Emanuele Florindi

Criptovalute: manuale di sopravvivenza

Guida pratica a bitcoin, monero, ethereum e blockchain

Imprimatur

ISBN 978 88 6830 677 9

Promozione e distribuzione Mondadori Libri

Sede legale e operativa:
Via Emilia all'Angelo, 7 - 42124 Reggio Emilia
Tel. 0522 232222

Introduzione

Negli ultimi tempi si sente molto parlare di bitcoin, spesso impropriamente, in maniera tale da indurre numerosi soggetti a pensare che gli stessi siano un facile viatico alla ricchezza.

L'ascesa del valore del bitcoin è innegabile: in pochissimo il bitcoin è passato da un valore di qualche dollaro (poco più di 10) a quasi 1000 dollari, per poi attestarsi, oggi, su un valore intorno ai 17 mila dollari; non male se si considera che il primo scambio documentato bitcoin-beni materiali ha visto, il 18 maggio 2010, offrire 10 mila bitcoin per un paio di pizze…

Quello che molti non sanno è cosa realmente sia il bitcoin e, per comprenderlo, dobbiamo fare un lungo viaggio nel mondo della Rete, partendo dalle zecche virtuali in cui il bitcoin viene prodotto ("minato" per impiegare il medesimo neologismo utilizzato nei forum) fino ai market più oscuri del *deep web*, dove spesso viene speso, perché la moneta virtuale più famosa del mondo viene controllata e scambiata interamente e solamente da computer e server sparsi per internet.

Il bitcoin è come denaro contante, anzi in un certo senso è IL denaro contante del web, ma, a differenza delle monete aventi corso legale, il suo valore viene costantemente stabilito dagli utenti: ogni bitcoin vale esattamente ~~anto~~ il valore di scambio che un utente è disposto ad attribuirgli rispetto a un bene concreto dato che lo stesso è fuori dal controllo delle riserve monetarie mondiali.

Nel corso del presente libro, cercherò di spiegare pregi, rischi e difetti delle principali criptovalute. Affronteremo, infatti, la tematica relativa ai sistemi di pagamento basati sulla cosiddetta *criptovaluta* e lo faremo utilizzando un linguaggio il più possibile semplice e comprensibile, anche a discapito di quella rigorosa precisone che richiederebbe un eccessivo impiego di termini tecnici.

Questo significa che, ove necessario, alcuni termini verranno utilizzati con un significato più ampio rispetto a quello strettamente tecnico (tanto informatico quanto giuridico) e che si cercherà di semplificare alcune nozioni e alcune procedure, ferma rimanendo la correttezza di base di tutte le informazioni fornite.

Allo stesso modo, l'esigenza di realizzare un manuale snello e di agevole lettura, ha reso impossibile

esaminare adeguatamente tutti gli argomenti e, per tale ragione, ho ritenuto opportuno inserire in queste pagine dei riferimenti alle fonti che è possibile utilizzare per approfondire.

Prima di procedere oltre, è opportuno chiarire il concetto di *criptovaluta* [in inglese *cryptocurrency*]: si tratta di una rete decentralizzata di pagamento peer-to-peer, gestita dai suoi utenti, senza alcuna autorità centrale o intermediari, e rappresenta la realizzazione di un concetto la cui idea di base venne descritta per la prima volta nel 1998 in una mailing list.

Con questo termine si indica, dunque, un mezzo di pagamento, decentralizzato la cui implementazione si basa sui principi della crittografia per convalidare le transazioni e la generazione della moneta e che, di solito, utilizza uno schema *proof-of-work* per ridurre il rischio di attacchi e tentare di salvaguardare la valuta dalla contraffazione digitale.

Uno schema proof-of-work (POW) è una misura dal costo contenuto per scoraggiare attacchi o altri abusi di un servizio; l'idea si basa sul fatto di imporre alcune attività al soggetto che richiede quello specifico servizio: di solito si tratta di un servizio asimmetrico, moderatamente complesso per il richiedente, ma facile da controllare per il fornitore del servizio.

In questo modo per un eventuale attaccante diventa antieconomico porre in essere la propria attività, mentre per un utente "legittimo" si tratta soltanto di un piccolo spreco di tempo.

Sebbene a oggi esista un grande numero di *criptomonete*, tutte le specifiche e i protocolli sono, per lo più, simili tra di loro e derivano dalla prima criptovaluta a essere implementata: il Bitcoin.

1. Le criptovalute (quali sono e come funzionano)

1.1 Una nuova forma di valuta

In precedenza, abbiamo detto che la prima criptovaluta a essere stata implementata, nonché la più conosciuta, è il bitcoin (simbolo ₿ ; abbreviazione BTC). Ci sembra, quindi, corretto iniziare il nostro discorso partendo proprio da questa moneta e descrivendola nel dettaglio.

Iniziamo con il dire che il bitcoin è una moneta elettronica e un sistema di pagamento digitale: l'idea venne presentata da Satoshi Nakamoto nel 2008, mentre il software venne sviluppato dallo stesso nell'anno successivo; dobbiamo poi precisare che il termine "Bitcoin", con l'iniziale in maiuscolo, si riferisce espressamente alla tecnologia e alla rete, mentre la parola "bitcoin", con l'iniziale minuscola, si riferisce alla valuta.

Una delle principali differenze tra il bitcoin e la maggior parte delle valute tradizionali è che nella tecnologia Bitcoin non è presente un ente centrale: viene impiegato un database distribuito tra i nodi della rete che tengono traccia delle transazioni, e si sfrutta la crittografia per gestire gli aspetti funzionali come la

generazione di nuova moneta e l'attribuzione di proprietà dei bitcoin.

Quest'ultima è considerata la prima criptovaluta sia per il suo notevole valore sia perché è stata la prima a essere conosciuta dalla massa degli utenti e, di conseguenza, la più diffusa come forma di pagamento.

Naturalmente, accanto al bitcoin, esistono anche altre monete e, pur non trattandosi di moneta avente corso legale in uno Stato, esistono borse valori in cui è possibile acquistare e scambiare criptovalute con denaro avente valore legale o con altre criptovalute:

Principali criptovalute »

Nome	Simbolo	Prezzo USD	Capitaliz. Mercato	Vol.	% Vol. totale	Prezzo BTC	Var. % 1G	Var. % 7G
Bitcoin	BTC	6.498,5	$103,72B	$1,67B	51,51%	1	+0,97%	+9,18%
Ethereum	ETH	303,23	$29,43B	$308,73M	9,51%	0,0495165	-0,07%	+0,09%
Ripple	XRP	0,19849	$7,81B	$32,38M	1,00%	0,00003257	+0,71%	-3,58%
Bitcoin Cash	BCH	498,80	$7,41B	$313,30M	9,65%	0,071005	+14,03%	+32,82%
Litecoin	LTC	55,420	$3,03B	$83,33M	2,57%	0,00907526	+0,02%	-2,78%
Dash	DASH	278,11	$2,16B	$40,80M	1,26%	0,0452432	+0,73%	-5,17%
NEO	NEO	27,270	$1,90B	$28,76M	0,89%	0,00469676	-4,17%	-5,60%
NEM	XEM	0,18033	$1,77B	$3,84M	0,12%	0,00003163	-3,59%	-7,30%
BitConnect	BCC	231,074	$1,70B	$19,66M	0,61%	0,037107	+1,25%	+16,41%
Monero	XMR	87,37	$1,35B	$24,38M	0,75%	0,0142114	+0,02%	-1,74%

Per capire il sistema Bitcoin è necessario partire dai suoi elementi base: la *blockchain*, i *miner* e i *wallet*.

A tal proposito, ci limiteremo per ora a dire che, con il termine *miner* (minatore), si indica un computer (e l'utente che lo controlla) impiegato dalla rete P2P di Bitcoin per l'operazione di verifica delle transazioni di denaro virtuale in modo che queste avvengano in modo lecito e sicuro: se un utente acquista un oggetto e lo paga in bitcoin, è necessario che una serie di calcoli

verifichi che i bitcoin spesi siano effettivamente prelevati dal suo portafoglio virtuale, evitando il fenomeno del *double spending* (doppia spesa), e trasferiti nel portafoglio del venditore. Se non esistesse questa verifica avremmo l'equivalente informatico della possibilità di pagare i nostri acquisti con denaro fotocopiato.

Proprio per tale ragione, ogni transazione viene archiviata in un apposito registro denominato *blockchain*, che consente di verificare che l'intera procedura sia andata a buon fine e che il valore transitato sia stato effettivamente posseduto prima e depositato poi dall'utente.

Questa verifica, che col passare del tempo ha richiesto sempre più potenza di calcolo, viene oggi fatta da utenti specializzati nel *mining*; sebbene il termine significhi letteralmente "estrazione", in pratica, i miner mettono a disposizione la potenza di calcolo dei loro computer e, in cambio, per ogni verifica andata a buon fine, ricevono dei bitcoin.

Mentre nei primi tempi anche un singolo utente dotato di un modesto elaboratore era in grado di svolgere molto lavoro, col passare del tempo si sono creati dei gruppi organizzati di miner (la cosiddetta pool) che, tramite appositi programmi, sono in grado di unire la potenza dei propri computer per effettuare il maggior numero possibile di verifiche, sul modello del calcolo distribuito.

Con il termine *wallet* (portafoglio) si indica, invece, il programma che permette di entrare nella rete Bitcoin e di conservare i propri bitcoin. Il portafoglio contiene, infatti, gli indirizzi e le chiavi per effettuare le transazioni economiche e questo rende il portafoglio di Bitcoin l'equivalente di un portafoglio materiale.

A ben guardare, il portafoglio non contiene tanto il denaro, quanto le chiavi private di conferma che

permettono all'utente di utilizzare i bitcoin. Con il termine "chiave privata" si indicano i dati segreti che provano la corretta identità dell'utente che utilizza un determinato portafoglio, grazie all'impiego di una firma elettronica.

A ciò deve aggiungersi che ogni portafoglio può mostrare il bilancio totale di tutti i bitcoin che controlla e permette all'utente di inviare cifre precise a una persona specifica.

1.2 La blockchain

Alla base di ogni criptovaluta troviamo una catena di blocchi (blockchain) che mantiene in modo continuo una lista crescente di record, i quali fanno riferimento a record precedenti presenti nella lista stessa. Questa catena è resistente a manomissioni.

Sebbene spesso blockchain e bitcoin vengano confusi, si tratta di due elementi molto diversi tra di loro: la blockchain più che una tecnologia rappresenta un vero e proprio paradigma di funzionamento, tanto che oggi ne esistono differenti definizioni [per approfondire si veda M. Bellini, *Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*, http://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/, per un simulatore di blockchain si veda, invece, la pagina https://lab-cryptotrend.herokuapp.com/].

Se è vero che il bitcoin, come criptovaluta, ha creato una serie di conflitti tra sostenitori e detrattori, possiamo affermare che l'intuizione alla base della blockchain, e la sua implementazione, ha messo tutti d'accordo, perché, per sua natura, rappresenta una soluzione in grado di garantire un elevato livello di

sicurezza, tanto da ricevere le lodi e l'interesse della stessa Autorità Bancaria Europea (EBA).

Vediamo quindi, per prima cosa, che cosa è e come funziona la blockchain.

1. La blockchain come database distribuito

Una prima definizione la identifica come un "database di transazioni" e, in effetti, si tratta di una tecnologia che permette la creazione e la gestione di un grande database distribuito (database in cui i dati non sono memorizzati su un solo computer ma su più macchine collegate tra loro, chiamate nodi) in grado di registrare e mantenere accessibili i dati di più transazioni condivisibili tra i differenti nodi di una rete.

Il database è strutturato in blocchi, identificati con i nodi della rete, collegati tra di loro da una catena (*chain*); in questo modo, ogni transazione avviata sulla rete viene a essere convalidata dalla rete stessa.

Questo è possibile perché ciascun nodo della rete viene a essere chiamato a vedere, controllare e approvare tutte le transazioni garantendo la loro affidabilità, la loro trasparenza e la loro tracciabilità e ogni blocco include l'hash del blocco precedente, collegando i blocchi insieme così che ogni blocco è anche un archivio per tutte le transazioni precedenti, riportando lo storico di ciascuna transazione che, in questo modo, diventa immodificabile e non ripudiabile se non attraverso la creazione di blocchi paralleli e la riproposizione degli stessi a tutta la rete. Questo, però, è possibile solo ottenendo il controllo del 50 per cento +1 dei blocchi.

In breve, i blocchi formano una catena, con ogni blocco addizionale che rinforza quelli precedenti rendendola immutabile.

A ciò deve aggiungersi che l'impiego di strumenti crittografici garantisce la massima sicurezza di ogni transazione.

2. La blockchain come evoluzione del concetto di "libro mastro" (ledger)

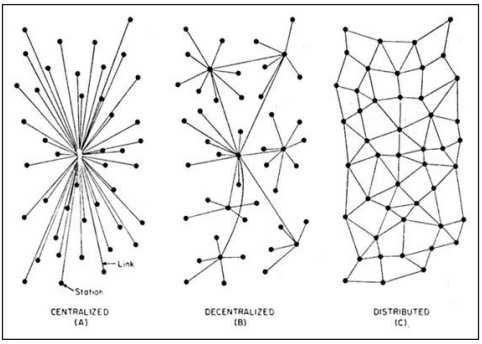
La blockchain può essere vista anche come una evoluzione del concetto di "libro mastro" che passa da essere centralizzato, gestito da una singola autorità, secondo lo schema tradizionale dell'uno a tanti fino ad arrivare a una logica distribuita in cui non esiste alcuna autorità centrale.

Il punto critico della visione classica, detta anche *centralized ledger*, è rappresentato dalla necessità che l'autorità centrale goda della piena fiducia di tutti i soggetti coinvolti e che sia in grado di resistere a eventuali tentativi di attacco o di manomissione da parte di soggetti interni e\o esterni.

Per ovviare a questo inconveniente era stato proposto uno schema decentralizzato (*decentralized ledger*), confidando nella difficoltà di colpire non più un unico obiettivo centrale, ma tanti obiettivi satellite. Pur frazionando il rischio, però, non lo si elimina, anzi, in qualche modo lo si aumenta in maniera direttamente proporzionata al numero di satelliti presenti.

Il vero cambiamento è, invece, rappresentato dal modello distribuito in cui non esiste più un'autorità centrale e tutti i soggetti coinvolti si trovano al medesimo livello decisionale: in questo modo è impossibile

che un soggetto possa prevalere sugli altri e il consenso alla transazione trova fondamento sulla "fiducia" posta dal singolo soggetto; quando questa fiducia raggiunge un livello predefinito (tipicamente 50 per cento +1) l'operazione viene confermata.



3. La blockchain come registro pubblico aperto a tutti

Trattandosi di un database decentralizzato che archivia asset e transazioni su una rete di tipo peer to peer, la blockchain può essere vista anche come un pubblico registro di tutte le transazioni che la compongono.

Ne consegue che la blockchain è, per sua stessa natura, "trasparente" in quanto questa caratteristica è necessaria per la gestione dei dati delle transazioni eseguite.

Dato che tutte le transazioni sono costituite da dati crittografati e risultano essere state verificate, approvate e successivamente registrate su tutti i nodi che partecipano alla rete, ne consegue che la medesima "informazione" si trova a essere presente su tutti i nodi con l'effetto di essere praticamente immodificabile.

Per tale ragione la blockchain è in grado di gestire in modo condiviso una lista crescente di record con la massima resistenza alle manomissioni, andando a costituire una sorta di libro mastro decentralizzato e sicuro per la gestione di transazioni su reti peer to peer.

La flessibilità di questa tecnologia la rende adattabile a ogni forma di transazione e collaborazione, dai pagamenti all'acquisto di beni o servizi: può trovare applicazione in ogni ambito in cui sia necessaria una relazione sicura tra più persone o gruppi senza la presenza di un'autorità centrale.

4. Blockchain, come funziona?

Dopo aver spiegato che cosa è una blockchain, cerchiamo di capire come funziona da un punto di vista tecnico.

In sintesi, la blockchain è una tecnologia basata sulla logica del database distribuito ed è composta da una lista, in continua crescita, di record (in ambito informatico si definisce "record" un tipo di dato strutturato che comprende diversi elementi di tipo eterogeneo chiamati campi o membri) detti "blocchi". I blocchi sono collegati tra di loro e protetti da eventuali manomissioni attraverso l'impiego della crittografia. La struttura è costruita in maniera tale che ogni blocco contenga un hash, collegato come link al blocco che lo precede, un marcatore temporale (timestamp) e i dati relativi alla validità della transazione; i blocchi così collegati formano una catena, con ogni blocco addizionale che rinforza la sicurezza di quelli precedenti.

Tutto il processo di validazione si basa sul concetto di Consenso Distribuito e prevede una fase di verifica e di approvazione interamente basata su risorse messe a disposizione dagli stessi partecipanti alla blockchain e impiegate per validare il blocco; una volta raggiunto questo obiettivo, il primo nodo ad aver ottenuto questo risultato riceverà un premio (di solito monete virtuali legate alla tipologia di blockchain).

Alla base di questo processo vi è la necessità di evitare il rischio di frodi da parte di un nodo e, a tal fine, è necessario incrementare la difficoltà del percorso di validazione fino a rendere "non conveniente" la falsificazione del nodo stesso.

In breve, attraverso questo sistema si viene a sostituire un rapporto di fiducia costruito sulla conoscenza reciproca con uno basato sulla concreta collaborazione alla soluzione delle prove che devono essere validate.

A questo punto si rende, però, necessario distinguere tra due approcci radicalmente differenti basati su due principi opposti: *permissionless blockchain* e *permissioned blockchain*.

In una *permissionless blockchain* (detta anche blockchain aperta), chiunque può partecipare alla rete dando il proprio contributo al processo di validazione dei blocchi; questo accade, ad esempio, nel sistema Bitcoin, Ethereum, Monero.

Al contrario una *permissioned blockchain* (detta anche blockchain chiusa) limita i soggetti abilitati a convalidare i blocchi: solo un ristretto numero di soggetti viene abilitato alla convalida.

Le differenze tra i due sistemi sono notevoli anche da un punto di vista pratico, vediamo qui le principali.

5. segue: permissionless vs permissioned blockchain

In un sistema permissionless gli utenti non hanno bisogno di dimostrare, e di rendere nota agli altri, la propria identità: fintanto che partecipano attivamente al processo di convalida possono accedere al processo di verifica e concorrere per l'attribuzione del relativo premio.

Al contrario, in una permissioned blockchain l'utente deve necessariamente essere un soggetto noto e approvato per essere abilitato a convalidare le transazioni. Questo significa che questa tipologia di blockchain può essere soggetta a forme di controllo e verifica dall'alto dato che, quando un nuovo record viene aggiunto, il sistema di approvazione non è legato alla maggioranza dei partecipanti, ma a un numero limitato di attori, definibili come *trusted*.

Un'altra differenza rilevante tra i due sistemi è legata al modello di convalida dei blocchi (mining), laddove le permissionless blockchain sono, generalmente, basate su un modello legato al principio della proof-of-work (POW) in cui i nodi mettono a disposizione la propria potenza di calcolo per costruire la fiducia: fintanto che il 50 per cento +1 dei nodi è onesto, il sistema è al sicuro.

Nelle permissioned blockchain, invece, essendo i soggetti noti ed essendo il blocco validato da utenti trusted, non vi è bisogno di mettere a disposizione la propria potenza di calcolo per ottenere fiducia; vengono, quindi, utilizzati altri algoritmi come, ad esempio, RAFT, Paxos o PBFT (Practical Byzantine Fault Tolerance) per validare il blocco senza dover ricorrere alla POW.

Questo modello trova il suo naturale ambito di applicazione nelle blockchain private dedicate al B2B (business-to-business) o ad ambiti definiti (mercati, affari

o finanza) in quanto presentano alcune caratteristiche che, in tali ambiti, le rendono particolarmente appetibili:

1. Riservatezza: una permissioned blockchain permette di limitare la lettura delle transazioni soltanto a soggetti determinati. Una permissionless blockchain rappresenta la scelta ideale per un database distribuito in cui chiunque può leggere qualunque informazione e questo non può essere accettato in determinati ambiti in cui la riservatezza delle informazioni è fondamentale.
2. Scalabilità: all'interno di una permissioned blockchain può essere implementato un modello semplificato per stabilire il consenso risparmiando tempo e risorse. Il risultato finale garantisce performance decisamente superiori al corrispettivo permissionless blockchain.
3. Controllo degli accessi: una permissioned blockchain consente di restringere l'accesso ai dati contenuti nel database come accade, per esempio, nel modello sviluppato da R3CEV, "Corda".

In estrema sintesi le permissioned blockchain garantiscono la possibilità di far operare in modo indipendente più attori, ma conservando il pieno controllo di coloro che sono considerati trusted; a ciò si aggiunga che permettono di limitare l'accesso e la visibilità dei dati introducendo nella blockchain un concetto di governance e di definizione di regole di comportamento.

(Per approfondire si rimanda a http://bornonjuly4.me/2017/01/10/blockchain-what-is-permissioned-vs-permissionless/)

1.3 Permissionless blockchain: il bitcoin come applicazione pratica

Nel paragrafo precedente abbiamo distinto tra le due tipologie di blockchain, ora andremo ad approfondire il sistema aperto attraverso l'analisi di quella che è, oggi, la sua più famosa implementazione: il Bitcoin.

L'idea del Bitcoin non nasce dal nulla: da decenni circolava in rete l'ipotesi di una moneta digitale decentralizzata e alcuni protocolli anonimi di moneta digitale vennero sviluppati tra gli anni Ottanta e Novanta, ma questi progetti fallirono, principalmente a causa della loro dipendenza da un intermediario centralizzato.

Poiché la moneta è un'applicazione first-to-file, dove l'ordine delle transazioni è spesso di cruciale importanza, le monete decentralizzate richiedono una soluzione al consenso decentralizzato. Satoshi ha fornito risposta a ciò, combinando un protocollo molto semplice, basato su dei nodi su cui avvengono le transazioni, in modo da dare vita a una catena in continua crescita attraverso la creazione di "blocchi" e in cui i nodi guadagnano il diritto di partecipare al sistema attraverso la proof-of-work.

Abbiamo visto che il processo di validazione si basa sul concetto di Consenso Distribuito e prevede una fase di verifica e di approvazione da parte di tutti i nodi. Tale fase è basata su risorse di calcolo messe a disposizione dagli stessi partecipanti alla blockchain tanto che, nel suo *paper* (S. Nakamoto, Bitcoin: *A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf), Satoshi Nakamoto definì il sistema «*a peer-to-peer electronic cash system*»: le risorse vengono impiegate per risolvere proble-

mi complessi o puzzle crittografici, ma l'aspetto interessante è che tutti coloro che partecipano alla risoluzione del problema, concorrendo dunque alla validazione del processo e della transazione, sono in gara tra di loro atteso che soltanto il primo nodo che riuscirà a risolvere il puzzle crittografico avrà il diritto di validare il blocco, mediante la presentazione della proof-of-work. Per questo risultato, il nodo riceverà un premio (di solito monete virtuali legate alla tipologia di blockchain).

Alla base di questo processo vi è la necessità di evitare il rischio di frodi da parte di un nodo e, a tal fine, è necessario incrementare la difficoltà del percorso di validazione fino a rendere "non conveniente" la falsificazione del nodo stesso.

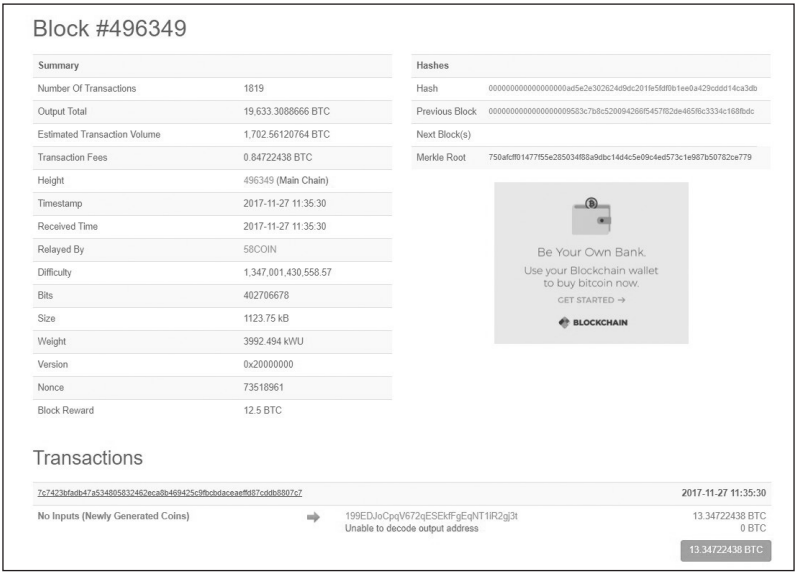
In breve, attraverso questo sistema, come detto, si viene a sostituire un rapporto di fiducia costruito sulla conoscenza reciproca con uno basato sulla concreta collaborazione alla soluzione delle prove che devono essere validate.

1. Le basi del sistema Bitcoin: i blocchi

Vediamo ora alcuni esempi pratici di applicazione della blockchain legate all'impiego di bitcoin.

Ricordiamo che, convenzionalmente, quando utilizziamo l'iniziale maiuscola (Bitcoin), facciamo riferimento alla tecnologia e alla rete, mentre quando scriviamo bitcoin con l'iniziale minuscola intendiamo la valuta; a tal proposito, è bene ribadire anche che il bitcoin non è una valuta a corso legale (cosiddetta valuta *fiat*) dato che nessuna legge ne garantisce valore e potere di acquisto.

Prendiamo un blocco della blockchain:



Block #496349

Summary	
Number Of Transactions	1819
Output Total	19,633.3088666 BTC
Estimated Transaction Volume	1,702.56120764 BTC
Transaction Fees	0.84722438 BTC
Height	496349 (Main Chain)
Timestamp	2017-11-27 11:35:30
Received Time	2017-11-27 11:35:30
Relayed By	58COIN
Difficulty	1,347,001,430,558.57
Bits	402706678
Size	1123.75 kB
Weight	3992.494 kWU
Version	0x20000000
Nonce	73518961
Block Reward	12.5 BTC

Hashes	
Hash	000000000000000000ad5e2e302624d9dc201fe5fdf0b1ee0a429cddd14ca3db
Previous Block	00000000000000000009583c7b8c52009426f5457f82de465f6c3334c168fbdc
Next Block(s)	
Merkle Root	750afcff01477f55e285034f88a9dbc14d4c5e09c4ed573c1e987b50782ce779

Transactions

7c7423bfadb47a534805832462eca8b469f425c9fbcbdaceaeffd87cddb8807c7 — 2017-11-27 11:35:30

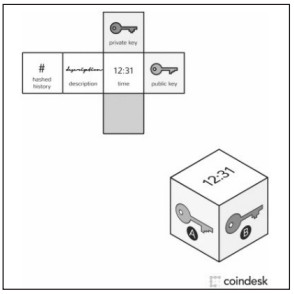
No Inputs (Newly Generated Coins) → 199EDJoCpqV672qESEkfFgEqNT1iR2gj3t (Unable to decode output address) — 13.34722438 BTC, 0 BTC

13.34722438 BTC

Nell'immagine che precede possiamo vedere le informazioni contenute in un blocco appena generato, ma come nasce questo blocco?

1. Tizio deve trasferire una quantità X di bitcoin a Caio;
2. Entrambi dispongono di un proprio wallet (NB con il termine *wallet* si indica un sistema, software o hardware, in grado di gestire le operazioni effettuate con una o più criptovalute, un po' come se si trattasse di un conto corrente autogestito), il che significa che entrambi hanno una propria coppia di chiavi (pubblica e privata);
3. A questo punto viene creato un "messaggio" (transaction request) composto dalla chiave privata di Ti-

zio (Tprk), la chiave pubblica di Caio (Cpuk), data e ora (timestamp), le informazioni rilevanti che vengono aggiunte al blocco in fase di "costruzione";



4. Il blocco, in sintesi una raccolta di messaggi tra cui quello con cui Tizio comunica a tutti gli altri nodi di aver inviato X BTC a Caio, viene caricato sulla rete e sottoposto a verifica da parte degli altri nodi (transaction request).

Fonte	Messaggio	Sicurezza
Tizio	Mio wallet: – X BTC wallet Caio: + X BTC	Tizio private key
Network	Check Richiesta di Tizio	Tizio public key
Network	Transazione autenticata	50 per cento+1 dei nodi la approva

Nella realtà una transazione avrà tre gruppi di informazioni:

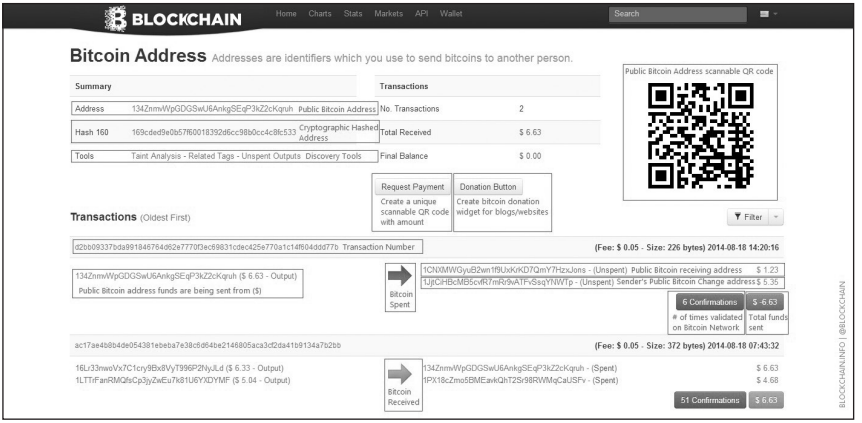
– Input: l'indirizzo da cui l'operazione ha origine;
– Ammontare;
– Output: l'indirizzo di destinazione;

e i nominativi saranno in realtà rappresentati da indirizzi alfanumerici come nell'immagine che segue:

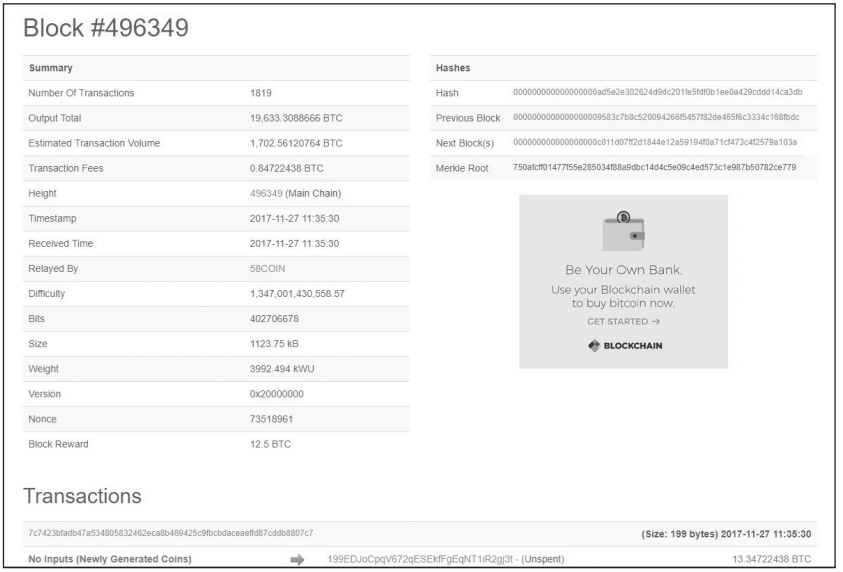
5. A questo punto, una volta convalidata la transazione, il blocco viene aggiunto alla catena e logicamente collegato al blocco precedente e, non appena questo viene "minato" (parleremo dell'attività di mining in uno dei prossimi paragrafi), al blocco successivo.

(Immagine tratta da Lauri Hartikka, A blockchain in 200 lines of code)

6. Le informazioni relative alla transazione vengono, poi, registrate nei wallet di Tizio e in quelli di Caio.

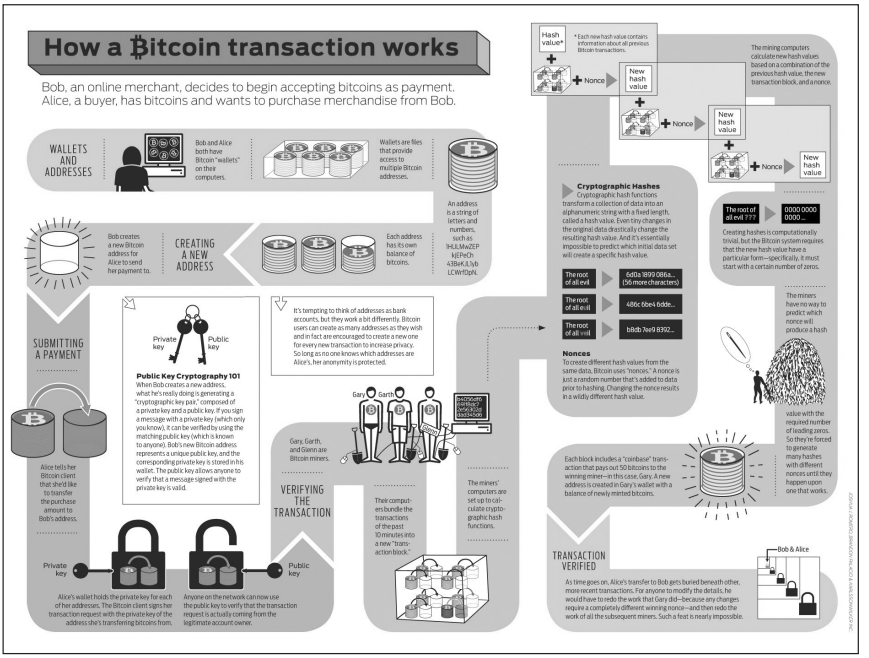


7. Si veda ora l'immagine che segue e che rappresenta lo stesso blocco di cui all'immagine a pagina 22 dopo una decina di minuti:



Il blocco è stato collegato a quello successivo e il suo hash è stato inserito in quest'ultimo, in questo modo diviene impossibile per chiunque modificare un blocco della blockchain senza compromettere anche tutti i blocchi successivi e questa circostanza determina una notevole sicurezza.

Riepiloghiamo ora, utilizzando un'immagine tratta da *How bitcoin works* (Joshua J. Romero, Brandon Palacio & Karlssonwilker Inc):



In estrema sintesi, possiamo vedere la blockchain come un libro mastro di cui i blocchi costituisco-

no le pagine. In ogni blocco sono segnate tutta una serie di transazioni che, fino all'approvazione del blocco, sono da considerarsi in fieri (tecnicamente lo "stato" nel Bitcoin è la raccolta di tutte le monete viste come "transazioni in uscita non spese" UTXO "*unspent transaction outputs*"). Ogni UTXO ha una denominazione e un proprietario (definito da un indirizzo da 20-byte, essenzialmente una chiave crittografica pubblica). Ogni input contiene un riferimento a un UTXO esistente, con una firma crittografica prodotta da una chiave privata associata all'indirizzo del proprietario, e uno o più output, ognuno contenente un nuovo UTXO che deve essere aggiunto allo stato.

A questo punto il sistema può risolvere l'input secondo questo schema:

S = (input UTXO - outpout UTXO), tuttavia se

– il riferimento UTXO non è in S: errore;
– la firma non combacia con il proprietario del UTXO: errore;
– la somma dei valori di tutti gli input UTXO è inferiore alla somma dei valori di tutti gli outpout UTXO: errore.

La prima verifica impedisce ai mittenti delle transazioni di spendere monete che non esistono, la seconda evita che vengano spese monete di altre persone, mentre la terza fa rispettare la conservazione del valore.

2. segue: hashcash come POW

Nel paragrafo precedente abbiamo visto che, prima di aggiungere un nuovo blocco di transazioni alla blockchain, questo deve essere controllato, validato e crittografato. Per arrivare a questo risultato è necessario che, per ogni singolo blocco, venga risolto un complesso problema matematico che richiede un notevole impegno in termini di potenza e capacità di calcolo. Questa operazione viene definita in gergo come *mining* ed è svolta dai cosiddetti miner.

In termini tecnici questa attività è chiamata proof-of-work, e il suo preciso scopo è quello di rendere economicamente non conveniente la falsificazione di un blocco: la potenza di calcolo necessaria per l'operazione sarebbe comunque superiore a quella che occorrerebbe per minarne uno lecito; caratteristica essenziale di questi schemi è la loro asimmetria: il lavoro deve essere complesso dal lato richiedente, ma facile da controllare per il fornitore del servizio.

Nella creazione dei bitcoin viene utilizzato un sistema basato su *hashcash*; si tratta di un algoritmo POW, ideato nel marzo del 1997 da Adam Back sulla base di un'idea presentata da Cynthia Dwork e Moni Naor nel 1992 (*Pricing via Processing or Combatting Junk Mail*), originalmente pensato per contrastare spam e attacchi DdOS.

L'algoritmo usa, infatti, inversioni di hash parziali per verificare che il lavoro sia stato correttamente eseguito e, nel suo modello originale, prevedeva l'inserimento di una stringa di testo negli header del messaggio: una sorta di francobollo elettronico destinato a provare che il mittente aveva speso un certo quantitativo di potenza e tempo di calcolo per inviare il messaggio:

From: Someone <test@test.invalid>
To: Adam Back <adam@cypherspace.org>
Subject: test hashcash
Date: Thu, 26 Jun 2003 11:59:59 +0000
X-Hashcash: 0:030626:adam@cypherspace.org:6470e06d773e05a8

blah blah

- Someone

(esempio tratto da www.hashcash.org)

L'header contiene data e ora di invio del messaggio e destinatario in modo da costringere il mittente a generare un header differente per ogni destinatario. Quest'ultimo non dovrà fare altro che verificare l'SHA-1 hash della riga: se i primi 20 bit dell'hash sono tutti 0, allora siamo in presenza di un hash accettabile.

Nel nostro esempio l'hash è
00000000c70db7389f241b8f441fcf068aead3f0,
quindi la POW è superata.

3. segue: hashcash e Bitcoin

Nel Bitcoin l'applicazione dell'hashcash avviene con modalità particolari che si discostano da quanto appena descritto: in primo luogo viene utilizzato un hash a 256 bit (SHA-256) anziché uno a 160 (SHA-1), in secondo luogo la soluzione del problema avviene in modalità competitiva tra i vari nodi tanto che soltanto il primo miner a fornire un valore corretto si aggiudicherà la ricompensa.

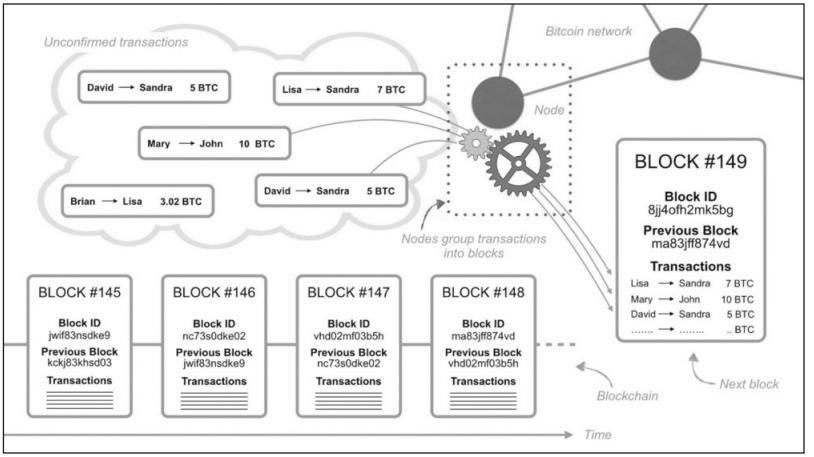
Nelle pagine precedenti abbiamo visto come viene costruito un blocco, ora vedremo come viene verifi-

cato prima di essere inserito nella blockchain. Spesso, infatti, si tende a collegare l'attività di mining alla sola produzione ed emissione di nuovi bitcoin, ma, in realtà, non è questo il suo scopo principale.

Scopo di questo processo è quello di garantire l'integrità e l'autenticità della blockchain, rendendola stabile, affidabile e soprattutto sicura rispetto a eventuali tentativi di contraffazione (si pensi, ad esempio, al rischio di convalidare più transazioni tra loro inconsistenti, *doublespending*).

Trattandosi di un sistema aperto (permissionless blockchain), questa attività può essere svolta da chiunque sia disponibile a installare il relativo programma e dedicarvi un'adeguata potenza di calcolo.

Facciamo un passo indietro e torniamo alla generazione del blocco:



(Immagine tratta da https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae)

Concentriamoci ora sugli header di ogni singolo blocco: si tratta di 80 byte di informazioni che contengono questi dati

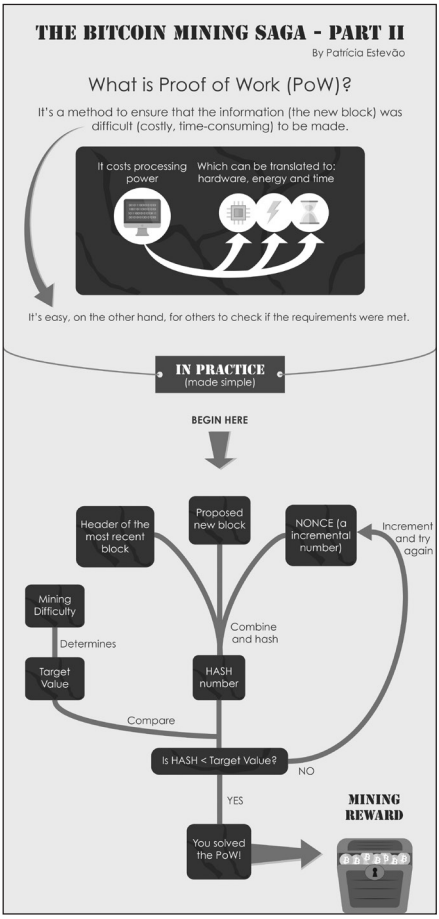
Campo	Descrizione	Dimensioni (in Bytes)
Version	Bitcoin version number	4
hashPrevBlock	256-bit hash del blocco precedente	32
hashMerkleRoot	256-bit hash del cosiddetto "merkle tree" di tutte le transazioni del blocco	32
Time	Timestamp del blocco in formato Unix	4
Difficulty target	Il livello di difficoltà del blocco	4
Nonce	32-bit number (starts at 0) – La soluzione alla POW	4

Abbiamo visto che ogni blocco contiene all'interno degli header l'hash SHA-256 del blocco che lo precede, questi dati sono contenuti all'interno del campo "hashPevBlock".

Nell'header viene, poi, inserita una marca temporale, in formato Unix, della data e dell'ora in cui il blocco viene convalidato: si tratta di un numero intero che indica i secondi trascorsi dal 01 gennaio 1970 UTC.

Questo tipo di rappresentazione offre alcuni vantaggi rispetto alla notazione classica: è compatta, indipendente dai fusi orari, ed è, quindi, direttamente confrontabile anche tra sistemi che si trovano a grandi distanze, ma ha lo svantaggio di richiedere una conversione per averne una rappresentazione facilmente interpretabile e, soprattutto, trattandosi di un campo composto da soli 32 bit, ha il grave difetto di essere vincolata ad un numero massimo pari a 2^{31} (ovvero 2.147.483.648). Questo valore sarà raggiunto il 19 gennaio 2038 alle

ore 03:14:08 GTM e, da quel momento, potranno verificarsi problemi e malfunzionamenti nei vari sistemi che non saranno più in grado di gestire correttamente la data (un po' quello che si temeva sarebbe accaduto alla mezzanotte del 31 dicembre 1999, con il passaggio dal 1999 al 2000, il cosiddetto millenium bug).



Nell'immagine che precede, vediamo uno schema semplificato della POW.

Il concetto di proof-of-work rappresenta il cuore del sistema: l'hash SHA-256 di ogni blocco, costituito come un numero di 256 bit, deve essere inferiore di un target regolato dinamicamente, in modo da rendere computazionalmente "difficile" la creazione di un blocco, prevenendo così gli attacchi.

Riepilogando, il processo di consenso decentralizzato del Bitcoin prevede che i nodi tentino di produrre pacchetti di transazioni chiamati "blocchi"; il sistema è studiato affinché venga prodotto un blocco ogni dieci minuti circa e ogni blocco deve contenere una marca temporale, un numero, un riferimento all'hash del precedente blocco e una lista di tutte le transazioni inserite nel blocco.

Ne consegue che, per poter controllare la validità di un blocco, dobbiamo procedere ai seguenti step:

1. il blocco precedente esiste ed è valido?
2. la marca temporale del blocco è successiva a quella del blocco precedente ed è inferiore di due ore nel futuro?
3. il proof of work sul blocco è valido?
4. S[0] è lo stato alla fine del blocco precedente?
5. le transazioni del blocco sono tutte valide?

Se le risposte sono tutte positive il blocco viene convalidato e si passa al successivo.

Le altre tre voci sono, invece, un po' più complesse da comprendere, quindi le analizzeremo nel dettaglio.

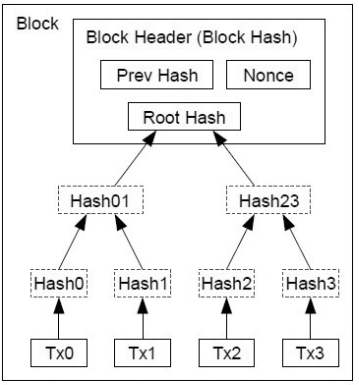
4. HashMerkleRoot

Con questo nome si indica un hash che sintetizza tutte le transazioni ricomprese nel blocco e considerate come le "foglie" di un albero di Merlke (*merkle tree*, dal nome del ricercatore informatico che per primo lo ha ideato).

Si tratta di un albero le cui ramificazioni sono legate a coppie e in cui ogni nodo è etichettato con l'hash dei suoi nodi figli secondo il seguente schema.

Viene acquisito l'hash SHA-256 della prima transazione (H_1), poi della seconda (H_2), della terza (H_3), della quarta (H_4) e così via. A questo punto viene acquisito l'hash della prima e della seconda transazione ($H_{(h1+h2)}$), poi quello della terza e della quarta ($H_{(h3+h4)}$) e così via.

Viene, infine, acquisito l'hash dei due hash ($H_{(h1+h2)}$) + ($H_{(h3+h4)}$) e così via fino a raggiungere la cima dell'albero:



Transactions Hashed in a Merkle Tree

La struttura consente di verificare, in maniera rapida ed efficiente, una grossa quantità di dati; come si evince dall'immagine (tratta da Satoshi Nakamo-

to, *Bitcoin: A Peer-to-Peer Electronic Cash System*), i dati vengono accoppiati a ogni livello fino ad arrivare a un unico hash chiamato top hash o *root*. Questo hash rappresenta la concatenazione di tutti gli hash precedenti quindi, per verificare l'integrità di un singolo blocco sarà possibile considerare solo una parte dell'albero rendendo la procedura molto più snella ed efficiente.

5. Nonce e difficoltà

Le ultime due voci sono strettamente correlate. Iniziamo con il termine *nonce* (che deriva dall'espressione inglese *number used once*, "numero usato una volta"). Con questo termine, in crittografia si indica un numero, generalmente casuale o pseudo-casuale, che ha un utilizzo unico.

Rappresenta il cuore della POW Bitcoin e si tratta di un numero, che i miner devono indovinare, attraverso una serie di tentativi, tale per cui l'hash SHA-256 dell'insieme di dati che rappresenta il blocco sia inferiore a una soglia data o, se preferite, contenga un determinato numero di 0 nei primi campi.

Facciamo un esempio ormai divenuto classico: immaginiamo di avere difficoltà 0, avremo un valore Target pari a 2^{256} combinazioni con una spesa, in termini di potenza richiesta, praticamente ridicola; mano a mano che riduciamo il valore T, però, le combinazioni possibili si riducono drasticamente di modo che appare evidente che più sono gli 0 all'inizio dell'hash, meno saranno le possibili soluzioni e, di conseguenza, maggiore sarà la potenza di calcolo necessaria per indovinare il numero.

Questa soglia, chiamata difficoltà, è ciò che determina la natura concorrenziale del mining di bitcoin;

maggiore è la potenza di calcolo immessa all'interno della rete bitcoin maggiore sarà la difficoltà, aumentando, di conseguenza, il numero di calcoli mediamente necessari a creare un nuovo blocco e incrementando anche il costo di creazione dello stesso.

Facciamo un esempio per chiarire il tutto: preso un blocco B, immaginiamo di voler individuare x (nonce) tale per cui T (l'hash SHA-256 dell'header del blocco composto dalla data di oggi e dalla parola "Esempio") dovrà essere inferiore a 2^{244} (il che equivale a un hash i cui primi tre valori siano uguali a 0): partiremo da questa formula $H(x) \leq T$ dove H(Bx) rappresenta l'hash SHA-256 dell'header.

Avremo:

02-dic-17Esempio1 > B9F3B445FEB7C546577511283C4AF4243685827B

02-dic-17Esempio2 > 02F6AAA4A200CF3B5F4BA7B76DBB55D0331684D7

02-dic-17Esempio > 01926C04D2F6F8DE657F601D5EF1D643A97817FA

02-dic-17Esempio4 > 392069ED667E9785F06F517EEA88A5DDA1939C24

02-dic-17Esempio5 > CBBBBD032AB60B178BCCC339F03854A6A4CCA940

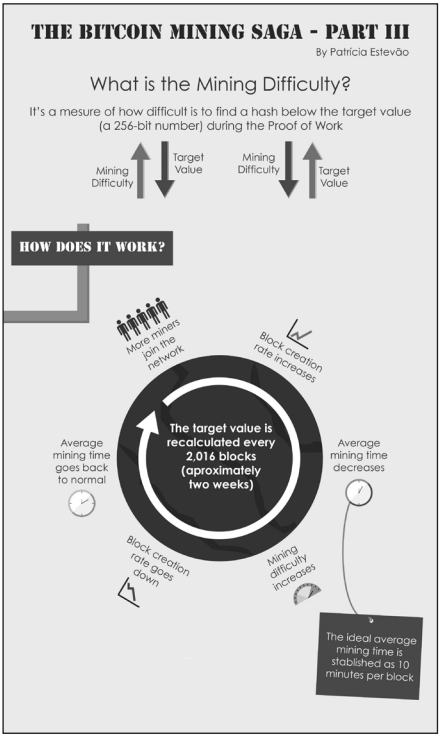
…

02-dic-17Esempio1308 > 0007C8075FC0092C732A222B4D5926CC7CDBBC4E

Abbiamo, dunque, risolto il quesito con soli 1308 tentativi! Naturalmente aumentando il livello di difficoltà, aumenteranno anche i tentativi necessari per risolvere il quesito e, di conseguenza, la potenza di calcolo necessaria.

Nel caso dei bitcoin il livello di difficoltà aumenta ogni due settimane circa, anzi, a voler essere precisi, ogni 2016 blocchi il sistema verifica, confrontando il *timestamp* inserito nei blocchi stessi, il tempo impiegato per generare quei blocchi. Se il valore è inferiore a 1.209.600 secondi (due settimane), il livello di difficoltà viene incrementato proporzionalmente di modo che i successivi 2016 blocchi richiedano esattamente due settimane per essere generati. In caso contrario il livello di difficoltà viene proporzionalmente ridotto.

Nell'immagine che segue, possiamo vedere uno schema semplificato:



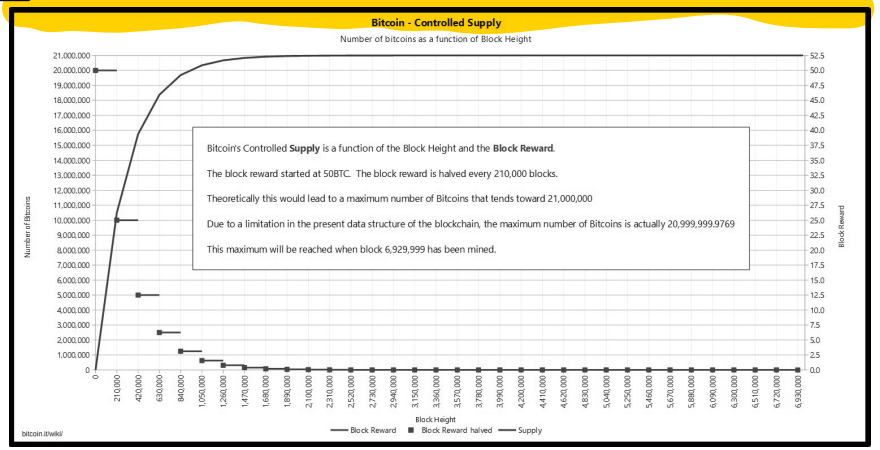
6. I miner

In precedenza, abbiamo fatto più volte riferimento ai miner spiegando che con questo termine si fa riferimento a coloro che materialmente svolgono i calcoli per confermare le transazioni.

Il loro lavoro, fondamentale nella gestione della blockchain e per la stabilità e sicurezza del sistema, è accessibile a chiunque ambisca a svolgerlo gareggiando per essere il primo a risolvere il problema matematico legato alla creazione di un nuovo blocco di transazioni.

I miner, naturalmente, non lavorano gratis: essendo il loro un impegno importante, anche in termini di risorse impiegate, la loro attività necessita di essere remunerata e incentivata attraverso un adeguato corrispettivo.

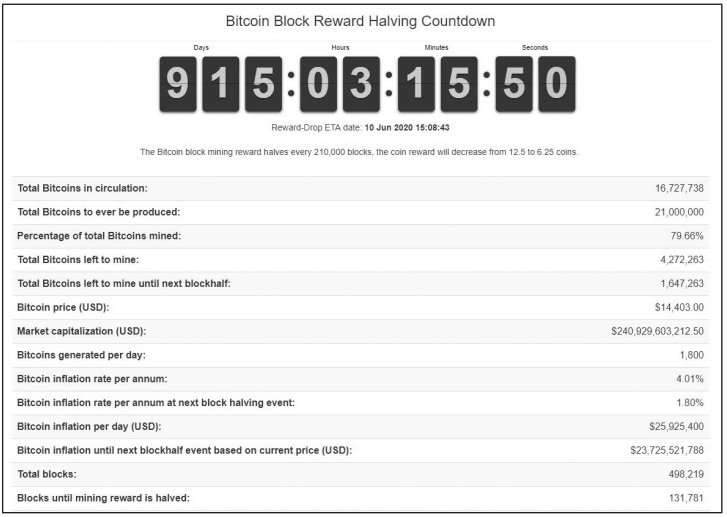
Il primo miner che crea un blocco valido e lo aggiunge alla catena viene ricompensato con il premio e con la somma delle commissioni per le transazioni che ha processato. Le commissioni fanno riferimento a valori unitari per ogni singola transazione e i blocchi posso-



no contenere migliaia di transazioni. Questo determina un valore del compenso molto significativo tanto che, nel progetto Bitcoin, è prevista una progressiva riduzione del premio: da un premio iniziale di 50 BTC (oltre alle commissioni) per ogni blocco si è passati a 25 BTC per ogni blocco nel novembre del 2012 e a 12,5 BTC per ogni blocco nel luglio del 2016:

Con la progressiva riduzione della ricompensa di generazione nel tempo, la fonte del guadagno per i minatori passerà dalla generazione della moneta alle commissioni di transazione incluse nei blocchi, fino al giorno in cui la ricompensa cesserà di essere elargita: per allora l'elaborazione delle transazioni verrà ricompensata unicamente dalle commissioni di transazione ~~stesse~~.

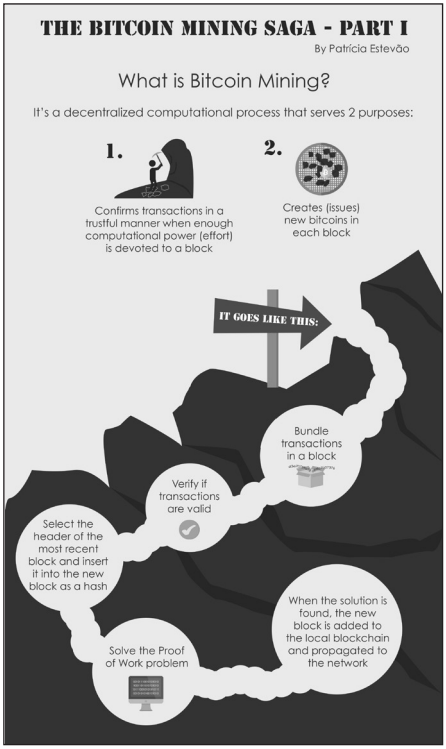
Questo avverrà perché Bitcoin è progettato per raggiungere un tetto massimo di 21 milioni di bitcoin, come si evince dall'immagine qui di seguito:



Al momento, l'importo della commissione può essere impostato liberamente da chi effettua una transazione, anche se dal maggio del 2013, con l'aggiornamento alla versione 0.8.2 del client ufficiale, le commissioni al di sotto della soglia di 0,0001 BTC vengono considerate non standard e, di conseguenza, le transazioni associate rischiano di non essere mai confermate.

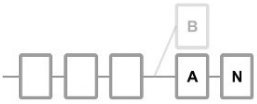
È evidente, quindi, che tanto più è alta la commissione, tanto più è probabile che venga inclusa nel primo blocco estratto, accelerando quindi la conferma; i minatori, avendo la libertà di scegliere quali transazioni includere nel blocco che stanno elaborando, hanno un incentivo a includere in esso le transazioni che garantiscono commissioni più alte. Gli utenti, dal canto loro, sono consapevoli che più alta è la commissione offerta, maggiori saranno le possibilità che la transazione venga elaborata più rapidamente.

Nell'immagine qui a fianco, una rappresentazione schematica delle fasi di mining:

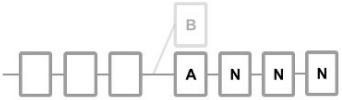


Potrebbe poi accadere che due o più blocchi vengano risolti simultaneamente, in questo caso entrambi verrebbero inviati alla catena ed entrambi verrebbero aggiunti in coda:

A questo punto, il primo nodo che risolve un altro blocco lo invia alla catena e il blocco viene aggiunto a uno dei due blocchi precedenti:



Tutti i blocchi successivi verranno aggiunti al ramo più lungo della catena risolvendo così, nell'arco di dieci minuti, eventuali situazioni di ambiguità:



Questo principio, noto come *longest chain rule*, ha lo scopo di mantenere la stabilità e la coerenza della blockchain evitando situazioni di ambiguità che potrebbero nuocere all'intero sistema.

7. segue: mining 4 dummies

L'attività di mining è particolarmente complessa e, data la sua natura ferocemente competitiva, molti utenti tendono ad associarsi in gruppi per dividere lavoro e ricompense.

Questi gruppi, definiti *mining pool*, lavorano in gruppo, condividendo la propria potenza di calcolo in modo da ottimizzare risultati e guadagni; a tal fine, prima di iniziare, è opportuno fare qualche piccola proiezione costi-benefici, utilizzando uno dei numerosi siti che, attraverso una comoda interfaccia web, consentono di calcolare il rapporto costi-benefici in caso di mining:

– http://99bitcoins.com/bitcoin-mining-calculator/
– http://www.mycryptobuddy.com/BitcoinMining Calculator
– http://www.cryptocompare.com/mining/calculator/

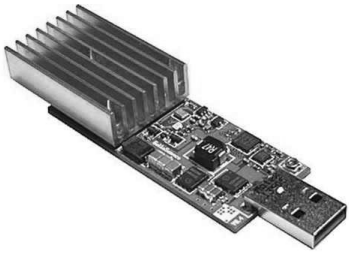
Fatti i nostri calcoli, abbiamo deciso di provare a estrarre bitcoin, che cosa ci occorre?

La prima possibilità è quella di sottoscrivere un contratto di *cloud mining*: in pratica si tratta di una procedura semplificata che libera l'utente dalle spese dell'energia elettrica, dall'acquisto dell'hardware e dall'installazione del software e dal loro monitoraggio quotidiano; l'utente si limita a noleggiare una determinata potenza di calcolo, come in ogni servizio in cloud, per poi trarre degli utili.

Se invece si decide di agire in prima persona, diventa necessario procedere alla valutazione e all'acquisto di hardware e software: in teoria si potrebbe utilizzare un qualsiasi computer, ma qualche rapido calcolo ci dimostra che l'operazione si rivelerebbe

economicamente svantaggiosa dato che la spesa, in termini di consumo energetico e usura del materiale, sarebbe decisamente superiore al guadagno.

Per tale ragione, chi decide di dedicarsi a questa attività, di solito ricorre a specifici hardware (ASIC) come quelli in figura:



A mero titolo di esempio, l'hardware rappresentato a sinistra costa circa 3000 euro, consuma circa 1.5 Kw/h ed è in grado di processare 14 terahash al secondo. Questo significa che, in teoria, è in grado di estrarre 1 BTC ogni 452 giorni circa, garantendo i seguenti guadagni (NB: le cifre sono soltanto indicative, ricavate ipotizzando un costo dell'energia elettrica pari a 0,07 €/Kw, una difficoltà e un valore BTC al giorno 8 dicembre 2017):

Tempo	BTC	Euro	Spesa	Ricavo
Ora	0.00009220	1.50	0.10	1.40
Giorno	0.00221284	35.99	2.36	33.63
Settimana	0.01548988	251.95	16.55	235.40
Mese	0.06638518	1,079.77	70.93	1,008.84
Anno	0.80768636	13,137.26	863.04	2,274.23

Per chi fosse interessato, nelle seguenti pagine è disponibile un'analisi dei differenti hardware:

- http://www.cryptocompare.com/mining/#/equipment
- http://www.bitcoinmining.com/bitcoin-mining-hardware/
- http://en.bitcoin.it/wiki/Mining_hardware_comparison

Per comparare correttamente i diversi hardware è necessario valutare le seguenti caratteristiche:

- *Hash rate* - hash al secondo "Hash/sec" prodotti in GH/s o TH/s;
- *Efficienza* - rapporto tra energia utilizzata e hash calcolati, a volte espressa in W/GH;
- *Prezzo* - costo dell'hardware.

Una volta scelto l'hardware, si rende necessario stabilire quale software utilizzeremo per iniziare a estrarre i bitcoin. Il software sarà responsabile di gestire l'intero processo collegandosi alla blockchain oppure al gruppo di estrazione.

Attraverso l'interfaccia software, sarà possibile consegnare il lavoro svolto dal nostro hardware alla rete Bitcoin e, al tempo stesso, rimanere aggiornati in merito al lavoro svolto dagli altri nodi.

A seconda del sistema operativo utilizzato, sarà necessario scegliere un software adeguato, ma, per fortuna, non mancano prodotti gratuiti per tutti i più diffusi sistemi operativi. A questo proposito, è indispensabile acquisire il software da un canale sicuro

perché, nel caso in cui il programma fosse compromesso, si correrebbe il rischio di inoltrare tutti i propri guadagni a qualcun altro.

Se si decide di giocare da free rider, un ulteriore controllo che bisogna effettuare è che il proprio software sia accettato dagli altri nodi della rete.

8. segue: mining pool

In precedenza, abbiamo visto che sempre più spesso gli utenti decidono di associarsi in "gruppi di lavoro" organizzati, definiti mining pool.

Il vantaggio di questa pratica è rappresentato dal fatto che, unendo le proprie risorse di calcolo, è molto più facile arrivare a essere il primo gruppo a convalidare un blocco e, quindi, è possibile ridurre al minimo il numero di blocchi estratti e non accettati dalla catena.

Ricordiamo, infatti, che ogni blocco deve contenere l'hash del blocco precedente, quindi ogni volta che un nodo estrae un blocco, tutti i calcoli fatti sino a quel momento dagli altri nodi diventano inutili.

In questa ottica, si comprende l'importanza di disporre di una potenza di calcolo tanto elevata da garantire una buona possibilità di essere i primi a estrarre un blocco e a ottenere il premio: questa potenza può essere messa in campo solo da gruppi sufficientemente grandi di utenti come quelli che si uniscono nelle principali e più remunerative pool.

In genere le associazioni richiedono il pagamento di una quota di ingresso, di una percentuale sui bitcoin guadagnati, mentre la ripartizione degli utili avviene in base alla potenza di calcolo messa a disposizione.

Le associazioni più importanti possono contare su decine di migliaia di utenti e sono in grado di processare qualche exa hash al secondo! Tanto per intenderci, un exa hash equivale a un trilione (10^{18}) di hash pari a oltre mille peta hash che a loro volta equivalgono a oltre mille tera hash.

Di fronte a una simile potenza di calcolo la possibilità di un free rider di arrivare primo è praticamente nulla.

Stabilito che la scelta più proficua è quella di aderire a un pool, si rende necessario valutare:

– tasse da pagare per la gestione: di solito variano dallo 0 per cento fino al 5 per cento, la media si attesta sul 2 per cento;
– pagamento minimo: rappresenta la soglia minima da raggiungere per poter ritirare i propri utili;
– vardiff: questo acronimo indica un livello di difficoltà variabile in modo da agevolare i miner più veloci e quelli più lenti;
– moneta da estrarre: alcune associazioni permettono di scegliere tra diverse criptovalute, mentre altre consentono di estrarre contemporaneamente diverse criptovalute senza perdita di efficienza;
– come viene pagato il premio una volta risolto un blocco. A questo proposito è necessario dare una definizione di *share*, in quanto tutti i sistemi di pagamento si basano sulla valutazione degli share condivisi dai singoli utenti. In breve si tratta di un hash più facile da trovare rispetto al "bersaglio" e che, per tale ragione, viene utilizzato per verificare il lavoro effettivamente svolto dai membri del pool.

• Pay-per-Share: (PPS - pagamento per condivisioni) offre un pagamento immediato per ogni share che

viene risolto da un utente. Questi ultimi vengono retribuiti dai fondi di cui dispone il pool e questo significa che l'associazione deve disporre di ingenti fondi per far fronte ai periodi sfortunati. Questo modello è quello che presenta i maggiori vantaggi per gli utenti che possono contare su un'entrata stabile, legata alla potenza di calcolo fornita traslando l'intero rischio sul pool.

- Proportional: (PROP - proporzionale): ogni volta che un blocco viene risolto, i minatori ricevono un compenso proporzionale agli share condivisi.
- Bitcoin Pooled mining: (BPM), noto anche come *slush's system* in quanto utilizzato per la prima volta in un'associazione nota come *slush's pool*, utilizza un sistema dove vengono valorizzati soprattutto gli ultimi share rispetto ai primi, in modo da vanificare la prassi di passare da un pool a un altro per massimizzare i profitti.[1]
- Pay-per-last-N-shares: (PPLNS) si tratta di un metodo simile al Proportional, ma il compenso dei miner viene calcolato esclusivamente sulla base degli ultimi N share inviati.
- Geometric method: (GM) detto anche SCORE metod, inventato da Meni Rosenfeld e basato su un'idea simile al PPLNS, il sistema prevede che il punteggio assegnato a ogni nuovo share sia tale da mantenere una determinata media di modo che non vi sia alcun vantaggio nel minare prima o dopo.

1. Quando si partecipa a un pool il rapporto costi-benefici è maggiore all'inizio dell'estrazione, in cui è più facile trovare share non ancora condivisi. Per tale ragione alcuni miner disonesti passano da un pool a un altro per massimizzare i profitti legati a questa prima fase.

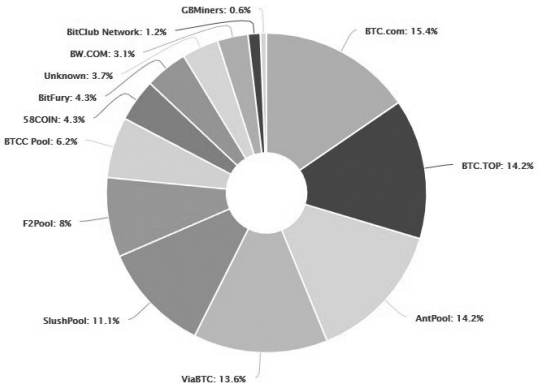
- Double Geometric method: (DGM) si tratta di un metodo che combina GM e PPLNS implementando nuovi parametri in modo da regolarizzare i pagamenti indipendentemente dal tempo necessario a estrarre un nuovo blocco valido.
- Shared Maximum Pay Per Share: (SMPPS) adotta un approccio simile al PPS, ma i pagamenti sono limitati ai bitcoin estratti dal pool.
- Equalized Shared Maximum Pay Per Share: (ESMPPS) simile al SMPPS, ma distribuisce equamente i pagamenti tra tutti i miner del pool.
- Recent Shared Maximum Pay Per Share: (RSMPPS) simile al SMPPS, ma privilegia gli ultimi share.
- Capped Pay Per Share with Recent Backpay: (CPPSRB) utilizza un sistema per pagare i miner il più possibile utilizzando i bitcoin precedentemente estratti con un sistema PPS, ma senza correre il rischio di andare in passivo.
- Pay on Target: (POT) variante del PPS che corrisponde un compenso in base alla difficoltà del lavoro svolto dai miner piuttosto che alla difficoltà del lavoro svolto dal pool.

A parte dobbiamo considerare il metodo Triplemining, generalmente adottato da pool di dimensioni medie senza commissioni. Gli amministratori, utilizzando parte dei bitcoin estratti, mettono in premio un jackpot che verrà assegnato all'utente che riesce a validare il blocco. In questo modo ogni utente ha una chance di incrementare i propri profitti, indipendentemente dalla Potenza di calcolo di cui dispone.

Nel caso di *multipool mining*, invece, il pool passa da una criptovaluta a un'altra dedicandosi a quella

che in quel dato momento garantisce i maggiori profitti per poi convertirli in una specifica criptovaluta, tipicamente i bitcoin.

Nell'immagine che segue, tratta da blockchain.info, una stima della distribuzione della potenza di calcolo erogata nelle ultime ventiquattro ore, dato acquisito il 16 dicembre 2017:



Per un confronto tra i differenti gruppi di lavoro si rimanda a:

http://en.bitcoin.it/wiki/Comparison_of_mining_pools

http://medium.com/@NikitaFreeman1ap/10-best-and-biggest-bitcoin-mining-pools-comparison-2017-cb4ef322eb4

http://www.buybitcoinworldwide.com/mining/pools/

9. segue: il software

Una volta stabilito quale hardware utilizzare e se aderire o meno a un mining pool è necessario stabilire quale software utilizzare: quest'ultimo ci collegherà alla blockchain se opereremo da free rider o alla mining pool se aderiremo a un gruppo di lavoro.

Molti dei programmi a disposizione possono funzionare in entrambe le modalità ("solo" o "pool") e alcuni di questi hanno già una serie di pool preconfigurati in modo da agevolare la connessione.

Il primo e principale compito del software sarà quello di metterci in contatto con il resto della rete, ricevendo il lavoro svolto dagli altri miner e inviando loro il nostro, monitorare il nostro hardware (hash rate, temperatura, consumi eccetera) e gestire i pagamenti attraverso il nostro e-wallet (portamonete virtuale).

A tal fine sarà importantissimo configurare correttamente l'indirizzo del nostro portafoglio virtuale dato che qui verranno inoltrati i pagamenti frutto della nostra attività: perdere l'accesso al wallet significa perdere senza possibilità di recupero tutti i nostri bitcoin.

Nella scelta del programma dovranno essere presi in considerazione questi elementi:

– Risorse impegnate dal programma – il programma dovrebbe occupare meno risorse possibili dato che l'obiettivo è dedicare la massima percentuale dalla potenza di calcolo all'estrazione.
– Affidabilità del programma – in genere si tende a preferire programmi open source e riconosciuti come affidabili dalla comunità.
– Costo del programma – esistono numerosi validi programmi open source o freeware.

– Accesso remoto – possibilità di gestire l'hardware da remoto.
– Multiminer support – possibilità di gestire più dispositivi hardware attraverso un'unica interfaccia.

Una volta installato il software, dovranno essere presi in considerazione i seguenti valori:

– Invalid Block/Stale Shares/Rejected Shares: indica che un blocco inviato non è stato accettato; di solito questo accade perché un blocco è arrivato in ritardo ed è già stato risolto da un altro nodo. Questo blocco non genererà alcun compenso e, perciò, questo valore dovrebbe essere il più basso possibile.
– HW Error – è la percentuale di hash che risultano sistematicamente errati, anche questo valore dovrebbe essere inferiore al punto percentuale.
– PoolUpTime – indica quando la pool è attiva; a differenza degli altri, questo valore dovrebbe essere superiore al 99 per cento.
– PCUptime – indica per quanto tempo il computer è rimasto con il programma attivo. Anche in questo caso l'obiettivo è raggiungere valori superiori al 99 per cento.

10. Browser mining

Una modalità particolarmente interessante, ma anche molto controversa, di mining è rappresentata dal cosiddetto *browser mining*: si tratta di integrare alcuni script nel codice delle pagine web di modo che, mentre l'utente visita il sito e fruisce dei contenuti, una percentuale della sua potenza di calcolo viene impiegata per minare criptovalute (generalmente monero, ma non solo).

Diciamo subito che, in linea di massima, non c'è nulla di male nell'impiegare questo sistema per autofinanziare e sostenere il proprio sito web, purché il tutto venga fatto alla luce del sole e senza pregiudicare la possibilità del visitatore di continuare a utilizzare la propria macchina.

A tal fine è necessario che l'attività venga adeguatamente pubblicizzata nel sito, mediante un banner o altro sistema, che informi i visitatori che non vengano effettuate richieste eccessive (al di sopra del 50 per cento della potenza disponibile) e, soprattutto, che l'attività di mining cessi non appena il visitatore abbandona il sito.

L'idea venne presentata nel maggio 2011 attraverso il sito BitcoinPlus.com

All'epoca minare bitcoin con la sola CPU era ancora possibile, ma in breve tempo il sito conobbe una rapida crescita per poi essere rapidamente sostituito dall'avvento dei dispositivi ASIC.

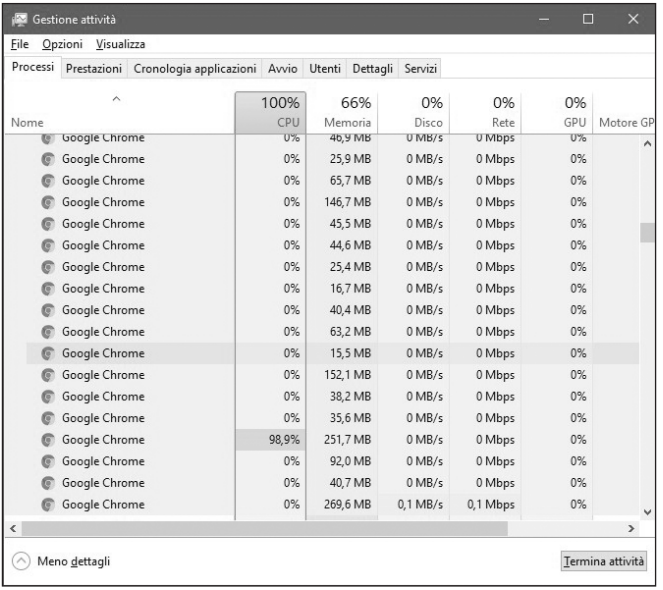
Nel 2013 il progetto venne ripreso da un gruppo di studenti del MIT come forma di autofinanziamento per siti web, ma Tidbit, questo il nome del progetto, venne bloccato dalla Division of Consumer Affairs che avviò un'indagine per accesso abusivo a sistemi informatici altrui.

Ancora una volta la chiave di volta dell'intera vicenda è la chiarezza: il browser mining può essere legittimamente utilizzato solo con il consenso dell'utente.

Nella seconda metà del 2017 Coinhive (coinhive.com) ha rilasciato un proprio script per inserire in un sito web un miner monero resuscitando, di fatto, il vecchio progetto di BitcoinPlus.

Purtroppo non è mancato chi, abusando dello strumento, ha iniziato a inserirlo in pagine web senza dire nulla ai propri utenti (cosa già di per sé gravissima), arrivando a creare script in grado di rimanere attivi anche dopo la chiusura della pagina di origine nel browser. Lo hanno rivelato i ricercatori di Malwarebytes, spiegando come sia possibile sfruttare un pop-under per raggiungere lo scopo: in pratica si tratta di una finestra che si apre, ma non va in primo piano come i tradizionali pop-up; in questo modo, sfruttando una minima percentuale della potenza di calcolo, ci sono buone probabilità che passi inosservata.

Di seguito un'immagine che mostra l'eccessivo utilizzo della CPU da parte di una pagina web:



A oggi la situazione è molto fluida anche se numerosi browser hanno iniziato a implementare plugin in grado di intercettare e bloccare le chiamate al pool di Coinhive rendendo di fatto inutile quello che ben avrebbe potuto rappresentare una valida alternativa alla pubblicità per i siti web che offrono contenuti.

Per approfondire si consiglia:

https://www.tomshw.it/mining-via-browser-continua-anche-se-chiudi-finestra-89987

https://www.extremetech.com/computing/257786-browser-cryptocurrency-mining-exploding-across-web

https://www.symantec.com/blogs/threat-intelligence/browser-mining-cryptocurrency

https://researchcenter.paloaltonetworks.com/2017/10/unit42-unauthorized-coin-mining-browser/

Per una guida su come rimuovere Coinhive Miner Trojan si veda: https://malwaretips.com/blogs/remove-coinhive-miner-virus/

1.4 Permissioned blockchain: oltre le criptovalute

Analizzare vantaggi e caratteristiche delle *permissioned blockchain* è attività che esula dalla portata del presente manuale, ragion per cui ci limiteremo qui a una rapidissima analisi delle loro caratteristiche principali.

L'estrema fluidità delle *permissionless blockchain*, la loro trasparenza, l'assenza di un'autorità di controllo e gli alti costi di gestione in termini di risorse di calcolo impiegate sono tutte circostanze in grado di spaventare molti potenziali utenti, tra cui l'alta finanza, la sanità e tutti quei sistemi che necessitano di forme centrali di controllo e di verifica e di garanzie in merito alla riservatezza dei dati.

Queste garanzie vengono generalmente offerte da modelli basati su permissioned blockchain, in cui le transazioni possono essere convalidate esclusivamente da un utente noto e approvato, garantendo forme di controllo e verifica dall'alto.

Un altro notevole vantaggio è rappresentato dalle migliori performance che una permissioned blockchain è in grado di garantire e dall'assenza di quello spreco di risorse che caratterizza le permissionless blockchain.

In linea di massima l'idea alla base di una permissioned blockchain non è differente da quella alla base di una permissionless se non per la presenza di un livello di controllo superiore in grado di inibire in tutto o in parte l'accesso (anche solo in scrittura) a nuovi nodi.

1. Blockchain e finanza: Corda

Una prima applicazione di questo modello al mondo della finanza è rappresentato dal modello costruito dal consorzio R3, composto da oltre settanta istituti di alta finanza e finalizzato a ricercare e sviluppare come utilizzare nel migliore dei modi questa tecnologia nel mondo della finanza.

A tal fine, il consorzio R3 ha realizzato e sviluppato una propria piattaforma chiamata Corda: sebbene si ispiri alla tecnologia alla base della blockchain, la piattaforma non è una blockchain propriamente detta, tanto che il consorzio preferisce parlare di *shared ledger* anziché *distributed ledger*.

La ragione di questa scelta è legata al fatto che l'ispirazione all'origine della blockchain è basata sul concetto che il consenso sull'affidabilità dell'informazione deve essere raggiunto a livello di registro: questo significa che i dati di tutte le transazioni devono essere propagati a tutti i nodi del registro e da questi devono essere approvati, il che, nel contesto bancario e finanziario, solleverebbe concrete problematiche legate alla tutela della riservatezza delle transazioni.

Corda adotta un approccio differente, basato sul concetto di *need to know*: le informazioni sulle transazioni vengono condivise soltanto tra coloro che sono parti della transazione stessa e che hanno bisogno di conoscerle; in questo modo viene garantita la riservatezza delle operazioni, con un approccio che sembra essere maggiormente coerente con i servizi finanziari in cui la riservatezza delle informazioni è un elemento fondamentale (CFR http://www.corda.net/).

Il codice sorgente di Corda è stato rilasciato rendendolo disponibile a tutti, nel tentativo di renderlo

uno standard condiviso in grado di sostituire il modello blockchain, come dichiarato dal consorzio R3:

> *We want other banks and other parties to innovate with products that sit on top of the platform, but we don't want everyone to create their own platform… because we'll end up with lots of islands that can't talk to each other… If we have one platform with lots of products on top, then we get something that's more like the internet, where we still get innovation but we can still communicate with each other.*

2. Blockchain e notariato: Notarchain

Un altro esempio di permissioned blockchain è rappresentato dal progetto *Notarchain*, presentato il 13 ottobre 2017 a Palermo; si tratta di una blockchain gestita dai notai in grado di rispondere alle esigenze di digitalizzazione del Paese e di garantire la sicurezza nelle transazioni.

In breve, si tratta di un'applicazione concreta della blockchain come registro diffuso: il progetto, in partnership con IBM, prevede la realizzazione di una permissioned blockchain nella quale le informazioni siano gestite dai notai italiani; la piattaforma, pur mantenendo intatte le potenzialità connesse alla velocità, all'assenza di costi per il cittadino fruitore, alla diffusione su scala mondiale, garantirebbe la veridicità dei dati contenuti grazie all'attività dei notai.

Si tratta di una base digitale di archiviazione e gestione di ogni tipo di file digitale e pertanto il suo utilizzo potrà in futuro essere esteso a molti ambiti applicativi che necessitano di un sistema di maggiore sicurezza e certificazione (disegni, opere d'arte, beni mobili in genere).

La stessa tecnologia di blockchain è alla base anche del secondo progetto presentato dal notariato in partnership con SIAE e finalizzato alla gestione del deposito e archiviazione dei codici sorgente.

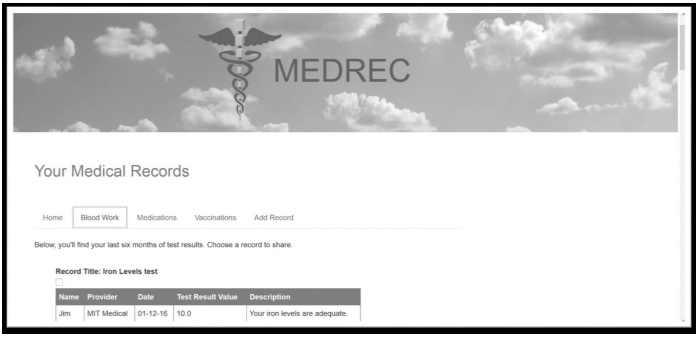
In questo modo sarà possibile depositare presso un qualsiasi notaio italiano il codice sorgente di un nuovo programma ottenendo, in tempo reale, l'inserimento di tale file in un registro condiviso con SIAE che permette l'immediata attribuzione di una marca temporale e quindi la certezza che nessuno possa in futuro appropriarsene.

3. Blockchain e salute: MedRec

Un altro ambito in cui può trovare impiego la blockchain è rappresentato dal progetto MedRec un prototipo per la raccolta, la conservazione e l'analisi dei dati medici (cfr. *A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data*, Asaph Azaria, Ariel Ekblaw, Thiago Vieira, Andrew Lippman, IEEE, 2016; http://www.pubpub.org/pub/medrec).

Il progetto MedRec si propone di realizzare un sistema in grado di offrire ai pazienti l'accesso ai propri dati sanitari in maniera decentralizzata, garantendone al contempo l'immutabilità utilizzando la blockchain; in questo modo sarà possibile garantire e gestire autenticazione, riservatezza, attendibilità, accessibilità e responsabilità delle informazioni immesse.

Smart contract su una blockchain Ethereum aggregheranno i dati e ne garantiranno la conservazione e l'accesso e l'integrazione esclusivamente a soggetti muniti di autorizzazione alla lettura o all'inserimento di nuovi dati attraverso una semplice interfaccia:



I dati immessi dai medici saranno resi accessibili ai ricercatori e ai laboratori che svolgeranno il ruolo di miner ottenendo in cambio metadati anonimizzati, ma comunque utili per la ricerca.

2. Le altre criptovalute

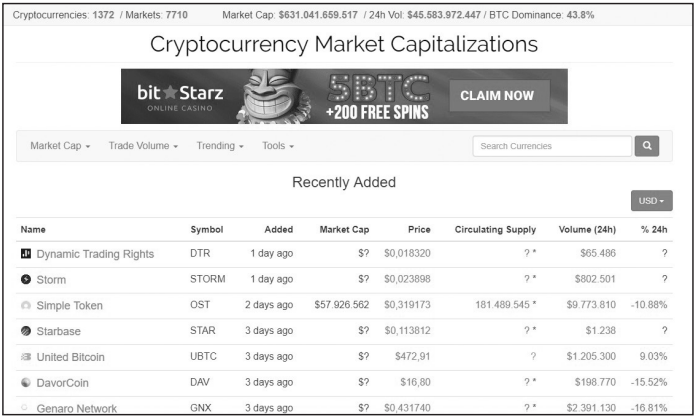
2.1 Criptovalute e valute complementari

Nel capitolo precedente abbiamo descritto il funzionamento della blockchain e il sistema Bitcoin, vediamo ora di scoprire alcune delle altre criptovalute confrontandone pregi e difetti.

La caratteristica open-source del progetto Bitcoin ha, infatti, non soltanto permesso la partecipazione di molti sviluppatori che nel corso degli anni hanno contribuito allo sviluppo del software e alla correzione delle vulnerabilità che via via si sono presentate, ma, soprattutto, ha consentito la nascita di numerose criptovaltute alternative generalmente indicate come *altcoin*.

Contare le altcoin è impossibile, nuove valute nascono ogni giorno mentre altre scompaiono, ma in linea di massima possiamo stimare il loro numero intorno alle millecinquecento, ~~ma~~ di queste solo alcune vengono realmente utilizzate.

Accanto alle altcoin virtuali esistono, poi, altre valute complementari utilizzate in determinati ambiti: si pensi ai sistemi di pagamento utilizzati in molti villaggi turistici o in club e pub, ma anche in alcune regioni.



È bene ricordare che tutte le valute complementari rappresentano meri strumenti di scambio, con cui è possibile scambiare beni e servizi affiancandosi in tal modo al denaro ufficiale; solitamente non hanno corso legale e sono accettate esclusivamente su base volontaria.

In breve, le valute complementari si collocano come "sistemi di scambio" all'interno di una comunità e vengono utilizzate a questi fini promuovendo una pianificazione a lungo termine e stimolando i partecipanti al circuito a investire in attività connesse, piuttosto che nell'accumulo, incoraggiando gli scambi e la cooperazione.

Esistono migliaia di sistemi di valuta complementare, anche se i principali sono essenzialmente riconducibili ad alcuni schemi-tipo come ad esempio le cosiddette "banche del tempo", in cui si attribuisce alle ore-lavoro dei partecipanti un valore che questi possono spendere per acquistare determinati beni o servizi. Alcuni sistemi funzionano come sistemi di credito reciproco mentre altri sono "garantiti" da un riferimento esterno.

In Italia esistono diversi progetti attivi come Sardex, Tibex, Scec, Ecoroma, Promessa di Pisa, Palanca di Genova ed EuroSic.

Un altro sistema che si sta diffondendo a livello mondiale è lo scambio di merci in compensazione, in questo modo imprese che aderiscono a un circuito specializzato acquistano beni o servizi assumendo un debito che compensano successivamente con la vendita di beni e servizi propri secondo lo schema del baratto.

Valute complementari possono essere considerate anche i buoni carburante, i buoni pasto, le miglia accumulate dai viaggiatori aerei, i punti dei supermercati, quelli delle stazioni di servizio, alcuni ticket-consumazione offerti in pub o discoteche eccetera.

Un aspetto comune a tutte le valute alternative è rappresentato dal fatto che il loro valore è direttamente proporzionale alla loro desiderabilità e spendibilità: finché questi due valori restano elevati il valore delle valute sale, anche rapidissimamente, come accaduto per i bitcoin, ma altrettanto rapidamente potrebbe crollare laddove questa fiducia dovesse venire a mancare.

Vediamo ora di conoscere alcune delle principali criptovalute.

2.2 Litecoin (LTC)

Litecoin è una valuta digitale peer-to-peer simile al bitcoin che promette pagamenti istantanei a costi molto bassi, indipendentemente dalla collocazione delle parti interessate. Rispetto a Bitcoin, Litecoin promette una maggiore frequenza nella conferma delle transazioni e una migliore efficienza nella conservazione dei dati.

A oggi, 27 dicembre 2017, Litecoin rappresenta la quinta valuta sul mercato con una capitalizzazione di oltre 17 miliardi di dollari (contro i 267 miliardi di Bitcoin).

1. Le principali differenze

Rispetto a Bitcoin, Litecoin presenta almeno tre differenze fondamentali che, nell'ottica degli sviluppatori, dovrebbero renderlo migliore.

Litecoin mira a elaborare un blocco ogni 2,5 minuti, rispetto ai 10 minuti previsti da Bitcoin; ciò determina una conferma più veloce delle operazioni al costo di un più veloce aumento delle proporzioni della blockchain e un numero maggiore di blocchi orfani.

Litecoin utilizza *scrypt* (si pronuncia "*ess crypt*" e non deve essere confuso con il termine "script" che in informatica designa una particolare tipologia di programmi) come algoritmo POW: l'algoritmo originale venne creato da Collin Percival per il servizio di backup online Tarsnap e aveva l'obiettivo di rendere eccessivamente costoso eseguire un attacco hardware su larga scala. Questa scelta rende i miner Litecoin più complicati da creare e più costosi da produrre rispetto a quelli per Bitcoin.

Litecoin è progettato con un tetto di 84 milioni di monete, il quadruplo rispetto a Bitcoin, il cui cap è fissato in 21 milioni di monete.

Di seguito una tabella con le principali differenze:

	Bitcoin	Litecoin
CAP	21 milioni	84 milioni
Algoritmo	SHA-256	Scrypt
Un nuovo blocco ogni	10 minuti	2.5 minuti
Aggiornamento difficoltà	2016 blocchi	2016 blocchi
Aggiornamento premio	Dimezzato ogni 210.000 blocchi	Dimezzato ogni 840.000 blocchi
Premio iniziale	50 BTC	50 LTC
Premio al 27/12/2017	12.5 BTC	25 LTC
Analisi blocchi	Blockchain.info	bchain.info/LTC/
Sito web	Bitcoin.org	Litecoin.org
Creatore	Satoshi Nakamoto	Charlie Lee
Data creazione	3 gennaio 2009	7 ottobre 2011

2. *SegWit*

Litecoin è stata una delle prime tra le criptovalute di punta ad adottare il sistema SegWit (Segregated Witness - Consensus layer), applicato anche a Bitcoin e finalizzato a rendere più veloci le transazioni.

A tal fine, semplificando al massimo, i dati relativi alle firme vengono rimossi dalle transazioni rendendo i rispettivi file più piccoli e alleggerendo anche i blocchi. Questo significa anche che più transazioni possono essere aggiunte a un singolo blocco rendendo il processo di convalida più veloce.

Tecnicamente, possiamo dire che si tratta di un *soft fork* che consentirà al software di produzione delle

transazioni di lavorare separando le firme (*witness data*) dalla parte "dati" e gestendola separatamente; in questo modo la sezione originale continuerà a conservare i dati di mittente e destinatario, mentre la nuova sezione *witness* conterrà gli script e le firme.

Per approfondire: https://cointelegraph.com/explained/segwit-explained

https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

2.3 Monero (XMR)

Monero (XMR) è una criptovaluta, creata nell'aprile 2014, che si focalizza sulla privacy, la decentralizzazione e la scalabilità. Sin dalla presentazione si dimostra focalizzata proprio sulla riservatezza e non tracciabilità:

> *Monero is a secure, private, and untraceable cryptocurrency. It is open-source and accessible to all. With Monero, you are your own bank. Only you control and are responsible for your funds. Your accounts and transactions are kept private from prying eyes.*
>
> (getmonero.org)

Monero basa la propria POW sull'algoritmo CryptoNight mentre la blockchain è basata sul protocollo CryptoNote, caratterizzato da differenze significative relative all'offuscamento della blockchain.

CryptoNote, concettualmente, rappresenta un'evoluzione indirizzata alla tutela della riservatezza delle idee sottostanti a Bitcoin; la blockchain in cui vengono memorizzate le transazioni è, infatti, quasi anonima dato che le valute basate su CryptoNote

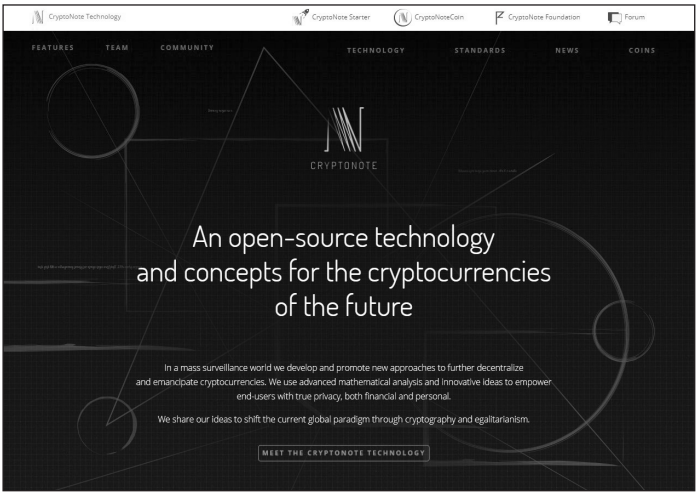
usano una "contabilità pubblica" distribuita in cui vengono registrati tutti i bilanciamenti e le transazioni della valuta, ma che non consente la tracciabilità tipica della blockchain Bitcoin. Le uniche persone ad avere accesso a tutte le informazioni sono chi invia e chi riceve il denaro.

Di seguito una tabella con le principali differenze:

	Bitcoin	Monero
CAP	21 milioni	18,4 mil. poi 0.6 XMR ogni 2'
Algoritmo	SHA-256	CryptoNight
Un nuovo blocco ogni	10 minuti	2 minuti
Aggiornamento difficoltà	2016 blocchi	Ogni blocco
Aggiornamento premio	Dimezzato ogni 210.000 blocchi	Riduzione progressiva
Premio iniziale	50 BTC	32 XMR
Premio al 27/12/2017	12.5 BTC	5,54
Analisi blocchi	Blockchain.info	bchain.info/LTC/
Sito web	Bitcoin.org	getmonero.org
Data creazione	3 gennaio 2009	18 aprile 2014

1. CryptoNote

Il progetto CryptoNote (cryptonote.org), basato su una licenza open source, si presenta come la criptovaluta del futuro e sostiene di rappresentare l'evoluzione *privacy oriented* del Bitcoin.



Nel suo white paper di presentazione (Cryptonote v 2.0) Nicolas van Saberhagen parte dall'analisi di quelle che, a suo avviso, rappresentano le principali criticità del sistema Bitcoin affermando che «*privacy and anonymity are the most important aspects of electronic cash*» per poi osservare che «*Bitcoin does not satisfy the untraceability requirement*».

La seconda critica che viene mossa al Bitcoin riguarda la POW adottata e la circostanza che, con il diffondersi delle mining pool, la potenza di calcolo sia sempre di più concentrata nelle mani di un ristret-

to numero di persone violando il principio «*one CPU, one vote*» che dovrebbe essere alla base del sistema:

> *Therefore, Bitcoin creates favourable conditions for a large gap between the voting power of participants as it violates the "one-CPU-one-vote" principle since GPU and ASIC owners posses a much larger voting power when compared with CPU owners. It is a classical example of the Pareto principle where 20 per cento of a system's participants control more than 80 per cento of the votes.*

Seguono, poi, altre critiche relative alla possibilità di prevedere con precisione il momento in cui il premio verrà dimezzato e di come questo momento porti alla momentanea perdita di interesse da parte di molti miner: si tratta della situazione migliore per perpetrare un attacco *double spending*, dato che è più facile puntare ad avere il controllo sul 50 per cento +1 dei nodi.

Le ultime critiche vengono mosse ai limiti tecnici del sistema, alla sua scarsa flessibilità e scalabilità, per poi passare a presentare CryptoNote, la cui principale caratteristica è indubbiamente la non tracciabilità delle transazioni.

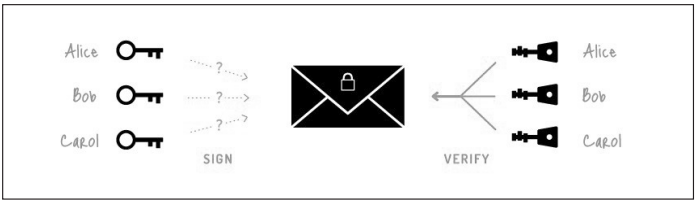
La filosofia alla base del progetto è di consentire la creazione di una criptovaluta completamente anonima, in cui tutti i nodi abbiano lo stesso "peso" indipendentemente dalla potenza di calcolo e completamente affidata al controllo degli utenti:

> *It is in our philosophy to encourage enlightenment through breakthrough innovations. Emancipation begins with laymen getting access to financial resources that will give the oppressed the hope for quality education, drinking water, and a better life. CryptoNote is not about creating yet another digital currency. It is the mindset and concepts that represent the*

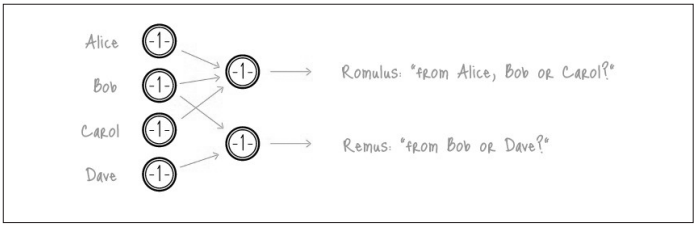
first small step to regain the power over ourselves in order to live peacefully and prosper.

I punti di forza di CryptoNote vengono indicati nel citato white paper e riassunti nel sito ufficiale del progetto (criptpnote.org - immagini, tratte da https://cryptonote.org/inside). Di seguito alcuni degli aspetti più rilevanti:

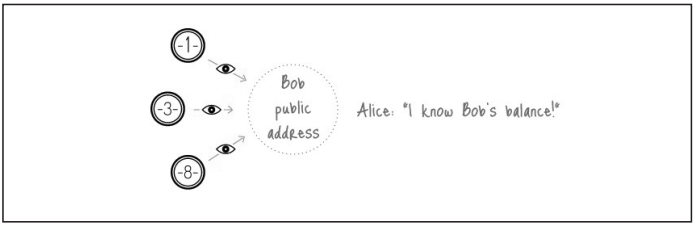
1. *Ring signatures*: i pagamenti non sono tracciabili. Nelle procedure ordinarie il processo di verifica richiede all'utente di utilizzare la propria coppia di chiavi, ma questa caratteristica rende possibile individuare l'autore della transazione; nel sistema adottato da CryptoNote, invece, abbiamo un gruppo di individui, ciascuno con la propria coppia di chiavi.
   A questo punto, la firma viene verificata con la chiave pubblica del gruppo: in questo modo per chi verifica sarà impossibile stabilire l'esatta identità del soggetto che ha effettuato la transazione.



Le chiavi pubbliche di Alice, Bob e Carol sono racchiuse nella chiave pubblica del gruppo: in questo modo Romulus, destinatario della transazione, non sarà in grado di sapere chi, tra i tre soggetti indicati, l'ha effettuata:

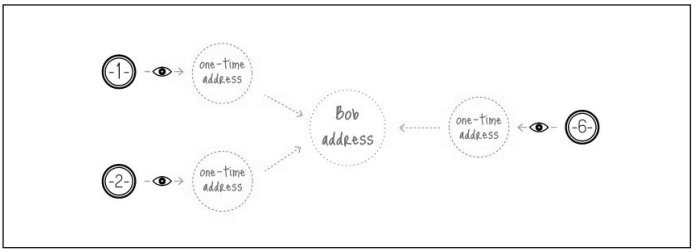


2. *One-time keys*: impossibilità di collegare le transazioni tra di loro. Di solito, quando un utente divulga il suo indirizzo pubblico, chiunque può verificare tutti i movimenti legati a quello specifico indirizzo:



Per evitare questo rischio è possibile creare un numero infinito di chiavi differenti, ma questo sistema priva l'utente del vantaggio di avere un unico indirizzo pubblico. Per ovviare a questo inconveniente, CryptoNote crea automaticamente delle chiavi pubbliche usa e getta, derivandole dall'indirizzo pubblico del destinatario e da un insieme randomico di dati: in questo modo il mittente genererà l'indirizzo a cui spedire la somma partendo dalla chiave pubblica del destinatario e aggiungendo alcuni dati casuali in modo da realizzare la chiave usa e getta. L'impiego di dati casuali consentirà di avere

una chiave unica anche in caso di più pagamenti da parte della stessa persona.
Una volta inviato il pagamento, il destinatario potrà incassarlo utilizzando la propria chiave privata, ma nessun altro sarà in grado di associare il pagamento a lui.



Questo sistema rende anche molto più difficile analizzare la blockchain per tracciare i movimenti di denaro garantendo un certo grado di resistenza nei confronti di tecniche finalizzate alla blockchain analysis.

3. *Double-spending proof*: il sistema è protetto dai doppi pagamenti grazie a una versione modificata del *Traceable ring signature*, in cui la tracciabilità è sostituita dal collegamento tra l'identità dell'utente e uno specifico marker creato attraverso una funzione non invertibile.

4. Scalabilità e POW: *Cryptonight*, l'algoritmo proof-of-work utilizzato da Monero, cerca di rendere la gara tra GPU, CPU e ASIC più equa possibile: anche coloro che hanno a un'incredibile potenza di calcolo ed efficienza non potranno assumere il controllo del mercato così facilmente come accade con Bitcoin. L'idea è quella di evitare la centralizzazione dei miner

ed evitare che alcuni gruppi di persone dominino il mercato grazie ai loro hash rate.

Pian piano monero sta diventando una valuta sempre più importante nel mercato online, potenzialmente sulla strada della popolarità dei bitcoin.

Un'altra caratteristica di Monero è l'assenza di un limite definito, il che significa che non ha una limitazione di blocchi da 1 Mb che impediscono la scalabilità come i bitcoin; è quindi ipotizzabile che continuerà a crescere fino a incontrare i limiti delle macchine su cui verrà fatto girare.

Fornendo un elevato livello di privacy, Monero offre, inoltre, alti livelli di fungibilità: ogni singola unità di valuta può essere sostituita da un'altra dato che non sarà possibile differenziare una moneta da un'altra.

2. *Monero e darknet*

Grazie alla sua vocazione *privacy friendly*, Monero sta rapidamente diventando la moneta preferita nelle darknet, tanto da suscitare l'interesse di FBI, Interpol ed Europol. Quest'ultima, in particolare, nel rapporto IOCTA 2017 ha osservato: «*While Bitcoin remains a key facilitator for cybercrime, other cryptocurrencies such as Monero, Ethereum and Zcash are also gaining popularity within the digital underground*».

Tutto ha avuto inizio allorché, ad agosto del 2016, Oasis e AlphaBay, due dei principali dark market, hanno annunciato di aver integrato Monero come sistema di pagamento, ma di questo parleremo più diffusamente nel capitolo dedicato agli utilizzi illeciti delle criptovalute.

2.4 Ripple (XRP)

Ripple, universalmente riconosciuto come uno dei principali concorrenti di Bitcoin, è un sistema di trasferimento di fondi in tempo reale che permette la spedizione di denaro grazie a un servizio garantito dall'omonima società ed è basato su un protocollo open source.

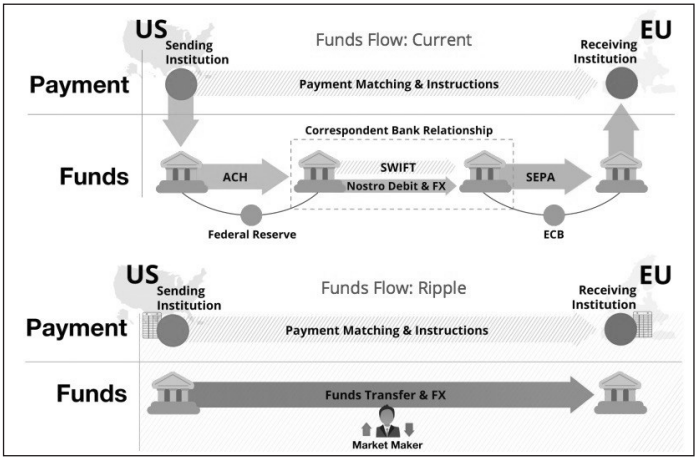
Come accade per Bitcoin, con lo stesso nome identifichiamo la rete, la criptovaluta (XRP) e il protocollo che gestisce la rete (Ripple Transaction Protocol, RTXP); quest'ultimo nasce nel 2012 con lo scopo di rendere possibili transazioni finanziarie a bassissimo costo e con il massimo livello di sicurezza a livello globale indipendentemente dagli importi.

Nella presentazione del progetto è possibile leggere

> *In a world where three billion people are connected online, cars drive themselves and appliances can communicate, global payments are still stuck in the disco era.*
> *Why? The payment infrastructure was built before the Internet with few updates.*
> *Ripple connects banks, payment providers, digital asset exchanges and corporates via RippleNet to provide one frictionless experience to send money globally.*

Il protocollo RTXP nasce, quindi, come una soluzione al fatto che «*sending money isn't as easy as sending an email*» e si propone come un'alternativa a bassissimo costo all'attuale sistema diventando, per il trasferimento di fondi, quello che l'http è per il web e l'SMTP per la posta elettronica: utilizzando questi protocolli, due sistemi possono comunicare liberamente, indipendentemente dalla loro collocazione geografica e dalle infrastrutture utilizzate.

Si osservi l'immagine che segue (tratta da https://gigaom.com/2014/09/24/two-us-banks-are-ready-to-embrace-the-ripple-protocol-allowing-instant-global-money-transfers/):



In breve, oggi i sistemi di pagamento, basati su banche di corrispondenza e protocolli come lo Swift, funzionano bene in singoli territori – Usa, Europa, Cina –, ma non sono interoperabili tanto che un bonifico transatlantico impiega giorni per arrivare e le banche spendono oltre 1600 miliardi l'anno per trasferire denaro. Il protocollo RTXP si propone di porre fine a questa situazione consentendo a ogni banca di comunicare e trasferire fondi a ogni altra banca attraverso un sistema P2P che consenta di scambiare valori in tempo reale e con un costo marginale prossimo allo zero, senza bisogno di depositi e di un corrispondente nei vari Paesi.

In un'intervista, rilasciata a «la Repubblica» a ottobre 2016, Chris Larsen (ad di Ripple) ha spiegato:

> Oggi abbiamo l'Internet delle informazioni. Noi vogliamo costruire l'Internet del valore. Una mail impiega frazioni di secondo per arrivare negli Stati Uniti, un bonifico cinque giorni. La colpa è della serie di intermediari che stanno in mezzo tra chi spedisce e chi riceve denaro. Quegli intermediari, dalle banche corrispondenti alle società di settlement, possono essere aggirati con la blockchain. O meglio: con un sistema finanziario distribuito.

Unicredit, Royal Bank of Canada, Santander, Standard Chartered hanno dimostrato un grandissimo interesse per questo progetto, intervenendo anche in qualità di finanziatori insieme a Google tanto che la RTXP si può oggi considerare un diretto concorrente dell'attuale sistema di interscambio bancario Swift. Ripple offre poi anche un nuovo approccio alla compensazione finanziaria (*clearing*), che è quel meccanismo che garantisce alle banche di chiudere la giornata in equilibrio tra dare e avere nella moltitudine delle transazioni reciproche gestite.

1. Verso l'internet dei pagamenti…

Vediamo ora le caratteristiche salienti del protocollo RTXP e il funzionamento di Ripple.

Immaginiamo che Bob (negli Stati Uniti) voglia inviare ad Alice (che si trova in Italia) 100 dollari. Scarta immediatamente l'ipotesi del bonifico internazionale: tempi e costi sono eccessivi in relazione alla somma in questione; basti considerare che, secondo il blog di Ripple,

in the US, a typical international payment takes 3-5 days to settle, has an error rate of at least 5 per cento and an average cost of $42. Worldwide, there are $180 trillion worth of cross-border payments made every year, with a combined cost of more than $1.7 trillion a year.

Bob decide, quindi, di ricorrere a Ripple: i 100 dollari vengono convertiti, direttamente dalla banca di Bob, in ripple e spostati, in questa forma, presso la banca di Alice che, a sua volta, si occuperà di convertire la somma in euro per poi accreditarli sul conto di Alice.

In questo modo, è possibile effettuare un trasferimento rapido (si parla di 2-5 secondi) ed economico; ovviamente sono stati implementati dei sistemi di controllo in grado di soddisfare le rigidissime policy antiriciclaggio degli Stati Uniti. Questi ultimi hanno, infatti, una severa normativa che impone alle banche di verificare l'identità dei propri client (cosiddette *know-your-customer* – KYC – *policies*), soprattutto quando i trasferimenti di denaro sono indirizzati oltreoceano: nessuno vuole permettere pagamenti istantanei a organizzazioni terroristiche!

Proprio per tale ragione, Ripple è in grado di individuare e segnalare in tempo reale eventuali operazioni sospette.

Come i bitcoin anche i ripple sono in quantità finita, ma i ripple sono già stati creati tutti: la società Ripple ha creato 100 miliardi di XRP, ma ne ha messa sul mercato soltanto una porzione (38 miliardi a dicembre 2017), i rimanenti verranno in parte rilasciati in maniera controllata per evitare fenomeni inflazionistici e in parte trattenuti presso la società per finanziare ricerca e sviluppo del sistema.

2. Transazioni e commissioni: neutral fees

Ogni transazione effettuata in Ripple comporta il pagamento di una commissione, ma, essendo RTXP un protocollo P2P e decentralizzato, nessuno può richiedere e incassare un compenso per l'utilizzo del sistema.

Le regole del registro XRP, tuttavia, prevedono alcuni tipi di commissioni come garanzia contro gli abusi del servizio: questi pagamenti, identificati come *neutral fee*, non vengono corrisposti a nessuno, ma vengono distrutti a ogni transazione, in modo da rendere eccessivamente costose attività di spam ed eventuali attacchi *denial-of-service*; per tale ragione, il sistema è progettato per aumentare il costo di queste commissioni all'aumentare del carico della rete.

Attualmente l'importo minimo richiesto per ogni transazione è pari a 0,00001 XRP (10 drops), ma può essere aumentato in presenza di un carico della rete superiore alla media.

Oltre a ciò, il registro XRP richiede la presenza di una riserva, in XRP, per proteggere il registro generale da una crescita eccessiva dovuta a spam o ad altri impieghi fraudolenti. L'obiettivo è quello di contenere le dimensioni del registro in modo da consentire una gestione agevole su macchine standard.

Attualmente la riserva minima ammonta a 20 XRP per un indirizzo senza alcun altro oggetto nel registro.

A questo proposito è necessario chiarire che nel registro XRP ogni account viene identificato da un indirizzo in base58. L'indirizzo viene ricavato dalla chiave pubblica dell'account, a sua volta derivante dalla chiave privata. Ogni indirizzo è rappresentato come una stringa in JSON (JavaScript Object Notation) e ha le seguenti caratteristiche:

– tra i 25 ed i 35 caratteri;
– inizia con il carattere "r";
– utilizza caratteri alfanumerici escludendo il numero 0 e le lettere maiuscole "O", "I" e la lettera minuscola "l";
– è case-sensitive;
– include un 4 byte checksum così che la probabilità di generare un indirizzo valido partendo da caratteri casuali sia all'incirca 1 su 2^{32}.

Un indirizzo valido diventa un account valido ricevendo un pagamento in XRP e rimane valido finché il suo saldo in XRP è pari o superiore alla riserva.

La riserva è distinta in *base reserve*, che indica l'ammontare minimo di XRP per ogni indirizzo, e *owner reserve*. Quest'ultima aumenta per ogni oggetto che l'indirizzo possiede nel registro e attualmente ammonta a 5 XRP per ogni oggetto rilevante. Con il termine "oggetto rilevante" si indicano particolari attività che vanno a "pesare" sulla riserva dell'indirizzo; quando un oggetto viene rimosso dal registro, smette di "pesare" sulla riserva.

Alcuni degli oggetti rilevanti sono:

Offers: le offerte appartengono all'indirizzo che le ha collocate e il processo di transazione le rimuove automaticamente quando sono completamente risolte o risultano essere prive di fondi. Il titolare può cancellare l'offerta inviando un comando "OfferCancel" oppure un comando "OfferCreate" che contenga un parametro "OfferSequence".

Trust lines: sono condovise tra due indirizzi e la riserva può essere applicata a uno soltanto oppure a entrambi gli indirizzi.

Held Payments (Escrow): pesano sulla riserva dell'indirizzo che li ha posti in essere.

Per approfondire si rimanda alle pagine ufficiali di Ripple:

http://ripple.com/build/fees-disambiguation/
http://ripple.com/build/reserves/

3. segue: optional fees

Ripple consente, inoltre, agli istituti finanziari di inserire delle proprie commissioni per ogni transazione, in questo caso il mittente si vedrà addebitata una maggiorazione pari alla commissione e il relativo importo verrà accreditato a favore dell'indirizzo dell'istituto.

In alternativa è sempre possibile che gli intermediary possano ideare altri sistemi per ottenere un compenso per la propria attività.

Gli analisti concordando nel ritenere che il sistema Ripple abbia un valore più per il protocollo con il quale gestisce le transazioni che per la valuta in sé, dato che quest'ultima ha il solo scopo di fungere da mezzo comune di scambio piuttosto che da mezzo di investimento: in breve l'idea alla base del sistema è che la banca XY, collocata in Giamaica, dovendo trasferire 100 dollari giamaicani in Angola, preferirà avere a disposizione un proprio fondo in ripple e utilizzarlo per trasferire direttamente l'importo alla banca destinataria piuttosto che passare attraverso diversi intermediari e acquistare il corrispettivo in kwanza angolani.

2.5 I fork

Alcune tra le altre criptovalute oggi in circolazione sono, di fatto, dei *fork* della blockchain originale Bitcoin. In programmazione con il termine *fork* si indica lo sviluppo di un nuovo progetto software che parte dal codice sorgente di un altro già esistente a opera di un programmatore.

Spesso il fork è dovuto a conflitti personali o diversità di vedute tra gli sviluppatori di un medesimo progetto che, a un certo punto, decidono di separare le proprie strade e di procedere autonomamente; in genere, quando si verifica un fork, entrambe le parti iniziano a lavorare partendo dalla medesima base di codice e il gruppo più numeroso, o quello che rappresenta il nucleo originario o che detiene i diritti, mantiene il nome e la comunità virtuale a esso legato, mentre l'altro è costretto a cambiare nome.

In merito al processo di fork, *The Jargon File* (considerato la "Bibbia degli hacker") si esprime così:

> *In the open-source community, a fork is what occurs when two (or more) versions of a software package's source code are being developed in parallel which once shared a common code base, and these multiple versions of the source code have irreconcilable differences between them. This should not be confused with a development branch, which may later be folded back into the original source code base. Nor should it be confused with what happens when a new distribution of Linux or some other distribution is created, because that largely assembles pieces than can and will be used in other distributions without conflict.*
> *Forking is uncommon; in fact, it is so uncommon that individual instances loom large in hacker folklore. Notable in this class were the Emacs/XEmacs fork, the GCC/EGCS fork*

(later healed by a merger) and the forks among the FreeBSD, NetBSD, and OpenBSD operating systems.

(The on-line Jargon File, v.4.4.7, gennaio 2018)

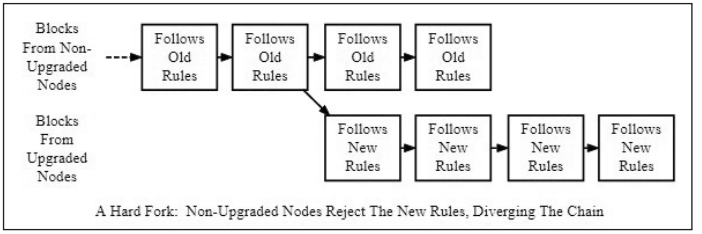
Nel network blockchain i fork vengono spesso attuati con lo scopo di migliorare le performance della blockchain e la gestione del protocollo, a tal fine si dividono in *soft fork* e *hard fork*.

1. Soft fork e hard fork

Con il termine s*oft fork*, si indica una scissione che si attua dando vita a una versione aggiornata del protocollo blockchain compatibile con le versioni precedenti. Il soft fork mette in atto un cambiamento reversibile che consente la partecipazione alla blockchain anche per tutti quei nodi che, per varie ragioni, decidono di non effettuare l'aggiornamento.

Con *hard fork*, invece, si indica un cambiamento irreversibile e, proprio per tale ragione, si distingue tra fork pianificati, *planned* o frutto di una scissione *contentious*. Nel primo caso (*hard fork planned*) non si tratta di un vero e proprio fork quanto di un aggiornamento non retrocompatibile del protocollo; il cambiamento, infatti, viene pianificato e il passaggio è approvato dai partecipanti alla community; non si ha quindi uno sdoppiamento della blockchain come, invece, accade nel caso di *hard fork contentious*.

In quest'ultimo caso si arriva, infatti, a una scissione della blockchain e, tipicamente, alla creazione di una nuova criptovaluta: alla comunità viene chiesto di schierarsi, scegliendo una delle due parti nella consapevolezza che, una volta fatta la propria scelta, non sarà possibile tornare indietro.



2. Fork, perché?

Le ragioni che possono portare a un hard fork, oltre a eventuali insanabili dissidi interni alla comunità degli sviluppatori, sono molteplici, ma possono essere sintetizzati in due grosse fattispecie di base:

1. Garantire un maggior equilibrio della blockchain attraverso modifiche che, a livello di protocollo, permettano di ridurre l'impatto della capacità di calcolo nella risoluzione della proof-of-work, ovvero introducendo meccanismi in grado di disincentivare un'eccessiva concentrazione dei miner.
2. Migliorare performance e scalabilità della blockchain, rendendo possibile processare un maggior numero di transazioni in tempi più brevi, ad esempio attraverso interventi volti a ridurre la difficoltà o ad aumentare le dimensioni dei blocchi.

3. Bitcoin fork: Namecoin

Per evidenti ragioni, Bitcoin è stato esposto a un grande numero di fork e analizzarli tutti sarebbe impossibile, ma credo sia giusto ricordare qui il primo fork di

Bitcoin, avvenuto nel 2011, che ha portato alla nascita di Namecoin (ℕ o NMC).

Namecoin è quasi interamente basato sul codice di Bitcoin (circa 400 righe di codice distinguono i due progetti), a cui sono state aggiunge alcune funzionalità specifiche del progetto che consentono agli utenti di registrare e trasferire nomi (keys) e contenuti (values). In parole povere Namecoin è una tecnologia che mira a garantire un sistema di registrazione e trasferimento di nomi a dominio indipendente dai DNS classici e in grado di garantire riservatezza e resistenza alle censure tanto che il motto del progetto è «*Bitcoin frees money – Namecoin frees DNS, identities, and other technologies*».

Utilizzando Namecoin gli utenti possono registrare un dominio .bit che somma le qualità dei classici domini (sicuri e facili da memorizzare) con le qualità proprie della blockchain Bitcoin (sicura e decentralizzata) accentrando su di sé tutti e tre gli elementi indicati nel triangolo di Zooko.

Namecoin è, infatti, sicuro, facilmente memorizzabile e privo di un'autorità centrale. I domini .bit possono essere creati e gestiti spendendo namecoin.

4. segue: Bitcoin Cash

Ad agosto 2017 abbiamo, invece, assistito al primo hard fork: a partire dal blocco 478558 la blockchain Bitcoin si è scissa in due differenti blockchain, di cui una ha mantenuto il nome originale, l'altra ha preso il nome di Bitcoin Cash (BCH).

Il fork è stato determinato dal malcontento che, da tempo, serpeggiava nella comunità Bitcoin a causa di

alcuni problemi legati alla velocità delle transazioni, al loro costo e alle dimensioni dei blocchi. Bitcoin Cash si presenta come la continuazione del progetto Bitcoin, ma con nuove regole di consenso che ne consentono una crescita maggiore e più rapida. In estrema sintesi, mentre il codice di Bitcoin consente blocchi con un limite massimo di dati di 1 Mb, ovvero circa 3 transazioni al secondo, Bitcoin Cash ha portato tale limite a 8 Mb dichiarandosi disponibile ad aumentarlo ancora laddove fosse necessario.

Al momento del fork, tutti i possessori di Bitcoin potevano decidere se convertire il loro portafoglio in Bitcoin Cash (a un tasso di cambio 1 a 1) oppure rimanere nella blockchain originale.

Dal blocco 478559, invece, tutte le transazioni sono completamente separate e le due blockchain sono indipendenti.

5. segue: altri hard fork

Da agosto 2017, anzi dal blocco 478558 in poi, si sono succeduti numerosi altri hard fork tra cui possiamo ricordare, in ordine cronologico:

478558, 1 agosto 2017 > *Bytether*, si tratta di un cros fork teso a ottenere un incrocio tra Bitcoin ed Ethereum.

491404, 24 ottobre 2017 > *Bitcoin Gold*, con l'obiettivo di azzerare il vantaggio dei miner ASIC impiega come POW Equihash, un algoritmo ASIC resistant.

495866, 24 novembre 2017 > *Bitcoin Diamond*, orientato alla riservatezza, alla rapidità e al contrasto dei miner ASIC, cifra l'ammontare delle transazioni e adotta un blocco da 8 Mb e impiega l'algoritmo X13.

498777, 12 dicembre 2017 > *UnitedBitcoin*, si tratta di un progetto per creare un'autorità dedicata allo sviluppo di software Bitcoin, con lo scopo di proteggere gli utenti dalle frodi, garantendo una crescita stabile del valore BTC e un funzionamento continuo e garantito della rete.

498848, 12 dicembre 2017 > *Bitcoin Hot*, introduce un nuovo algoritmo POW, blocchi da 16 Mb e un maggior numero di monete in circolazione.

498888, 12 dicembre 2017 > *Super Bitcoin*, orientato alla riservatezza e con blocchi da 8 Mb

- *BitcoinX*, riservatezza, smart contract, DPOS consensus.
- *Oil Bitcoin*, riservatezza, blocchi da 8 8 Mb, Equihash come POW.

499777, 17 dicembre 2017 > *Bitcoin World*.

499999, 19 dicembre 2017 > *Lightning Bitcoin.*

- *Bitcoin Stake*.

501118, 26 dicembre 2017 > *Bitcoin Top*.

501225, 27 dicembre 2017 > *Bitcoin God.*

- *Bitcoin File*.

501451, 28 dicembre 2017 > *Bitcoin SegWit2X X11*.

Altri fork, sono in progetto al momento di andare in stampa:

BitEthereum, ipotizzato per la fine di febbraio 2018;

Bitcoin Smart, ipotizzato per il blocco 505050, ad oggi non risulta ancora attivato (http://bcs.info/#roadmap) ed è orientato agli smart contract;

Bitcoin Interest, ipotizzato per il blocco 505083 e attivato il 22 gennaio 2018 (https://www.bitcoininterest.io/);

Bitcoin LITE, ipotizzato per il febbraio 2018;

Bitcoin ATOM: attivato a fine gennaio 2018 (https://bitcoinatom.io/)

Una lista aggiornata dei fork può essere trovata qui: https://bitcoinforks.io/

3. Ethereum: verso gli smart contract

Un'altcoin particolare di cui è necessario parlare ora è Ethereum; si tratta di una piattaforma decentralizzata, orientata alla creazione e pubblicazione peer-to-peer di contratti intelligenti (i cosiddetti smart contract, sul punto si veda più sotto): proprio quest'ultimo aspetto caratterizza Ethereum rispetto a Bitcoin.

In breve, quello che Ethereum intende garantire è una blockchain che integri un linguaggio di programmazione di Turing completo, costruito al suo interno; questo linguaggio potrà essere usato per creare "contratti" e per codificare le funzioni arbitrarie di transizione, permettendo agli utenti di implementare uno specifico utilizzo della piattaforma semplicemente scrivendone la logica di funzionamento in poche righe di codice (Cfr. Leonardo Maria Pedretti, *Ethereum: Libro Bianco - White Paper* - Traduzione, http://ethereumbuilders.gitbooks.io).

Per poter girare sulla rete peer-to-peer, i contratti di Ethereum "pagano" l'utilizzo della sua potenza computazionale tramite un'unità di conto, detta ether, che funge quindi sia da criptovaluta sia da carburante.

In altri termini, contrariamente a molte altre cripto-

valute, l'obiettivo di Ethereum non è quello di costituire un network per lo scambio di valore monetario, ma quello di creare un protocollo alternativo per la costruzione di applicazioni decentralizzate, fornendo un insieme eterogeneo di regole che potranno essere adattate per realizzare una larga classe di applicazioni.

Tutto questo viene garantito dalla costruzione di una blockchain con un linguaggio di programmazione al suo interno; in questo modo, ognuno può scrivere e realizzare smart contract e applicazioni decentralizzate in cui impostare proprie regole arbitrarie in grado di gestire la proprietà, i formati delle transazioni e le funzioni di transizione di stato.

3.1 Conoscere Ethereum

La piattaforma fu inizialmente menzionata nel 2013 da Vitalik Buterin nella rivista «Bitcoin Magazine», di cui lo stesso era fondatore, ed è stata successivamente sviluppata nel white paper dello stesso Buterin, per poi essere formalizzata da Gavin Wood nel suo *Yellow Paper*, a inizio 2014.

In questo documento Wood, prima di passare alla descrizione dettagliata del protocollo Ethereum, scrive

> *Ethereum is a project which attempts to build the generalized technology; technology on which all transactionbased state machine concepts may be built. Moreover it aims to provide to the end-developer a tightly integrated end-to-end system for building software on a hitherto unexplored compute paradigm in the mainstream: a trustful object messaging compute framework.*

A maggio del 2015 veniva avviata la fase di test del sistema (Olympic) e il 30 luglio 2015 avveniva il rilascio della prima versione *live* della piattaforma (Frontier). Nel 2016 Ethereum dovette affrontare un contentious fork che portò alla creazione di due differenti blockchain (Ethereum ed Ethereum Classic) mentre l'ultimo e più recente hard fork (planned) ha visto nascere Metropolis. Oggi Ethereum è una delle principali criptovalute per valore e quota di mercato, ma, soprattutto, è uno dei principali sistemi in tema di smart contract.

Con questo termine si indicano dei protocolli per computer che facilitano, verificano o fanno rispettare la negoziazione o l'esecuzione di un contratto sulla base di regole precise e senza il bisogno di ricorrere a intermediari.

L'idea venne sviluppata nel 1994 da Nick Szabo, crittografo ed esperto di diritto, che si rese conto come il registro decentralizzato potesse essere utilizzato per realizzare dei contratti, gli smart contract appunto, trascrivendo le singole clausole in un linguaggio di programmazione in modo da poterli gestire attraverso una rete di computer collegati alla blockchain.

In questo modo sarà possibile automatizzare moltissime attività (si pensi alla presenza in un contratto di eventuali clausole risolutive espresse a termini o condizioni) riducendo notevolmente la stessa alea contrattuale.

3.2 Gli smart contract prima e dopo Ethereum

I contratti intelligenti, i cosiddetti smart contract, non sono una prerogativa di Ethereum, già il protocollo del Bitcoin, anche senza nessuna estensione, ne implementa una versione basilare.

La voce UTXO può, infatti, essere rappresentata anche da uno script più complesso, espresso in un

semplice linguaggio di programmazione; il meccanismo della proprietà della chiave pubblica è, infatti, implementato con uno script che impiega una firma a curva ellittica come input: confrontando questa con la transazione e l'indirizzo che possiede la UTXO, fornisce come risultato 1 se la verificazione è andata a buon fine, 0 in caso contrario.

Altri script più complessi possono essere sviluppati, ma il linguaggio di scripting implementato nel Bitcoin presenta alcune importanti limitazioni se confrontato con il linguaggio di Turing, tra cui una delle più rilevanti è l'assenza di loop. È pur vero che qualsiasi loop può essere simulato semplicemente ripetendo il codice sottostante più volte con un'istruzione "if", ma questo porta a scripts che sono inefficienti dal punto di vista dello spazio.

1. Ethereum

(Fonti: Gavin Wood, *Ethereum: a secure decentralised generalised transaction ledger*, EIP-150 REVISION (87ed994 - 2018-01-17); Vitalik Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*)

Ethereum nasce con lo scopo di creare un protocollo in grado di superare i limiti di Bitcoin in modo da poter essere la base per una larga classe di applicazioni decentralizzate, in particolare in quelle situazioni in cui è importante un rapido tempo di sviluppo, la sicurezza per applicazioni raramente utilizzate e la capacità da parte di differenti applicazioni di interagire molto efficacemente.

Per ottenere questo risultato Buterin ha pensato di

sviluppare una blockchain con un linguaggio di programmazione Turing-complete costruito al suo interno e in grado di garantire a chiunque la redazione di smart contract e di ogni genere di applicazioni decentralizzate.

Senza voler qui eseguire una dettagliata analisi del protocollo Ethereum, possiamo limitarci a osservare che in Ethereum lo stato è costituito da oggetti chiamati *accounts*, in cui ogni account ha un indirizzo di 20 byte e le transizioni di stato sono trasferimenti diretti del valore e dell'informazione tra gli accounts.

Un tipico account Ethereum contiene quattro campi:

– Il *nonce*, utilizzato per assicurarsi che ogni transazione possa essere elaborata una sola volta.
– Il conto corrente dell'account *ether balance*.
– Il codice contratto dell'account, se presente, *contract code*.
– Lo storage dell'account (vuoto da default), *storage*.

La criptovaluta ether rappresenta il carburante interno di Ethereum, e viene utilizzata per pagare le commissioni di transazione.

Gli account possono essere di due tipi:

– account esterni (*externally owned account*), sono controllati da chiavi private, non contengono codice e possono essere utilizzati per inviare messaggi creando e firmando una transazione;
– account contratto (*contract account*), controllati dal loro codice di contratto di modo che, ogni volta che questo riceve un messaggio, il suo codice si attiva, permettendogli di leggere e scrivere verso uno storage interno, spedire altri messaggi o creare ulteriori contratti.

Si noti che quando parliamo di "contratti" in Ethereum non dobbiamo pensare a semplici moduli o formulari da riempire, ma ad "agenti autonomi" che vivono all'interno dell'ambiente di esecuzione di Ethereum, eseguendo sempre una specifica parte di codice quando vengono "colpiti" (*poked*) da un messaggio o da una transazione ed avendo un controllo diretto sul proprio bilancio di ether e sulla propria chiave/valore di store al fine di tenere traccia delle variabili persistenti.

Il termine "transazione" (*transaction*) viene utilizzato per riferirsi al pacchetto di dati che rappresenta un messaggio da inviare da un account esterno e questi dati sono:

– destinatario del messaggio;
– la firma che identifica il mittente;
– l'ammontare di ether da trasferire al destinatario;
– un campo dati opzionale;
– un valore "STARTGAS", che rappresenta il massimo numero di passaggi computazionali che l'esecuzione della transazione può impiegare;
– un valore "GASPRICE", che rappresenta la commissione che il mittente paga per il passaggio step computazionale.

Mentre i primi tre campi rappresentano uno standard presente in qualsiasi criptovaluta, gli altri tre hanno delle funzioni particolari.

Gli ultimi (STARTGAS e GASPRICE) sono cruciali per il buon funzionamento della rete in quanto finalizzati a prevenire loop infiniti, accidentali o ostili, o altri sprechi di risorse.

L'unità base è il *gas* e di solito uno step computazionale costa 1 gas, ma ci sono dei casi in cui i costi sono maggiori in quanto si tratta di operazioni computazionalmente più complesse. È poi presente una commissione proporzionata ai byte contenuti nei dati della transazione in modo da costringere un eventuale aggressore a pagare in maniera proporzionale alle risorse consumate.

Il campo dati, invece, può essere utilizzato dalla macchina virtuale nell'ambito dell'esecuzione di un contratto. Per esempio, immaginiamo un servizio di registrazione di dominio basato sulla blockchain, la macchina avrà bisogno di interpretare i dati inseriti in questo campo come appartenenti a due campi: il dominio da registrare e l'indirizzo IP da registrare.

I contratti hanno la capacità di "messaggi" ad altri contratti: si tratta di oggetti virtuali, che esistono solo nell'ambiente di esecuzione di Ethereum e contengono:

– il mittente del messaggio (implicito);
– il destinatario del messaggio;
– l'ammontare di ether da inviare attraverso il messaggio;
– un campo dati opzionale;
– un valore STARTGAS.

Di fatto un messaggio è come una transazione, a eccezione del fatto che viene prodotto da un contratto e non da un attore esterno. Un messaggio viene prodotto quando un contratto effettua una operazione "CALL" e, come una transazione, ogni messaggio fa sì che l'account del destinatario esegua il proprio codice; ne consegue che i contratti possono avere rela-

zioni con altri contratti esattamente come avviene per gli attori esterni.

2. *Il codice dei contratti*

(fonti: Gavin Wood, *Ethereum: a secure decentralised generalised transaction ledger*, EIP-150 REVISION (87ed994 - 2018-01-17); Vitalik Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*)

Il codice utilizzato nei contratti Ethereum è scritto in un linguaggio di basso livello, stack-based, bytecode (il codice consiste in una serie di byte, dove ogni byte rappresenta un'operazione) denominato *Ethereum Virtual Machine code* o EVM code.

L'Ethereum Virtual Machine rappresenta l'innovazione principale del progetto Ethereum: si tratta di una macchina virtuale, ideata per essere eseguita da tutti i partecipanti a una rete peer-to-peer, in grado di leggere e scrivere su una blockchain sia codice eseguibile che dati, verificare firme digitali ed eseguire delle istruzioni quando riceve un messaggio verificato da una firma digitale e quando l'informazione contenuta nella blockchain le dirà che è appropriato farlo.

Le applicazioni del codice possono essere ricondotte a tre grandi categorie:

1. le applicazioni finanziarie, che forniscono agli utenti numerosi modi di gestire contratti di vario genere tra cui le sub-monete, i derivati finanziari, i libretti di risparmio, i testamenti eccetera.
2. le applicazioni semi-finanziarie, dove è coinvolto il denaro, ma sono coinvolti in maniera rilevante

anche aspetti non strettamente monetari come, per esempio, accade nell'auto-assegnazione di premi per le soluzioni di problemi computazionali.
3. le applicazioni non finanziarie come quelle finalizzate a gestire il voto online, il governo decentralizzato eccetera.

In conclusione, Ethereum è stato originariamente concepito per fornire caratteristiche avanzate attraverso un linguaggio di programmazione completo; si tratta dunque di molto più che una valuta: la sua implementazione è virtualmente ipotizzabile in ogni ambito di applicazione.

3.3 Smart contract tra presente e futuro

In precedenza, ci siamo limitati a fornire una definizione e una descrizione generale dei contratti intelligenti, ma è giunto ora il momento di capire meglio come funzionano e, soprattutto, i loro possibili sviluppi partendo dall'analisi di casi concreti di loro utilizzo e di sviluppo.

L'idea iniziale di Nick Szabo, secondo cui uno smart contract è un contratto in forma di codice che rimanda l'esecuzione di alcune o tutte le sue clausole a un software, è ancora valida e ci fornisce un ottimo punto di partenza per analizzare le implicazioni pratiche di questa tecnologia.

L'ipotesi base riguarda l'acquisto di un software: l'utente accetta uno smart contract di licenza e il software sarà in grado di intervenire, bloccando l'esecuzione del programma al verificarsi di determinate condizioni quali, ad esempio, il mancato rinnovo della licenza, la

violazione di una clausola contrattuale eccetera, ma le possibili implicazioni sono virtualmente infinite, soprattutto grazie alla diffusione del cosiddetto internet delle cose: si immagini una lavatrice acquistata a rate che smette di funzionare in caso di mancato pagamento di una o più rate, oppure un contratto di RCA auto in grado di variare dinamicamente l'importo del premio in base allo stile di guida tenuto dal conducente o alla tipologia di strada percorsa…

Da un punto di vista tecnico, uno smart contract si compone di tre parti:

1. il codice, che diventa l'espressione della logica contrattuale;
2. gli eventi, che il programma acquisisce e che vanno a interagire con il contratto;
3. gli effetti determinati dagli eventi.

In breve, mentre un contratto tradizionale è scritto per essere interpretato ed eseguito da esseri umani, un contratto intelligente è scritto per essere compreso da esseri umani, ma interpretato ed eseguito da un sistema automatico. A questo proposito è opportuno precisare che i contratti possono astrattamente essere codificati su qualsiasi blockchain, ma al momento Ethereum sembra essere la piattaforma più sfruttata a questo scopo dato che offre una capacità di elaborazione senza limite.

Da un punto di vista giuridico, possiamo definire uno smart contract come la "trasposizione" in codice di programmazione di un contratto in modo da verificare in automatico l'avverarsi di determinate condizioni o termini (controllo di dati di base del contratto) ed eseguire in automatico le azioni collegate a tali eventi.

In altre parole, in uno smart contract tanto gli elementi essenziali (volontà, oggetto, causa e forma) quanto quelli accidentali (termini e condizioni) del contratto non cambiano rispetto ai contratti tradizionali, ma vengono implementate delle regole, basate sul codice di programmazione, che garantiscono gli effetti del contratto all'avverarsi di determinati eventi, nonché la sua esecuzione secondo quanto concordato, riducendo notevolmente il contenzioso.

Le applicazioni pratiche sono virtualmente infinite, ci limiteremo quindi a tre semplici esempi.

1. Smart contract e assicurazioni

Pensiamo al mondo delle assicurazioni per autoveicoli: sulla base dei dati rilevati e comunicati da apparecchiature installate a bordo delle *smart car*, si pensi alle cosiddette "scatole nere" e alle, sempre più diffuse, *dash cam*. Le vetture sono in grado di fornire dati sul comportamento del conducente e, da questi dati, le assicurazioni possono agevolmente ricavare informazioni in grado di valutare il profilo di rischio di un conducente e, di conseguenza, inserire eventuali condizioni contrattuali in grado di attivare o disattivare clausole contrattuali.

Ad esempio, il mancato rispetto dei limiti di velocità o il mancato utilizzo dei segnalatori di direzione o il mancato rispetto della segnaletica stradale possono essere interpretate come condizioni di maggior rischio e, di conseguenza, determinare un peggioramento delle condizioni applicate e un aumento del premio assicurativo. Al contrario una condotta di guida virtuosa potrebbe attivare delle

clausole di minor rischio e determinare una riduzione del premio.

Lo stesso potrebbe accadere in presenza di una manutenzione regolare del veicolo o di altre condotte ritenute "virtuose".

2. Leasing, noleggio e vendita di automobili

Un altro ambito che ben si presta all'applicazione di smart contract è quello legato alla compravendita di automobili e ai servizi connessi.

Attraverso clausole contrattuali volte a salvaguardare il valore dell'auto nel tempo sarà possibile applicare prezzi più vantaggiosi legandoli a ben definite condotte di guida da parte dell'utente e automatizzare molte delle procedure di noleggio e utilizzo promiscuo dei veicoli.

In un prossimo futuro si potrebbe arrivare all'automatizzazione della procedura di erogazione del leasing/finanziamento trasformando la stessa in un processo "premi, firma e guida" in cui il potenziale cliente sceglie l'auto e, una volta sedutosi al posto di guida, firma un contratto dinamico dove le clausole legate al costo di gestione vengono aggiornate in base al suo stile di guida.

Oppure, potremmo ipotizzare un servizio automatico di noleggio in cui l'utente inserisce i propri dati, viene riconosciuto e abilitato alla guida del veicolo scelto, lo utilizza e, al momento della consegna, paga in base all'effettivo uso e alle modalità con cui ne ha usufruito.

3. Banche e istituti finanziari

Banche e istituzioni finanziarie saranno probabilmente tra i primi servizi a giovarsi degli smat contract e, in effetti, la svizzera UBS, la britannica Barclays e l'italiana UNICREDIT già stanno studiando e sperimentando alcune applicazioni pratiche destinate ad accelerare le funzioni di back office e a ridurre tempi e costi di gestione.

Non è certo un caso che le principali banche siano tra i principali investitori nelle startup che operano nel comparto delle tecnologie blockchain e negli smart contract.

3.4 Problematiche legali

Naturalmente non sono tutte rose e fiori e, come osserva il dottor Manente (componente della Commissione Informatica del Consiglio Nazionale del Notariato), sarà necessario garantire l'esatta corrispondenza tra ciò che si vuole e ciò che viene scritto nel contratto stesso.

Lo smart contract, infatti, sarà scritto attraverso un codice di programmazione, quindi non sempre sarà interamente comprensibile all'utente medio. Sebbene sia ipotizzabile che verranno sviluppate delle interfacce semplificate che consentiranno di visualizzare e accettare termini e condizioni, il codice resterà pur sempre qualcosa di non immediatamente comprensibile (un po' come accade per una pagina web: l'utente si limita a prendere visione del risultato restituitogli dal proprio browser e molto raramente si spinge a leggere e tentare di comprendere il codice sorgente della pagina che sta visitando).

Firmare uno smart contract sarà, allora, quasi un atto di fede: nella corretta presentazione dei contenuti nel linguaggio umano e nell'assenza di clausole nascoste nel codice; proprio relativamente a questo punto dovranno entrare in campo nuove generazioni di professionisti del diritto in grado di garantire la corrispondenza tra il contenuto percepibile del contratto e il suo contenuto effettivo.

A ciò deve aggiungersi che ogni contratto dovrà anche essere conforme alle leggi e, proprio per questa ragione, sarà impossibile, o molto rischioso, non avvalersi dell'ausilio di professionisti preparati.

Oltre a una corretta programmazione, uno smart contract avrà poi bisogno di una piattaforma su cui girare, come accade per esempio nel caso di Ethereum, e questa piattaforma dovrà offrire adeguate garanzie di stabilità, sicurezza e, soprattutto, durata nel tempo.

Sebbene l'analisi delle problematiche legali connesse agli smart contract sia questione che esula dalla portata del presente volume, ritengo opportuno evidenziare qui alcuni aspetti della questione.

1. Alcune definizioni

In primo luogo, è bene chiarire che gli smart contract non sono necessariamente dei contratti telematici; questi ultimi sono, infatti, caratterizzati dall'incontro a distanza tra acquirente e venditore. Tanto per fare un esempio, le parti potrebbero benissimo stipulare il contratto a distanza o potrebbero incontrarsi fisicamente per sottoscriverlo.

I contratti telematici devono farsi rientrare nella categoria dei contratti *inter absentes*, ma con alcune

particolarità. La prima è che non esiste un solo tipo di contratto telematico, pertanto l'approccio dovrà essere differente a seconda della situazione.

Nella loro forma più elementare, gli smart contract possono essere visti come un contratto automatico al pari del classico distributore di bevande, ma nella loro forma più avanzata è innegabile che questi rappresentino un mezzo integrativo della volontà umana andando a configurare quello che è già stato definito come "contratto cibernetico".

Caratteristica essenziale del contratto cibernetico è che, quando si utilizza il computer come mezzo integrativo della volontà umana, pur facendolo funzionare come un automatico, il procedimento adottato dalla macchina è talmente elaborato e sofisticato da non poter assolutamente essere paragonato ai tradizionali negozi automatici caratterizzati dall'assoluta prevedibilità del comportamento tenuto dalla macchina.

Quest'ultima, a meno di un malfunzionamento, non devierà mai dallo schema tipo pagamento-consegna merce; tutt'al più, nel caso di automatici particolarmente sofisticati, si potrà permettere all'acquirente di modificare vari fattori, che però nell'ambito del contratto hanno un'importanza sicuramente marginale (cioè, quantità della merce, colore, dimensioni…), ma negli smart contract il computer *integra e sostituisce l'operatore umano* che si limita a stabilire a priori, utilizzando un programma in grado di dotare la macchina di un'intelligenza artificiale, come il computer dovrà comportarsi nelle varie circostanze che si possono verificare.

Il termine *intelligenza artificiale* (A.I.) viene, in genere, utilizzato per indicare la capacità di un programma di ricreare all'interno di un computer alcuni dei

processi mentali tipici dell'uomo, dotando la macchina di un'attitudine al "ragionamento" sempre maggiore, adattandosi alle varie vicende che potrebbero verificarsi in sede di conclusione del contratto o nel corso della sua efficacia.

2. Smart contract e rappresentanza

Nelle loro forme più complesse e articolate, gli smart contract possono essere immaginati come una proiezione predefinita, ma estremamente flessibile, della volontà di stipulare un contratto da parte di due soggetti tanto da poter quasi affermare che il computer da semplice *nuncius* diverrebbe l'alter ego dei contraenti sia pur limitatamente al principio dell'imputazione agli stessi degli atti.

Di certo non possiamo parlare di rappresentanza in senso tecnico, in quanto non esistono due soggetti con due volontà distinte, ma non sembra trascurabile il fatto che la volontà del computer, se pure è la stessa del *dominus* per quanto riguarda l'origine, è invece sua, cioè del computer stesso, quanto al modo e al tempo in cui concretamente si manifesta; in alcuni casi tale volontà potrebbe apparire non prevedibile anche per lo stesso programmatore. Le variabili potrebbero essere talmente numerose e talmente articolate da non permettere a nessuno di prevedere quella che sarà la scelta, *rectius* il risultato dell'elaborazione, del computer. In ogni caso il dominus avrà la certezza che il computer ha fatto la scelta migliore, in base alle istruzioni impartitegli in precedenza.

È opportuno ribadire ancora una volta che, in una tale situazione, il computer non si limita a eseguire

meccanicamente delle disposizioni, come invece avviene nel caso di un negozio automatico semplice, ma, elaborando tutti i dati in suo possesso, prende una decisione che potremmo ben definire *autonoma*; in altri termini, il computer non si limita a trasmettere le decisioni prese dall'uomo, ma è in grado di elaborare, decidere e trasmettere decisioni proprie, come se fosse un essere che pensa e vuole autonomamente.

All'assenza di un intervento umano in fase di stipula corrisponde anche l'assenza di un contributo interpretativo in fase di esecuzione, e questo rende necessario che il contratto sia basato su descrizioni estremamente precise per tutte le circostanze, tutte le condizioni e tutte le situazioni che possono essere previste.

Ne consegue che la gestione dei dati, tanto dei cosiddetti Big data quanto delle fonti dei dati alle quali il contratto è chiamato ad attenersi, diventa un fattore critico essenziale per stabilire la qualità dello smart contract (Bellini, *Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*).

Per poter funzionare correttamente, infatti, gli smart contract devono elaborare una grande quantità di dati e di informazioni e i soggetti ritenuti attendibili devono essere ben individuati e definiti (si pensi all'esempio del contratto di assicurazione: chi è il soggetto idoneo a comunicare al veicolo il superamento dei limiti di velocità e i limiti in vigore in quel tratto di strada?).

Lo smart contract rappresenta il frutto dell'esecuzione di un codice da parte di un computer e questo determina che il "codice" ha il potere, e la responsabilità, di decidere mentre ai contraenti spetta solo l'onere di accettare o non accettare termini e condizioni al momento della stipula.

3. Profili giuridici

Resta da valutare e affrontare la problematica legata alla possibilità di imputare al contraente gli effetti giuridici delle scelte operate dal sistema.

A tal proposito, non sembra rilevante che programmatore e dominus siano o meno la stessa persona. Infatti, anche se il programmatore è una persona differente e distinta dal dominus, andrebbe comunque considerato come un mero esecutore materiale di ordini, alla stregua di uno scriba o di un traduttore limitatosi a trasferire la volontà del dominus in un linguaggio comprensibile per la macchina. La responsabilità del programmatore, nel caso in cui questi non abbia utilizzato la necessaria diligenza nel lavoro svolto, sarà rilevante soltanto tra programmatore e dominus, ma non potrà mai essere opposta ai terzi in buona fede.

A mio avviso le decisioni del computer devono essere sempre imputate all'uomo che lo ha programmato, in quanto nel programma va ravvisata la proiezione nel futuro del pensiero e della volontà dell'essere umano e, quindi, anche la capacità, sia pure contenuta entro limiti predeterminati, di intendere e di volere. In alcune particolari situazioni, però, le decisioni del computer possono non essere state previste dal programmatore ed essere estranee alla sua volontà, se non addirittura contrarie a essa.

È evidente che, al verificarsi di una simile fattispecie, il dominus non sarà vincolato dall'affare concluso dal computer, soltanto nel caso in cui riesca a dimostrare che questo è stato indotto a concludere il contratto da un malfunzionamento, rectius da un errore, che lo ha spinto a uscire dai limiti di quel "mandato digitale" rappresentato dal programma.

Resta il problema, non indifferente, della tutela del terzo che, fidandosi delle apparenze, ha concluso il contratto cibernetico. L'unica soluzione possibile sembra debba essere ravvisata nell'estensione per analogia della disciplina dell'errore commesso dal rappresentante e quindi, in base al rinvio effettuato dall'articolo 1390 c.c., della disciplina dell'errore in generale. Una volta compiuta questa operazione, sarà agevole applicare alle varie fattispecie di contratto digitale le disposizioni codicistiche con cui queste presentano le maggiori affinità: *ubi eadem ratio, ibi eadem dispositio*.

A ciò si aggiunga che, indipendentemente dal fatto che a compiere materialmente un determinato atto sia stato un computer, questo deve necessariamente essere stato precedentemente programmato da un operatore umano, che ha provveduto a istruire la macchina determinando comportamenti e risposte alle richieste della controparte.

Il giudice, nell'esaminare il "comportamento" tenuto dal computer, dovrà necessariamente confrontarlo con quello previsto, almeno in linea di massima, dal programmatore per poi verificare se, ed eventualmente perché, la macchina se ne sia discostata. È evidente che ciò può essere avvenuto fondamentalmente per tre ragioni:

a. il programmatore è incorso in un errore di codice mentre digitava le istruzioni per la macchina (*errore ostativo*), in tal caso troverà applicazione l'art. 1433 c.c.;
b. il programma è stato volontariamente manomesso in modo da indurlo a commettere errori; la manomissione potrà essere stata compiuta da uno dei contraenti (art. 1439, 1° comma c.c.), oppure da un

terzo, ma essere stata comunque sfruttata a proprio vantaggio da uno dei contraenti (art. 1439, 2° comma), in tal caso troveranno applicazione gli artt. 1439-1440 c.c.;

c. il computer ha concluso il negozio perché caduto in errore su un elemento essenziale dello stesso, o a causa di un errore nell'elaborazione delle informazioni oppure perché il programmatore ha erroneamente programmato alcune delle istruzioni necessarie alla macchina per elaborare i dati. In tali casi troveranno applicazione gli articoli 1428 ss. c.c. (si osservi, in via incidentale, che l'ipotesi "errore del computer" ha scarsissima rilevanza pratica, in quanto è virtualmente impossibile che un computer, se ben programmato, commetta degli errori).

È, comunque, necessario mitigare la portata di quanto appena affermato, ricordando che è sempre opportuno leggere gli articoli sopra riportati alla luce di quanto stabilito dall'art. 1390 c.c. in relazione a eventuali vizi della volontà in cui sia incorso il rappresentante:

> Il contratto è annullabile se è viziata la volontà del rappresentante.
> Quando però il vizio riguarda elementi predeterminati dal rappresentato, il contratto è annullabile solo se era viziata la volontà di questo.

A tale proposito, la Corte di Cassazione ha affermato che

> nei contratti conclusi dal rappresentante, sia nell'ipotesi di rappresentanza volontaria, sia in quella di rappresen-

tanza legale, occorre avere riguardo per i vizi della volontà che rendono annullabile il negozio, agli stati soggettivi del rappresentante e non a quelli del rappresentato.

D'altra parte, in caso di vizio della volontà del dominus, il problema di quali norme applicare non si porrebbe comunque.

4. Criptovalute e sicurezza

Un aspetto molto importante in tema di criptovalute è quello legato alla loro sicurezza; per loro stessa natura, infatti, l'utilizzo delle criptovalute presenta delle peculiarità e degli specifici rischi nelle varie fasi della loro gestione:

– acquisto;
– conservazione;
– trasferimento.

Nelle prossime pagine cercherò di fornire una guida utile per tentare di evitare i principali rischi legati alle truffe a cui sono esposti gli utenti meno esperti che decidono di acquistare criptovalute e di utilizzarle. Per comodità espositiva, faremo riferimento essenzialmente a Bitcoin, salvo specificare di volta in volta eventuali peculiarità legate ad altre criptovalute.

4.1 L'acquisto

La domanda più frequente che si legge nei forum dedicati alle criptovalute è quella relativa alle modalità di acquisto.

Tralasciando qui il mining, in merito al quale si rimanda a quanto detto sopra, due sono le principali modalità di acquisto per una criptovaluta: acquistandola direttamente oppure in cambio di beni o servizi. In merito a quest'ultima modalità si rimanda al paragrafo relativo al trasferimento.

Resta quindi da affrontare la problematica legata all'acquisto. Questo può avvenire con differenti modalità tra cui una delle più diffuse è quella di ricorrere a un servizio di cambiavalute (*exchange service*).

Questi servizi, che possono essere fisici oppure online, svolgono la medesima attività dei cambiavalute tradizionali: accettano valuta fiat e in cambio trasferiscono all'utente criptovaluta.

1. Exchange online

Si tratta, forse, del sistema più diffuso. In rete esistono differenti servizi, più o meno simili tra loro, ma è bene chiarire fin da subito che non tutti godono della medesima affidabilità.

Ricordiamo, infatti, che non esiste alcun registro pubblico o ufficiale dei cambiavaluta e che, a oggi, chiunque potrebbe offrirsi come intermediario per l'acquisto di bitcoin o altre criptovalute.

Prima di procedere all'acquisto è quindi opportuno verificare, nei forum o nei gruppi di discussione, il rating del servizio che si intende utilizzare al fine

di ridurre il rischio di incappare in truffatori che, una volta ricevuto il denaro, spariscono senza inviare le criptovalute.

Un buon punto di partenza è rappresentato dal gruppo Bitcoin-Italia, al cui interno sono presenti varie discussioni in merito alle principlai problematiche legate ai differenti exchange (http://www.facebook.com/groups/bitcoinitalia/).

A oggi i più famosi e importanti exchange online sono Bitstamp, The Rock Trading, Coinbase. In tutti questi servizi, per effettuare l'acquisto di Bitcoin è necessario iscriversi attraverso una pagina di registrazione e inviare una copia dei propri documenti (dalle varie discussioni emerge che il documento che garantisce il miglior tempo di risposta è il passaporto) che verranno, poi, verificati dal sito stesso.

Prima di procedere alla registrazione è opportuno verificare tutti i costi del servizio (soprattutto per quanto riguarda il mantenimento dell'account, la presenza di commissioni di acquisito\vendita\trasferimento o altri costi), dato che queste voci possono variare notevolmente da un servizio a un altro.

Un altro aspetto da valutare è il costo di vendita\acquisto delle criptovalute: servizi differenti hanno spesso prezzi differenti anche di alcuni punti percentuale, come ben sanno gli utenti più esperti.

La questione è stata affrontata nel dicembre 2017 dal quotidiano «Il Sole 24 Ore» che, nell'articolo *Bitcoin: piattaforma che vai prezzo che trovi*, ha analizzato le differenze di prezzo tar le varie piattaforme partendo dal presupposto che, a differenza di quanto accade per le valute fiat, non esiste un prezzo universalmente riconosciuto: in alcuni casi si sono osservate oscillazioni superiori ai 2000 dollari tra una piattaforma e l'altra!

Una volta effettuata la procedura iniziale di iscrizione, l'utente ha la possibilità di scegliere uno dei differenti metodi di pagamento disponibili (che possono variare in base al sito scelto, anche se generalmente vengono accettati i bonifici bancari, PayPal, Postepay o la carta di credito). Scelto il metodo di pagamento, è possibile procedere all'acquisto delle monete virtuali, ma non sempre l'operazione è immediata. Anche in questo caso è opportuno leggere con attenzione il regolamento del servizio scelto, in modo da sapere se è il caso di preoccuparsi oppure no.

2. Exchange fisici

L'alternativa è quella di rivolgersi a un soggetto, fisicamente presente, che svolga il ruolo di venditore. Questi potrebbe essere una persona che intende vendere i propri bitcoin o un intermediario che svolge abitualmente questa attività: in entrambi i casi il rischio è inversamente proporzionato alla sua affidabilità.

A questo scopo esistono community, come Localbitcoin, che agevolano i passaggi di bitcoin tra utenti privati e in cui è possibile lasciare un feedback, utile a garantire l'affidabilità di un trader. In tal caso a far variare il prezzo dei bitcoin saranno tanto l'affidabilità del venditore quanto il metodo di pagamento scelto.

Come sempre in queste circostanze valgono le regole delle transazioni di persona, tra perfetti sconosciuti: meglio essere prudenti, presentarsi a un appuntamento in un luogo isolato con una valigetta di euro da cambiare in bitcoin potrebbe non essere la migliore delle idee.

A tal proposito interessante si rivela l'iniziativa di un imprenditore italiano che ha aperto a Rovereto, in provincia di Trento, il primo negozio in cui è possibile comperare bitcoin e articoli legati a questa criptovaluta.

L'obiettivo è quello di diventare un vero e proprio cambiavalute, dove chiunque potrà acquistare bitcoin a norma di legge; a questo proposito Marco Amadori, ceo di inbitcoin, tra i promotori dell'iniziativa, ha affermato la propria volontà di adeguarsi alle normative più severe in tema di cambiavalute: in pratica per acquistare più di 50 euro di bitcoin ci si dovrà registrare con un documento valido, ed è previsto un limite all'approvvigionamento di card da parte di una singola persona.

3. ATM

Un altro modo per acquistare bitcoin è rappresentato dagli ATM: si tratta di apparecchi simili agli sportelli bancomat in cui è possibile inserire denaro (o la carta di credito) e che inviano bitcoin al nostro wallet (con o senza registrazione, dipende dal Paese e dal modello di ATM). Sebbene essi siano abbastanza diffusi all'estero, in Italia ce ne sono meno di venti, alcuni dei quali non funzionanti, collocati soprattutto al Nord (una mappa aggiornata è disponibile su coinatmradar.com).

Il vantaggio degli ATM è l'immediatezza mentre i prezzi, commissioni incluse, sono mediamente più alti degli exchange.

4. In contanti: Bitboat

Last but not least esiste un servizio italiano, con sede a Londra, che consente di acquistare i bitcoin in contanti, senza alcun incontro tra acquirente e venditore, attraverso la piattaforma che Bitboat mette loro a disposizione.

Sulla piattaforma di scambio Bitboat è possibile acquistare tutte le principali criptovalute in circolazione senza alcun tipo di registrazione.

È sufficiente andare alla pagina di acquisto, riempire il relativo modulo, confermare l'ordine attraverso una mail e recarsi in una ricevitoria convenzionata per pagare l'importo preciso entro la scadenza dell'ordine.

4.2 La conservazione

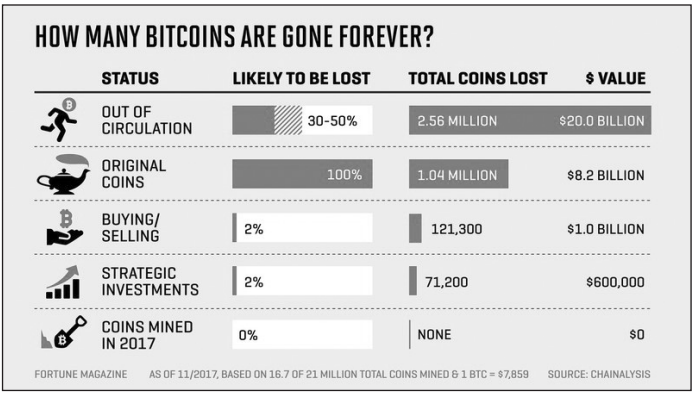
Per acquistare una criptovaluta è necessario avere a disposizione un portafoglio elettronico, cosidetto wallet, in cui custodirla e attraverso cui operare.

Il portafoglio è l'interfaccia personale dell'utente sulla rete della criptovaluta scelta, come se si trattasse di un conto corrente, anche se in realtà esso contiene password, codici segreti e stringhe di numeri che consentono all'utente di eseguire operazioni sulla propria criptovaluta.

La conservazione della criptovaluta rappresenta uno di momenti più delicati, dato che chiunque entri in possesso della password è in grado di impiegare in maniera irreversibile il contenuto del wallet.

Allo stesso modo, lo smarrimento delle credenziali di accesso rende impossibile, per chiunque, accedere al contenuto del wallet: tanto per intenderci, da una ricerca effettuata tra novembre e dicembre 2017 risul-

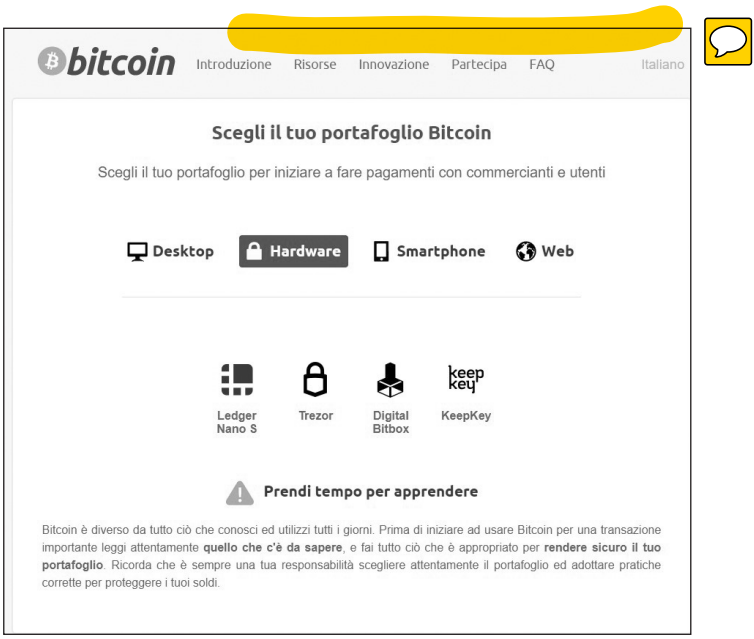
tavano "smarriti" circa tra i 2.78 e i 3.79 milioni di bitcoin (si tratta di una percentuale che oscilla tra il 17 e il 23 per cento dei bitcoin esistenti), per un valore superiore ai 40 miliardi di dollari.



Come è possibile? Semplice, smarrire una criptovaluta è molto più facile che smarrire una valuta reale: basta dimenticare una password oppure perdere un hard disk a causa di un danno hardware o, ancora, smarrire, buttare o farsi rubare il supporto (ad esempio il cellulare) in cui era conservata.

Per conservare il nostro denaro virtuale, l'alternativa è quella di utilizzare una delle tante piattaforme online, anche se pure questa soluzione presenta notevoli rischi: pericolo di subire accessi abusivi, affidabilità della piattaforma, scelta e garanzia di stabilità della stessa nel tempo non sono elementi marginali!

I portali e le piattaforme online, infatti, rappresentano un bersaglio privilegiato per i criminali, come



hanno scoperto a loro spese gli utenti di una nota piattaforma online che è stata violata determinando perdite per oltre 70 milioni di dollari.

Altra ragione di rischio legata a una piattaforma online è che essa non sia gestita nel pieno rispetto della legalità (il rischio che le criptovalute vengano utilizzate per agevolare attività criminali o per commettere il reato di riciclaggio è concreto) e che, quindi, incorra in problemi di natura legale: in caso di perquisizione e sequestro della piattaforma è possibile che tutto il nostro denaro diventi indisponibile per un tempo che può variare da pochi giorni all'eternità…

1. Hardware wallet

Ad avviso di chi scrive, la scelta migliore è quella di utilizzare un dispositivo fisico su cui è possibile esercitare un controllo diretto, tipo una chiavetta USB o, meglio ancora, uno dei tanti wallet hardware che si trovano in commercio.

Un portafoglio hardware è un dispositivo elettronico realizzato al solo fine di consentire l'utilizzo della criptovaluta. Prima di poter effettuare una transazione, infatti, questa deve essere autorizzata attraverso il dispositivo hardware in cui sono conservate le chiavi private dell'utente. Queste ultime vengono tenute in un ambiente offline, sicuro e protetto anche nel caso in cui il dispositivo venga collegato a un computer infettato da malware (almeno il più delle volte…).

I principali vantaggi di un hardware wallet rispetto a uno software possono essere riassunti nei seguenti punti:

a. le chiavi private sono spesso conservate in un'area sicura e non possono essere esportate come testo;
b. i dispositivi sono immuni ai comuni virus informatici pensati per rubare chiavi e codici di accesso dai software wallet;
c. possono essere utilizzati in maniera sicura direttamente senza bisogno di trascrivere il codice come, invece, avviene per la conservazione cartacea;
d. il più delle volte utilizzano software open source;
e. il più delle volte dispongono di strumenti di recupero in caso di furto, smarrimento o guasto hardware.

In breve, i portafogli hardware rappresentano di certo un'ottima scelta, ma non sono bulletproof…

A oggi non risultano report di furti di bitcoin av-

venuti da un portafoglio hardware, ma dato che si tratta di una tecnologia piuttosto nuova è possibile che nuovi attacchi vengano studiati e posti in essere soprattutto quando inizieranno a scarseggiare le prede più facili (portafogli software).

Battute a parte, è evidente che gli hardware wallet rappresentino un bersaglio privilegiato e di altissimo valore e le possibilità di attacco sono numerose, è bene esserne consapevoli.

Il primo e principale attacco si basa sull'inganno del titolare del wallet: un malware installato nel computer utilizzato potrebbe eseguire un attacco *man in the middle* e stornare, modificando l'indirizzo, alcune o tutte le transazioni dell'utente. Prima e principale contromisura contro questo attacco è la prassi di applicare sempre una doppia conferma su canali separati dell'indirizzo a cui inviare i bitcoin.

Sviluppo e distribuzione di un RNG (Random Number Generator) non sicuro: hardware wallets basano la propria sicurezza su un RNG, spesso integrato nell'hardware, in modo da generare in maniera sicura le chiavi private. Purtroppo è molto difficile verificare che le chiavi siano effettivamente generate attraverso un meccanismo casuale; in questo l'analisi del codice sorgente aiuta. Se la chiave non è generata in maniera casuale, un attaccante potrebbe riuscire a ricostruirla e utilizzarla abusivamente. Contro questa tipologia di attacco la scelta deve ricadere soltanto su dispositivi affidabili e testati evitando di optare per soluzioni economiche o di dubbia origine.

Allo stesso modo, eventuali bug o difetti di progettazione o programmazione del wallet potrebbero renderlo vulnerabile. Bug a livello di software, firmware o hardware possono aprire letteralmente le porte a un

attaccante e, anche se il progetto è perfetto, l'utente deve monitorare costantemente gli alert di sicurezza e mantenere il prodotto aggiornato.

La presenza di backdoor è il rischio maggiore; ancora una volta la presenza di software open source è una garanzia, ma è necessario che l'utente tenga alta la soglia di attenzione e non si lasci cullare dalla falsa convinzione di utilizzare un dispositivo inattaccabile. Un corollario a questo rischio è rappresentato dalla possibilità che l'hardware venga compromesso in fase di spedizione: le cifre in gioco sono rilevanti e altrettanto rilevanti sono le risorse messe in atto dai criminali.

2. Software wallet

Si tratta di portafogli che vengono installati su dispositivi elettronici come computer, cellulari o tablet. Le password sono rappresentate da codici segreti, ma dato che la loro sicurezza è legata al sistema in cui girano sono molto più facili da attaccare rispetto a un hardware wallet.

La scelta del wallet dipende da un grande numero di fattori, in primis dal proprio sistema operativo, dato che non tutti i wallet sono disponibili per tutte le piattaforme, e, in secondo luogo, dalla criptovaluta scelta (alcune utilizzano un proprio wallet specifico mentre alcuni wallet sono focalizzati soltanto su alcune criptovalute), per poi passare ad analizzare altri elementi più soggettivi e, tipicamente, dipendenti dalle nostre preferenze ed esigenze.

Alcuni portafogli sono orientati alla sicurezza, mentre altri sono più concentrati sulla privacy degli utenti o sulla semplicità e immediatezza di utilizzo.

NB: fate attenzione perché praticamente ogni giorno nuovi portafogli truffa vengono aggiunti sui vari por-

tali promettendo miracoli, mentre in realtà sono stati progettati per rubare il denaro collocato in essi; verificate sempre l'affidabilità dello sviluppatore e, in caso di dubbio, optate per un'altra soluzione: nessuno potrà mai restituirvi il denaro rubato.

L'ultimo aspetto da considerare, e non in ordine di importanza, è la sicurezza e la stabilità del sistema in cui viene installato il portafoglio software: molti bitcoin sono andati irrimediabilmente perduti a seguito di un evento imprevisto che ha danneggiato l'hard disk del computer in cui era installato il portafogli software oppure il cellulare o il tablet: è bene avere sempre un backup del proprio portafoglio e conservarlo in un luogo sicuro!

3. The importance of being smart

A prescindere dal portafoglio scelto, è necessario ricordare che la sicurezza del denaro è direttamente proporzionale alla robustezza e segretezza della password che lo protegge.

Per prevenire furti, truffe o qualsiasi altra perdita di denaro è quindi opportuno generare le password in un ambiente sicuro, possibilmente offline, eseguire più di un backup delle password e conservarlo in un luogo sicuro e, da ultimo, il portafoglio dovrebbe essere crittografato per aumentarne la sicurezza.

4.3 Trasferimento

Nella fase di trasferimento il denaro passa da un conto a un altro con modalità che variano da sistema a sistema.

Semplificando al massimo, per trasferire denaro da un portafogli a un altro, è necessario avere un collega-

mento che punti all'indirizzo verso il quale si vuole effettuare la transazione. Se chiave e indirizzo collimano il sistema consente la transazione e la registra. Tutta l'operazione viene naturalmente gestita dal wallet e, così facendo, è possibile utilizzare le criptovalute in maniera estremamente agevole: per esempio si può effettuare un pagamento utilizzando un semplice QR code…

In alcuni sistemi (come Bitcoin) le transazioni sono trasparenti e chiunque può conoscere il wallet di origine e quello di destinazione, in altri sistemi solo il mittente può conoscere il wallet di destinazione e in altri ancora l'indirizzo di destinazione è costituito da un collegamento usa e getta in modo da garantire l'anonimato dei soggetti coinvolti.

Qualunque sia il sistema scelto, la transazione è irrevocabile e questa circostanza ha introdotto non pochi problemi nel mondo del commercio online, soprattutto in quegli ambienti in cui la fiducia non è propriamente di casa. Il punto centrale di tutta la questione resta, dunque, la sicurezza delle transazioni e la stabilità del sistema: nessun sistema economico può, infatti, essere ritenuto affidabile se non è stabile.

1. Escrow for dummies

Uno dei principali "problemi" delle transazioni online è rappresentato dal fatto che, molto spesso, acquirente e venditore non si conoscono tra di loro e, soprattutto, non si fidano l'uno dell'altro.

Più precisamente, l'acquirente ben di rado è disponibile a pagare in anticipo, perché sa bene che, una volta trasferito il denaro al venditore, per lui sarà estremamente difficile, se non impossibile, annullare l'operazione, anche laddove si sia trattato di una truffa.

Allo stesso modo, il venditore non ha alcuna intenzione di inviare il bene all'acquirente prima di essere pagato dato che, così facendo, non ha alcuna garanzia che quest'ultimo paghi la merce dopo averla ricevuta.

La soluzione a questa tipologia di problemi è rappresentata dalla nascita e dalla diffusione di vari servizi di *escrow* (lett. "deposito in garanzia", ma a volte tradotto anche con "conto di garanzia").

Per comprendere l'escrow come *hidden service*, nonché come e perché viene impiegato, è necessario partire dall'analisi di come l'escrow viene visto e, soprattutto, utilizzato, nel *surface web*.

Questo servizio, perfettamente legale e ampiamente diffuso nelle transazioni internazionali, nasce principalmente per "proteggere/incrementare" il livello di fiducia tra il venditore e l'acquirente, soprattutto laddove i due non si conoscano: immaginiamo di dover acquistare un computer, ma, prima di inviare il bene, il venditore vuol essere sicuro che verrà pagato.

Naturalmente, noi non abbiamo alcuna intenzione di pagare prima di ricevere il computer, quindi, per riuscire a superare l'impasse, decidiamo di rivolgerci a un terzo di cui ci fidiamo entrambi ed a cui io (acquirente) consegnerò il denaro a garanzia del pagamento.

A questo punto, una volta che il denaro è stato depositato sul conto di deposito a garanzia, il venditore procede alla consegna del computer, poi, dopo che l'acquirente ha confermato di aver ricevuto il bene, l'escrow procede a versare al venditore l'importo pattuito.

Naturalmente le parti dovranno stabilire nel dettaglio tutte le condizioni del contratto, soprattutto per quanto riguarda le condizioni che dovranno avverarsi prima di poter procedere al pagamento.

È bene evidenziare che l'*escrow service* dovrà essere un

soggetto che entrambe le parti ritengono essere affidabile e neutrale, disposto a fare da arbitro o mediatore in caso di dispute e, per il suo servizio, ricevere un compenso in proporzione al valore dell'affare.

La principale e, forse unica, caratteristica che distingue l'escrow service nel surface web dall'escrow hidden service è rappresentata dal fatto che, in questo secondo ambiente, l'unico modo di verificare l'affidabilità dell'escrow è dato dalla sua reputazione presso gli altri utenti.

Nel *dark web*, infatti, nessuno si fida di nessuno e, con queste premesse, solo un pazzo si sognerebbe di inviare denaro a un altro utente in cambio di un prodotto che potrebbe non arrivare mai; allo stesso modo, nessuno si azzarderebbe a inviare un qualsiasi tipo di bene a un individuo che potrebbe benissimo svanire nel nulla senza pagare.

L'unica soluzione a questo problema è rappresentata dalla possibilità di avvalersi di un servizio di escrow e, infatti, molti dei dark market consentono di avvalersi di un simile servizio.

Ovviamente, nessun servizio può essere ritenuto davvero affidabile al 100 per cento dato che il gestore potrebbe lasciarsi corrompere o ricattare… In breve, l'ultima parola spetta all'utente, che deve decidere a quale servizio rivolgersi, in base alle caratteristiche e alle regole pubblicate nel sito.

2. Bitcoin e anonimato

Giova qui osservare che uno dei più comuni errori che vengono commessi in relazione a Bitcoin è quello di considerarlo un sistema di pagamento anonimo; in realtà il sistema non è affatto anonimo dato che, per impedire la possibilità di utilizzare più volte la stessa

moneta, la rete implementa un sistema di marcatura oraria peer-to-peer, che assegna identificatori sequenziali a ognuna delle transazioni che vengono poi rafforzate nei confronti di tentativi di modifica.

In precedenza, abbiamo analizzato il funzionamento della blockchain e abbiamo visto come, a ogni nuovo blocco, la catena si allunghi e contenga lo storico di tutti i movimenti di tutti i bitcoin generati a partire dall'indirizzo del loro creatore fino all'ultimo proprietario, rendendo le transazioni perfettamente tracciabili.

È un po' come se i numeri di serie di una banconota venissero annotati in un pubblico registro ogni volta che questa viene spesa; a ciò deve aggiungersi che, nonostante il database aumenti di dimensioni nel tempo, è sempre possibile averne una versione ridotta che riguardi nel dettaglio solo alcune transazioni, ma che rimanga completamente verificabile in maniera indipendente.

Ovviamente, esistono vari modi per accrescere la privacy delle transazioni effettuate utilizzando i bitcoin: il primo è quello di servirsi di un nuovo indirizzo per ogni pagamento ricevuto, mentre il secondo è quello di usare differenti wallet in modo da rendere molto difficile, ma non impossibile, l'associazione tra i vari indirizzi e le varie transazioni.

Per rendere impossibile tale associazione esistono differenti strumenti: il primo è noto come *Dark Wallet*, è stato realizzato da Cody Wilson ed è finalizzato a rendere del tutto irrintracciabili le transazioni in BTC.

L'idea alla base di Dark Wallet, un progetto che ha raccolto migliaia di dollari in finanziamenti da parte del pubblico, è quella di mischiare il nostro acquisto con quello di (almeno) un'altra persona rendendo vir-

tualmente impossibile l'identificazione sicura di chi ha acquistato cosa; allo stesso modo, chi vende, può usare lo strumento per generare un indirizzo "in incognito" e crittografato, e condividerne l'accesso solo con uno specifico cliente che, ovviamente, dovrà usare anche lui Dark Wallet.

In alternativa, altri strumenti molto utilizzati per impedire l'identificazione dei soggetti che impiegano i bitcoin, sono i cosiddetti *mixing service* (noti anche come *tumbler*), e cioè servizi in grado di mescolare le transazioni di differenti utenti così da renderle non rintracciabili.

Prima dell'avvento di sistemi maggiormente sicuri, i mixing service rappresentavano il principale strumento per offuscare le transazioni effettuate in bitcoin con operazioni che rappresentavano l'equivalente digitale dello spostamento di fondi nei vari paradisi fiscali.

È appena il caso di notare che questi servizi richiedono una profonda fiducia nei soggetti che li gestiscono, data l'estrema facilità con cui questi potrebbero "perdere" o, più probabilmente, rubare i fondi a essi affidati.

Oggi il "problema" è superato dalla diffusione nel dark web di nuove criptovalute maggiormente orientate verso la tutela della privacy degli utenti, ma di questo parleremo in maniera più approfondita nel capitolo dedicato ai loro utilizzi illegali.

5. Criptovalute e diritto penale

Nelle pagine precedenti abbiamo visto gli aspetti positivi delle modifiche che le criptovalute hanno portato nel nostro modo di interpretare le relazioni finanziarie internazionali, i pagamenti online e le loro ripercussioni nel mondo della finanza, soprattutto per quanto riguarda l'impiego della blockchain, e nel mondo della contrattualistica, ipotizzando la prossima nascita e la successiva diffusione dei cosiddetti smart contract.

Ora è giunto il momento di analizzare gli aspetti legati all'impiego criminale di questi strumenti.

A giugno 2017, l'FBI ha affermato di avere bisogno di ottanta nuove posizioni lavorative e di un budget di 21.6 milioni di dollari per incrementare le proprie capacità investigate relativamente alle attività illegali legate al dark web e alle criptovalute. Nel documento si legge:

> *Some of our criminal investigators face the challenge of identifying online pedophiles who hide their crimes and identities behind layers of anonymizing technologies, or drug traffickers who use virtual currencies to obscure their transactions*.

E lo stesso problema è stato sollevato da Europol che, a marzo 2017, ha denunciato:

The widening criminal use of decentralised virtual currencies and the increased use of tumbler/mixer services, effectively prevent law enforcement to 'follow the money' and significantly complicate the possibilities for asset recovery and the prevention of fraudulent transactions. The lack of (minimum) standards for due diligence and Know-Your-Customer for such services and the non-application of existing regulations compound to the problem.

(Per approfondire si veda: https://www.fbi.gov/services/operational-technology/going-dark)

5.1 Cyberlaundering e acquisto di merci illegali

1. Le problematiche legate all'impiego criminale dei bitcoin

Gli ambienti criminali hanno apprezzato sin da subito molte delle caratteristiche delle criptovalute, con particolare riguardo alla facilità con cui possono essere rese anonime e ripulite.

Sebbene sia noto che i bitcoin non possano essere considerati un sistema di pagamento anonimo, la loro altissima diffusione li rende ancor oggi uno dei modi principali di pagamento per operazioni illecite e questa circostanza ha reso necessario sviluppare e diffondere sistemi in grado di aumentarne il livello di anonimato.

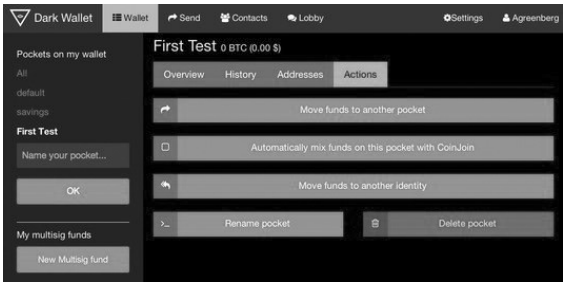
Dark Wallet

Uno di questi strumenti è rappresentato da Dark Wallet, presentato nel 2014 e ancora molto, diffuso sebbene in fase di beta testing. Si tratta di un software sviluppato con il preciso scopo di rendere impossibile il tracciamento delle transazioni effettuate in bitcoin, cifrando e mescolando le transazioni degli utenti.

Il software è potenzialmente esplosivo e ne è facilmente ipotizzabile un utilizzo illegale tanto che, durante un

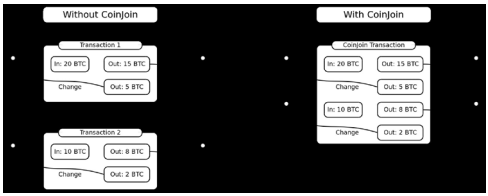
dibattito al New York's Museum of Modern Art a marzo 2014, il suo ideatore Cody Wilson ha descritto così il suo programma: «*It's just money laundering software*», mentre in un'intervista ha dichiarato: «*I want a private means for black market transactions, whether they're for non-prescribed medical inhalers, MDMA for drug enthusiasts, or weapons*».

Ciò nonostante Wilson sostiene che il suo sviluppo è tutelato dal Primo Emendamento della Costituzione degli Stati Uniti, come strumento per la tutela della libertà di opinione. Nell'immagine che segue, tratta da Wired (http://www.wired.com/2014/04/dark-wallet/), possiamo osservare uno screenshot dell'interfaccia di DarkWallet: è evidente l'opzione per mescolare i bitcoin attraverso la funzione Coinjoin.



Si tratta di una funzione di riciclaggio, ideata da Gregory Maxwell, basata sull'idea di mescolare tra di loro differenti transazioni in modo che sia impossibile stabilire a chi appartenga ogni singola transazione.

Si veda lo schema seguente:



Le transazioni di Bob e Alice saranno mescolate tra di loro e un eventuale osservatore vedrà soltanto una singola transazione, registrata nella blockchain e non gli sarà possibile attribuirla con certezza a uno specifico utente. Più transazioni vengono svolte in sequenza, più sarà difficile individuare gli effettivi soggetti coinvolti.

A ciò si aggiunga che Dark Wallet offre anche la possibilità di utilizzare un'ulteriore tecnica nota come *stealth address*: un utente può generare un indirizzo segreto e utilizzarlo per richiedere un pagamento. Quando il mittente invia i bitcoin a questo indirizzo, Dark Wallet li invia a un altro indirizzo che rappresenta il risultato di una cifratura casuale dell'indirizzo segreto. A questo punto Dark Wallet analizza la blockchain alla ricerca di un indirizzo che può essere decifrato utilizzando la propria chiave e, una volta individuato, rivendica il pagamento. Tuttavia, se un qualsiasi soggetto effettua una ricerca nella blockchain per individuare l'indirizzo segreto, non è in grado di trovare i pagamenti legati a quell'indirizzo.

Samourai

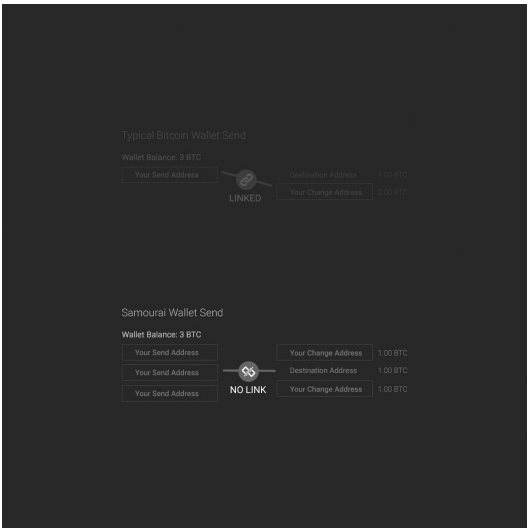
Accanto a Dark Wallet esiste un altro strumento similare: Samourai (samouraiwallet.com/). Open source e privacy oriented, Samourai è stato rilasciato nel maggio del 2015, è ancora in versione alpha e si presenta come «*a modern bitcoin wallet hand forged to keep your transactions private, your identity masked, and your funds secure*».

Il wallet sembra essere focalizzato tanto sulla sicurezza quanto sulla riservatezza tanto da implementare, unico nel suo genere, una funzione di autodistruzione tramite sms.

Gli sviluppatori di Samourai si presentano come «*privacy activists who have dedicated our lives to creating the software that Silicon Valley will never build, the regu-*

lators will never allow, and the VC's will never invest in. We build the software that Bitcoin deserves».

La fase di mixing, gestita in maniera differente rispetto a Dark Wallet, viene descritta nel dettaglio all'interno del blog ufficiale di Samourai (http://blog.samourai-wallet.com/):



In breve, mentre un wallet ordinario consente sempre di collegare le varie transazioni all'account originario, Samourai non utilizza mai due volte un medesimo indirizzo per inviare bitcoin e non consente di collegare le singole transazioni all'account originario.

Particolarmente interessante è la funzione che consente di recuperare o cancellare, come detto, tramite un sms il proprio wallet: inviando al cellulare il messaggio «SW seed YOUR_PIN_CODE» l'utente potrà ricevere il proprio seed HEX attraverso cui potrà ripristinare l'accesso ai propri bitcoin mentre, uti-

lizzando il comando «SW wipe YOUR_PIN_CODE» l'utente potrà cancellare il proprio wallet.

Una funzione "segreta" consente poi di nascondere la presenza dell'applicazione, che potrà essere avviata solo digitando un apposito numero di telefono.

A ciò deve aggiungersi che Samourai è protetto da una crittografia AES-256 e che, per poter accedere, è richiesta una passphrase robusta.

Altri wallet

Nel dark web esistono, poi, altri wallet che si propongono di mantenere al sicuro l'identità degli utenti, ma si tratta prevalentemente di wallet collocati su piattaforme online, con tutti i rischi che questo comporta.

2. Bitcoin laundering - Bitcoin anonymization taken seriously

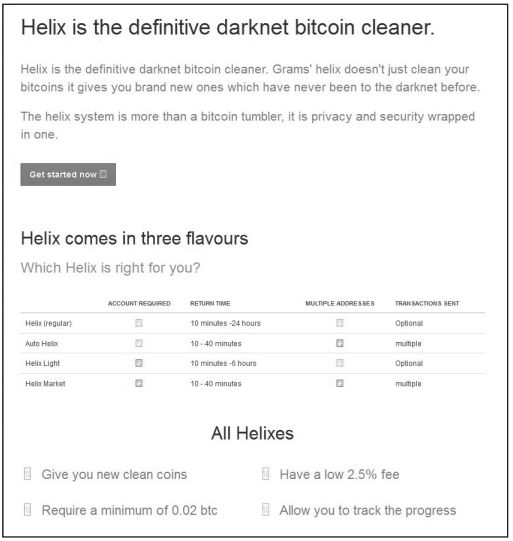
Nelle prossime pagine di questo paragrafo analizzeremo nel dettaglio alcuni degli strumenti maggiormente utilizzati per "offuscare" i bitcoin attraverso servizi di mixing.

Diciamo subito che, nella maggior parte dei casi, questi servizi sono delle "lavatrici", servizi tesi non soltanto a garantire la tutela dell'anonimato degli utenti, ma anche ad agevolare il riciclaggio di denaro sporco (in merito al cyber-riciclaggio si vedano i prossimi paragrafi).

Il primo strumento di cui parleremo è Helix: si tratta di un servizio molto popolare e, per questa ragione, viene fatto spesso oggetto di imitazioni, tese a ingannare gli utenti e rubare i loro bitcoin.

Helix dichiara espressamente di "ripulire" i bitcoin rendendoli "come nuovi", come se non fossero mai stati impiegati nel darknet.

Il processo viene eseguito in base a una nuova tecnologia proprietaria e il denaro non viene solo mescolato, ma scambiato con monete nuove prima di essere "lavorato" in modo da non poter essere tracciato. Questa circostanza, inoltre, fa sì che il sistema abbia sempre una riserva di denaro "pulito" da reimmettere subito nel circuito in presenza di importi modesti.


Helix is the definitive darknet bitcoin cleaner.

Helix is the definitive darknet bitcoin cleaner. Grams' helix doesn't just clean your bitcoins it gives you brand new ones which have never been to the darknet before.

The helix system is more than a bitcoin tumbler, it is privacy and security wrapped in one.

Get started now

Helix comes in three flavours

Which Helix is right for you?

	ACCOUNT REQUIRED	RETURN TIME	MULTIPLE ADDRESSES	TRANSACTIONS SENT
Helix (regular)	☐	10 minutes -24 hours	☐	Optional
Auto Helix	☐	10 - 40 minutes	☑	multiple
Helix Light	☑	10 minutes -6 hours	☐	Optional
Helix Market	☑	10 - 40 minutes	☑	multiple

All Helixes

☐ Give you new clean coins

☐ Have a low 2.5% fee

☐ Require a minimum of 0.02 btc

☐ Allow you to track the progress

In media, l'operazione di "lavaggio" impiega almeno quaranta minuti per essere portata a termine, ma i tempi possono aumentare notevolmente se l'utente inserisce un ritardo casuale ovvero quando la transazione coincide con una delle operazioni di manutenzione del server.

Un ulteriore vantaggio di Helix è rappresentato dal fatto che la "lavatrice" è direttamente integrata con l'account che l'utente utilizza nei dark market rendendo tutto molto più semplice; a titolo di provvigione, i gestori trattengono il 2,5 per cento dell'importo "lavato".

Una volta che l'operazione di lavaggio è stata portata a termine, l'utente riceve una comunicazione di conferma che si autodistrugge dopo essere stata letta e tutti i log vengono cancellati al massimo dopo una settimana, sempre che l'utente non chieda di cancellarli prima.

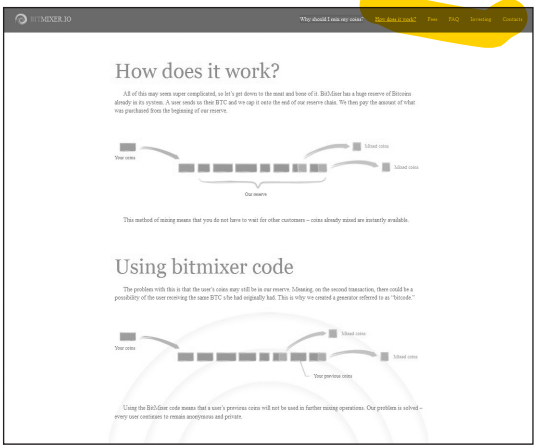
Un altro servizio di *cyberlaundering*, è rappresentato da Pay Shield, che opera mescolando tra di loro i bitcoin dei propri utenti in modo da rendere impossibile attribuire una specifica operazione a un determinato utente.

Il lavaggio richiede circa trenta minuti, i gestori trattengono il 2 per cento dell'importo a titolo di provvigione e, per aumentare il livello di sicurezza e di riservatezza, l'importo della commissione viene leggermente modificato in maniera casuale; una volta eseguita la pulizia dei bitcoin, l'utente ha ventiquattr'ore di tempo per impiegare la somma e inviare il pagamento prima che il sistema elimini automaticamente ogni traccia dell'operazione compiuta.

Il sistema offre anche un'opzione per consentire agli utenti di inviare un pagamento direttamente a un altro portafoglio attraverso "*Pay someone with mixed coins*".

Altri sistemi, simili ai due già analizzati, sono BitMixer, WashBit e Bitcoin Blender.

Nell'immagine a seguire possiamo vedere lo schema grafico di funzionamento di BitMixer: il denaro sporco



entra nella "cassa comune" di BitMixer e all'utente viene erogato altro denaro già presente in cassa.

In questo modo viene interrotta la continuità della blockchain e non è più possibile collegare un determinato gruppo di bitcoin a una specifica operazione di acquisto o vendita.

Particolarmente interessante si rivela la guida pubblicata dal servizio di Bitcoin Blender, in quanto in essa vengono illustrati alcuni "trucchi" per rendere ancora più efficace la procedura di pulizia:

1. le quote delle provvigioni non devono essere fisse, ma devono variare in modo da impedire che un attaccante possa facilmente individuare la somma ripulita mediante un semplice calcolo; in breve, se io so che la provvigione del servizio di lavanderia è pari al 2 per cento e so che Tizio deve "lavare" 100 BTC, non dovrò fare altro che tracciare tutte le operazioni pari a 98 BTC nelle ventiquattr'ore successive all'avvio del lavaggio;

2. impiego di più conti in modo da rendere più difficile tracciare le operazioni: se può essere facile tracciare i movimenti di 50 BTC, tutt'altra impresa si rivela tracciare la stessa cifra ripartita in maniera casuale in cinque conti di appoggio;
3. possibilità di impostare un ritardo casuale, da poche ore a una o più settimane, si rivela utile per impedire agli investigatori di notare uno schema temporale nei movimenti di bitcoin del sospetto;
4. possibilità di ritirare gli importi scaglionandoli in maniera automatica nel tempo tra i vari conti gestiti dal sistema in modo da non destare alcun sospetto con movimenti rintracciabili.

3. L'impiego delle altcoin

Preso atto delle carenze, in termini di anonimato, di Bitcoin, la criminalità organizzata e non ha iniziato a spostare il proprio interesse verso altre criptovalute maggiormente privacy oriented.

Nei primi mesi del 2017 l'FBI ha rilevato l'aumento delle transazioni effettuate nei dark market utilizzando Monero tanto che l'agente speciale Joseph Battaglia, FBI Cyber Division di New York, ha chiaramente detto, durante un evento organizzato da New York's Fordham University a gennaio 2017, che la diffusione di transazioni in criptovalute pseudoanonime o anonime ha radicalmente modificato il modo in cui l'Agenzia conduce le proprie indagini.

L'agente, che ha espressamente fatto riferimento a Monero, ha poi concluso dichiarando:

> *We're going to look at what catches on, and what becomes mainstream, and then we're going to keep an eye on that, because*

usually not long after that is when you start to see some of the fraud and some of the more nefarious uses of that technology.

A settembre 2017 il concetto è stato ribadito da un agente del Department Homeland Security (DHS) che in un'intervista alla CNBC ha dichiarato:

What the criminals are starting to see, and some of the trends we're picking up as well, is that bitcoin also works equally just as much against you as it does for you.

Al momento le criptovalute preferite dai criminali sembrerebbero essere Monero e ZCash, che si presenta come una criptovaluta in grado di fornire una robusta protezione alla riservatezza delle transazioni.

Sebbene non sia possibile conoscere l'esatto ammontare delle transazioni illegali, Blockchain Intelligence Group ha affermato che le transazioni illecite che coinvolgono l'impiego di bitcoin sono calate fino ad arrivare a meno del 20 per cento di tutte le transazioni.

4. Dalla moneta reale alla moneta virtuale

Nelle pagine precedenti abbiamo visto come funziona tecnicamente il cyberlaundering, ora è giunto il momento di affrontarne i principali aspetti legali e investigativi.

L'esperienza investigativa ha ampiamente dimostrato che, nel corso degli anni, la criminalità organizzata è sempre stata pronta a individuare e sfruttare nuove fonti di reddito: a tale ricerca non potevano, ovviamente, sfuggire le enormi potenzialità offerte dall'informatica.

Si pensi, per esempio, a quanto appaia attraente per il crimine organizzato la possibilità di trasferire ingenti capitali, direttamente in forma elettronica, inviandoli alle "lavatrici" semplicemente con un click

del mouse, riducendo notevolmente il rischio che il denaro venga individuato, intercettato e sequestrato alla frontiera da parte delle Forze dell'Ordine.

Le organizzazioni criminali, infatti, non hanno soltanto bisogno di assicurarsi un flusso costante di risorse finanziarie, ma devono anche riuscire a reinvestire e utilizzare proficuamente il denaro raccolto.

5. Un po' di storia

In Italia, già nel 1998, Alessandro Pansa, all'epoca direttore del Servizio Centrale Operativo della polizia di Stato ed ex capo del DIS (Dipartimento delle informazioni per la sicurezza), osservava che i cartelli colombiani, avendo esigenza di raccogliere il denaro sparso in tutto il mondo e guadagnato vendendo droga, necessitavano di una grossa rete di comunicazione per recuperarlo e farlo poi confluire verso i cosiddetti broker. Questi sono intermediari finanziari che poi, a loro volta, devono far confluire i soldi sporchi verso le "cosiddette case di cambio" (una sorta di banche non ufficiali gestite direttamente dai cartelli colombiani).

In questi circuiti illeciti le reti di comunicazione, che fino a qualche anno fa erano gestite via fax trasmettendo messaggi codificati, sono oggi gestite attraverso i più moderni strumenti di comunicazione elettronica: ognuno di questi singoli operatori/riciclatori dei cartelli colombiani viene, quindi, dotato di un personal computer portatile, di un accesso alla rete e di un programma di comunicazione con un codice di criptazione estremamente complicato che viene modificato continuamente.

Sulla questione è intervenuto anche Umberto Rapetto, all'epoca tenente colonnello della guardia di finanza, che nel 1999 evidenziò come uno scenario poco

rassicurante si prospettasse agli occhi di chi si trovava a operare sul campo per contrastare in maniera efficace il sempre più impressionante fenomeno del riciclaggio del denaro sporco: il *corporate* e l'*home banking* avevano portato i tradizionali sportelli sulle scrivanie degli uffici e delle case, consentendo a operatori non bancari di immettere denaro nel circuito creditizio, effettuare pagamenti e, soprattutto, movimentare capitali.

L'attività degli operatori di polizia si era notevolmente complicata in quanto i milioni di agenzie e filiali di banca si erano centuplicati: ogni presa telefonica può consentire a un computer di entrare in rete e – magari per pochi minuti – trasformarsi in una postazione bancaria.

A ciò deve aggiungersi che anche i servizi segreti italiani, allertati da alcune operazioni finanziarie sospette tra l'Italia e la Russia, hanno avuto modo di verificare come, negli ultimi venticinque anni, la criminalità organizzata e il terrorismo internazionale si siano spostati sul web, trovando in esso un utile strumento per raccogliere fondi e riciclare i proventi delle attività illecite.

Si è poi osservato che, molto probabilmente, la criminalità organizzata sta utilizzando le conoscenze e le abilità intrusive di alcuni criminali informatici al fine di violare, per fini illeciti, importanti sistemi computerizzati, articolati in rete, per carpire, modificare o distruggere dati sensibili, anche di carattere riservato, o per occultare le tracce del trasferimento di denaro "sporco".

D'altra parte, gli esperti di cyber sicurezza sono perfettamente consapevoli che internet si presta ottimamente a tali scopi, consentendo lo sviluppo di attività criminali di vario genere e favorendo in vario modo il riciclaggio del denaro sporco.

È altresì evidente e innegabile che lo sviluppo delle transazioni bancarie effettuate tramite internet ab-

bia garantito un notevole risparmio, in termini economici e di ore lavorative, sia per gli utenti sia per le banche, andando a rappresentare uno strumento utile e irrinunciabile.

La questione è nota e ampiamente dibattuta anche oltreoceano, dove, già negli ultimi anni del secolo scorso, in relazione al possibile abuso delle reti telematiche per trasferire e riciclare il denaro l'Internet Fraud Complaint Center affermava:

> *Digital transfers are anonymous. Even if the cyberbanks that accept anonymous E-cash are somehow subject to the same laws and regulations that financial institutions in the tangible world are, the launderer must first be caught. The reports will be virtually useless, as the banks have no knowledge as to which funds are the launderer's. This provides for anonymous money laundering. Structuring of transactions so as to avoid currency reporting requirements becomes less risky if the funds used to structure are virtually untraceable.*
> *In addition, the filing of currency transaction reports may be pointless if the money can not be traced into a specific account. However, the actual requirement that a transaction report be filed may be nonexistent if cyberbanks that accept E-cash deposit accounts do not fall under current federal or state regulation of financial institutions (IFCC).*

Anche in Svizzera il Dipartimento della Giustizia ha riunito un gruppo di esperti il quale ha redatto un rapporto dal titolo *New media and the law* da cui emerge con chiarezza che il riciclaggio segue, ormai da anni, lo sviluppo dei pagamenti elettronici; il Dipartimento afferma trattarsi di un settore ad alto rischio, specialmente quando sarà molto più diffuso il cosiddetto "borsellino elettronico", in grado di permettere pagamenti elettronici direttamente tra i singoli individui al di fuori dell'infrastruttura finanziaria e bancaria.

6. Riciclaggio digitale: strumentale e integrale

Dall'analisi del *modus operandi* emerge chiaramente che i criminali tengono due distinte tipologie di condotta relativamente al riciclaggio in internet: una prima indicata come "riciclaggio digitale strumentale" e una seconda definita "riciclaggio digitale integrale".

Si parla di "riciclaggio digitale strumentale" quando la rete internet viene presa in considerazione come mero strumento, ma l'attività illecita prende le mosse dai cosiddetti "paradisi fiscali"; in questo caso, dunque, la tecnologia viene utilizzata per perfezionare e migliorare le strategie classiche del riciclaggio dei proventi illeciti sostituendo con un computer il classico corriere.

In origine il riciclaggio era essenzialmente un'attività fisica, svolta nel mondo reale con corrieri in carne e ossa, un'attività finalizzata a nascondere l'esistenza, l'origine illegale o l'illegalità delle attività in cui quel denaro aveva trovato applicazione, e la necessità di poter poi "lavorare" quei soldi in modo da poterne simulare un'origine lecita richiedeva che il "lavandaio" avesse la possibilità di trasportare fisicamente il denaro contante.

Il gioco si basava, e si basa ancora oggi, sulla capacità di evitare di attirare attenzioni indesiderate da parte delle agenzie governative preposte al controllo dei flussi finanziari.

Il riciclaggio a "bassa tecnologia" esigeva, essenzialmente, la capacità, da parte degli operatori, di manipolare il mondo circostante, ingannare o corrompere gli operatori delle dogane, contrabbandare il contante attraverso varchi non sorvegliati per poi farlo giungere in Paesi con una normativa bancaria più favorevole, dove trovare banche e banchieri compiacenti che non facessero troppe domande sull'origine dello stesso.

Non a caso i corrieri erano detti "muli": semplici "animali" da soma che dovevano trasportare somme relativamente modeste in modo da aggirare le norme in materia di circolazione del denaro contante.

Con l'evolversi della normativa antiriciclaggio e l'intensificarsi dei controlli, la criminalità organizzata ha dovuto iniziare a trovare delle valide alternative al trasporto "fisico" del denaro cominciando a sfruttare in maniera sempre più approfondita e complessa i trasferimenti elettronici di denaro.

La rete ha iniziato a giocare, dunque, un ruolo sempre più significativo, a volte essenziale, in ciascuna delle tre fasi che l'attività investigativa ha individuato come tipiche del riciclaggio:

– la fase di *placement*;
– la fase di *layering*;
– la fase di *integration*.

La fase di *placement* coincide con l'"emersione" del denaro e il suo collocamento nel circuito finanziario o nel commercio legale; indubbiamente si tratta del momento di maggior rischio per i criminali in quanto, proprio in questa fase, più alta è la possibilità di essere individuati, arrestati e di vedersi confiscare i proventi del reato.

Vi è, inoltre, il grosso rischio di creare e mantenere la cosiddetta "strada di carte", e cioè tutta quella serie di documenti in grado di aiutare gli investigatori a identificare i membri dell'organizzazione. In breve, la vita del "riciclatore classico" era tutt'altro che facile: costretto a trasportare da un Paese all'altro ingenti quantità di denaro, avvalendosi di corrieri che potevano facilmente essere arrestati, tradire il proprio datore di lavoro tenendosi il contante o collaborare con le forze dell'ordine consegnando loro informazioni e documenti…

Da questo punto di vista, l'utilizzo di internet è risultato strategico per varie ragioni: in primo luogo questo strumento si è rivelato in grado di garantire una notevole certezza sull'identità dell'interlocutore; pur in assenza di comunicazione di dati anagrafici o di conoscenza diretta, è infatti sufficiente l'utilizzo di un qualsiasi sistema di firma elettronica e una *chain of trust* per essere ragionevolmente certi che l'interlocutore è chi dice di essere e non un impostore.

In secondo luogo, la rete rende spesso superata la necessità di corrompere i cosiddetti "intermediari necessari", soggetti in grado di monitorare e tracciare il trasferimento del denaro consentendo, al contrario, trasferimenti di valuta per ammontare illimitati e senza alcun intermediario.

A tale proposito Umberto Rapetto osservava che storicamente si è sempre fatto affidamento sull'intermediazione delle banche e delle altre istituzioni finanziarie, in modo da disporre di passaggi obbligati attraverso i quali denaro e altri fondi dovevano necessariamente transitare e dove rimanevano annotate e registrate le tracce delle relative operazioni.

Attraverso il meccanismo della disintermediazione questi passaggi obbligati vengono eliminati, essendo sufficiente la semplice connessione alla rete per ottenere il trasferimento di valori finanziari tra soggetti diversi senza coinvolgere alcuna entità terza operante sotto il controllo di un ente governativo.

Tuttavia, se il ruolo di internet è importante in relazione ai primi due aspetti, diventa addirittura strategico nel momento in cui si tratta di migliorare altri due importanti elementi: la riservatezza delle comunicazioni e l'occultamento dei beneficiari delle operazioni.

La riservatezza viene garantita dalla disponibilità di

molteplici software di crittografia o di steganografia, di fatto spesso inviolabili per qualsiasi agenzia di controllo del crimine. Non si può, poi, ignorare la concreata eventualità di operare in internet in totale anonimato frustrando qualsiasi tentativo di intercettazione, e a ciò si aggiunge la possibilità di acquistare caselle postali anonime con possibilità di rinvio postale, oppure numeri di telefono in altre nazioni che vengono automaticamente "girati" su un'utenza nazionale in modo da poter efficacemente costruire identità fittizie.

Una volta immesso il denaro nel circuito bancario è necessario procedere al suo "lavaggio". Si tratta della fase cosiddetta di *layering* e consistente nell'esecuzione di molteplici operazioni finanziarie o commerciali finalizzate al mascheramento dell'origine del denaro.

È proprio in tale fase che l'utilizzo delle banche online offre i migliori risultati, consentendo di spostare il denaro in maniera rapida ed economica restando comodamente seduti alla propria scrivania o, magari, standosene tranquillamente in spiaggia sotto l'ombrellone!

Non si possono poi trascurare le possibilità di riciclaggio offerte dai casinò e dalle scommesse effettuate in internet. Il business delle case da gioco virtuali è letteralmente esploso in questi ultimi anni e spesso si tratta di "locali" che operano in paradisi fiscali o in Paesi dalla normativa anti-riciclaggio a dir poco "allegra". Le giocate vengono pagate con qualsiasi sistema, evitando controlli o comunicazioni che possano insospettire qualche autorità di vigilanza.

Vengono poi rilasciati certificati di vincita ed è persino possibile acquistare gli stessi da qualche casinò virtuale senza scrupoli, per non parlare della gestione di queste attività da parte delle stesse organizzazioni dedite al riciclaggio. Una volta che il denaro è stato

debitamente ripulito, l'organizzazione criminale non deve fare altro che reinvestirlo in attività perfettamente lecite: si tratta della cosiddetta fase di *integration*, qui il ruolo della rete è soltanto quello di agevolare la gestione di un patrimonio ormai perfettamente legittimo.

7. segue: il riciclaggio digitale integrale

Nel riciclaggio digitale integrale si ha una completa sostituzione del denaro convenzionale con moneta virtuale e questa trasformazione rende gli scambi molto più difficili da tracciare.

Basti qui osservare che la fase di placement viene condotta direttamente in forma digitale riducendo notevolmente tutti i rischi connessi a tale attività e, spesso, rendendo persino superflue le altre due fasi.

Può prevedersi l'utilizzo di almeno quattro differenti tipologie di strumenti di cyber pagamento:

– sistemi basati sul ricorso a reti telematiche connesse a valute legali (bonifici online *et similia*);

sistemi basati su valute virtuali non aventi corso legale (si pensi alle varie criptovalute);

– soluzioni fondate sull'utilizzo di valori conservati su carte intelligenti o smart card con trasferimento diretto di fondi da una carta all'altra, come nel caso del cosiddetto borsellino elettronico;
– sistemi alternativi di pagamento (buoni virtuali di acquisto, credito telefonico, crediti da spendere presso e-store o simili).

In tutti questi casi, il denaro "fisico" viene convertito in moneta elettronica molto tempo (e molti passaggi) prima di essere utilizzato per finalità illecite e, quindi, si tratta

di denaro perfettamente "pulito" e facilmente spendibile.

Ovviamente, prevalentemente per ragioni di riservatezza, la criminalità preferisce avvalersi dei sistemi "alla pari", e cioè senza alcun intermediario tra le parti, in quanto le transazioni sono molto più facili da gestire e, soprattutto, occultare. Le ipotesi di utilizzo pratico di tali sistemi sono virtualmente infinite e garantiscono una sicurezza pressoché assoluta, sia dal punto di vista della riservatezza sia da quello della certezza della transazione.

Immaginiamo che Tizio, spacciatore affiliato all'organizzazione XY, non voglia maneggiare denaro contante. Non deve fare altro che pretendere che i suoi clienti lo paghino utilizzando schede prepagate con cui ricaricare la propria scheda GSM (ovviamente registrata sotto falso nome).

Una volta caricata la scheda Tizio, per trasferire il denaro all'estero, non dovrà fare altro che effettuare delle chiamate a *hot-line* fittizie collocate in Paesi di comodo oppure acquistare beni fisici o virtuali utilizzando come sistema di pagamento il proprio credito telefonico.

Effettuate le chiamate, l'organizzazione XY dovrà soltanto occuparsi di gestire le *hot-line* e verificare la regolarità delle chiamate senza alcuna operazione bancaria da giustificare e con i fondi già "ripuliti" e comodamente disponibili in un conto estero, oppure occuparsi di gestire la vendita al dettaglio dei beni acquistati presso gli e-store.

Un'ipotesi simile può farsi in caso di utilizzo del borsellino elettronico, soprattutto se caricato con bitcoin. Attraverso una semplice operazione è possibile trasferire i bitcoin da un borsellino all'altro, comprando un qualsiasi bene illegale senza dover adoperare denaro fisico: si inserisce il numero di borsellino del venditore, si indica l'importo da trasferire, si digita la propria passphrase, si impartisce l'ordine di trasferimento e il gioco è fatto.

Nell'immagine a fianco vediamo la schermata di un moderno bitcoin wallet in grado di gestire in automatico l'intera transazione fornendo al soggetto tenuto al pagamento un comodo QR-code, da acquisire con il proprio cellulare, per attivare immediatamente il trasferimento della corretta somma in bitcoin verso il borsellino del soggetto venditore.

Lo spacciatore, ad esempio, direttamente attraverso il proprio cellulare, può immediatamente riscontrare l'avvenuto pagamento e procedere alla cessione della droga al cliente.

A questo punto, i bitcoin che sono stati "caricati" sul borsellino a fronte dell'operazione illecita di spaccio di stupefacenti possono essere agevolmente trasferiti e ripuliti in diverse maniere.

5.2 Ransomware

Un altro ambito criminale in cui le criptovalute sono particolarmente apprezzate è legato alla diffusione dei cosiddetti *ransomware*. Si tratta di software che prendono in "ostaggio" i dati dell'utente crittografandoli e chiedendo il pagamento di un riscatto per consentire di accedere nuovamente agli stessi. Secondo la definizione dell'FBI, «*ransomware is a form of malware that targets both human and technical weaknesses in organizations and individual networks in an effort to deny the availability of critical data and systems*».

Si tratta di un fenomeno in rapidissima crescita e che ha visto in qualità di vittime ospedali, aziende, privati e liberi professionisti con un tasso di crescita del 36 per cento tra il 2015 e il 2016 (dati Symantec) e ancora maggiore nel corso del 2017 (secondo Symantec nel solo primo semestre si sono contati 319 mila attacchi contro i 470 mila contati in tutto il 2016) con un preoccupante aumento degli attacchi mirati contro obiettivi specifici.

L'importo del riscatto varia tra i 500 e i 1000 dollari e, generalmente, viene pagato in bitcoin o in monero.

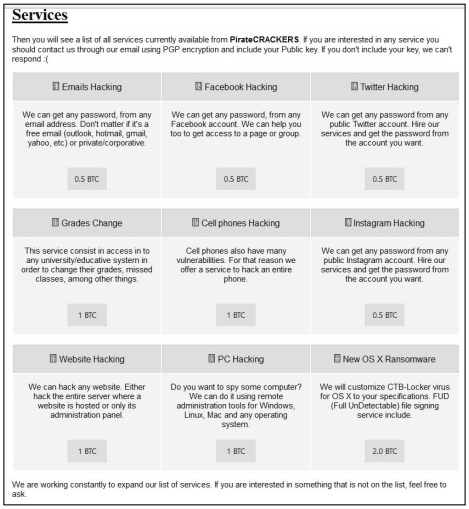
1. Ransomware-as-a-service

Particolarmente rilevante è la diffusione del modello Ransomware-as-a-Service, in cui all'utente viene fornito tutto il necessario per attaccare una serie di obiettivi identificati garantendogli il supporto tecnico e logistico.

Nel mese di maggio 2016 Kaspersky Lab ha scoperto l'esistenza di Petya, il quale non solo codifica i dati custoditi sul computer dell'utente, ma sovrascrive l'MBR (Master Boot Record) dell'unità hard disk, in modo tale che i computer infetti non siano più in grado di avviare il sistema operativo. Si tratta di uno dei più recenti modelli di Ransomware-as-a-Service e, per essere sicuri di mettere le mani sulla loro quota di profitto, gli autori del programma hanno inserito all'interno di Petya appositi "meccanismi di protezione" che non consentono un impiego non autorizzato dei sample del malware.

Altri esempi di RAS sono Petya/Mischa e Shark, in seguito ribattezzato con il nome di Atom (fonte Rapporto Kaspersky Lab).

A questo proposito si veda l'immagine che segue, tratta da uno dei tanti servizi del dark web. In basso a destra appare l'offerta del servizio.



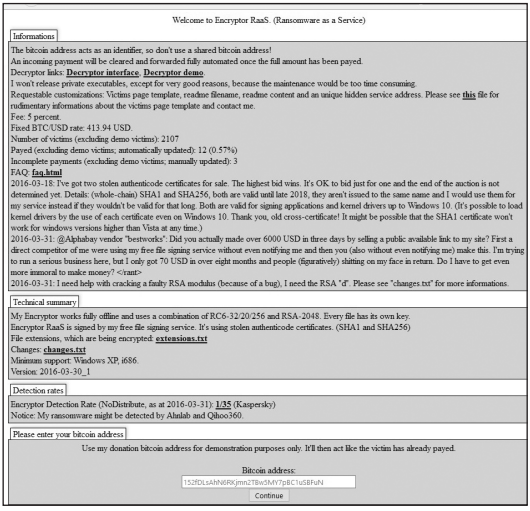
Services

Then you will see a list of all services currently available from **PirateCRACKERS**. If you are interested in any service you should contact us through our email using PGP encryption and include your Public key. If you don't include your key, we can't respond :(

Emails Hacking	Facebook Hacking	Twitter Hacking
We can get any password, from any email address. Don't matter if it's a free email (outlook, hotmail, gmail, yahoo, etc) or private/corporative.	We can get any password, from any Facebook account. We can help you too to get access to a page or group.	We can get any password from any public Twitter account. Hire our services and get the password from the account you want.
0.5 BTC	0.5 BTC	0.5 BTC
Grades Change	**Cell phones Hacking**	**Instagram Hacking**
This service consist in access in to any university/educative system in order to change their grades, missed classes, among other things.	Cell phones also have many vulnerabilities. For that reason we offer a service to hack an entire phone.	We can get any password from any public Instagram account. Hire our services and get the password from the account you want.
1 BTC	1 BTC	0.5 BTC
Website Hacking	**PC Hacking**	**New OS X Ransomware**
We can hack any website. Either hack the entire server where a website is hosted or only its administration panel.	Do you want to spy some computer? We can do it using remote administration tools for Windows, Linux, Mac and any operating system.	We will customize CTB-Locker virus for OS X to your specifications. FUD (Full UnDetectable) file signing service include.
1 BTC	1 BTC	2.0 BTC

We are working constantly to expand our list of services. If you are interested in something that is not on the list, feel free to ask.

Nel caso specifico si tratta di un tool per la realizzazione di copie personalizzate di CBT-Locker. Viene poi fornito il supporto per realizzare la piattaforma per incassare il riscatto e fornire la chiave di decrittazione.



Welcome to Encryptor RaaS. (Ransomware as a Service)

Informations

The bitcoin address acts as an identifier, so don't use a shared bitcoin address!
An incoming payment will be cleared and forwarded fully automated once the full amount has been payed.
Decryptor links: **Decryptor interface**, **Decryptor demo**.
I won't release private executables, except for very good reasons, because the maintenance would be too time consuming.
Requestable customizations: Victims page template, readme filename, readme content and an unique hidden service address. Please see **this** file for rudimentary informations about the victims page template and contact me.
Fee: 5 percent.
Fixed BTC/USD rate: 413.94 USD.
Number of victims (excluding demo victims): 2107
Payed (excluding demo victims; automatically updated): 12 (0.57%)
Incomplete payments (excluding demo victims; manually updated): 3
FAQ: **faq.html**
2016-03-18: I've got two stolen authenticode certificates for sale. The highest bid wins. It's OK to bid just for one and the end of the auction is not determined yet. Details: (whole-chain) SHA1 and SHA256, both are valid until late 2018, they aren't issued to the same name and I would use them for my service instead if they wouldn't be valid for that long. Both are valid for signing applications and kernel drivers up to Windows 10. (It's possible to load kernel drivers by the use of each certificate even on Windows 10. Thank you, old cross-certificate! It might be possible that the SHA1 certificate won't work for windows versions higher than Vista at any time.)
2016-03-31: @Alphabay vendor "bestworks": Did you actually made over 6000 USD in three days by selling a public available link to my site? First a direct competitor of me were using my free file signing service without even notifying me and then you (also without even notifying me) make this. I'm trying to run a serious business here, but I only got 70 USD in over eight months and people (figuratively) slatting on my face in return. Do I have to get even more immoral to make money? <:rant>
2016-03-31: I need help with cracking a faulty RSA modulus (because of a bug), I need the RSA "d". Please see "changes.txt" for more informations.

Technical summary

My Encryptor works fully offline and uses a combination of RC6-32/20/256 and RSA-2048. Every file has its own key.
Encryptor RaaS is signed by my free file signing service. It's using stolen authenticode certificates. (SHA1 and SHA256)
File extensions, which are being encrypted: **extensions.txt**
Changes: **changes.txt**
Minimum support: Windows XP, i686.
Version: 2016-03-30_1

Detection rates

Encryptor Detection Rate (NoDistribute, as at 2016-03-31): **1/35** (Kaspersky)
Notice: My ransomware might be detected by Ahnlab and Qihoo360.

Please enter your bitcoin address

Use my donation bitcoin address for demonstration purposes only. It'll then act like the victim has already payed.

Bitcoin address:

152fDLsAhN6RKjmn2TBw5MY7pBC1uSBFuN

Continue

I servizi possono essere di diverso tipo, il primo sito, illustrato nell'immagine che precede, offre, in cambio di una percentuale sui guadagni, un servizio di ransomware che potremmo definire "chiavi in mano", mentre il sito di cui all'immagine che segue si offre semplicemente di fare da intermediario per incassare i riscatti legati a estorsioni o altro.

Il 25 luglio 2016, la Nationale Politie (polizia nazionale) olandese, Europol, Intel Security e Kaspersky Lab annunciavano il lancio del progetto No More Ransom (NMR), un'iniziativa congiunta condotta a fini non commerciali, la quale riunisce organizzazioni pubbliche e private e che, oltre a informare le persone riguardo ai pericoli generati dal ransomware, si prefigge di aiutare gli utenti-vittima a recuperare i loro dati. Il relativo portale online conta, attualmente, ben cinquanta tool di decodifica, sette dei quali sono stati realizzati da Kaspersky Lab. Dal lancio dell'iniziativa NMR, oltre 29 mila vittime del ransomware, situate in tutto il mondo, sono state in grado di poter sbloccare e ripristinare gratuitamente i loro file – compromessi dal malware – grazie agli strumenti messi a disposizione da Kaspersky Lab. Il portale NMR è attualmente disponibile in quat-

tordici lingue: inglese, olandese, francese, italiano e portoghese, tedesco, spagnolo, sloveno, finlandese, ebraico, ucraino, coreano e giapponese.

2. To pay or not to pay?

Una volta infettata, la vittima può solo decidere se pagare o meno; in quest'ultimo caso potrà tentare di recuperare i propri file attraverso uno dei tanti programmi messi a disposizione dai vari fornitori di servizi antivirus.

Sebbene le forze dell'ordine sconsiglino di pagare il riscatto, circa il 34 per cento delle vittime decide di piegarsi e versare quanto richiesto dagli estorsori.

In ogni caso, per le forze dell'ordine è sempre possibile tentare di identificarli attraverso l'analisi dell'indirizzo bitcoin fornito alla vittima e, se anche si tratti di un indirizzo mai utilizzato, è comunque utile aggiungerlo alla lista di indirizzi noti per essere stati impiegati per attività illecite: potrebbe essere stato adoperato da altre vittime per pagare il riscatto e, in questo modo, le forze dell'ordine avranno a disposizione una pista da seguire.

Gli indirizzi utilizzati dalle vittime che decidono di pagare, infatti, possono essere analizzati da uno dei *blockchain analysis tools* a disposizione delle forze dell'ordine in modo da generare, e mantenere, una lista di wallet associati ad attività criminali e, auspicabilmente, identificare i soggetti che li utilizzano.

Joe Battaglia, un agente speciale dell'FBI addetto alla sezione Crimini informatici, ha dichiarato: «*I might find that those transactions occur within another cluster of bitcoin addresses that I don't know anything*

about, and my analysis tool doesn't know anything about. But I can take those addresses, pull them out, plug them into our case management system».

L'obiettivo è chiaramente quello di raccogliere abbastanza dati da poter incrociare le informazioni, in modo da ricostruire i collegamenti tra le varie transazioni, fino ad individuare uno o più soggetti identificabili.

I dati vengono passati al setaccio allo scopo di rintracciare schemi di pagamento verso determinati account e, da questi, trasferimenti verso conti correnti in fiat money.

Naturalmente, gli investigatori devono affrontare ulteriori difficoltà, tra cui il probabile impiego di VPN e fake server da parte dei "cattivi", ma individuare i wallet e i conti di destinazione rappresenta indubbiamente un valido punto di partenza.

5.3 Bitcoin scam

La caratteristica di irrevocabilità legata alle transazioni in criptovalute le rende lo strumento privilegiato per porre in essere truffe di vario genere, tipicamente attraverso la proposta di beni o servizi che, una volta pagati, non vengono inviati.

Tralasciando tutte le fattispecie legate all'acquisto di prodotti on line utilizzando bitcoin, a seguito dell'eccezionale aumento di valore dei bitcoin, si sono diffuse diverse truffe specificatamente legate alle criptovalute. In gergo, queste truffe vengono definite *scam*, mentre chi le pone in essere è identificato come *scammer*.

Per difendersi, il modo migliore è quello di conoscerle, così da essere in grado di individuare i segnali

di allerta che è necessario tenere in considerazione: a tal fine nelle prossime pagine individueremo e analizzeremo le metodologie di azione più utilizzate.

1. Inviami i bitcoin…

Contesto: acquisto di bitcoin.

Si tratta di uno scam semplicissimo da attuare e altrettanto semplice da contrastare, che si basa esclusivamente sulla convinzione del venditore di dover inviare il denaro.

Siamo in presenza di un acquisto di bitcoin, l'acquirente si presenta al venditore, tipicamente in una chat o con altri strumenti non facilmente tracciabili, chiedendogli di acquistare un certo importo di bitcoin.

L'acquirente si dimostra interessato all'acquisto e avvia una serie di trattative con il venditore fino a raggiungere un accordo; a questo punto l'acquirente dichiara di aver provveduto al pagamento e inizia a pressare il venditore per sollecitare l'invio dei bitcoin, fino a ottenere che questi proceda prima di poter verificare l'effettivo accredito del pagamento.

Ottenuti i bitcoin, l'acquirente sparisce lasciando il venditore con il classico pugno di mosche.

La regola per difendersi da questo scam è molto semplice: mai inviare i bitcoin se non si è prima ricevuta l'effettiva prova dell'avvenuto pagamento; ricordiamo, infatti, che il trasferimento di bitcoin è un'operazione non revocabile e difficile da tracciare, mentre un bonifico (o un pagamento paypal) offre maggiori garanzie di tutela per chi pone in essere l'operazione.

È quasi banale ricordare che un semplice screenshot dell'avvenuto pagamento non rappresenta

una prova sufficiente, dato che si tratta di un "documento" facilmente falsificabile: l'unica garanzia è l'effettivo accredito del denaro.

2. segue: revoca della transazione

Si tratta di una variante del precedente scam, con la differenza che in questo caso il pagamento viene effettivamente inviato; per porre in essere lo scam, l'acquirente utilizza una funzione di paypal, paradossalmente nata proprio per tutelare gli utenti da eventuali truffe e, dopo l'invio del denaro, si attiva per stornare la transazione congelando il conto del venditore.

Per evitare questa truffa, è necessario esigere che i pagamenti tramite paypal vengano effettuati sempre e soltanto utilizzando un account paypal verificato, cioè un account collegato con successo a una carta prepagata/carta di credito, in modo da avere la possibilità di risalire all'identità di chi ha effettuato l'operazione.

Varianti di questa truffa possono prevedere l'impiego di assegni falsi o rubati, oppure di carte di credito rubate o contraffatte.

3. Schema Ponzi

Con questo termine si indica un modello economico truffaldino che promette forti guadagni alle vittime invitandole a reclutare nuovi "investitori" che, a loro volta, diventeranno vittime della truffa.

Questo schema, infatti, permette forti guadagni soltanto a chi si colloca ai vertici della catena e, eventualmente, ai soggetti coinvolti, richiedendo inoltre un costante afflusso di nuove vittime disposte a pa-

gare la propria quota di ingresso per essere inserite nell'investimento.

I guadagni derivano, infatti, solo ed esclusivamente dalle quote pagate dai nuovi investitori e non da attività produttive o finanziarie, il che significa che il sistema è naturalmente destinato a implodere travolgendo la maggior parte dei partecipanti che si troveranno a perdere tutti i soldi "investiti".

Tanto Bitcoin quanto le altre altcoin, quelle serie almeno, non possono assolutamente essere considerate uno schema Ponzi, ma ciò non toglie che si tratti di strumenti che ben si prestano a essere utilizzati per tale fine; accanto alle altcoin serie, tuttavia, esiste tutta una serie di criptovalute che non hanno altro scopo se non quello di trarre in inganno e truffare eventuali malcapitati.

Le caratteristiche tipiche che ci permettono di individuare uno schema Ponzi sono le seguenti:

a. promessa di alti guadagni a breve termine e senza alcun rischio, grazie a sistemi finanziari o investimenti documentati in modo poco chiaro;
b. offerta rivolta a un pubblico non competente in materia finanziaria;
c. investimento legato a un solo promotore o azienda;
d. invito a trovare nuovi investitori per far "crescere" l'investimento;

a cui, nel caso delle criptovalute si aggiungono:

e. il *premining* ingiustificato è uno dei segnali di allarme più importanti; se una criptovaluta presenta un'alta percentuale di monete preminate senza una valida giustificazione, è assai probabile che si tratti di una truffa;

f. un numero sproporzionato di monete minate al momento del lancio è un altro indizio che qualcosa non torna; lo stesso discorso può essere applicato all'ipotesi in cui un ampio numero di monete sia stato minato in un tempo relativamente breve;
g. il rilascio iniziale in un angolo remoto del web, attraverso un sito personale e con un mining iniziale gestito da pochissimi soggetti; di fatto si tratta di un tentativo di mascherare un premining;
h. client compromesso o buggato al momento del rilascio: sebbene possa trattarsi di semplice incompetenza del programmatore, è bene valutare adeguatamente l'affidabilità di una criptovaluta che poggia la sua base su di un cliente non affidabile al 100 per cento;
i. come viene presentato e divulgato, a partire dalla scelta del nome e del logo;
j. la presenza e la qualità della comunità che ruota intorno al progetto; una comunità attiva e stabile è indice di buona salute del progetto e, di riflesso, di una sua intrinseca affidabilità;
k. da ultimo, la competenza dello sviluppatore è forse la vera cartina di tornasole, dato che una criptovaluta è tanto affidabile quanto è buono il suo sviluppatore. Un altro aspetto da valutare è se lo sviluppo è ancora attivo e se i parametri scelti sono realistici o no.

L'ufficio SEC (Securities and Exchange Commission - Commissione per i Titoli e gli Scambi) per gli investitori ha evidenziato il rischio dell'impiego di criptovalute negli schemi Ponzi.

Per approfondire:

http://www.reddit.com/r/altcoin/comments/7rjzbd/known_crypto_scams_and_ponzi_schemes/

http://truffacoin.com

https://99bitcoins.com/bitcoin-scam-test/

4. Il gioco delle tre carte

Un'altra truffa, particolarmente pericolosa, legata ai bitcoin è quella del "gioco delle tre carte" e consiste nello sfruttare lo pseudo anonimato dei bitcoin per incassare il denaro e poi sparire nel nulla.

In breve, Tizio vuole vendere i propri bitcoin, Caio si offre di acquistarli e ottiene da Tizio gli estremi del metodo di pagamento (ad esempio, bonifico bancario). A questo punto Caio pubblica un annuncio con cui mette in vendita, a un prezzo estremamente conveniente, uno o più prodotti.

Sempronio si offre di acquistare i suddetti prodotti e contatta Caio che, per ricevere il pagamento dei prodotti, utilizza l'IBAN che gli ha fornito Tizio. ~~A questo punto~~ Tizio visualizza l'avvenuto pagamento e, convinto del buon esito dell'operazione, trasferisce a Caio i bitcoin.

A questo punto Caio sparisce nel nulla, naturalmente senza inviare a Sempronio i prodotti offerti, lasciando a Tizio la briga di risolvere il problema della vendita con Sempronio.

Si tratta di una truffa molto pericolosa, in quanto il venditore rischia non solo da un punto di vista economico, ma anche da un punto di vista legale essendo, a sua volta, passibile di azioni penali a opera di Sempronio.

6. Bitcoin e fiscalità

L'ultimo aspetto da prendere in considerazione, anche se non per importanza, riguarda il regime fiscale da applicare ai bitcoin e, di riflesso, alle criptovalute.

La questione è stata affrontata per la prima volta dall'Agenzia delle Entrate con la risoluzione 2 settembre 2016, n. 72 in cui l'Agenzia, rispondendo all'interpello presentato da un contribuente, osservava che la circolazione dei bitcoin, quale mezzo di pagamento, si fonda sull'accettazione volontaria da parte degli operatori del mercato che, sulla base della fiducia, la ricevono come corrispettivo nello scambio di beni e servizi, riconoscendone quindi il valore di scambio indipendentemente da un obbligo di legge.

Lo scambio dei bitcoin tra utenti e operatori, sia economici sia privati, avviene per mezzo di una applicazione software e, per poterli utilizzare, gli utenti devono entrarne in possesso tramite l'acquisto da altri soggetti in cambio di valuta legale oppure accettandoli come corrispettivo per la vendita di beni o servizi.

La criptovaluta viene, quindi, utilizzata sia come alternativa alle valute tradizionali, come mezzo di pagamento per regolare gli scambi di beni e servizi, sia

per finalità meramente speculative, attraverso piattaforme online che consentono lo scambio di bitcoin con altre valute tradizionali sulla base del relativo tasso di cambio, come avviene per le valute tradizionali.

A questo punto l'Agenzia, con riferimento al trattamento fiscale applicabile alle operazioni relative ai bitcoin e alle valute virtuali, osservava come non si possa prescindere da quanto già affermato dalla Corte di Giustizia dell'Unione europea nella sentenza 22 ottobre 2015, causa C-264/14.

1. La Corte di Giustizia dell'Unione europea

La questione era nata nel contesto di una controversia tra lo Skatteverket (amministrazione finanziaria svedese) e il signor Hedqvist, relativa al parere preliminare dato dalla commissione tributaria (Skatterättsnämnden) quanto all'assoggettamento all'imposta sul valore aggiunto delle operazioni di cambio della valuta virtuale bitcoin in una valuta tradizionale o viceversa, che il signor Hedqvist intendeva effettuare con la mediazione di una società.

Punto di partenza è l'articolo 2 della direttiva IVA secondo cui:

> 1. Sono soggette all'IVA le operazioni seguenti:
> a) le cessioni di beni effettuate a titolo oneroso nel territorio di uno Stato membro da un soggetto passivo che agisce in quanto tale;
> (…)
> c) le prestazioni di servizi effettuate a titolo oneroso nel territorio di uno Stato membro da un soggetto passivo che agisce in quanto tale…

Secondo l'articolo 14, paragrafo 1 «Costituisce "cessione di beni" il trasferimento del potere di disporre di un bene materiale come proprietario» mentre in base all'articolo 24, paragrafo 1 «Si considera "prestazione di servizi" ogni operazione che non costituisce una cessione di beni».

Secondo l'articolo 135 della direttiva, gli Stati membri esentano

d) le operazioni, compresa la negoziazione, relative ai depositi di fondi, ai conti correnti, ai pagamenti, ai giroconti, ai crediti, agli assegni e ad altri effetti commerciali, ad eccezione del ricupero dei crediti;

e) le operazioni, compresa la negoziazione, relative a divise, banconote e monete con valore liberatorio, ad eccezione delle monete e dei biglietti da collezione ossia monete d'oro, d'argento o di altro metallo e biglietti che non sono normalmente utilizzati per il loro valore liberatorio o presentano un interesse per i numismatici;

f) le operazioni, compresa la negoziazione ma eccettuate la custodia e la gestione, relative ad azioni, quote parti di società o associazioni, obbligazioni e altri titoli, ad esclusione dei titoli rappresentativi di merci e dei diritti o titoli di cui all'articolo 15, paragrafo 2…

La corte svedese, richiamando una relazione del 2012 della Banca centrale europea sulle valute virtuali, affermava che una valuta virtuale può essere definita come un tipo di moneta digitale, non regolamentata, emessa e controllata dai suoi sviluppatori e utilizzata e accettata tra i membri di una specifica comunità virtuale e che le valute virtuali sono simili a ogni altra valuta convertibile per quanto riguarda il loro uso nel mondo reale, consentendo l'acquisto di beni e servizi sia reali sia virtuali.

Il signor Hedqvist aveva dichiarato di voler operare per via elettronica, mediante il sito internet della sua

società, che avrebbe provveduto ad acquistare bitcoin direttamente da privati e società o da una piattaforma di cambio internazionale per poi venderli o tenerli in deposito. In caso di vendita a privati il prezzo proposto dalla società era definito in funzione del prezzo attuale di una particolare piattaforma di cambio con l'aggiunta di una determinata percentuale di ricarico: la differenza tra il prezzo di acquisto della società e il prezzo di vendita avrebbe costituito il guadagno della società del signor Hedqvist, che non avrebbe provveduto a fatturare altre spese.

In breve, le operazioni poste in essere dal signor Hedqvist si sarebbero limitate all'acquisto e alla vendita di bitcoin in cambio di valute tradizionali mentre, dalla decisione di rinvio, non risulta che esse vertessero su pagamenti in bitcoin.

In un parere del 14 ottobre 2013, la commissione tributaria svedese statuiva, sul fondamento della sentenza First National Bank of Chicago (C-172/96, EU:C:1998:354), che il signor Hedqvist avrebbe prestato un servizio di cambio a titolo oneroso e che tale servizio di cambio sarebbe ricaduto nell'esenzione prevista dal capo 3, articolo 9, della legge sull'IVA.

Secondo la commissione tributaria, infatti, la valuta virtuale bitcoin rappresenterebbe un mezzo di pagamento utilizzato in maniera corrispondente a mezzi legali di pagamento, ma lo Skatteverket proponeva ricorso contro la decisione della commissione tributaria dinanzi allo Högsta förvaltningsdomstolen (Corte suprema amministrativa), sostenendo che il servizio di cui alla domanda del signor Hedqvist non ricadrebbe nell'esenzione prevista dal capo 3, articolo 9, della legge sull'IVA.

Nutrendo dei dubbi sulla corretta interpretazione,

lo Högsta förvaltningsdomstolen decideva di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

1) Se l'articolo 2, paragrafo 1, della direttiva IVA debba essere interpretato nel senso che le operazioni indicate come cambio di valuta virtuale contro valuta tradizionale e viceversa, effettuato dietro un corrispettivo che il fornitore della prestazione integra all'atto della determinazione dei tassi di cambio, costituiscono prestazione di servizi effettuata a titolo oneroso.
2) In caso di risposta affermativa alla prima questione, se l'articolo 135, paragrafo 1, [di detta direttiva] debba essere interpretato nel senso che le operazioni di cambio sopra descritte sono esenti da imposizione.

In merito alla prima questione, la Corte preliminarmente osservava che i bitcoin oggetto di cambio contro valute tradizionali non potevano essere qualificati come "bene materiale" ai sensi dell'articolo 14 della direttiva IVA, dato che questa valuta virtuale non ha altre finalità oltre a quella di essere un mezzo di pagamento esattamente come accade per le valute tradizionali, in quanto si tratta di monete che costituiscono mezzi di pagamento legali (si veda, in tal senso, sentenza First National Bank of Chicago, C-172/96, EU:C:1998:354, punto 25).

Conseguentemente, le operazioni oggetto del procedimento principale, che consistono nel cambio di diversi mezzi di pagamento, non ricadono nella nozione di "cessione di beni", prevista da detto articolo 14 della direttiva. In questo contesto, tali operazioni costituiscono prestazioni di servizi ai sensi dell'articolo 24 della direttiva IVA.

Per quanto riguarda, in secondo luogo, il carattere oneroso di una prestazione di servizi, occorre ricorda-

re che una prestazione di servizi è effettuata "a titolo oneroso", ai sensi dell'articolo 2, paragrafo 1, lettera c), della direttiva IVA, e non è pertanto assoggettata a IVA, solo se sussiste un nesso diretto fra il servizio prestato e il corrispettivo ricevuto dall'amministrato (sentenze Loyalty Management UK e Baxi Group, C-53/09 e C-55/09, EU:C:2010:590, punto 51, nonché la giurisprudenza ivi richiamata, e Serebryannay vek, C-283/12, EU:C:2013:599, punto 37).

Tale nesso diretto risulta acclarato qualora tra il prestatore e il destinatario intercorra un rapporto giuridico nell'ambito del quale avvenga uno scambio di reciproche prestazioni e il compenso ricevuto dal prestatore costituisca il controvalore effettivo del servizio prestato al beneficiario (sentenza Le Rayon d'Or, C-151/13, EU:C:2014:185, punto 29 e giurisprudenza ivi richiamata).

Nel caso in esame tra la società del signor Hedqvist e le altre parti contraenti sussisteva un rapporto giuridico sinallagmatico, nell'ambito del quale le parti dell'operazione si erano impegnate reciprocamente a cedere importi in una certa valuta e a riceverne il controvalore in bitcoin o viceversa. Risultava parimenti che tale società veniva retribuita per la sua prestazione di servizi da una controprestazione corrispondente al margine, che essa integrava nel calcolo dei tassi di cambio ai quali era disposta a vendere e acquistare le valute in parola.

La Corte riteneva che queste operazioni costituivano prestazioni di servizi effettuate a fronte di una controprestazione che presentava un nesso diretto con il servizio prestato, vale a dire prestazioni di servizi a titolo oneroso ai sensi dell'articolo 2, paragrafo 1, lettera c), della direttiva IVA. Rispondeva, quindi, alla prima questione dichiarando che l'articolo 2, pa-

ragrafo 1, lettera c), della direttiva IVA doveva essere interpretato nel senso che

> costituiscano prestazioni di servizi effettuate a titolo oneroso, ai sensi di tale disposizione, operazioni, come quelle oggetto del procedimento principale, che consistono nel cambio di valuta tradizionale contro unità della valuta virtuale "bitcoin" e viceversa, effettuate a fronte del pagamento di una somma corrispondente al margine costituito dalla differenza tra, da una parte, il prezzo al quale l'operatore interessato acquista le valute e, dall'altra, il prezzo al quale le vende ai suoi clienti.

Sulla seconda questione, dopo aver ricordato che, secondo la giurisprudenza della Corte, le esenzioni di cui all'articolo 135, paragrafo 1, della direttiva IVA costituiscono nozioni autonome del diritto dell'Unione, che mirano a evitare divergenze nell'applicazione del sistema dell'IVA da uno Stato membro all'altro (si vedano, segnatamente, sentenze Skandinaviska Enskilda Banken, C-540/09, EU:C:2011:137, punto 19, nonché la giurisprudenza ivi richiamata, e DTZ Zadelhoff, C-259/11, EU:C:2012:423, punto 19) e che i termini con i quali sono state designate dette esenzioni devono essere interpretati restrittivamente in quanto costituiscono deroghe al principio generale secondo cui l'IVA è riscossa per ogni prestazione di servizi effettuata a titolo oneroso da un soggetto passivo, la Corte osservava che, conformemente agli obiettivi perseguiti dalle esenzioni previste all'articolo 135, paragrafo 1, della direttiva IVA e nel pieno rispetto delle prescrizioni derivanti dal principio di neutralità fiscale inerente al sistema comune dell'IVA, questa regola d'interpretazione restrittiva non comportava che i termini utilizzati per definire le esenzioni di cui al detto articolo 135, paragrafo 1, dovessero essere inter-

pretati in un modo che privasse tali esenzioni dei loro effetti (si vedano, segnatamente, sentenze Don Bosco Onroerend Goed, C-461/08, EU:C:2009:722, punto 25; DTZ Zadelhoff, C-259/11, EU:C:2012:423, punto 21, e J.J. Komen en Zonen Beheer Heerhugowaard, C-326/11, EU:C:2012:461, punto 20).

A questo punto, atteso che le esenzioni previste dall'articolo 135, paragrafo 1, lettere da d) a f) sono intese a ovviare alle difficoltà collegate alla determinazione della base imponibile nonché dell'importo dell'IVA detraibile, per essere considerate operazioni esenti, i servizi devono formare un insieme distinto, valutato globalmente, che abbia l'effetto di adempiere le funzioni specifiche ed essenziali di un servizio descritto da tale disposizione (si veda, sentenza Axa UK, C-175/09, EU:C:2010:646, punti 26 e 27, nonché giurisprudenza ivi richiamata).

Dal disposto dell'articolo 135, paragrafo 1, lettera d), della direttiva IVA, letto alla luce della sentenza Granton Advertising (C-461/12, EU:C:2014:1745, punti 37 e 38), risulta anche che le operazioni di cui a tale disposizione riguardano servizi o strumenti le cui modalità di funzionamento implicano un trasferimento di denaro e che tale disposizione non riguarda le operazioni che vertono sulla valuta in quanto tale, dal momento che tali operazioni sono disciplinate da una specifica diposizione, vale a dire l'articolo 135, paragrafo 1, lettera e), della direttiva IVA.

Il bitcoin, pur essendo un mezzo di pagamento contrattuale, costituisce un mezzo di pagamento diretto tra gli operatori che l'accettano, pertanto operazioni come quelle oggetto del procedimento principale non ricadono nella sfera di applicazione delle esenzioni previste da tale disposizione.

Tuttavia, come ricordato ai punti 36 e 37 della decisione, le esenzioni previste dall'articolo 135, paragrafo 1, lettera e), della direttiva IVA sono intese, segnatamente, a ovviare alle difficoltà collegate alla determinazione della base imponibile, nonché dell'importo dell'IVA detraibile, che sorgono nel contesto dell'imposizione delle operazioni finanziarie. Queste operazioni con valute non tradizionali costituiscono di fatto operazioni finanziarie, purché le valute vengano accettate dalle parti di una transazione quale mezzo di pagamento alternativo ai mezzi di pagamento legali e non abbiano altre finalità oltre a quella di un mezzo di pagamento.

A ciò deve aggiungersi che, nel caso particolare di operazioni quali quelle di cambio, le difficoltà collegate alla determinazione della base imponibile nonché dell'importo dell'IVA detraibile possono essere identiche, indipendentemente dal fatto che si tratti di cambio di valute tradizionali, normalmente esentate in forza dell'articolo 135, paragrafo 1, lettera e), della direttiva IVA, o di cambio di tali valute contro valute virtuali a flusso bidirezionale che, senza essere mezzi di pagamento legali, costituiscono un mezzo di pagamento accettato dalle parti di una transazione, e viceversa.

In breve «risulta pertanto dal contesto e dalla ratio di detto articolo 135, paragrafo 1, lettera e), che un'interpretazione di tale disposizione secondo la quale essa disciplina le operazioni relative alle sole valute tradizionali si risolverebbe nel privarla di parte dei suoi effetti».

A questo punto, preso atto che i bitcoin non abbiano altre finalità oltre a quella di essere un mezzo di pagamento e che essa sia accettata come tale da alcuni operatori, ne consegue che

l'articolo 135, paragrafo 1, lettera e), della direttiva IVA disciplina anche le prestazioni di servizi come quelle oggetto del procedimento principale, che consistono nel cambio di valuta tradizionale contro unità della valuta virtuale "bitcoin" e viceversa, effettuate a fronte del pagamento di una somma corrispondente al margine costituito dalla differenza tra, da una parte, il prezzo al quale l'operatore interessato acquista le valute e, dall'altra, il prezzo al quale le vende ai suoi clienti.

La Corte concludeva osservando che

alla luce dei suesposti rilievi, occorre rispondere alla seconda questione dichiarando che:

– l'articolo 135, paragrafo 1, lettera e), della direttiva IVA, va interpretato nel senso che prestazioni di servizi, come quelle oggetto del procedimento principale, che consistono nel cambio di valuta tradizionale contro unità della valuta virtuale "bitcoin" e viceversa, effettuate a fronte del pagamento di una somma corrispondente al margine costituito dalla differenza tra, da una parte, il prezzo al quale l'operatore interessato acquista le valute e, dall'altra, il prezzo al quale le vende ai suoi clienti, costituiscono operazioni esenti dall'IVA ai sensi di tale disposizione;
– l'articolo 135, paragrafo 1, lettere d) e f), della direttiva IVA, va interpretato nel senso che siffatte prestazioni di servizi non ricadono nella sfera di applicazione di tali disposizioni.

Per comodità riproduciamo qui il dispositivo integrale della sentenza.

PER QUESTI MOTIVI, LA CORTE (QUINTA SEZIONE) DICHIARA:

1) L'articolo 2, paragrafo 1, lettera c), della direttiva 2006/112/CE del Consiglio, del 28 novembre 2006, relativa al sistema

comune d'imposta sul valore aggiunto va interpretato nel senso che costituiscono prestazioni di servizi effettuate a titolo oneroso, ai sensi di tale disposizione, operazioni, come quelle oggetto del procedimento principale, che consistono nel cambio di valuta tradizionale contro unità della valuta virtuale "bitcoin" e viceversa, effettuate a fronte del pagamento di una somma corrispondente al margine costituito dalla differenza tra, da una parte, il prezzo al quale l'operatore interessato acquista le valute e, dall'altra, il prezzo al quale le vende ai suoi clienti.

2) L'articolo 135, paragrafo 1, lettera e), della direttiva 2006/112 va interpretato nel senso che prestazioni di servizi, come quelle oggetto del procedimento principale, che consistono nel cambio di valuta tradizionale contro unità della valuta virtuale "bitcoin" e viceversa, effettuate a fronte del pagamento di una somma corrispondente al margine costituito dalla differenza tra, da una parte, il prezzo al quale l'operatore interessato acquista le valute e, dall'altra, il prezzo al quale le vende ai suoi clienti, costituiscono operazioni esenti dall'imposta sul valore aggiunto ai sensi di tale disposizione.
L'articolo 135, paragrafo 1, lettere d) e f), della direttiva 2006/112 va interpretato nel senso che siffatte prestazioni di servizi non ricadono nella sfera di applicazione di tali disposizioni.

2. *La risoluzione 72 del 2016*

Alla luce della decisione della Corte europea, l'Agenzia delle Entrate osservava che, in assenza di una specifica normativa applicabile al sistema delle monete virtuali, la citata sentenza della Corte di Giustizia costituisce necessariamente un punto di riferimento sul piano della disciplina fiscale applicabile alle monete virtuali e, nello specifico, ai bitcoin.

In ossequio a quanto affermato dai giudici europei, pertanto, l'Agenzia riteneva che l'attività di intermediazione di valute tradizionali con bitcoin, svolta in modo professionale e abituale, costituisce un'attività rilevante oltre che agli effetti dell'IVA anche per Ires e Irap.

Trattamento IVA

Ai fini del trattamento IVA, nel caso di un soggetto che svolga attività di cessione e acquisto di valuta virtuale (bitcoin) in cambio di valuta "tradizionale", il compenso per tale attività è determinato in misura pari al margine che scaturisce dalla differenza (ipotizzando il caso di vendita di bitcoin da parte dell'operatore), da un lato, tra il prezzo che il cliente è disposto a pagare per acquistare una unità di moneta virtuale e, dall'altro, la miglior quotazione del bitcoin stesso disponibile sul mercato.

Da queste premesse, l'Agenzia, nel riepilogare le conclusioni della Corte, ricordava che:

– l'attività di commercializzazione di bitcoin deve essere qualificata quale prestazione di servizi effettuata a titolo oneroso;
– le prestazioni in esame, pur riguardando operazioni relative a valute non tradizionali (e cioè diverse dalle monete con valore liberatorio in uno o più Paesi), «costituiscono operazioni finanziarie in quanto tali valute siano state accettate dalle parti di una transazione quale mezzo di pagamento alternativo ai mezzi di pagamento legali e non abbiano altre finalità oltre a quella di un mezzo di pagamento».

Sussistendo tali condizioni, le prestazioni di servizi in esame rientrano nella previsione di esenzione di cui all'articolo 135, paragrafo 1, lettera e), della direttiva 2006/112/CE.

Alla luce di tali principi, l'Agenzia riteneva che l'attività che la Società intendeva porre in essere, remunerata attraverso commissioni pari alla differenza tra l'importo corrisposto dal cliente intenzionato ad acquistare/vendere bitcoin e la migliore quotazione reperita dalla Società sul mercato, doveva essere considerata ai fini IVA quale prestazione di servizi esenti ai sensi dell'articolo 10, primo comma, n. 3), del dpr 26 ottobre 1972, n. 633.

Tassazione diretta

In merito alla tassazione diretta, coerentemente all'inquadramento giurisprudenziale europeo, l'Agenzia riteneva che la Società dovesse assoggettare a imposizione i componenti di reddito derivanti dall'attività di intermediazione nell'acquisto e vendita di bitcoin, al netto dei relativi costi inerenti a detta attività.

Riepilogando da un punto di vista operativo:

- in caso di ordine di acquistare, il cliente anticipa le risorse finanziarie alla Società che, effettuato l'acquisto di bitcoin, provvede a registrare nel wallet ("borsellino") del cliente i codici relativi ai bitcoin acquistati;
- in caso di ordine di vendere, la Società preleva dal cliente i bitcoin e gli accredita, successivamente al completamento effettivo della vendita, la somma convenuta.

Il guadagno (o la perdita) di competenza della Società è rappresentato dalla differenza tra quanto anticipato dal cliente e quanto speso dalla Società per l'acquisto o tra quanto incassato dalla Società per la vendita e quanto riversato al cliente.

Tale elemento di reddito – derivante dalla differenza (positiva o negativa) tra prezzi di acquisto sostenu-

ti dall'istante e costi di acquisto a cui si è impegnato il cliente (nel caso in cui quest'ultimo abbia affidato alla Società l'incarico a comprare) o tra prezzi di vendita praticati dall'istante e ricavi di vendita garantiti al cliente (nel caso di affidamento di incarico a vendere) – è ascrivibile ai ricavi (o ai costi) caratteristici di esercizio dell'attività di intermediazione esercitata, che, pertanto, contribuiscono quali elementi positivi (o negativi) alla formazione della materia imponibile soggetta a ordinaria tassazione ai fini Ires (e Irap).

Bitcoin residui

Con riferimento ai bitcoin che a fine esercizio sono nella disponibilità (a titolo di proprietà) della Società, l'Agenzia ha ritenuto che gli stessi debbano essere valutati secondo il cambio in vigore alla data di chiusura dell'esercizio e che tale valutazione assuma rilievo ai fini fiscali ai sensi dell'articolo 9 del Testo unico delle imposte sui redditi approvato con dpr 22 dicembre 1986, n. 917 (Tuir).

Occorre, quindi, far riferimento al valore normale, intendendosi come tale il valore corrispondente alla quotazione degli stessi bitcoin al termine dell'esercizio; dato che non esiste una quotazione ufficiale, l'Agenzia ritiene che a tal fine potrebbe farsi riferimento alla media delle quotazioni rinvenibili sulle varie piattaforme online in cui avvengono le compravendite di bitcoin.

Per quanto riguarda invece la tassazione ai fini delle imposte sul reddito dei clienti della Società, persone fisiche che detengono i bitcoin al di fuori dell'attività d'impresa, si ricorda che le operazioni a pronti (acquisti e vendite) di valuta non generano redditi imponibili mancando la finalità speculativa.

La Società, pertanto, non è tenuta ad alcun adempimento come sostituto d'imposta, ferma rimanendo la

possibilità che l'Amministrazione finanziaria, in sede di controllo, chieda di acquisire le liste della clientela al fine di porre in essere le opportune verifiche anche a seguito di richieste da parte dell'Autorità giudiziaria.

Per tale ragione, la società sarà tenuta agli obblighi di adeguata verifica della clientela, di registrazione nonché di segnalazione ai sensi del decreto legislativo n. 231 del 2007.

3. Il Tribunale di Verona

In data 24 gennaio 2017, la Seconda Sezione Civile del Tribunale di Verona ha emesso la sentenza n. 195 con la quale affronta un caso di crowdfunding strutturato tramite un'operazione in criptovaluta.

La tematica, inedita per la giurisprudenza italiana, ha dovuto risolvere la questione relativa a un conferimento in fiat money in cambio di moneta virtuale, nello specifico bitcoin.

La somma, conferita da una persona fisica a beneficio di una società di informatica, era stata trasferita in funzione della costituzione di una provvista finanziaria utile per un'operazione di crowdfunding, disciplinato dall'art. 50-quinquies del d.lgs. 24 febbraio 1998 n. 58 sulla gestione di portali per la raccolta di capitali per le PMI.

Il processo era stato avviato perché il conto wallet in bitcoin non era stato aperto dalla società che aveva ricevuto i fondi e il privato era stato costretto a rivolgersi al Tribunale per tutelare i propri interessi.

Uno degli aspetti più interessanti della decisione, probabilmente la prima in tema di bitcoin, è rappresentato dal fatto che il magistrato ha così definito il contratto di acquisto:

Per quanto qui interessa, tanto la CGUE quanto l'Agenzia delle Entrate italiana definiscono operazioni in questione (ciò è a dire «cambio di valuta tradizionale contro unità della 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») come «prestazioni di servizio a titolo oneroso» (sub specie di «intermediazioni nell'acquisto e vendita di Bitcoin»), che – in quanto «… relative a divise, banconote e monete con valore liberatorio» – sono riconducibili all'art. 135, paragrafo I, lettera e), della Direttiva 2006/112/CE, onde poi trarne l'inclusione nelle prestazioni esenti ex art. 10, comma primo, n. 3), DPR n. 633/1972 (non assoggettabilità ad IVA e, per converso, assoggettabilità ad IRES ed IRAP dei margini di profitto generati).

4. D.lgs 25 maggio 2017 n. 90

Con il d.lgs 90/2017 è stato introdotto nel nostro sistema normativo il concetto di valute virtuali e di prestatori di servizi relativi all'utilizzo di valuta virtuale, anticipando gli altri stati membri nell'adozione della IV Direttiva antiriciclaggio (Direttiva UE 2015/859).

La definizione di valute virtuali (art. 1 del d.lgs. 231/2007, lett. qq) è sicuramente un passo avanti importante, anche se i riflessi giuridici, al di là delle previsioni antiriciclaggio, sono modesti.

Secondo il testo normativo si definisce valuta virtuale «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».

Al momento di andare in stampa, è ancora pendente la procedura di consultazione pubblica della bozza di decreto ministeriale sulla valuta virtuale, in cui vengono fornite le definizioni di "prestatori di servizi relativi all'utilizzo di valuta virtuale" (ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale) e di "valuta virtuale" (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).

Viene, inoltre, istituita un'apposita sezione nel registro pubblico informatizzato, istituito presso l'OAM, ai sensi dell'articolo 17-bis del decreto legislativo 13 agosto 2010, n.141 e successive modificazioni, in cui sono tenuti a iscriversi i prestatori di servizi relativi all'utilizzo di valuta virtuale, al fine del legale esercizio della prestazione di servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale.

Scopo del decreto è di acquisire informazioni in ordine alla dimensione e all'operatività del mercato dei servizi relativi all'utilizzo di valuta virtuale, ai fini dell'efficiente popolamento della sezione speciale del Registro.

A tale scopo, dalla data di entrata in vigore del decreto e fino al primo luglio 2018, chiunque sia interessato a svolgere sul territorio della Repubblica italiana l'attività di prestatore di servizi relativi all'utilizzo di valuta virtuale è tenuto a darne comunicazione al Ministero dell'Economia e delle Finanze.

Coloro che già sono operativi nel territorio della Repubblica italiana alla data di entrata in vigore del decreto, in qualità di prestatori di servizi relativi all'utilizzo di valuta virtuale, devono effettuare la comunicazione entro sessanta giorni dalla predetta data.

I suddetti dati verranno inoltrati alla guardia di finanza e alla polizia postale e delle comunicazioni che, nell'esercizio dei poteri inerenti le sue attribuzioni, ne faccia richiesta a supporto di eventuali attività di indagine riconducibili al contrasto del riciclaggio e del finanziamento del terrorismo.

Bibliografia e sitografia

Lauri Hartikka, *A blockchain in 200 lines of code*, https://medium.com/@lhartikk/a-blockchain-in-200-lines-of-code-963cc1cc0e54;

Mauro Bellini, *Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*, http://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/

https://www.chainalysis.com/

FBI, *2016 Internet Crime Report*, https://pdf.ic3.gov/2016_IC3Report.pdf

http://truffacoin.com

https://bitcointalk.org/index.php?board=159.0

https://www.bitcoin-italia.org/

Indice

5 Introduzione

9 1. Le criptovalute
(quali sono e come funzionano)

60 2. Le altre criptovalute

87 3. Ethereum: verso gli smart contract

108 4. Criptovalute e sicurezza

125 5. Criptovalute e diritto penale

156 6. Bitcoin e fiscalità

174 Bibliografia e sitografia

Editing e impaginazione: Antonella Targher

Questa parte di albero
è diventata libro
sotto i moderni torchi
di Rotolito Lombarda, Pioltello (MI)
nel mese di marzo 2018.
Possa un giorno
dopo aver compiuto il suo ciclo
presso gli uomini desiderosi di conoscenza
ritornare alla terra
e diventare nuovo albero.