importanza utilizzare un sistema di creazione e firma delle transazioni che lo coinvolga senza richiedere l'accesso alle sue chiavi o credenziali.

Il metodo consigliato in questo caso, già

anticipato poco addietro, consiste nel predisporre le transazioni utilizzando un wallet "watch only", cioè in grado di vedere gli indirizzi, preparare transazioni ma non in grado di firmarle. Anche questo aspetto - come tanti nel mondo Bitcoin/Blockchain - è spesso ostico da comprendere. Chiunque è in grado di predisporre una transazione valida che sposti criptomoneta fuori da un wallet. Solamente chi ha a disposizione le chiavi private, o la frase mnemonic, sarà però in grado di firmare tale transazione e renderla così "valida" per la immissione sulla rete. Il terzo passo infatti, cioè la distribuzione della rete della transazione per renderla "attiva", può essere nuovamente fatto da

chiunque, a patto che la transazione sia firmata e valida.

Nel caso in cui non sia stata fornita la password del wallet, esiste sempre la possibilità di forzare il portafoglio con un brute force attack tentando di accedervi con tutte le password che riteniamo plausibili. Si potranno, quindi, utilizzare wordlist provenienti dal dizionario della lingua parlata dal soggetto, le liste che si trovano online con le password più utilizzate o anche procedere per tentativi casuali, per quanto quest'ultima possibilità raramente abbia successo e sia preferibile una wordlist, anche lunga oppure generata in base a criteri specifici.

Un ottimo strumento in grado di eseguire un attacco di brute force sulla maggior parte dei wallet software a disposizione è BTCRecover, scaricabile gratuitamente dal sito github.com/gurnec/btcrecover. La configurazione avanzata permette di preparare opportunamente un elenco di password da testare (in genere definito "password list") specificando le combinazioni con le quali le parole devono essere mescolate tra di loro, anche eventualmente utilizzando contatori, omettendo lettere o copiandone altre in particolari posizioni, forzando il sistema a tentare anche errori comuni come inversione di lettere ma anche mappatura di caratteri

tipicamente utilizzati nelle password al posto di altri, come il dollaro ‘$’ al posto della lettera ‘S’, il numero ‘4’ al posto della lettera ‘A’ e così via, così da poter “indovinare” anche password del tipo “p4$$w0rd”.

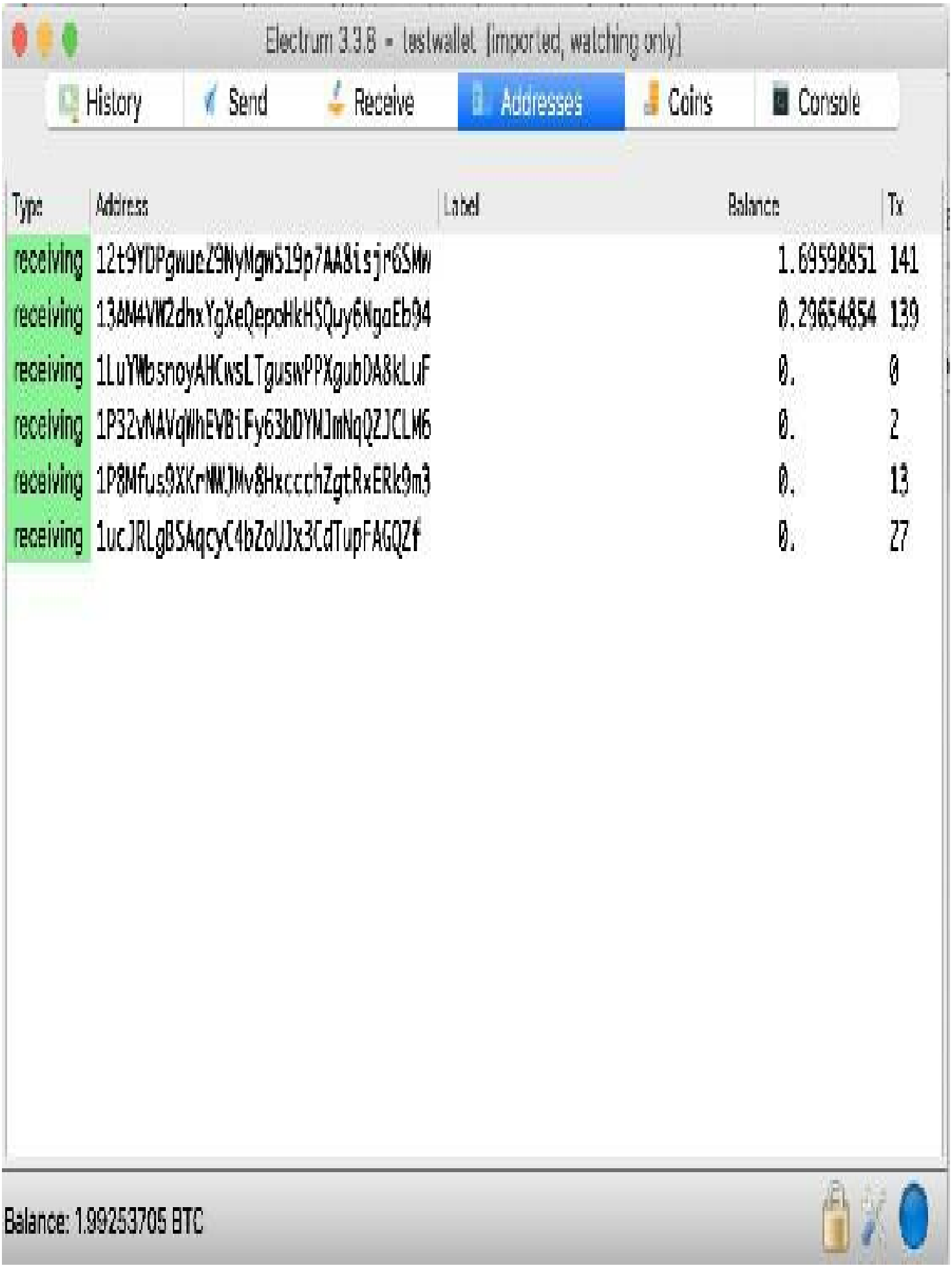
Nella figura seguente, mostriamo come un wallet di Electrum sul quale è stata impostata una delle password più utilizzate e rinvenibili in qualunque elenco online, può essere forzato in meno di un secondo.

```
qwert@tsurugivm:~/.electrum/wallets$ btcrecover.py --wallet default_wallet --pas
swordlist pwdlist.txt
Starting btcrecover 0.17.10 on Python 2.7.12 64-bit, 21-bit unicodes, 64-bit int
s
Wallet difficulty: 1024 PBKDF2-SHA512 iterations + ECC
Using 2 worker threads
3 of 25 [#####.....................................] 0:00:00, ETA:  0:00:00
Password found: '12345678'
qwert@tsurugivm:~/.electrum/wallets$ head pwdlist.txt
123456
123456789
qwerty
12345678
111111
1234567890
1234567
password
123123
987654321
qwert@tsurugivm:~/.electrum/wallets$
```

Forzatura della password di un wallet Electrum tramite BTCRecover

Ovviamente, nel caso in cui si dimostri necessario eseguire un attacco di forza bruta alla password del wallet di un soggetto, possiamo aspettarci con buona probabilità che egli - o chi per esso - abbia già provveduto a movimentare i fondi prima dell'attività di sequestro, lasciandoci un portafoglio vuoto. Anche in questo caso, però, non tutto è perduto. Risulta, infatti, possibile innanzitutto monitorare il wallet per verificare se e quando sono stati fatti prelievi, così da identificare i periodi e collegarli eventualmente ad attività svolte dal soggetto.

Prendiamo come esempio questo wallet, generato prelevando alcuni indirizzi dal sito Bitcoin Abuse, dove vengono segnalati i dettagli dei portafogli asseritamente legati ad attività illecite in ambito di criptomoneta.


Electrum 3.3.8 - testwallet [imported, watching only]
History
Send
Receive
Addresses
Coins
Console
Type
Address
Label
Balance
Tx
receiving 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw 1.69598851 141
receiving 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 0.29654854 139
receiving 1LuYWbsnoyAHCwsLTguswPPXgubDA8kLuF 0. 0
receiving 1P32vNAVqWhEvBiFy63bDYMJmNqQZJCLM6 0. 2
receiving 1P8Mfus9XKrMWJWv8HxccchZgtRxERk9m3 0. 13
receiving 1ucJRLgBSAqcyC4bZoUJx3CdTupFAGQZf 0. 27
Balance: 1.99253705 BTC

Visualizzazione di un wallet e del saldo attuale degli indirizzi su Electrum

Poniamoci nella situazione nella quale il wallet sia stato sequestrato e ci sia voluto del tempo per ottenere le credenziali di accesso, ricavate ad esempio tramite brute force di un file contenente gli indirizzi rinvenuto sul PC di un indagato. Caricando l'intero wallet (o i singoli indirizzi, singolarmente) su Electrum, possiamo osservare il saldo dell'intero portafoglio (1.99253705 BTC nell'esempio) ma anche dei singoli indirizzi. Ad esempio, l'indirizzo _6SMw ha quasi 1.7 BTC ancora presenti mentre altri quattro sono

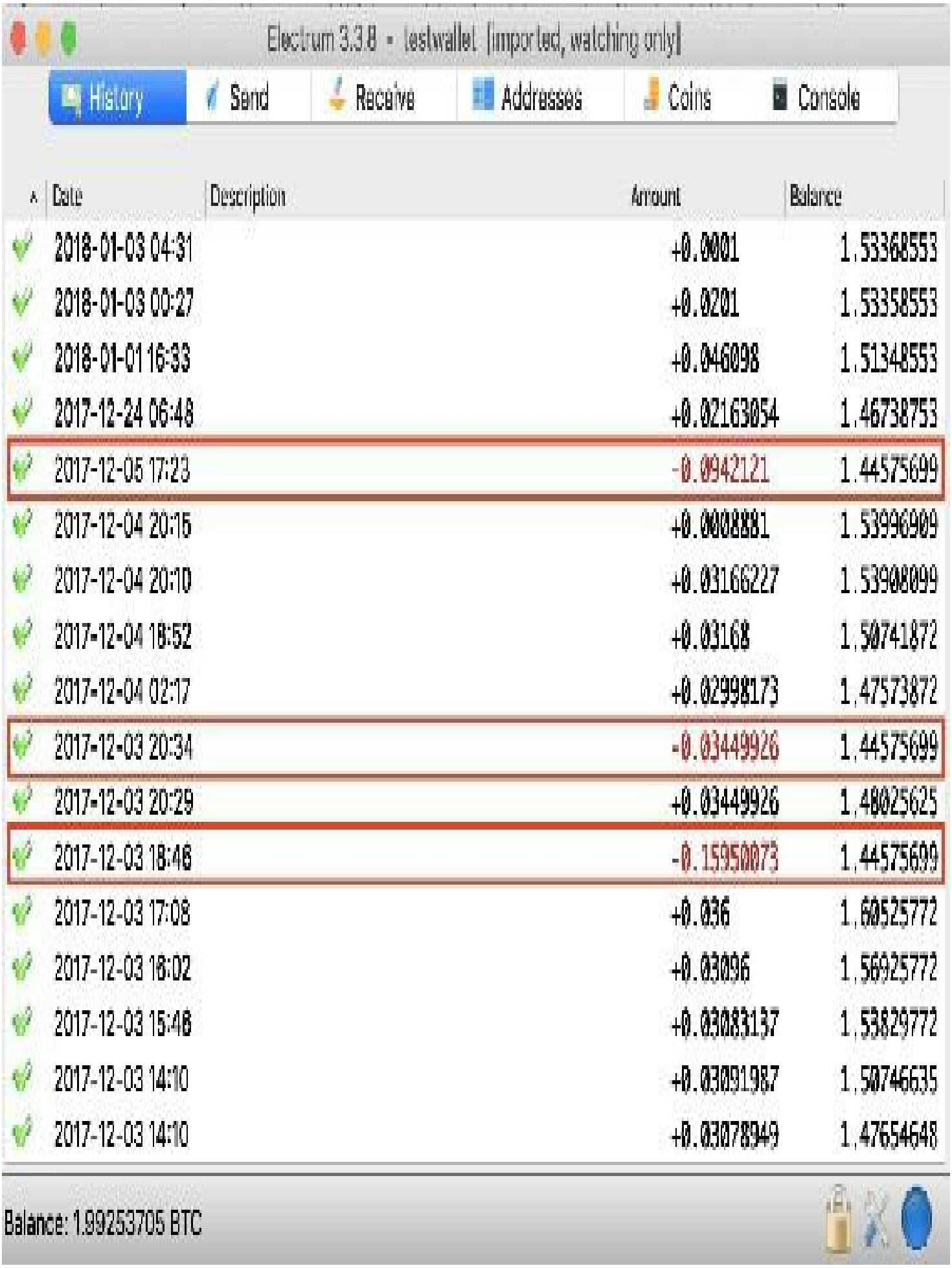
completamente vuoti e tre di questi in passato hanno avuto movimentazioni mentre uno non è mai stato utilizzato, né per ricevere né per inviare criptomoneta.

Il dettaglio che interessa, in questo caso, è lo storico delle movimentazioni, che su Electrum possiamo visionare semplicemente selezionando il tab “History”.


Electrum 3.3.8 - testwallet [imported, watching only]
History
Send
Receive
Addresses
Coins
Console
Date
Description
Amount
Balance
2018-08-10 17:12 +0.00000546 1.99253705
2018-08-09 02:36 +0.00000546 1.99253159
2018-07-19 00:23 +0.003 1.99252613
2018-07-01 18:52 +0.04804808 1.94852613
2018-05-22 13:02 +0.00000888 1.94147805
2018-05-19 12:57 +0.00001 1.94146917
2018-04-22 09:10 +0.0584 1.94145917
2018-04-15 17:46 +0.00011798 1.88305917
2018-04-08 00:00 +0.00006406 1.88294119
2018-04-07 23:54 +0.00006408 1.88287713
2018-04-01 23:43 +0.00012324 1.88281305
2018-03-27 06:24 +0.00017742 1.88268981
2018-01-16 13:45 +0.00288652 1.88251239
2018-12-07 11:55 +0.093 1.87962587
2018-12-06 23:16 +0.00013005 1.78662587
2018-10-05 09:31 +0.0459 1.78649582
2018-07-10 02:23 +0.00143988 1.74059582
Balance: 1.99253705 BTC

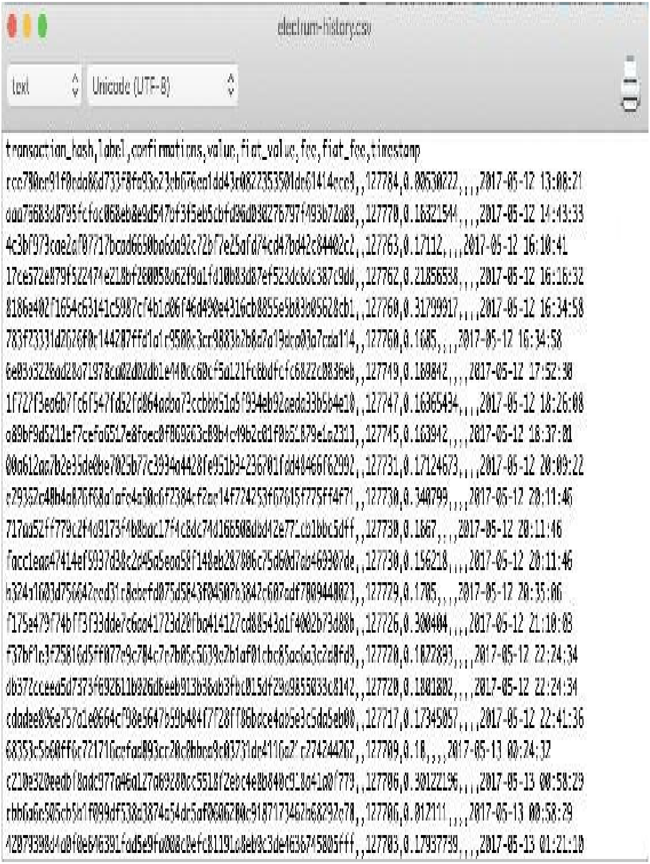
Visualizzazione dello storico delle transazioni di un wallet su Electrum

Scopriamo così che, per quanto ancora utilizzato per ricevere criptomoneta, nulla è uscito dal wallet nell'ultimo anno. Risalendo indietro con lo storico delle transazioni, si osserva come le ultime transazioni in uscita risalgono a dicembre 2017 e sono evidenziate in rosso nell'output di Electrum.


Electrum 3.3.8 - testwallet [imported, watching only]
History
Send
Receive
Addresses
Coins
Console
Date
Description
Amount
Balance
2018-01-03 04:31 +0.0001 1.53368553
2018-01-03 00:27 +0.0201 1.53358553
2018-01-01 16:33 +0.046098 1.51348553
2017-12-24 06:48 +0.02163054 1.46738753
2017-12-05 17:23 -0.0942121 1.44575699
2017-12-04 20:15 +0.0008881 1.53996909
2017-12-04 20:10 +0.03166227 1.53908099
2017-12-04 18:52 +0.03168 1.50741872
2017-12-04 02:17 +0.02998173 1.47573872
2017-12-03 20:34 -0.03449926 1.44575699
2017-12-03 20:29 +0.03449926 1.48025625
2017-12-03 18:46 -0.15950073 1.44575699
2017-12-03 17:08 +0.036 1.60525772
2017-12-03 16:02 +0.03096 1.56925772
2017-12-03 15:48 +0.03083137 1.53829772
2017-12-03 14:10 +0.03091987 1.50746635
2017-12-03 14:10 +0.03078949 1.47654648
Balance: 1.99253705 BTC

Evidenziazione delle transazioni di spesa di un wallet tramite Electrum

A fini investigativi, può essere utile - per documentare ad esempio un'attività di monitoraggio - esportare lo storico degli indirizzi del wallet in formato CSV, così da poterlo importare in un foglio di calcolo. Il comando "Wallet → History → Export" permette di scegliere un file nel quale riversare l'intera storia di transazioni del wallet caricato su Electrum, ottenendo un file come il seguente, importabile in ulteriori fogli di calcolo per successive analisi.




```
transaction_hash,label,confirmations,value,fiat_value,fee,fiat_fee,timestamp
ecc790ec91f0eda86d733f8fa93c23eb676ca1dd43c0822353501dc61414ecc9,,127784,0.00530222,,,,2017-05-12 13:08:21
daa75683d8795fcfac068eb8e9d547bf3f5eb5cbfd96d030276797f493b72d89,,127770,0.16321544,,,,2017-05-12 14:43:33
4c3bf973cae2af07717bcad6650ba6da92c72bf7e25afd74cd47bd42c84402c2,,127763,0.17112,,,,2017-05-12 16:10:41
17ce572e879f52247e218bf26005806f9a1fd10b83d87ef523dc6dc387c9dd,,127762,0.21856538,,,,2017-05-12 16:16:32
8186e402f1654c63141c5987cf4b1d06f46d490e4316cb8855e5b83b05628cb1,,127760,0.31799917,,,,2017-05-12 16:34:58
783f23331d2626f0c144207ffd1a1c9500c3cc9883b2b8a7a19dca03a7cda114,,127760,0.1685,,,,2017-05-12 16:34:58
6e03a3226ad28a71978ca02d02db1e440cc60cf5a121fc8bdfcfc6822c0836eb,,127749,0.169842,,,,2017-05-12 17:52:30
1f727f3ea6b7fc6f547fd52fd864adba73ccbbb51a5f934eb92aeda33b5b4e20,,127747,0.16365434,,,,2017-05-12 18:26:08
a89bf9d5211ef7cefa6517e8faec0f069263c89b4c49b2c01f0b51079e1a2313,,127745,0.163942,,,,2017-05-12 18:37:01
00a612aa7b2e35de0be7025b77c3934a4428fe951b34236701fdd48466f62992,,127731,0.1712467З,,,,2017-05-12 20:09:22
e29352c40b4a876f68a1afc4a50c6f2384cf2ae14f724253f67615f775ff4f71,,127730,0.340799,,,,2017-05-12 20:11:46
717ad52ff779c2f4d9173f4b8bac17f4c8dc74d166508dbd42e77cb1bbc5dff,,127730,0.1667,,,,2017-05-12 20:11:46
facc1eaa47414ef5937d38c2d45a5eaa58f148eb287006c75d60d7ab469307de,,127730,0.156218,,,,2017-05-12 20:11:46
b324a1603d75b642ced31c8cbefd075d5843f04507b3842c607adf7009440021,,127729,0.1705,,,,2017-05-12 20:35:06
f175e479f74bff3f33dde7c6aa41723d20fba414127cd8543a1f4002b73d88b,,127726,0.300404,,,,2017-05-12 21:10:03
f37bf1c3f25816d5ff077e9c704c7c7b05c5639c2b1af01cbc85ac6a3c2a0fd9,,127720,0.1022893,,,,2017-05-12 22:24:34
db372cceed5d7373f692611b026d6eeb913b36ab3fbc015df29a9855033c8142,,127720,0.1801802,,,,2017-05-12 22:24:34
cdadee896e757a1e0664cf98e5647b59b4841f728f186bdce4ab5e3c5da5eb00,,127717,0.1734057,,,,2017-05-12 22:41:36
68353c5b60ff6c72171 6ccfad093cc20c0bbca9c03731dc4116a2cc27424426 2,,127709,0.10,,,,2017-05-13 00:24:32
c210e320eedbf8adc977a46a127a69280cc5518f2ebc4e8b840c9130410a0f779,,127706,0.30122196,,,,2017-05-13 00:58:29
cbb6a6c505cb5a1f099df538a3874a54dc5af0606200c9187173462b68292c70,,127706,0.012111,,,,2017-05-13 00:58:29
4207939804a0f0e6f6391fad5e9fa008c0efc8119La8eb9c3de463674580 5fff,,127703,0.17937739,,,,2017-05-13 01:21:10
```

Esportazione delle transazioni di un wallet tramite Electrum

Arrivati infine al dunque, cioè al momento in cui eseguire effettivamente le transazioni di trasferimento della criptomoneta verso l'indirizzo o gli indirizzi creati per il sequestro, ci troviamo di fronte a due alternative. Nel caso in cui abbiamo a disposizione le chiavi private o le credenziali di accesso a un wallet sia esso fisico, hardware o web, si può procedere come meglio si crede con la movimentazione. Documentando il più possibile quanto si andrà a svolgere, ad esempio tramite videoregistrazione del desktop e

acquisizione del traffico di rete, si può importare il portafoglio su un client come Electrum, impostare la transazione di trasferimento, firmare e trasmettere sulla rete Bitcoin il risultato. La trasmissione sul network può essere attivata direttamente all'interno del client utilizzato (se si è online, connessi alla rete) oppure eseguita a mano copiando la transazione firmata su siti come coinb.in/#broadcast oppure www.blockchain.com/btc/pushtx, così da tracciare anche il momento in cui viene lanciato il broadcast. Il consiglio è quello di utilizzare una combinazione di wallet Bitcoin (da mantenere offline configurandovi un portafoglio watch-only) e un PC online dal quale eseguire

solamente il broadcast delle transazioni di spostamento verso i wallet del sequestro. In questo modo, le chiavi private saranno sempre al sicuro (ad es. nel caso di infezione da malware sul PC utilizzato) mentre le transazioni firmate (quindi non più modificabili) saranno le sole a essere maneggiate su un PC connesso alla rete.

Allo stesso modo, se non si hanno a disposizione le chiavi private perché si è scelto l'approccio di non entrarne in contatto lasciandole in disponibilità del soggetto che è disposto a cooperare, l'approccio è simile. Il consiglio è sempre quello di operare - o far operare il soggetto - su due ambienti separati, uno connesso alla rete (quindi a rischio)

e uno sconnesso dalla rete. Gli operatori potranno, in tal caso, creare le transazioni utilizzando un wallet "watch only" di sola visualizzazione (quindi senza chiavi private) e salvarle in un file TXT, ovviamente non firmate. Il file dovrà quindi essere consegnato al soggetto che, nel suo sistema preferibilmente offline, procederà alla firma ma non alla trasmissione sulla rete Bitcoin, a meno che il tutto non avvenga sotto la stretta supervisione degli operatori. Il motivo è che, prima della trasmissione, è necessario che qualcuno verifichi che le transazioni firmate dal soggetto siano esattamente quelle che gli sono state fornite e che, in caso di malintenzionati, potrebbero anche essere

modificate, ad esempio, inserendo un diverso indirizzo di destinazione. In alternativa, le transazioni possono essere preparate dal soggetto, se disposto a collaborare, e operare l'attività sotto la supervisione degli operatori. Una volta firmate le transazioni, dovranno essere consegnate agli operatori che le andranno a verificare, ad esempio importando le stesse su un'istanza di Electrum oppure analizzandole con gli script scaricabili dal sito Coinb.in. A seguito di verifica circa la correttezza delle transazioni firmate dal soggetto, si potrà procedere alla diffusione delle stesse sulla blockchain inviandole tramite un qualunque servizio di broadcast di

quelli segnalati sopra oppure importando le stesse in Electrum e inviandole attraverso la rete di nodi Bitcoin ai quali è connesso.

Una nota sulle commissioni di transazione, le cosiddette “transaction fee”: è consigliabile non essere troppo parchi altrimenti si corre il rischio di dover attendere ore (se non giorni, nei periodi “peggiori”) per poter vedere le transazioni andate a buon fine e quindi poter confermare che il sequestro è stato operato correttamente.

1.5 DISSEQUESTRO

La fase di dissequestro ripercorre, in

sostanza, all'inverso quella della creazione del wallet e poi del trasferimento delle somme sequestrate. In sostanza, invece di creare nuovamente il wallet è necessario accedervi, risolvendo ad esempio gli algoritmi matematici di Shamir per generare un unico wallet a partire da chiavi distinte.

Se si è utilizzato un wallet hardware, depositato ad esempio in un caveau di una banca o una cassetta di sicurezza, è necessario utilizzare un eventuale PIN di accesso per lo sblocco e l'accesso alla firma con le chiavi private in esso contenute. In base al tipo di hardware potrebbe essere necessario rompere eventuali sigilli (si pensi ad esempio alle chiavi Opendime) o inserire PIN

tramite pulsantiera, con la cautela di non inserirne di errati per non causare la cancellazione delle chiavi private contenute nella smartcard.

Se è stato creato un backup delle chiavi o delle parole mnemonic, si può considerare l'alternativa di utilizzare quelle per la configurazione di un nuovo hardware (cosa essenziale, ad esempio, in caso di danni fisici al dispositivo depositato) o anche, tramite software, la ricostruzione del portafoglio su di un PC, ovviamente sconnesso dalla rete per finalità di sicurezza.

Una volta abilitati all'accesso alle chiavi o al loro utilizzo, si potrà procedere con il trasferimento dei fondi verso il wallet dell'avente diritto o, in

caso di confisca e vendita, dell'acquirente. Tale fase appare altrettanto delicata quanto quella del sequestro, con il vantaggio però di poter operare senza necessità di ausilio da parte di un eventuale soggetto terzo detentore delle chiavi e di poter gestire il tutto in ambiente sicuro e controllato, possibilmente con tempo sufficiente per pianificare le eventuali verifiche che durante le fasi di sequestro spesso procedono invece a ritmi serrati.

Così come in fase di sequestro, si raccomanda di verbalizzare il più possibile, eventualmente registrando lo schermo del PC e acquisendo il traffico di rete del sistema, così da avere una sorta di "report" forense delle attività

svolta, utile soprattutto se qualcosa non dovesse andare come previsto. Tutto ciò che viene raccolto e registrato può poi essere compresso in un archivio ZIP, cui apporre data certa (es. tramite timestamp Infocert, Namirial, Aruba, etc.) o persino utilizzando la blockchain stessa tramite protocolli come Open Timestamp. Infine si raccomanda, così come consolidato in ambito di informatica forense, il calcolo dei valori hash MD5 ed eventualmente anche SHA1/SHA256 sull'archivio, con verbalizzazione cartacea dei risultati, in particolare se non è possibile apporre data certa tramite i canali ufficiali o la blockchain.

Una nota, forse per taluni scontata,

quella delle commissioni di transazione che in diversi casi possono essere anche alte e vanno tenute in considerazione sia nella fase di sequestro sia in quella di dissequestro o vendita. In sostanza, sequestrare 10 Bitcoin e dissequestrarli avrà un costo che dipenderà dal periodo, dalla concorrenza, dai minatori ma che andrà considerato come importo che andrà a ridurre la cifra sequestrata e, ulteriormente, quella dissequestrata.

1.6 RIEPILOGO E SVILUPPI FUTURI

Come si sarà percepito, l'operazione di sequestro di cripotomonete è un'attività

che presenta rischi, richiede pianificazione e rispetto di vincoli di sicurezza, dalla fase di creazione del wallet di destinazione a quella del trasferimento, fino all'ultimo passo consistente nel dissequestro o la confisca e vendita delle monete matematiche.

Nel testo sono stati presi come riferimento i bitcoin e il loro protocollo, sul quale numerose operazioni sono ormai consolidate e gli strumenti divenuti altamente affidabili. Esistono ovviamente decine di altre criptomonete di uso comune, centinaia di uso ristretto a cerchie di utenti e migliaia presenti sul mercato, magari usate poco o soltanto in tempi passati. In base al valore dei

wallet, potrà essere necessario operare sequestri su cryptocurrency rare, dismesse o per le quali non esistono, ad esempio, software con capacità di creazione di wallet multisig. In alcuni casi si dovrà improvvisare, valutare la soluzione migliore tra una singola chiave, un wallet software o hardware, una eventuale condivisione di segreti realizzata con tecniche non standard (es. suddivisione della mnemonic in gruppi con sovrapposizione sufficiente a tollerare la perdita di una parte dei segreti) o persino l'apertura di un wallet presso un Exchange.

La storia è ancora da scrivere, in ambito di criptomonete: benché siano ormai utilizzate da anni in modo massivo, esse

rappresentano ancora un argomento di nicchia, con rapide evoluzioni, svolte impreviste, novità che rendono l'argomento uno fra i più interessanti in ambito investigativo ma anche uno dei più complessi. La speranza è che, con i contributi tecnici e Giuridici delle Forze dell'Ordine, dei Consulenti, dei Giudici, dei Pubblici Ministeri, delle Università e dei ricercatori, si arrivi a creare uno "standard" condiviso di procedure, strumenti e metodologie per imparare dal passato e prepararsi al futuro.

CONCLUSIONI

La presente opera, a parere di chi scrive, rappresenta un punto di partenza, senza avere ambizione di aver trattato in maniera completa ed esaustiva ogni singolo aspetto, per tutti coloro che hanno intenzione di approcciare al vasto e ancora sconosciuto mondo delle criptomonete.

Si ritiene inoltre utile per approfondimenti operativi e suscitare nuovi spunti di riflessione e approfondimenti ulteriori nei lettori più attenti e interessati, poiché – come detto – molto è stato scritto sul tema ma molto

altro dovrà essere ulteriormente investigato per recuperare informazioni sempre più utili e metodologie quanto più condivise per l'analisi e la ricerca sullo specifico tema.

Il vero punto di forza di questa esperienza di ricerca è stata la possibilità di riunire in un'unica opera il contributo derivante da differenti esperienze sul campo e di ricerca, con background e *hnow-how* differenti: ciò ha reso possibile affinare taluni aspetti, come ad esempio le metodologie di sequestro di criptomonete e delle tecniche di analisi della blockchain, che, se non fossero unite da una esperienza sul campo e da problematiche tipiche della pratica quotidiana, sarebbero

apparse piuttosto sterili e non contestualizzate.

Volendo riassumere lo spirito che ha condotto l'esperienza di questa ricerca, è il caso di citare la celebre frase di Marcel Proust che affermò che "*L'unico vero viaggio verso la scoperta non consiste nella ricerca di nuovi paesaggi, ma nell'avere nuovi occhi*", ove si ritrova l'intento degli autori di fornire innovativi punti di osservazione di tematiche caratterizzate da un elevato tecnicismo sia giuridico-economico sia tecnico-pratico.

In ultima istanza, ciò che vuole emergere da questa esperienza sta nel fatto che il ruolo di analista, di consulente o di investigatore resta pertanto

imprescindibile e fondamentale per garantire un approccio di successo nella complessa attività di deanonimizzazione delle transazioni in criptovalute, che deve essere sempre più ispirata, oltre che dall'intuito, da una metodologia basata su solide teorie di derivazione tecnico-scientifica.

Paolo Dal Checco
Marco Stella

BIBLIOGRAFIA

[1] N. C. P. Iemma, La qualificazione giuridica delle criptovalute: affermazioni sicure e caute diffidenze, Diritto Bancario Approfondimenti, 2018.

[2] E. C. M. M. D. Capoti, Bitcoin Revolution. La moneta digitale alla conquista del mondo,, Milano: Ulrico Hoepli Editore, 2015.

[3] P. M. Morini Tommaso, «Il boom di Bitcoin non è per tutti,» *il Sole 24 ORE,* 27 novembre 2017.

[4] U. W. Chohan, «Cryptocurrencies: A Brief Thematic Review,» University of

New South Wales, 2017.

[5] L. D'AGOSTINO, «Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D. Lgs. 90/2017,» *Rivista di Diritto Bancario, 1/2018,* 2018.

[6] M. Mancini, «Valute virtuali e Bitcoin,» *Analisi giuridica dell'economia,* 2015.

[7] E. FERRARI, «Bitcoin e criptovalute: la moneta virtuale tra fisco e antiriciclaggio,» *Fisco,* 2018.

[8] G. R., "Tutto su Blockchain",

Hoepli, 2018.
[9] G. R., «Valute virtuali e moneta elettronica: cosa cambia con il recepimento in Italia della quarta direttiva antiriciclaggio,» PagamentiDigitali, 2017.
[10] M. S. e. M. V., «I bitcoin e le altre valute virtuali: regime fiscsle e orientamenti interpretativi in ambito comunitario e nazionale,» *Rivista della Guardia di Finanza,* n. 2, marzo - aprile 2018.
[11] G. Gasparri, Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?, Diritto dell'informatica,

2015.

[12] B. d'Italia, «Avvertenza sull'utilizzo delle cosiddette "valute virtuali",» 30 gennaio 2015.

[13] R. Bocchini, « "Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche",» Diritto dell'Informazione e dell'informatica, febbraio 2017.

[14] G. Gasparri, «"Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?",» Diritto dell'Informazione e

dell'informatica , 2015.

[15] E. V. M. Torre, «La moneta virtuale, tra regole (poche) e prassi (devianti),» *Rivista della Guardia di Finanza,* n. 3, maggio - giugno 2018.

[16] N. Vardi, «"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei bitcoin",» Diritto dell'Informazione e dell'informatica, giugno 2015.

[17] M. Passaretta, «"Bitcoin: il leading case italiano",» Banca Borsa Titoli di Credito, 2014.

[18] P. CENDON, Commentario al Codice Civile, Torino, 2001.

[19] F. I. R. Vigorita, «"Profili giuridici del Bitcoin: la moneta

diventa digitale",» 2016.

[20] e. a. A. Capogna, «Bitcoin: profili giuridici e comparatistici. Analisi e sviluppi futuri di un fenomeno in evoluzione,» Diritto mercato tecnologia, 2015.

[21] F. D. Vizio, «Lo statuto giuridico delle valute virtuali: le discipline e i controlli Tra oro digitale ed ircocervo indomito,» in *Convegno annuale "BITGENERATION Criptovalute tra tecnologia, legalità e libertà", Fondazione Cav. Lav. Carlo Pesenti e Fondazione Corriere della Sera*, MIlano, 15 marzo 2018.

[22] E. B. A. (EBA), «Opinion on "Virtual Currencies",» 4 luglio

2014.

[23] L. B. D. P. R. D. CARIA, «Bitcoin e le altre criptomonete. Inquadramento giuridico e fiscale,» 2014.

[24] M. MANCINI, Valute Virtuali e Bitcoin, Analisi Giuridica dell'Economia, 2015.

[25] Lewis-Mizen, Monetary Economics, Oxford, 2000.

[26] N. Szabo, «Smart Contracts: Building Blocks for Digital Markets,» 1996.

[27] M. Krogh, «Gli obblighi e le nuove sanzioni antiriciclaggio nel dlgs 25 maggio 2017, n. 90,» Notariato, 2017.

[28] «Wei Dai - B money,»

[Online]. Available: http://www.weidai.com/bmoney.txt . [Consultato il giorno 08 11 2018].

[29] S. Minnucci, «Blockchain, la rete anarchica dietro i Bitcoin,» 16 01 2018. [Online]. Available: https://www.democratica.com/focus/la-rete-anarchica-dietro-bitcoin/ . [Consultato il giorno 08 11 2018].

[30] G. Regiroli, «Bitcoin. Le radici filosofiche,» 16 05 2018. [Online]. Available: http://www.mondomarziale.org/bitc le-radici-filosofiche/ . [Consultato il giorno 08 11 2018].

[31] «Donate to WikiLeaks,» [Online]. Available: https://shop.wikileaks.org/donate .

[Consultato il giorno 08 11 2018].
[32] M. Moser, «Anonymity of Bitcoin Transactions,» in *Munster Bitcoin Conference (MBC)*, Munster, 2013.
[33] «https://www.torproject.org/,» [Online]. Available: https://www.torproject.org/ .
[34] NATO, «Intelligence Exploitation of the Internet,» 10 2002. [Online].
[35] A. L. Barabasi, Network Science, Glasgow: Cambridge university Press, 2016.
[36] B. F. Matthias Lischke, «Analyzing the Bitcoin Network: The First Four Years,» 07 03 2016. [Online]. Available:

https://www.mdpi.com/1999-5903/8/1/7/htm . [Consultato il giorno 10 11 2018].

[37] F. S. Stefano Bistarelli, «Go with the -Bitcoin- Flow, with Visual Analytics,» in *ARES17*, Reggio Calabria, 2017.

[38] J. D. Nick, «Data-Driven De-Anonymization in Bitcoin,» 09 08 2015. [Online]. Available: https://jonasnick.github.io/papers/the . [Consultato il giorno 08 11 2018].

[39] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» 2011. [Online]. Available: https://bitcoin.org/bitcoin.pdf . [Consultato il giorno 08 11 2018].

[40] N. Furneaux, «Transactions,» in

Investigating Cryptocurrencies, Indianapoli, John Wiley & Sons, Inc., 2018, pp. 79-81.

[41] «Gephi - Download,» [Online]. Available: https://gephi.org/users/download/ . [Consultato il giorno 10 11 2018].

[42] «gephi-bitcoin,» 07 08 2018. [Online]. Available: https://github.com/totetmatt/gephi-bitcoin/blob/master/complete.py . [Consultato il giorno 10 11 2018].

[43] S. S. G. T. Matthieu Roy, «Modeling and Measuring Graph Similarity: The Case for Centrality Distance,» 20 06 2014. [Online]. Available: https://arxiv.org/pdf/1406.5481.pdf

.

[44] J. H. T. M. S. Gago, «Notes on betweenness centrality of a graph,» 19 05 2009. [Online]. Available: https://core.ac.uk/download/pdf/417

.

[45] H. Z. X. H. P. H. H. D. S. Chris H.Q. Dingy, «Link Analysis: Hubs And Authorities On The World Wide Web,» 07 05 2001. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/doi=10.1.1.63.2781&rep=rep1&typ

.

[46] «Graph drawing library for JavaScript,» 31 12 2018. [Online]. Available: https://github.com/anvaka/VivaGrap

.

[47] S. H. T. V. M. B. Mathieu Jacomy, «ForceAtlas2, A Continuous Graph Layout Algorithm for Handy Network Visualization,» 01 08 2012. [Online]. Available: https://medialab.sciencespo.fr/publi Force_Atlas2.pdf .

[48] E. M. R. Thomas M. J. Fruchterman, «Graph Drawing by Force-directed Placement,» *SOFTWARE—PRACTICE AND EXPERIENCE, VOL. 21(1 1),* pp. 1129-1164, 11 1991.

Note

[←1]

Secondo alcune tesi non si tratterebbe, in realtà,

di un’unica persona, ma di un gruppo di esperti che ha lavorato insieme per la realizzazione di Bitcoin. Recentemente Craig Wright, un imprenditore australiano esperto di tecnologia, ha dichiarato di essere il volto che si nasconde dietro lo pseudonimo di Satoshi Nakamoto. Ad oggi permangono ancora dubbi sulla reale identità dell’ideatore dei bitcoin.

[←2]

Il Sole24Ore del 15/12/2018, “Per il bitcoin è panico da bolla” di Pierangelo Soldavini.

[←3]

Investitori che si rivolgono in prevalenza ai cosiddetti fondi istituzionali, quali fondazioni bancarie, enti previdenziali, enti pubblici territoriali, assicurazioni e istituti bancari, per raccogliere capitali a favore di una start up cui forniscono un business plan e, a seconda dei casi, anche competenze tecniche, manageriali, nonché relazioni e rapporti, che portino la società a migliorare i propri risultati. In altri casi, il venture capital attende unicamente che la start-up cresca, anche sotto il profilo degli utili, per arrivare al momento dell'exit definitiva dall'investimento effettuato.

[←4]

Una persona fisica che si appassiona a una startup, la finanzia e l'aiuta, portando, oltre al capitale, le proprie esperienze, conoscenze e contatti.

[←5]

Guida a Ethereum, in CryptoTrend, 23 ottobre 2017.

[←6]

Il 24 agosto 2017 il Canadian Securities Administrators ha emesso una nota ricalcando sostanzialmente il contenuto del report SEC; il 28 settembre 2017 la Australian Securities ed Investment Commission ha emanato un "Information Sheet" (INFO 225) ritenendo applicabile il Corporation Act 2001 quando il token emesso sia assimilabile ad un titolo partecipativo o ad un derivato; il 5 settembre 2017 la Securities and future Commission di Hong Kong ha emesso uno statement indicando i criteri per considerare come securities i token emessi in occasione di una ICO; stesso approccio ha adottato la Banca Centrale di Singapore il 15 novembre 2017.

[←7]

Così la FINMA, ossia l'autorità di supervisione finanziaria svizzera, nelle linee guida 4/2017 del 29 settembre 2017; la FSA giapponese nel proprio warning del 27 ottobre 2017, nonché la European Securities and Markets Authority (ESMA) la quale il 13 novembre 2017 ha emesso due comunicati sia per allertare gli investitori sui rischi derivanti dall'investimento in criptovalute sia per avvertire i soggetti promotori delle ICO della necessità di rispettare la normativa europea dove applicabile.

[←8]

Nel linguaggio economico, la moneta cartacea inconvertibile, generalmente accettata come mezzo di pagamento in quanto dichiarata a corso legale (detto anche forzoso) dallo Stato che la emette, indipendentemente dal suo valore intrinseco.

[←9]

In un sistema di crittografia a chiave pubblica, chiunque può cifrare un messaggio usando la chiave pubblica del destinatario, ma tale messaggio può essere decifrato solo con la chiave privata del destinatario. Per fare ciò, deve essere computazionalmente facile per un utente generare una coppia di chiavi pubblica e privata da utilizzare per cifrare e decifrare. La forza di un sistema di crittografia a chiave pubblica si basa sulla difficoltà di determinare la chiave privata corrispondente alla chiave pubblica.

La sicurezza dipende quindi solo dal mantenere la chiave privata segreta, mentre la chiave pubblica può essere pubblicata senza compromettere la sicurezza.

La crittografia asimmetrica, conosciuta anche come crittografia a coppia di chiavi, crittografia a chiave pubblica/privata o anche solo crittografia a chiave pubblica, è un tipo di crittografia dove, come si evince dal nome, ad ogni attore coinvolto nella comunicazione è

associata una coppia di chiavi:

- la chiave pubblica, che deve essere distribuita,
- la chiave privata, appunto personale e segreta,

evitando così qualunque problema connesso alla necessità di uno scambio in modo sicuro dell'unica chiave utile alla cifratura/decifratura presente invece nella crittografia simmetrica. Il meccanismo si basa sul fatto che, se con una delle due chiavi si cifra (o codifica) un messaggio, allora quest'ultimo sarà decifrato solo con l'altra.

[←10]

Articolo 2, punto 2, della direttiva 2009/110/CE (la c.d. “EMD2” o “IMEL2”).

[←11]

Articolo 4, punto 25, della direttiva (UE) 2015/2366 (la c.d. “PSD2”).

[←12]

Articolo 3, lettera k) della direttiva (UE) 2015/2366 (la c.d. “PSD2”).

[←13]

Articolo 3, lettera l) della direttiva (UE) 2015/2366 (la c.d. “PSD2”).

[←14]

Il numero totale di bitcoin tende asintoticamente al limite di 21 milioni. La disponibilità di nuove monete cresce come una serie geometrica ogni 4 anni; nel 2013 è stata generata metà delle possibili monete e per il 2017 saranno i tre quarti, in questo modo in meno di 32 anni verranno generate tutte le monete.

[←15]

Cfr. la sentenza della Corte di Giustizia UE C-461/12 del 12 giugno 2014.

[←16]

Comunicazione CONSOB n. DTC/13038246 del 6 maggio 2013.

[←17]

Cfr. la sentenza della Corte di Giustizia UE C-461/12 del 12 giugno 2014.

[←18]

Art. 42 Cost., II comma: “La proprietà privata è riconosciuta e garantita dalla legge, che ne determina i modi di acquisto, di godimento e i limiti allo scopo di assicurarne la funzione sociale e di renderla accessibile a tutti”.

[←19]

La caratteristica dei diritti reali è l'assolutezza, nel senso che il soggetto passivo del rapporto giuridico si trova in una situazione di dovere e non di obbligo, come colui sul quale gravi un'obbligazione.

[←20]

Gerald Cotten, fondatore dell'exchange Quadriga CX è scomparso a fine 2018: solo lui conosceva le credenziali per accedere al tesoro in criptovalute e non ha lasciato le password per accedere al suo portafoglio e patrimonio digitale. Centocinquanta milioni di dollari (circa 130 milioni di euro) sono andati persi per sempre. Ora nessuno sa come recuperare tutto quel denaro depositato nella cassaforte online, visto che Cotten – da buon informatico quale era – aveva messo in sicurezza il proprio pc con sistemi di crittografia più che avanzati. Un computer che rimane così inaccessibile, come racconta disperata la vedova del ragazzo, Jennifer Robertson: parte di quel tesoretto virtuale da 150 milioni di dollari è depositato e messo al sicuro in un "cold wallet", ovvero un deposito digitale legato a doppio filo al computer di Cotten, finché qualcuno riuscirà – sempre se ci riuscirà – a forzare i notebook del defunto. Franco Grilli - Il Giornale - 05/02/2019.

[←21]

CommonAccord è un’iniziativa, sostenuta dal MIT (Massachusetts Institute of Technology in USA), volta a creare codici globali di transazioni legali codificando e automatizzando documenti giuridici, inclusi contratti, permessi, documenti organizzativi e consensi.

[←22]

Legalese è un software che permette di sostituire la redazione di contratti da parte di avvocati con un programma intelligente di stesura di atti legali.

[←23]

Monax’s Dual integration è una soluzione che offre una doppia integrazione, ovvero l’inserimento di un contratto legale specifico in un determinato contratto intelligente eseguito su un archivio dati distribuito. Ciò consente alle parti di utilizzare i processi di risoluzione delle controversie giurisdizionali, utilizzando un contratto intelligente come meccanismo primario per la gestione dell'interazione basata sui dati che definiscono l'accordo tra le parti.

[←24]

Ricardian contract è stato inventato da Ian Grigg nel 1996 e rappresenta un metodo per registrare un documento come un contratto legale e collegarlo in modo sicuro a sistemi informatici, che, grazie all'identificazione tramite funzione di hash crittografica, rendono fruibile un linguaggio di marcatura ai fini di un utilizzo in campo legale.

[←25]

Dato pubblicato dal sito coinmarketcap.com.

[←26]

Rese tali dalla cosiddetta blockchain ovvero l’elenco di tutte le transazioni di bitcoin effettuate.

[←27]

Negli USA, ad esempio, è stato avviato un sistema che permette di gestire una sorta di "energia di vicinato": i pannelli solari producono energia che non viene immessa nella rete ma scambiata tra i partecipanti, in modo sicuro e trasparente, utilizzando una piattaforma basata sulla blockchain di Ethereum, E. Comelli, L'energia di vicinato gira su blockchain, in Il Sole 24 Ore del 24/09/2017.

[←28]

Già nel 2013 un primo aggiornamento ha consentito di ridurre le spese di transazione e ha potenziato il sistema di sicurezza. Nel 2014 è stata rilasciata una nuova versione di Litecoin che ha risolto ulteriori problematiche riscontrate dagli utenti sull'anonimizzazione.

[←29]

Il FMI, istituito nel 1945 in seguito agli accordi di Bretton Woods negli Stati Uniti, è composto da 189 Paesi e promuove la cooperazione monetaria internazionale e facilita l'espansione del commercio internazionale.

[←30]

Il PIL misura il valore di mercato di tutte le merci finite e dei servizi prodotti in un territorio ed in un periodo di tempo.

[←31]

Il termine sarebbe nato negli Stati Uniti allorquando il governatore Leon Abbet del New Jersey, altrimenti chiamato Garden State (Stato Giardino), nel 1887, al fine di rimpinguare le casse statali assicurò una tassazione di favore a tutte le aziende che avrebbero preso dimora stabile nel New Jersey.

[←32]

L’OCSE è composto da 35 Paesi ed effettua studi economici. Attraverso un’Assemblea è punto di confronto per le politiche commerciali internazionali.

[←33]

V. PELLEGRINI e E. TOSTI, Alla ricerca dei capitali perduti: una stima delle attività all'estero non dichiarate dagli italiani, in <Questioni di Economia e Finanza>, n. 97, Banca d'Italia, Roma 2011, pag. 12.

[←34]

Legge 18 giugno 2015, n. 95 recante Ratifica ed esecuzione dell'Accordo tra Italia e Stati Uniti d'America finalizzato a migliorare la compliance fiscale internazionale e ad applicare la normativa FATCA (Foreign Account Tax Compliance Act) nonché disposizioni concernenti gli adempimenti delle istituzioni finanziarie italiane ai fini dell'attuazione dello scambio automatico di informazioni derivanti dal predetto accordo e da accordi tra l'Italia e altri Stati esteri.

[←35]

Decreto Legislativo 15 marzo 2017, n. 32 recante attuazione della Direttiva (UE) 2015/2376 per quanto riguarda lo scambio automatico obbligatorio di informazioni nel settore fiscale.

[←36]

Si rammentano nel tempo:

- le Convenzioni bilaterali contro le Doppie Imposizioni (DTA), che prevedono lo scambio di informazioni su richiesta dell'Amministrazione Fiscale del Paese richiedente, senza l'opponibilità del segreto bancario quando l'informazione è "prevedibilmente pertinente". L'Italia ha stipulato 103 accordi convenzionali;
- la Convention on Mutual Administrative assistance in Tax Matters (MAAT), ratificata dall'Italia con Legge 10 febbraio 2005, n. 19. Gli elementi

caratteristici della Convenzione sono rappresentati dalle clausole in materia di scambio di informazioni su richiesta e di assistenza alla riscossione;

- la Tax Information Exchange Agreement (TIEA), modello di accordo internazionale che prevede dal 2016 lo scambio di informazioni a richiesta senza opponibilità del segreto bancario ed assenza del rifiuto di collaborazione. L'Italia ha stipulato accordi con 7 Paesi (Bermuda, Cayman, Gibilterra, Cook, Guernsey, Man Island e Jersey).

[←37]

Riguarda i seguenti Paesi:

- che si impegnano al primo scambio di informazioni dal 2017: Anguilla, Argentina, Barbados, Belgio, Bermuda, British Vergin Island, Bulgaria, Cayman, Cile, Colombia, Croazia, Curacao, Cipro, Cechia, Danimarca, Dominica, Estonia, Faroer, Finlandia, Francia, Germania, Gibilterra, Grecia, Groenlandia, Guernsey, Ungheria, Islanda, India, Irlanda, Isle Man, Italia, Jersey, Korea Sud, Lettonia, Liechtenstein, Lituania, Lussemburgo, Malta, Mauritius, Messico, Montserrat, Olanda, Niue, Norvegia, Polonia,

Portogallo, Romania, San Marino, Seychelles, Slovacchia, Slovenia, Sud Africa, Spagna, Svezia, Trinidad e Tobago, Turks e Caicos, Regno Unito, Uruguay;

- che si sono impegnati dal 2018: Albania, Andorra, Antigua e Barbuda, Arabia Saudita, Aruba, Australia, Austria, Bahamas, Belize, Brasile, Brunei, Canada, Cina, Costa Rica, Grenada, Hong Kong, Indonesia, Israele, Giappone, Marshall, Macao, Malesia, Monaco, Nuova Zelanda, Qatar, Russia, Saint Kitts e Nevis, Samoa, Saint Lucia, Saint Vincent e Grenadine, Singapore, Sint Maarten, Svizzera, Turchia, Regno

Unito;

- che non hanno indicato una data di inizio: Bahrein, Cook, Nauru, Panama, Vanuatu.

[←38]

In merito vi sono stati beni sequestrati pari ad oltre 16.000 per un valore di circa 7 miliardi di euro, nonché beni confiscati nel numero di 3.500 per un valore di 3,5 miliardi di euro riferiti all'anno 2012, cfr. Senato della Repubblica, Relazione illustrativa – Analisi di impatto della Regolamentazione sullo schema di Atto del Governo n. 389 di attuazione della Quarta Direttiva antiriciclaggio, Roma 2017.

[←39]

Tale condotta è punita dall'articolo 8, Emissione di fatture o altri documenti per operazioni inesistenti, del Decreto Legislativo nr. 74/2000.

[←40]

“Frode Carosello” è un sistema fraudolento dell'IVA attuato mediante vari passaggi di beni in genere provenienti ufficialmente da un Paese dell'U.E., al termine del quale l'impresa italiana acquirente detrae l'Iva nonostante che il venditore compiacente (prestanome e nullatenente) non l'abbia versata.

[←41]

L’interposizione fittizia è sanzionata dall’articolo 10-bis, Disciplina dell’abuso del diritto o elusione fiscale, della legge 27 luglio 2000, n. 212, recante disposizioni in materia di statuto dei diritti del contribuente.

[←42]

Guardia di Finanza, Rapporto Annuale, Roma 2017. Peraltro il Comitato di Sicurezza Finanziaria, Analisi nazionale dei rischi di riciclaggio e finanziamento del terrorismo, Roma 2014, rilevava nelle province di Benevento, Biella, Caserta, Catania, Catanzaro, Cosenza, Foggia, Isernia, Macerata, Messina, Napoli, Reggio Calabria e Vibo Valentia, quelle ad alto rischio nell'utilizzo del denaro contante.

[←43]

Nel 2015 le SOS pervenute all'UIF hanno riguardato per il 20% la Regione Lombardia e per l'11% le Regioni Lazio e Campania e sono riferite per il 46% a transazioni finanziarie avente un valore tra i 50.000 ed i 500.000 euro, nonché bonifici per il 32% e contanti per il 26%, con una provenienza del 60% da banche ed intermediari finanziari.

[←44]

Ratificata dall'Italia con legge del 18 marzo 2008, n. 48. Alla Convenzione hanno aderito: Albania, Andorra, Argentina, Armenia, Arzebaijan, Australia, Austria, Belgio, Bosnia, Bulgaria, Canada, Capo Verde, Cechia, Cile, Cipro, Colombia, Costa Rica, Croazia, Danimarca, Estonia, Filippine, Finlandia, Francia, Georgia, Germania, Ghana, Giappone, Gran Bretagna, Grecia, Irlanda, Islanda, Israele, Italia, Lettonia, Liechtenstein, Lituania, Lussemburgo, Macedonia, Malta, Marocco, Mauritius, Messico, Moldavia, Monaco, Montenegro, Nigeria, Norvegia, Paesi Bassi, Panama, Paraguay, Perù, Polonia, Portogallo, Repubblica Dominicana, Romania, Russia, San Marino, Senegal, Serbia, Slovacchia, Slovenia, Spagna, Sri Lanka, Stati Uniti, Sud Africa, Svezia, Svizzera, Tonga, Tunisia, Turchia, Ucraina, Ungheria. L'ultimo Paese a dare attuazione alla Convenzione è stato il Paraguay al 01/11/2018. Il Ghana l'ha ratificata a partire dal 01/04/2019.

[←46]

https://github.com/iancoleman/bip39

[←47]

https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki#Compatible_wallets

[←48]

https://www.blockplate.com/blogs/blockplate/list-of-bip39-wallets-mnemonic-seed

Table of Contents

1.4. Definizion giuridica dei Bitcoin

1.5 Smart

1.2 Anonimizz e processam dello streaming di dati dalla Blockchai

1.3 Costruzion
di un
modello
di
rappresent
relazionale
delle
transazioni

1.4 Il problema dell'analisi dei dati relativi alle transazioni e agli indirizzi Bitcoin

2.3 Strumenti di analisi visuale real time della Blockchai

2.4 Tagging e clustering: tecniche analitiche a contrasto

Bibliografia