CRIPTOVALUTE

COSA SONO E COME USARLE AL MEGLIO

AGID CERT-PA

Le pillole di sicurezza

Chi siamo

Il CERT-PA è una struttura che opera all'interno dell'Agenzia per l'Italia Digitale (AGID) ed è preposta al trattamento degli incidenti di sicurezza informatica del dominio costituito dalle pubbliche amministrazioni.

Contattaci

Se sei una PA accreditata puoi contattarci:
AGID CERT-PA

Email: cert-pa@cert-pa.it

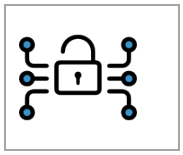
Web: www.cert-pa.it

COMPUTER EMERGENCY RESPONSE TEAM
PUBBLICA AMMINISTRAZIONE
CERT - PA

INDICE

I NOSTRI SERVIZI

ANALISI E INDIRIZZO



Supporto alla definizione dei processi di gestione della sicurezza, lo sviluppo di metodologie, il disegno di processi e di metriche valutative per il governo della sicurezza cibernetica

SERVIZI PROATTIVI

Raccolta e elaborazione di dati significativi ai fini della sicurezza cibernetica, emanazione di bollettini e segnalazioni di sicurezza, implementazione e gestione di basi dati informative

SERVIZI REATTIVI

Gestione degli allarmi di sicurezza e supporto ai processi di gestione e risoluzione degli incidenti di sicurezza all'interno del dominio delle PA

FORMAZIONE E COMUNICAZIONE

Promozione della cultura della sicurezza cibernetica, favorendo il grado di consapevolezza e competenza all'interno delle PA, attraverso la condivisione di informazioni

COS'È UNA VALUTA?

Con questo termine generico si indicano le monete in circolazione in un paese e i biglietti di banca che le rappresentano. Vengono di norma emesse da stati o gruppi di stati (si pensi all'euro) per lo più attraverso la propria banca centrale in regime di monopolio.

Seguendo l'evoluzione della natura della moneta distingueremo tra:

- **moneta merce** - un bene dotato di valore intrinseco proprio che viene usato come strumento di pagamento (ad es. metalli preziosi non coniati, bestiame, sale ecc.)
- **moneta rappresentativa** – ad es. un documento cartaceo che attribuisce al possessore il diritto di ricevere una certa quantità di metallo prezioso da parte di un orafo o di un banchiere
- **moneta fiduciaria** – si riferisce a tutti gli strumenti di pagamento che circolano accettati finché la gente ripone fiducia sull'emittente (ad es. le banconote e le monete metalliche di materiali non preziosi o comunque con un valore nominale diverso rispetto al valore intrinseco)
- **moneta digitale o elettronica** - Oggi la moneta può esistere anche indipendentemente da una rappresentazione fisica, ad esempio su un conto corrente come registrazione informatica, oppure come deposito su un conto a risparmio. La moneta digitale, o elettronica, costituisce valore monetario memorizzato, ad esempio, in una carta prepagata o uno smartphone

Qualunque sia la sua forma, una moneta ha tre funzioni:

- è un **mezzo di scambio**, cioè un mezzo di pagamento per l'acquisto di beni o servizi
- è un'**unità di conto** che permette di attribuire un prezzo a beni e servizi (ad es. un libro=5 euro, un uovo=1 euro e così via) inalterato su tutto il territorio sotto la giurisdizione di un ente fiduciario (come una banca)
- è una **riserva di valore** Si riferisce all'accumulo di moneta legale a fini di risparmio

COS'È UNA BANCA?

La banca è un intermediario finanziario che esercita essenzialmente due funzioni:

- la **funzione di deposito**: i clienti possono depositare i propri risparmi per motivi di praticità a fronte del pagamento di un interesse che la banca corrisponde (interesse passivo). In questa fase la banca è debitrice nei confronti dei clienti
- la **funzione creditizia**: i clienti, in grado di dimostrare una solidità finanziaria sufficiente, possono richiedere prestiti (es. mutui) ad un tasso di interesse attivo. In questa fase la banca è creditrice nei confronti dei clientiexchane

La banca ricopre il ruolo di intermediario in quanto raccoglie fondi da chi ne ha in eccesso e li ridistribuisce a chi ne necessita per gestire le spese o finanziare investimenti.

Nel caso di una banca centrale vi è anche una terza funzione che è la

- **funzione monetaria:** consiste nella gestione della moneta circolante ad esempio tramite l'emissione di nuova valuta

Nella sua funzione di deposito, la banca si configura come un gestore di conti. Ogni conto ha un

proprietario (o più di uno) e associato a un conto è una certa quantità di denaro. Il denaro può essere trasferito da un conto a un altro a richiesta del proprietario del conto. Per poter fare questo, la banca deve accertarsi che 1) chi compie un'operazione sia effettivamente il proprietario del conto 2) la somma scambiata nella transazione sia effettivamente posseduta dal conto di partenza. Se queste condizioni sono soddisfatte, la banca trasferisce i soldi in nostra vece.

Il rapporto del cliente con la banca è basato sulla fiducia che la banca possa restituire in qualsiasi momento il denaro posto in deposito e possa rendersi garante della legittimità di un'operazione finanziaria.

COS'E UNA CRIPTOVALUTA?

Una criptovaluta è una valuta esclusivamente digitale che usa un sistema decentralizzato (cioè senza un'entità regolatrice fidata centrale come una banca) per la generazione di nuove unità di valuta e per la gestione e la registrazione delle transazioni. Inoltre, dal punto di vista tecnologico essa si affida alla crittografia per la prevenzione delle truffe.

L'architettura delle criptovalute è normalmente del tipo peer-to-peer (p2p), cioè lo scambio di valuta avviene direttamente tra gli utenti. D'altra parte le transazioni sono anonime, nel senso che ogni utente usa uno o più pseudonimi, ma completamente trasparenti, cioè ogni transazione è visibile a tutti.

Al cuore delle criptovalute vi è la blockchain che è una base di dati distribuita e che funziona come Registro delle transazioni o Libro Mastro (Distributed Ledger). Il nome "blockchain" è dovuto al fatto che le transazioni vengono raggruppate, in un certo numero, in strutture denominate "blocchi". Ogni blocco è collegato a quello che lo precede a formare una catena ininterrotta. Il legame tra i blocchi è tale che l'alterazione di uno solo di questi invaliderebbe anche i successivi e quindi tutta la catena.

COME SI È ARRIVATI A BITCOIN?

Le origini di Bitcoin stanno nel libertarianismo, un'ideologia politica che ritiene che l'autorità centralizzata dovrebbe essere minima e che, d'altra parte, l'individuo dovrebbe poter decidere il più possibile autonomamente il corso della propria vita, rinunciando il meno possibile ai propri diritti a favore dello Stato. Per questo, uno dei concetti chiave è il rispetto della Privacy. Da questa filosofia, nel mondo online sono emersi due gruppi: i Cypherpunks e i Crypto-anarchist. Entrambi propugnano l'uso della crittografia per proteggere la privacy intesa come "diritto dell'individuo di rivelarsi in modo selettivo al mondo". In una società aperta questo richiede sistemi di transazioni anonime. Nei tempi passati, l'acquisto di beni, fatto con moneta contante, era fondamentalmente anonimo ma ai giorni nostri, grazie al digitale, le banche hanno la capacità di controllare facilmente i nostri conti correnti e come spendiamo i nostri soldi. Bitcoin non è nato fuori dal nulla ma ha avuto dei precursori che, però, non hanno avuto la stessa fortuna: Digicash, HashCash e B-Money (ma ci sono anche Flooz e Beenz). Il primo ha introdotto le

firme digitali nelle transazioni, il secondo il proof-of-work e il terzo il registro delle transazioni distribuito. Nell'ottobre 2008 comparve online, nella cryptography mailing list, un lavoro dal titolo "Bitcoin: A Peer-to-Peer Electronic Cash System" di Satoshi Nakamoto (nome fittizio) e fu registrato il dominio bitcoin.org.

COSA È BITCOIN?

Bitcoin è una criptovaluta quindi è anonimo, trustless e decentralizzato. Tutte le transazioni sono peer-to-peer cioè il trasferimento di valuta avviene senza intermediari; l'identità dell'utente è completamente svincolata da quella del mondo reale; l'archivio delle transazioni (blockchain) è distribuito, piuttosto che centralizzato com'è il caso della banca; si dà fiducia solo al protocollo e alla rete Bitcoin.

La più piccola suddivisione di un Bitcoin è il Satoshi, che è la sua centomilionesima parte.

Chiunque dotato di computer e connessione a internet può unirsi alla rete Bitcoin. Ciascun computer è un nodo e può verificare in ogni momento la storia di una transazione e le cifre scambiate. La moneta viene generata e distribuita non attraverso una zecca e una banca centrale ma attraverso il mining. Un miner è un tipo speciale di nodo che ha il compito di costruire nuovi blocchi della blockchain attraverso la risoluzione di un problema crittografico e, quindi, consumando potenza di calcolo. Dal momento che chiunque può essere miner il processo è completamente decentralizzato. Bitcoin è disegnato in modo da essere una moneta deflazionaria nel senso che c'è un valore massimo di bitcoin che possono essere prodotti, specificatamente quasi 21 milioni.

Il lavoro del miner, da cui il nome, è proprio simile a quello di un minatore che passa il tempo a scavare alla ricerca di metalli preziosi. Quando trova un blocco di metallo il suo lavoro viene premiato. Analogamente, ogni miner ottiene una certa quantità di valuta per aver aggiunto un blocco ma il valore di questo premio decresce col tempo. E' iniziato a 50 bitcoin ma si dimezza ogni 210.000 blocchi. Attualmente è di 12.5 bitcoin. Arriverà a zero quando il numero massimo di bitcoin sarà raggiunto.

La prima transazione bitcoin è stata fatta il 12 gennaio 2009 tra Hal Finney e Satoshi Nakamoto. Nel blocco zero, il blocco genesi, era contenuto una frase da The Times of London che diceva "Il Cancelliere è vicino al secondo piano di salvataggio per le banche" in memoria delle radici libertarie di bitcoin. All'inizio le persone si scambiavano bitcoin per gioco, senza un reale scambio di beni ma il 18 maggio del 2010 apparve un messaggio, da parte di Laszlo Hanyecz, in cui si prometteva di pagare 10000 bitcoin in cambio di due pizze. Il 22 maggio del 2010 ricevette due pizze per un valore dell'ordine di 25 USD. Questa è stata la prima transazione al mondo in cui beni reali sono stati scambiati con bitcoin. Il 15 marzo 2018 il valore di queste due pizze era di 81 milioni di dollari.

Nel 2010 Jed McCaleb crea Mt.Gox, il più grande bitcoin exchange online. Dichiara bancarotta nel 2014 dopo aver scoperto un enorme furto di bitcoin. Sempre

nel 2014 i primi commercianti iniziarono ad accettare bitcoin come moneta di acquisto.

CHE TIPO DI UTENTI TROVIAMO IN UNA RETE BITCOIN?

In una rete Bitcoin possiamo trovare vari tipi di utenti/nodi, a seconda di quali e quante funzioni implementano tra le quattro possibili:

1. network routing – permette di collegarsi alla rete bitcoin p2p
2. mining – genera nuovi blocchi nella blockchain
3. blockchain - mantiene una copia completa della blockchain (circa 200 GB)
4. wallet - gestisce coppie di chiavi tramite un wallet e quindi può spedire/ricevere bitcoin

Un **nodo completo**, detto anche Reference Client o Bitcoin core, implementa tutte e quattro le funzioni sopra. Un **solo miner** differisce dal nodo completo perché non ha il wallet e quindi implementa le funzioni da 1 a 3. I **nodi di mining** (mining nodes), invece, implementano solo le funzioni 1 e 2. In un mining pool (v. domanda apposita) il pool manager è un nodo completo e i membri del pool sono nodi di mining.

COSA È UNA COPPIA DI CHIAVI CRITTOGRAFICHE?

Nella crittografia simmetrica, esiste una sola chiave che viene usata sia per criptare che per decrittare un messaggio. Nella crittografia asimmetrica, invece, le chiavi sono due e vengono derivate algoritmicamente l'una dall'altra: la prima viene usata per criptare e la seconda per decrittare. Le due chiavi non sono equivalenti: una viene detta *chiave privata* e deve essere gelosamente custodita dal proprietario e l'altra viene detta *chiave pubblica* e può essere data a chiunque.

Nei Digital Signature Scheme (DSS) un destinatario di un messaggio firmato con un'opportuna chiave privata dovrebbe essere in grado di garantire:

- **Origine del messaggio** - il mittente, proprietario della chiave privata, ha autorizzato il messaggio/transazione
- **Non ripudio** - il mittente, proprietario della chiave privata, non può negare di aver spedito il messaggio
- **Integrità del messaggio** - il messaggio non può essere stato modificato dopo essere stato spedito

In Bitcoin la coppia di chiavi è creata attraverso un algoritmo chiamato ECDSA (Elliptic Curve Digital Signature Algorithm). La chiave privata viene generata in modo casuale. Da questa, attraverso la moltiplicazione nel campo delle curve ellittiche (una curva ellittica ha la forma y^2=x^3+ax+b) viene generata la chiave pubblica in modo one-way (cioè non è possibile, nota la chiave pubblica, ricavare la chiave privata). Dalla chiave pubblica (di 256 bit), attraverso hashing, si può generare un indirizzo di 160 bit, sempre one-way.

COSA È UNA FUNZIONE DI HASHING CRITTOGRAFICA?

E' una funzione che prende un input e lo trasforma in un output pseudorandom (hash o impronta) di lunghezza fissata. E' pseudorandom perché lo stesso

input genera lo stesso output. Queste funzioni godono di tre proprietà:

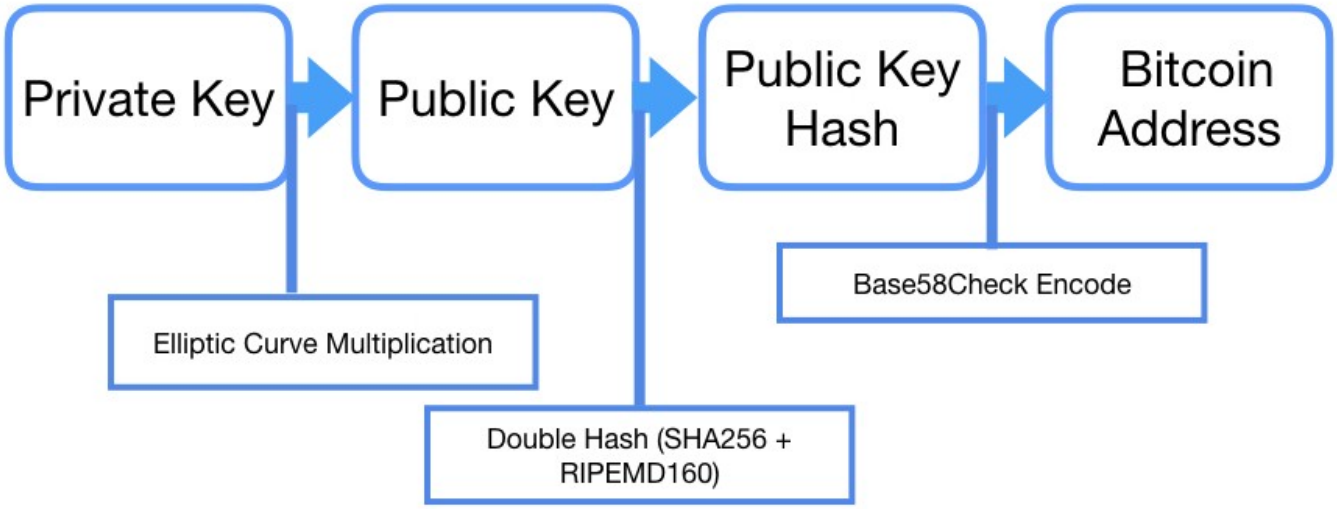
- dato un certo output deve essere computazionalmente difficile trovare l'input che lo ha prodotto = di chi sono queste impronte?
- dato un certo input, è computazionalmente difficile trovare un altro input che dia lo stesso output = puoi trovare un'altra persona che ha le tue stesse impronte digitali?
- è computazionalmente difficile trovare due qualsiasi input che diano lo stesso output = non è possibile trovare due persone diverse con le stesse impronte digitali

Una conseguenza è il cosiddetto "effetto valanga": differenze, anche piccole, tra due input provocano output altamente diversi. Questo previene la possibilità di avvicinarsi via via progressivamente, per approssimazioni sempre più piccole, a un certo risultato. Come sarà ormai chiaro, queste funzioni hanno scopo anti-tampering nel senso che un'alterazione anche piccolissima del dato in input deve risultare in un'amplificazione della diversità degli output. Così non sarà possibile evitare che un dato venga manomesso ma in compenso, se questo accadesse, verrebbe certamente notato. Così, visto che la blockchain è un database distribuito, se qualcuno cercasse di alterare una transazione nella propria copia locale questa diventerebbe vistosamente diversa dalle altre copie e quindi rigettata.

Nel caso specifico di Bitcoin, la funzione usata è SHA-256 (https://www.xorbin.com/tools/sha256-hash-calculator) o, meglio una sua doppia applicazione, cioè x'=SHA256(SHA256(x)). Questa funzione, il cui nome significa Secure Hash Algorithm, è stata inventata dalla NSA (National Security Agency). Prende un input di dimensione minore di 2^64 bit e produce un output di lunghezza fissata di 256 bits.

COSA È UN INDIRIZZO?

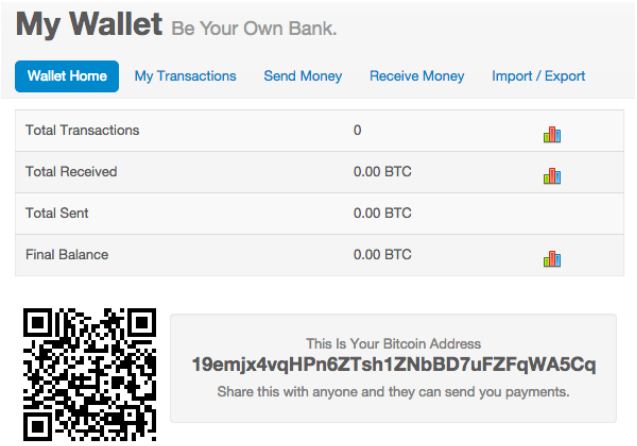
Un indirizzo Bitcoin è una stringa di 26-35 caratteri alfanumerici (ad es. 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2) che rappresenta una possibile destinazione per un



pagamento bitcoin. Esso viene generato per hashing (con più operazioni) a partire dalla chiave pubblica di un utente con un procedimento one-way, cioè non è possibile risalire dall'indirizzo alla chiave pubblica. L'indirizzo è costruito in modo tale da non contenere quei caratteri che possono essere scambiati l'uno per l'altro, come lo zero e la lettera O e la l minuscola e la I maiuscola. E' consigliato generare un indirizzo per ogni transazione distinta, cioè in modo che sia a uso singolo. E' possibile anche creare indirizzi offline, senza essere collegati alla rete bitcoin, e in modo massivo. Ad esempio, in un sito di e-commerce, si può pregenerare un certo numero di indirizzi e usarne uno per ogni utente quando questi selezioni l'opzione "paga con Bitcoin". Oggi è possibile creare indirizzi bitcoin anche a partire da più chiavi pubbliche nel caso si voglia fare un pagamento multiplo, cioè ad es. "paga il sig. A e anche il sig. B". Facendo un parallelo con il mondo delle e-mail, un indirizzo è come un indirizzo di posta elettronica con la sola differenza che viene usato una sola volta. La chiave privata è come la password per accedere alla casella di posta e il wallet è come il software usato per accedere alla casella.

COS' È UN WALLET?

Nella rete Bitcoin la chiave privata di un utente è quella che permette l'accesso alla sua identità virtuale perché dalla chiave privata, tramite la corrispondente chiave pubblica, si genera l'indirizzo univoco da cui spedire e ricevere valuta. Per evitare il furto di identità la chiave privata va custodita gelosamente. Il wallet è lo strumento la cui funzione principale è la gestione delle chiavi. I produttori software, poi, sono soliti arricchire i wallet anche con altre funzionalità come ad esempio la gestione delle transazioni (lista, invio e ricezione valuta) e di tutta l'attività relativa alla rete blockchain, la possibilità di convertire tra criptovalute, tenere d'occhio l'andamento di bitcoin sui mercati e così via.



Ci sono vari tipi di wallet (v. ad es. https://www.buybitcoinworldwide.com/wallets/): su Web, sul computer, digitale o fisico. Più in generale, ci sono due categorie di wallet, a seconda se siano collegati a internet o no:

- **hot** – connessi a internet
  - app per smartphone (es. Mycellium, AirBitz)
  - online web (es. Blockchain.info, coinbase.com)
- **cold** – non connessi a internet
  - Paper wallet – sono veri e propri pezzi di carta con su stampata la chiave privata (es. bitcoinpaperwallet.com, bitaddress.org)
  - Hardware wallets – sono periferiche connesse ad es. via usb e che firmano le transazioni al posto nostro (es. Ledger, Trezor, Case, Keepkey)

- Brain wallet – consiste nel semplicemente memorizzare la chiave privata ad esempio attraverso una combinazione mnemonica di parole

COME OTTENERE BITCOIN?

Ci sono vari modi per acquisire Bitcoin:

- **Mining** Il modo base è quello di fare il miner e sperare di ricevere il premio per aver risolto più velocemente degli altri il cryptoenigma. Questo richiede ovviamente la disponibilità di hardware performante.
- **Bitcoin ATM**, cioè un bancomat Bitcoin, se disponibile
- **Exchange** è, come dice la parola stessa, un cambiavalute (un elenco qua https://bitcoin.org/en/exchanges). Qui è possibile, ad esempio, scambiare euro con bitcoin e viceversa ma anche criptovalute tra loro. La loro importanza risiede nel fatto che qui viene fissato il valore di mercato del bitcoin. Si distingue tra *exchange centralizzati (CEX)* e *decentralizzati (DEX)*. I primi si appoggiano a terze parti fidate (di solito grosse compagnie) e sono i più semplici da usare ma anche quelli più esposti a censura e attacchi hacker perché tengono i bitcoin in custodia (gli utenti non hanno accesso alle chiavi private dei propri account, per questo è un sistema trusted) per facilitare la movimentazione. Riescono a fornire servizi a un prezzo più basso perché si basano su un'economia di scala. A oggi si stima che quasi il 99% del mercato delle criptovalute avvenga qua. Alcuni esempi sono Binance, Bittrex, Bitfinex, Coinbase e Kraken. I secondi (DEX) sono trustless, perché gli utenti continuano a tenere i fondi nel proprio wallet, possono solo convertire criptovalute tra loro e non con moneta fisica, non si appoggiano a terze parti centralizzate ma sono del tipo peer-to-peer. Inoltre, sono in esecuzione su centinaia di nodi, fornendo una soluzione migliore contro il downtime e la compromissione. Sono più costosi e complicati da usare. Alcuni esempi di exchange decentralizzati sono Bitsquare, Bitshares, OpenIdeger, NXT e CounterParty.

COSA È UNA TRANSAZIONE BITCOIN?

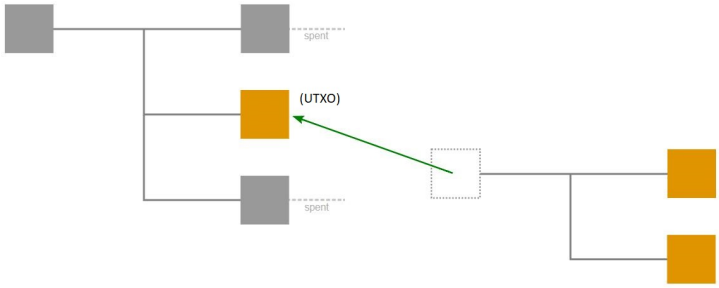
Una transazione si ha quando una certa quantità di valuta viene trasferita da un indirizzo ad un altro. Tecnicamente, una transazione è un messaggio firmato digitalmente e spedito sulla rete bitcoin per la verifica. Per questo, tutte le transazioni sono pubbliche e vengono scritte sul registro digitale (Digital Ledger) che prende il nome di Blockchain. La storia di ogni transazione è percorribile all'indietro fino al punto in cui i bitcoin hanno avuto origine.

Perché una transazione sia valida deve avere tre caratteristiche:

1. proof of ownership (una firma)
2. fondi disponibili
3. nessuna altra transazione che usi gli stessi fondi

Relativamente al punto 2, di solito in una banca un cliente ha un conto associato e a questo corrisponde un determinato saldo. Quando l'utente spende dei soldi, la banca verifica che la somma sia disponibile sul conto e il saldo viene modificato. La proof of ownership è data dalla Proof-of-Identity, cioè si verifica che chi spende sia effettivamente il proprietario del conto. Bitcoin, invece, non opera con il concetto di conto (account) individuale ma con quello di UTXO

(Unspent Transaction Output). Il problema fondamentale da risolvere è quello del cosiddetto *double spending* che è espresso dal punto 3 sopra. Supponiamo, per semplicità, di partire da un utente/nodo, con il suo wallet completamente vuoto. Potrà, allora, acquisire bitcoin mediante uno dei metodi visti sopra. Al momento necessario, il wallet genererà un indirizzo su cui verranno depositati i bitcoin iniziali tramite una transazione. Supponiamo ora che l'utente desideri acquistare qualcosa e pagarlo tramite bitcoin. Il wallet del venditore, perciò, genererà una nuova coppia di chiavi privata/pubblica e da quest'ultima, via hash, un indirizzo che trasmetterà al compratore. Quest'ultimo, userà quindi l'output (non ancora speso) della prima transazione per generare



una nuova transazione avente come input la quantità di bitcoin da trasferire e l'indirizzo su cui stanno i suoi bitcoin. L'output sarà invece l'indirizzo del venditore. Una cosa importante da sapere è che l'output, a differenza di quanto succede in un portafoglio reale, non può essere speso in parte ma in toto. Così, quando verrà fatta la transazione, il venditore prenderà la sua parte e creerà una nuova transazione per dare il resto al compratore su un apposito nuovo indirizzo che il wallet del compratore avrà generato. Ora il compratore avrà un nuovo indirizzo su cui è depositato un output non speso. E così via.

Per poter riscattare i bitcoin, il venditore dovrà dimostrare di essere il vero possessore dell'indirizzo fornendo la sua firma e la chiave pubblica completa. In questo modo il venditore potrà usufruire dell'output della transazione creata dal compratore.

Una transazione è formata da tre sezioni principali:

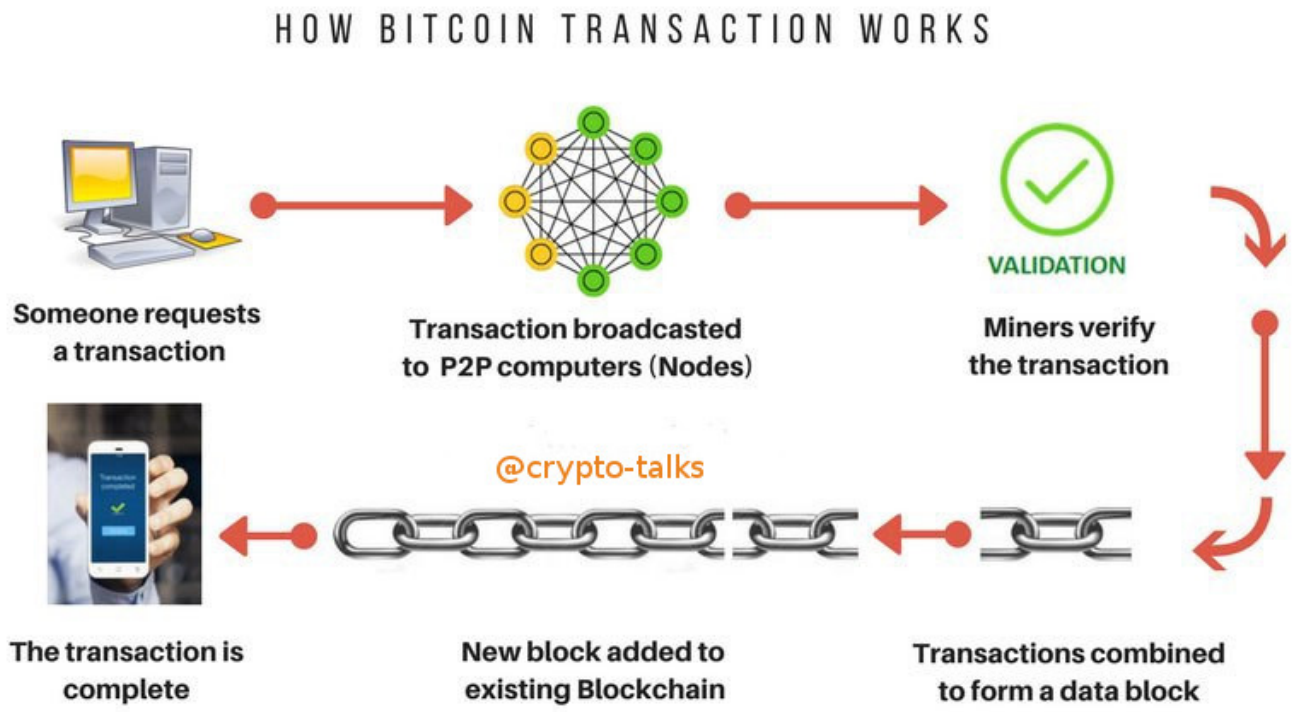
- **Metadata** – contiene alcuni dettagli relativi alla transazione come l'identificativo (che è un hash), la dimensione, il locktime, il numero di UTXO in input e il numero di UTXO in output, la versione del software di Bitcoin in uso. Il locktime permette di far valere la transazione (nel senso che potrà essere inserita in un blocco valido) a partire da un certo tempo assoluto futuro (in formato unix timestamp) oppure quando si sarà depositato un certo numero di blocchi sul blocco corrente. Nel primo caso occorre far attenzione che nella blockchain non esiste un tempo globale e quindi una condizione di intervallo di tempo già passato per un peer potrebbe non essere tale per un altro.
- **Input** – contiene una lista di identificativi (quelli che compaiono nelle sezioni metadata) di UTXO creati in precedenza e un proof che certifica che il proprietario può riscuotere gli UTXO e usarli per produrre nuovi output
- **Output** – contiene una lista di UTXO che verranno spediti a nuovi indirizzi. Ogni UTXO indica quanti satoshi verranno trasferiti e la condizione (proof) per cui sarà possibile riscattare il valore della transazione, ad esempio dopo aver dimostrato l'identità del beneficiario. Bitcoin utilizza degli script per poter costruire output complessi. Questi script bloccano (lock) l'output della transazione finchè una condizione di sblocco non viene soddisfatta, come ad esempio la verifica dell'identità corretta del destinatario

Una volta che la transazione è stata costruita, viene inviata a tutti i nodi perché la includano in un blocco

valido nuovo che verrà aggiunto alla blockchain. Questo processo impiega circa 10 minuti.

Una cosa importante da osservare è che sono permesse anche transazioni con più input e più output. Così, con una sola transazione è possibile pagare più persone oppure è possibile usare più input per fare un pagamento sostanzioso. Questo scenario prende il nome di *Pay to Pub Key Hash, P2PKH.* Una versione un po' più complicata si ha se il venditore vuole aggiungere un po' di logica di business alla transazione. Supponiamo ad esempio che si tratti di un'offerta a tempo limitato oppure che ci sia la necessità di più firme per validare la transazione (ad es. la vendita di una casa posseduta da più eredi). In questo caso il venditore, piuttosto che fornire al compratore un indirizzo, cioè l'hash della sua chiave pubblica, creerà uno script contenente la logica necessaria, ne calcolerà l'hash e invierà questo al compratore. Stavolta, quando questi creerà la transazione per il pagamento, il venditore dovrà fornire come prova la sua firma e lo script completo. Questo nuovo scenario prende il nome di *Pay to Script Key Hash, P2SH*.

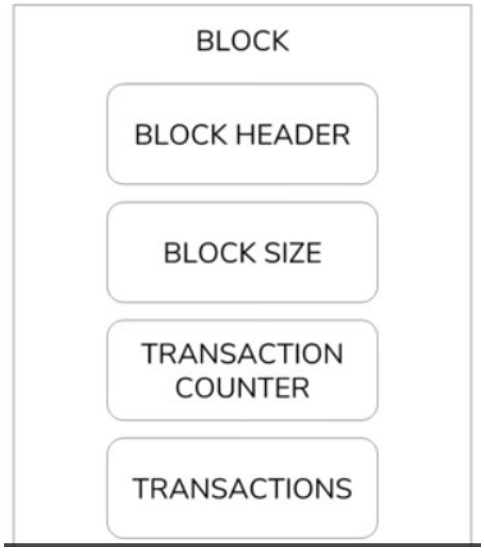
Vediamo ora meglio come funzionano le transazioni multifirma, dette anche M-di-N. E' possibile fare in modo che una transazione venga autorizzata da più proprietari e fare in modo che, ad esempio, per essere valida deve avere almeno M firme su un totale di N possibili. Questo rende possibili scenari che utilizzano un wallet condiviso (ad esempio di un'associazione o di una famiglia) o anche come modo per risolvere il problema della perdita o del furto di una chiave privata. In quest'ultimo scenario il proprietario può impostare più chiavi private e rendere valida la transazione ad



esempio utilizzandone 2 di 3. Così, se anche ne viene persa una è possibile risolvere la situazione con le altre due.

COSA È LA BLOCKCHAIN?

La blockchain è la struttura che si trova al cuore di una criptovaluta e rappresenta l'archivio di tutte le transazioni eseguite. Per capire com'è fatta occorre prima capire come è fatto un blocco.



Facendo riferimento alla figura, un blocco è composto da:

- **Block size** è la dimensione del blocco (di solito 1 MB)
- **Block header** rappresenta i metadati necessari per capire i componenti del blocco
- **Transaction counter** dice quante transazioni sono contenute nel blocco
- **Transactions** è il campo che contiene effettivamente le transazioni

Il *Block Header* è quello che assicura la sicurezza del database e contiene sei campi di cui i più importanti sono mostrati nella figura successiva. Il Merkle root rappresenta un sommario delle transazioni. Il Previous Block Hash è l'hash del block header del blocco precedente nella catena e rappresenta la concatenazione perché se un blocco viene alterato allora tutti i successivi saranno alterati. Il Nonce rappresenta il Proof of work. Il block id è l'hash di tutti questi campi concatenati.

Il Merkle root è la cima del Merkle Tree che è una struttura di dati crittografici sotto forma di albero binario. Questo è un albero in cui ogni nodo ha al più due figli. In un Merkle tree al livello più basso c'è un numero di figli pari a una potenza di due e questi sono gli hash delle informazioni di cui vogliamo fare un sommario. Per costruire l'albero si parte da un insieme di transazioni che sono state verificate. Si dispongono in un livello. Si calcola l'hash di ognuna. Per ogni

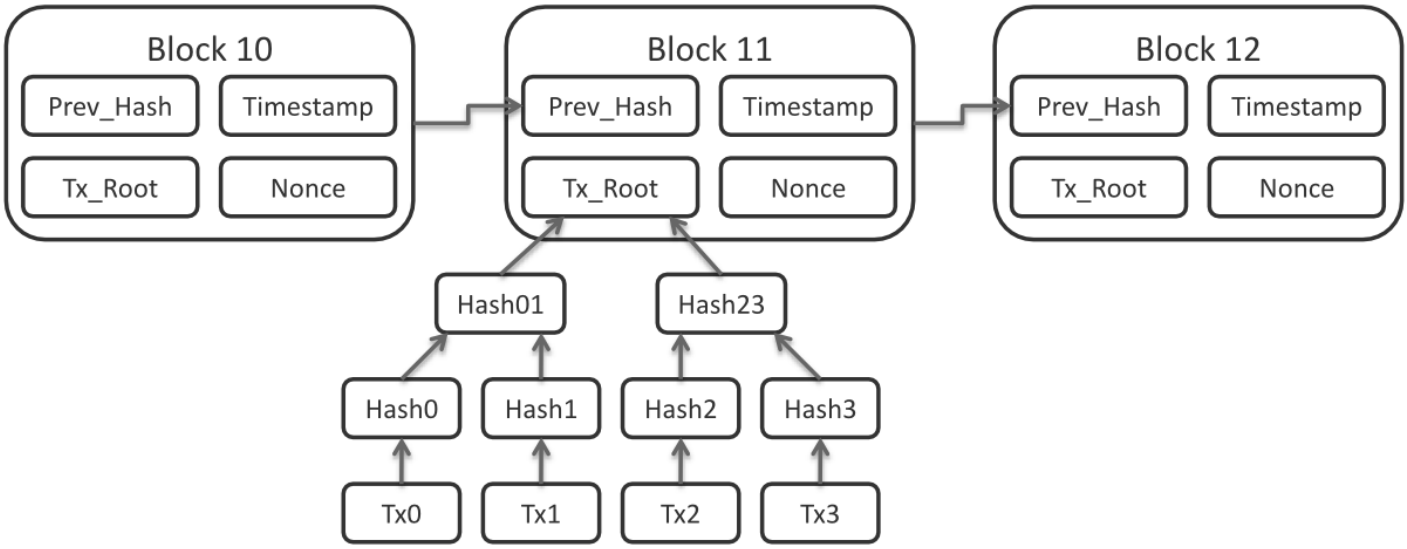
coppia si calcola l'hash e si dispone al livello successivo che quindi conterrà la metà degli elementi di partenza. Si continua in questo modo finchè alla fine non ci sarà un solo elemento in cima, il Merkle root appunto. In questo modo è possibile rilevare se ci sono state alterazioni nell'insieme di transazioni perché se una sola transazione viene alterata questo si propaga fino alla radice dell'albero.

Il Proof of Work in Bitcoin è implementato come segue. Prima di tutto deve essere un problema computazionalmente difficile, parametrizzabile (nel

senso di aggiustabile, in modo che il problema non sia né troppo facile né troppo difficile) e facilmente verificabile. L'idea è quella di trovare un nonce tale che l'hash del block header sia minore di un certo valore assegnato algoritmicamente. Questo lavoro è svolto dai miners. L'attività di mining è paragonata a quella di un giocatore di freccette con una benda sugli occhi. C'è un'uguale probabilità di colpire qualsiasi punto del bersaglio e non c'è alcun modo per sapere quanto si è andati vicino o lontano. L'unica cosa che si può fare è continuare a giocare finchè il punto scelto non viene colpito. Questo potrà avvenire più o meno rapidamente a seconda della velocità della CPU. La difficoltà di risolvere il problema è data dal numero di calcoli necessari per risolverlo. L'obiettivo è quella di avere un tempo medio di risoluzione pari a 10 minuti tenendo conto che la rete dei miner è variabile in quanto nel corso del tempo nuovi miner si aggiungono e altri lasciano. Per poter avere una stima, e quindi aggiustare la difficoltà, questa viene definita come se stessa moltiplicata per due settimane / (tempo per fare il mining dei precedenti 2016 blocchi). Ogni due settimane si verifica il tempo che è stato necessario per fare il mining di 2016 blocchi. Se è esattamente due settimane allora la difficoltà per un blocco è pari al valore desiderato di 10 minuti. In caso contrario i parametri vanno aggiustati. Se un miner ha successo nell'inserire un blocco, riceve un premio che diventerà la prima transazione del Merkle tree.

La catena più lunga è quella che corrisponde alla potenza di calcolo impiegata maggiore e quindi alla maggioranza della rete. Se tale maggioranza è "onesta" allora la catena è corretta. Vedremo successivamente che, se un eventuale attaccante riuscisse ad appropriarsi del 51% delle risorse di calcolo della rete riuscirebbe a sovvertirla perché potrebbe generare a piacimento la catena più lunga.

Tramite https://www.blockchain.com/explorer è possibile visualizzare i blocchi della blockchain Bitcoin senza doverla scaricare in toto. A marzo 2018, i



blocchi bitcoin sono creati ogni 10 minuti e possono contenere 1 MB di transazioni, cioè circa 1-3000. Quindi la blockchain bitcoin è in grado di processare circa tre transazioni al secondo (per fare un confronto, Visa processa circa 1600 transazioni al secondo).

Affinchè un client possa verificare se la propria transazione è inclusa o meno in un blocco della bitcoin blockchain non è necessario che si scarichi l'intera blockchain. Se così fosse limiterebbe moltissimo le caratteristiche del device che contiene il wallet. Piuttosto vengono scaricati tutti i block header che contengono l'elenco di tutte le transazioni processate. Questo metodo prende il nome di Simple Payment Verification (SPV).

COSA È IL MINING?

Un Bitcoin miner ha il compito di aggiungere un nuovo blocco di transazioni alla catena blockchain. Per fare questo dovrà competere con tutti gli altri per risolvere un puzzle crittografico usando una discreta quantità di risorse di calcolo e elettricità. Per questo, i gruppi più grossi di miner tendono a concentrarsi i quei paesi dove questi costano meno. Una volta che ci si è dotati dell'hardware necessario, altamente specializzato, va installato il software per connettersi alla rete bitcoin (es. https://www.buybitcoinworldwide.com/mining/software/ o www.bitcoinx.com/bitcoin-mining-software/). In alternativa, si potrà fare **Cloud Mining**, in cui cioè si paga un provider (come AWS ad esempio) per fare il mining al posto nostro. E' importante osservare che i miner hanno un ruolo importantissimo nella rete Bitcoin perché tanto più grosso è il loro numero, tanto più le risorse di calcolo sono distribuite e tanto più è valido il modello trustless, nel senso che non esiste un'unica entità potente che decide. Inoltre il loro contributo è fondamentale per la sicurezza perché ovviamente è più difficile compromettere molti nodi e quindi falsare l'integrità della blockchain.

Nel dettaglio, le operazioni che un miner dovrà effettuare sono le seguenti:

1. **scaricamento in locale dell'intera blockchain** – questo passo permette di avere la storia completa in modo da poter verificare le transazioni future
2. **verifica delle transazioni in arrivo** – queste riempiranno il blocco da aggiungere alla blockchain con transazioni valide. Nuove transazioni vengono inserite dagli utenti ogni secondo ed è compito dei miners verificarle. Finchè questo non succede, l'utente vedrà la transazione nel suo wallet nello stato "pending". Una volta ricevute, esse vengono depositate temporaneamente in un'area chiamata mempool in attesa di essere inserite in un blocco. L'operazione di verifica consiste che si tratti di un output non speso e che la firma digitale sia corretta
3. **creazione del blocco** – viene costruito il merkle tree (e in particolare il merkle root) a partire dalle transazioni verificate che faranno parte del blocco e con tutti i metadati necessari come tempo, versione e destinazione. Viene calcolato l'hash dell'header del blocco precedente
4. **ricerca del Proof-of-Work** – è il nonce che risolve l'enigma crittografico. Il nodo miner che ci riesce per primo acquisisce il diritto di aggiungere il blocco alla blockchain
5. **broadcast del blocco** – una volta risolto il problema, se non sono ancora arrivate soluzioni dai concorrenti, si invia il blocco a tutta la rete che si sincronizzerà con il nuovo aggiornamento, dopo che ogni nodo ha verificato la validità del nuovo blocco

6. **riscatto del premio** – se il blocco è stato inserito nella catena più lunga viene accreditato il premio. E' necessario specificare la condizione perché potrebbe succedere che qualche altro nodo abbia già trovato la soluzione ma che non sia ancora arrivata fino a noi. In questo caso vince chi per primo associa il blocco alla catena più lunga. Il premio consiste di due parti: uno per ogni blocco confermato, che attualmente è pari a 12.5 bitcoin ma che si dimezza ogni 210000 blocchi (approssimativamente 4 anni) e uno come transazione speciale per se stesso. Quest'ultimo è un premio (transaction fee) che viene impostato da chi crea una transazione in modo che il miner sia portato a includerla nel blocco tanto prima quanto più è alto il premio che riceve. Va considerato che, col passare del tempo, via via che diminuisce il premio per la creazione del blocco, il premio per la transazione diventerà sempre più importante.

Chi decide di fare il miner deve fare un accurato bilancio tra costi e guadagni se, alla fine, vuole ottenere un profitto. I costi si suddividono tra costi fissi e costi operativi. I primi si riferiscono all'hardware da acquistare, i secondi all'elettricità, alle risorse umane necessarie per far funzionare quotidianamente il tutto e alle strutture dove ospitare l'apparecchiatura di mining.

COS' È UN MINING POOL?

Una volta acquisito l'hardware necessario (v. ad es. https://www.buybitcoinworldwide.com/mining/hardware/ per qualche suggerimento) il prossimo possibile passo per un miner è quello di entrare a far parte di un Mining Pool (v. ad es. https://www.buybitcoinworldwide.com/mining/pools/). Questo è un gruppo di miner che accettano di cooperare nella risoluzione del puzzle crittografico condividendo i risultati e velocizzando così la ricerca. In cambio, si accetta di suddividere l'eventuale premio tra i partecipanti (con vari schemi di assegnazione delle quote del premio possibili). Un mining pool viene gestito da un pool manager, o pool operator, che è l'unico ad eseguire il software di mining completo e che, parallelizzando il compito da risolvere, suddivide il problema in blocchi di calcolo e assegna ogni blocco a un membro del pool. Se viene risolto il puzzle crittografico, il premio va al pool manager che, dopo aver trattenuto una parte per sé, lo dividerà tra i partecipanti. A oggi, i mining pool più grandi si trovano in Cina. Ci sono due modalità principali per il pagamento di un membro di un mining pool: Pay-per-Share e Proportional. Nel primo caso, si riceve una fee indipendentemente dal fatto che un blocco valido venga trovato o meno. Nel secondo invece si viene pagati in proporzione alle risorse utilizzate per la soluzione dell'enigma crittografico ma solo se questo viene risolto dal pool. Una delle obiezioni che viene fatta al modello trustless di Bitcoin è il fatto che l'esistenza di mining pool tende a distruggere questo paradigma perché la concentrazione di risorse di mining importanti (anche se su base volontaria) nelle mani di un unico soggetto, il pool manager, tende a fornire più potere nelle sue mani e quindi a ricreare il modello di valuta centralizzata che Bitcoin è nato per negare. Il cosiddetto "**attacco del 51%**" si avrebbe nell'eventualità che un miner o un mining pool da solo riuscisse a gestire il 51% della potenza della rete e quindi a rovesciarla. Per evitare la concentrazione di grosse risorse in poche mani si può procedere in vari modi, nessuno dei quali totalmente risolutivo. Come

abbiamo detto, l'hardware per effettuare il mining in modo accettabile è altamente specializzato per calcolare velocemente determinate funzioni di hashing (ASIC, Application Specific Integrated Circuit). Per questo si dice di solito che un ASIC è buono per la rete/valuta per cui è disegnato. Per scoraggiare l'uso di questo tipo di hardware e cercare di rendere il mining "ASIC resistant", si possono utilizzare catene di funzioni di hashing (ad es. X11 o X13 che combinano 11 o 13 funzioni diverse), come si fa con la criptovaluta DASH, oppure si può cambiare periodicamente il tipo di puzzle da risolvere, scegliendo funzioni di hashing diverse. Il problema non è comunque di facile soluzione in particolare perché deve rispettare i requisiti di essere complesso nel calcolo ma semplice nella verifica.

COME FUNZIONANO GLI AGGIORNAMENTI DI BITCOIN?

Il gruppo *Bitcoin core* è deputato a rilasciare gli aggiornamenti del software di base. D'altra parte, pure questa sarebbe centralizzazione e, ancora una volta, è quello che deve essere evitato. Così l'idea è che anche gli aggiornamenti devono essere guidati dal consenso (*consensus update*). Questo si ottiene lasciando agli utenti la decisione di quali versioni del codice e quindi quali funzionalità installare. Ad esempio, il gruppo Bitcoin core potrebbe decidere a un certo momento di portare il limite di valuta dagli attuali 21 milioni di Bitcoin a 42 milioni. Verrebbe così rilasciata una nuova versione; però a questo punto potrebbe succedere che una parte degli utenti resti sulla vecchia e una parte si trasferisca sulla nuova. In generale, distingueremo perciò tra **hard fork** e **soft fork**: nel primo caso l'aggiornamento non è retrocompatibile perché rende possibili cose che non erano permesse prima (ad es. il raddoppiamento del limite di cui sopra), nel secondo invece è il contrario cioè l'aggiornamento è retrocompatibile perché pone nuove restrizioni alle regole (ad es. la dimensione del blocco passa da 1 MB a 500 KB). In questo secondo caso la nuova rete è compatibile con la vecchia ma non viceversa. Qualunque sia il caso, alla base dell'aggiornamento c'è una discussione della community.

Tutto ha inizio con un **BIP** (**Bitcoin Improvement Proposal**) che può essere di tre tipi diversi:

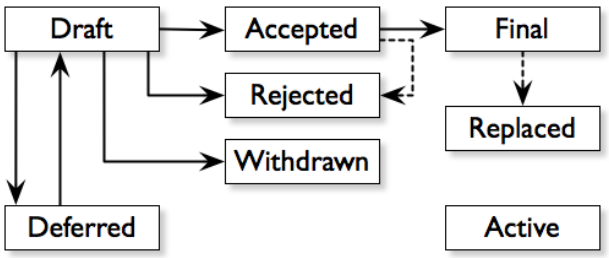
- *standard* – è un aggiornamento o un cambiamento al protocollo Bitcoin
- *informativo* – sono linee guida su come le persone dovrebbero comportarsi (ad es. come dovrebbe essere un mining pool)
- *di processo* – concerne le best practice

I miner votano gli aggiornamenti includendo un riferimento al BIP nel blocco che stanno generando.

Un tema molto dibattuto ad esempio è se sia utile nonchè eticamente disponibile l'enorme dispendio di energia necessario a fare il mining di bitcoin.

L'idea che è nata è quella di cercare di portare a casa due obiettivi contemporaneamente e cioè usare algoritmi complessi "utili", come ad es. calcolare grossi numeri primi, cercare gli alieni, generare modelli climatici predittivi, simulare le proteine a livello atomico ecc., per fare ANCHE il cryptomining. La difficoltà per

questo genere di approccio è il Proof-of-Work nel senso che non è semplice parametrizzare questi problemi in modo da renderli più semplici o più difficili a seconda delle necessità e inoltre non è chiaro quale debba essere esattamente il puzzle da risolvere. Inoltre le soluzioni possibili non sono tutte equiprobabili. Ad es. se il problema fosse "cercare pianeti abitabili nell'universo" non tutte le aree del cielo avrebbero la stessa densità di stelle. Lo spazio di soluzioni di Bitcoin è invece piatto, tutte le soluzioni sono equiprobabili e quindi il problema è risolubile solo provando e riprovando.



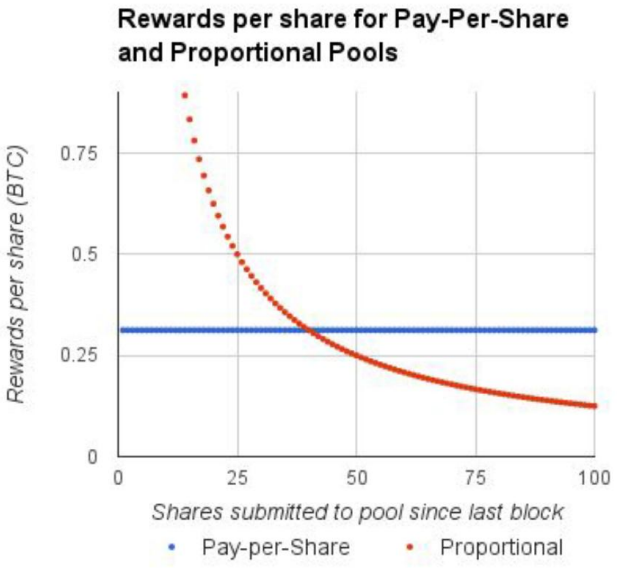
CHE TIPO DI ATTACCHI POSSONO ESSERE FATTI?

51% attack

E' un attacco che può essere scagliato da un miner o gruppo di miner che possegga il 51% della potenza di calcolo della rete. Questo renderebbe possibile il double spending e impedire la validazione delle transazioni, bloccando i pagamenti tra utenti. Il mining pool Glash.io nel luglio 2014 ha ecceduto il 50% di potenza di calcolo totale della rete Bitcoin e il problema è stato risolto dagli utenti che hanno volontariamente abbandonato il pool. D'altra parte, l'attacco è stato effettivamente scagliato nel caso di Krypton and Shift, due blockchains su ethereum nell' Agosto 2016 e, più di recente, nel maggio 2018 verso Bitcoin Gold, che era allora la ventiseiesima criptovaluta più grossa.

Pool hopping

Se confrontiamo le due modalità principali con cui i miner hanno un profitto con la loro attività, e cioè Pay-per-Share e Proportional, vediamo che il primo ha rendimento costante mentre il secondo è alto se l'enigma crittografico viene risolto velocemente e basso col passare del tempo. In entrambi i casi il profitto è dato dall'area sotto la curva. Confrontando le due curve vediamo che esiste un punto in cui le due curve si intersecano.



Per questo, la strategia migliore da usare è il cosiddetto *pool hopping* che consiste nello stare in un pool che paga in modo proporzionale all'inizio. Se il blocco non viene trovato velocemente, passando il punto di intersezione, non conviene più restare lì perché altrimenti i costi sarebbe più alti ma conviene di più spostarsi in un pool che paga in modo costante. Questo meccanismo in realtà è un vero e proprio attacco nei confronti dei miner onesti che sono fedeli al gruppo ed è il motivo principale per cui non è conveniente la modalità di premio Proporzionale.

Pool cannibalization

Dal momento che nel modello Pay-per-Share si ottiene un profitto costate, indipendentemente dal fatto che si risolva o no il puzzle, l'idea è quella di condividere con il pool solo i blocchi non validi e tenere quello buono per sé. Questo tipo di attacco consiste nel distribuire una piccola quantità di potenza di calcolo con gli altri pool senza mai sottoporre blocchi validi. In questo modo l'attaccante si prende il profitto costante di tutti i pool in cui partecipa senza mai contribuire. Questa strategia massimizza il profitto di un miner per cui questo è più motivato a comportarsi disonestamente che contribuire al bene comune.

Double spending attack

Il double spending consiste nello spendere la stessa valuta due volte. Questo obiettivo può essere ottenuto tramite un *race attack* che sfrutta accuratamente il timing della rete. Supponiamo che A compri qualcosa da B spendendo Bitcoin. In questo caso può iniviare una valida transazione con la somma pattuita a B. Per il funzionamento della rete la transazione non entra subito in un blocco valido ma serve un certo lasso di tempo (tipicamente 10 minuti ma si è arrivati anche a 4 giorni). Se B spedisce subito l'oggetto a A, A può inviare sulla rete un'altra transazione in cui usa lo stesso denaro in un'altra transazione magari a se stesso però con un transaction fee più alto, invogliando così gli altri nodi a includerla in un blocco valido prima di quello inviato a B. Così quando verrà finalmente presa in considerazione la transazione di B verrà rigettata. In questo modo si è prodotto un fork della blockchain. Per ovviare a questo tipo di attacco è necessario che il venditore aspetti una quantità di tempo sufficiente prima di spedire l'oggetto. In particolare dovrà attendere non solo che la sua transazione venga inclusa in un blocco valido ma anche che quest'ultimo faccia parte effettivamente della catena più lunga cioè che altri blocchi validi si sovrappongano al suo. L'attaccante infatti, mentre il venditore aspetta, potrebbe nel frattempo, sfruttando il proprio potere di calcolo, costruire un certo numero di blocchi validi contenenti la transazione truffaldina e mettere insieme così la catena più lunga. I calcoli probabilistici mostrano che un attaccante con il 51% del potere di calcolo complessivo della rete potrebbe sempre fare double spending.

Goldfinger attack

Nel caso in cui un attaccante con potenza di calcolo sufficiente riuscisse a fare un double spending, nel momento in cui la rete se ne accorgesse, immediatamente la valuta crollerebbe di valore

portandosi dietro, quindi, pure il valore dei bitcoin posseduti dall'attaccante e anche quello dell'hardware, altamente specializzato, in suo possesso. Nonostante ciò, l'attaccante potrebbe comunque guadagnare attraverso un Goldfinger attack, che consiste nello scommettere prima sull'abbassamento di valore della valuta e poi condurre l'attacco double spending. Il nome di questo attacco deriva dal personaggio Godfinger di un film di James Bond che cerca di aumentare il valore dell'oro in proprio possesso rendendo indisponibile l'oro della Federal Reserve di Fort Knox.

Censorship Attack

Questo tipo di attacco mira a isolare un utente o un gruppo di utenti dalla rete ignorandone le transazioni e quindi rendendo di fatto i bitcoin posseduti privi di utilità. Per poterlo condurre, occorre avere il controllo sul 51% della rete. L'obiettivo è quello generare una blockchain che non contenga nessuna transazione che riguarda la vittima (*blacklisting*). Se qualche miner include queste transazioni, l'attaccante dovrà fare un fork generando una catena più lunga che non le contiene in modo da invalidare i blocchi indesiderati. Inoltre, questo avrà anche l'effetto che i miner "avversari" non riceveranno mai un premio e alla lunga si stancheranno di includere le transazioni della vittima (*punitive forking*).

Il *Feather forking* è un'altra strategia che può essere messa in atto anche se non si ha il controllo del 51% della rete. In questo caso l'attaccante annuncia che se vedrà una transazione della vittima inclusa in un blocco valido cercherà di fare il fork e si arrenderà solo dopo un po'. L'attacco ha successo con solo il 20% del controllo della rete perché la vittima, per avere speranza di far includere dai miner le proprie transazioni, dovrà alzare via via sempre di più le transaction fee fino a rendere di fatto impraticabile la difesa.

Selfish mining attack

Questo attacco è condotto da un miner che riesce a formare prima degli altri un blocco valido. A differenza però di ciò che si fa di solito, non lo annuncia alla rete, non riscuote il premio e sfrutta il vantaggio acquisito cercando subito di agganciarci un altro blocco valido e così via, costruendo la propria catena nascosta. Quando il primo blocco valido fosse annunciato da qualcun altro, lui potrebbe sempre tirar fuori due blocchi validi e quindi una catena più lunga a cui gli altri si aggancerebbero e riscuoterebbe così due premi. Se non ha ancora trovato un altro blocco valido, potrebbe sperare di diffondere sulla rete il suo blocco prima di quello del concorrente e ricevere così il premio.

Sybil attack

Il nome "Sybil" di questo attacco viene dal nome della protagonista del romanzo omonimo di F. R. Schreiber che soffriva di dissociazione della personalità. Esso consiste nell'impersonare più identità ed è un problema tipico di reti p2p dove non esistono entità centralizzate che verificano l'identità degli utenti/nodi. Le reti p2p si basano spesso sull'esistenza di nodi

distinti per distribuire risorse in modo da ottenere alta disponibilità e resistenza ai guasti, oppure su meccanismi di voto, come è il caso della rete Bitcoin, in cui si assume l'esistenza di un numero abbastanza grosso di nodi "onesti" da poter certificare determinate operazioni come, nel nostro caso, la validità di un blocco o di una transazione. Un attaccante che volesse sfruttare questo tipo di attacco farebbe perciò in modo da impersonare più identità distinte in modo da avere più "potere di voto" e sovvertire l'integrità della rete. Il modo utilizzato da Bitcoin per contrastare questo problema è il *Proof-of-Work*. In questo caso, la creazione di un'altra identità comporterebbe l'aggiunta di un ulteriore nodo di mining e quindi di potenza di calcolo per la risoluzione di un problema crittografico. Vista la complessità dello stesso, aggiungere più identità vorrebbe dire aggiungere potenze di calcolo che crescono sempre di più. Inoltre, già nel 2015 fu calcolato che la quantità di energia elettrica necessaria per una transazione Bitcoin era pari a quella consumata in un giorno da 1,57 case americane.

Per questi motivi, un altro meccanismo che può essere usato è il *Proof-of-Stake (PoS)*. A differenza del Proof-of-Work, in cui l'attività di mining è legata alla potenza di calcolo, in questo caso essa è legata alla quantità di criptovaluta posseduta. Per questo, piuttosto che utilizzare energia per risolvere i puzzle crittografici, un miner PoS può fare il mining di un numero di transazioni proporzionale alla valuta da lui posseduta. In questo modo, per poter scagliare un attacco 51%, il miner deve possedere il 51% della valuta e d'altra parte, se dovesse sovvertire la rete e la cosa fosse scoperta, la valuta in suo possesso perderebbe di valore e sarebbe quindi controproducente. La prima criptovaluta ad aver utilizzato questo metodo è il Peercoin.

Timewarp attack

Come abbiamo visto in precedenza, la rete bitcoin adatta la difficoltà nella soluzione del puzzle enigmistico in funzione della potenza di calcolo (hashrate) utilizzata in modo che il tempo medio per l'estrazione di un blocco valido resti intorno ai 10 minuti. Questo tipo di attacco mira ad abbassare la difficoltà in modo da rendere più veloce il mining.

COSA SONO I CRYPTO-MALWARE?

Una conseguenza dell'enorme attenzione che è stata ricevuta dalle criptovalute e dell'enorme quantità di soldi reali che ha cominciato a girarci intorno è stato l'arrivo dei primi malware ingegnerizzati appositamente per sfruttarne le debolezze. Ad esempio, due criptovalute diventate molto popolari tra i cybercriminali sono Monero e ZCash per le loro caratteristiche di privacy e mancanza di tracciabilità.

In particolare, sono state individuate almeno tre categorie:

- **Cryptominer**
- **Wallet stealer**
- **Clipboard hijacker**

I *cryptominer* sono un tipo di malware che sfrutta le risorse del computer dell'utente per fare il mining di criptovaluta a sua insaputa. E' stato calcolato da Kasperski che una singola botnet di mining computer può portare circa 30000$ al mese ma c'è anche il caso di un gruppo hacker che in soli sei mesi ha guadagnato almeno 7 milioni di dollari. Verso la fine del 2017 circa 2,7 milioni di utenti hanno avuto a che fare con un attacco cryptojacking ed il numero è in rapida ascesa. Il più diffuso malware è stato Coin Hive ma c'è anche XMRig. Entrambi fanno il mining di Monero. Riguardo a Bitcoin, invece, ci sono ad esempio OTORun, Kolab e BTMIne. L'utente attaccato sperimenta tipicamente un uso della CPU molto vicino al 100% per periodi prolungati.

I *wallet stealer* mirano invece a rubare le chiavi private dell'utente in modo da impossessarsi delle sue transazioni non spese. Tra questi malware citiamo ad esempio Pony e Azorult.

I *Clipboard hijackers*, invece, sfruttano la difficoltà mnemonica degli indirizzi. Di solito, infatti, gli utenti fanno il copia e incolla quando devono eseguire delle transazioni. Questo tipo di malware sostituisce al volo un indirizzo con un altro, quello dell'attaccante.

Tra i nomi da ricordare ci sono ComboJack, CryptoShuffler, Evrial, NjRAT Lime e anche una variante di Phorpiex.

Ci sono poi malware che sfruttano semplicemente vecchie tecniche come il keylogging.

COSA È UNA ICO?

Una ICO (Initial Coin Offering) è una modalità di crowdfunfding utilizzata al lancio sul mercato di nuove criptovalute in modo molto simile alla offerta pubblica iniziale o IPO (dall'inglese initial public offering) che è un'offerta al pubblico dei titoli di una società che intende quotarsi per la prima volta su un mercato regolamentato. Ci sono tre differenze importanti tra le due: le ICO sono decentralizzate, nel senso che non c'è un organismo centrale che le gestisce; le ICO non sono regolamentate in alcun modo; le ICO hanno una struttura più libera nel senso che è possibile preimpostare il numero massimo di monete (token) che verranno cedute e il valore oppure lasciarlo variabile come in un'asta ecc.

Quando una startup di criptovaluta vuole lanciare una ICO viene prodotto un documento in cui spiega in cosa consiste il progetto, di quanti fondi ha bisogno, come verranno spesi e in che tempi, quale tipo di valuta è accettata, quanto durerà la raccolta fondi e, infine, cosa otterranno gli investitori in cambio del finanziamento. Di solito questi ultimi aderiranno in previsione di un aumento di valore, in tempi più o meno rapidi, della criptovaluta. Se la raccolta fondi non avviene nelle modalità sperate, i soldi vengono restituiti.

Se si desidera investire in una ICO ci sono siti come ad es. https://icowatchlist.com/ per restare aggiornati.

COSA SONO LE ALTCOIN?

In questo lavoro abbiamo parlato molto di Bitcoin sia perché è stata la prima criptovaluta "importante", sia per il suo ruolo nel panorama attuale (https://coinmarketcap.com/it/) che per aver costituito il modello di riferimento per le altre criptovalute che si sono succedute, ognuna con le sue caratteristiche peculiari e che sono nate per risolvere i problemi di Bitcoin, tra cui ad esempio gli alti tempi necessari per la validazione delle transazioni, che ne limitano l'uso come valuta cash, le alte commissioni, l'alta volatilità, la limitazione nel supporto agli smart contract e così via. Tra le criptovalute attualmente sul mercato, in particolare, citeremo:

- **Ethereum** – è la seconda moneta per capitalizzazione del mercato dopo Bitcoin e anche una delle più interessanti per il suo supporto agli smart contract. E' stata creata nel 2015 dal programmatore russo Vitalik Buterin. A differenza di Bitcoin, che si basa sulle UTXO, Ethereum è account-based, come una banca tradizionale. Inoltre Ethereum ha un linguaggio di scripting molto più potente che è poi quello con cui vengono scritti gli smart contract. Come funzione di hashing viene usata Ethash, a differenza di Bitcoin che usa la SHA-256.
- **Ripple (XRP)** –creata nel 2012 da Chris Larsen e Jed McCaleb, è una tecnologia per lo scambio di fondi in tempo reale con costi bassissimi da una valuta all'altra e ad uso delle istituzioni finanziarie. A oggi sono affiliate più di 50 banche. Si propone come alternativa a Western Union o SWIFT. Utilizza un sistema di consenso che non è il proof-of-work di bitcoin né un proof-of-stake. XRP è il nome della valuta digitale che viene scambiata sulla rete (detta RippleNet) come "lingua franca" tra le varie valute. Al momento della nascita sono stati creati 100 miliardi di XRP, dopodiché la valuta viene decrementata a ogni transazione. Inoltre, XRP è una valuta centralizzata (controllata dall'azienda Ripple) e non se ne può fare il mining
- **Litecoin** – questa moneta è stata creata nel 2011 su Github, appena due anni dopo Bitcoin, di cui è sostanzialmente un fork, da Charlie Lee, un laureato del MIT ed ex dipendente Google, ed ha il suo principale punto di forza nella velocità di esecuzione delle transazioni, che qui impiegano circa 2,5 minuti piuttosto che i 10 di Bitcoin. Per questo si presta a pagamenti istantanei. Ad esempio, non si può pagare un caffè con Bitcoin perché una transazione richiede circa 10 minuti per essere validata. Come nel caso di Bitcoin esiste un valore massimo pari a 84 milione di unità. Come funzione di hashing viene usata Scrypt, a differenza di Bitcoin che usa la SHA-256
- **Monero (XMR)** – il suo nome in esperanto significa moneta. E' stata creata nel 2014 da Riccardo Spagni, Fransisco Cabañas e altri come fork di Bitcoin. Anche in questo caso esiste un valore massimo di 18,4 milioni, che si esauriranno entro otto anni. I punti di forza di questa valuta sono la privacy e la mancanza di tracciabilità: tutti gli indirizzi e le somme scambiate sono offuscate. Viene utilizzato lo stesso Proof-of-Work di Bitcoin però con algoritmo CryptoNight
- **Bitcoin Cash** – è stato creato nell'agosto 2017 come hard fork di Bitcoin in quanto usa blocchi di dimensione 8 MB per ridurre i tempi delle transazioni, che è un grosso problema di scalabilità di Bitcoin (addirittura nell'agosto 2017 ci sono stati utenti che hanno atteso 4

giorni per la validazione delle transazioni su Bitcoin). Il prezzo da pagare per questo aumento di dimensione del blocco è la maggiore difficoltà di creazione per i piccoli miner a causa dell'aumentata potenza di calcolo richiesta, togliendo quindi democrazia alla rete. Un'altra caratteristica di questa valuta è il costo ridotto delle transazioni

- **Tether (USDT)** – è nata nel 2015 con il nome di Realcoin ed è stata disegnata per essere una "stable coin" nel senso che ha fluttuazioni di valore molto più limitato rispetto a Bitcoin e altre valute. Per fare questo si aggancia al dollaro in quanto è possibile creare una nuova unità solo se è coperta da un dollaro nelle riserve della Tether Limited, società delle Isole Vergini britanniche (in teoria, in quanto attualmente c'è il sospetto che non sia proprio così e che la società abbia emesso una quantità di criptovaluta maggiore rispetto alle riserve).
- **Cardano (ADA)** – è stata creata da Charles Hoskinson, co-fondatore di Ethereum, a settembre 2017. E' basata sul Proof-of-Stake, invece che sul Proof-of-Work come Bitcoin, che non richiede miner ed è anche eco-sostenibile (Si stima per esempio che il Bitcoin necessiti più energia dell'Irlanda). Supporta gli smart contract
- **Dash** – originariamente nota come XCoin ed in seguito Darkcoin, il suo nome deriva da "digital cash" ed è nata a gennaio 2014 a opera di Evan Duffield. Il limite massimo di monete è di 18 milioni. Le transazioni vengono confermate velocemente (circa 2,5 minuti) e in modo non tracciabile con bassissime commissioni. Oltre ai nodi miner ci sono i MasterNode, che gestiscono la governance della rete.

Autore
Alessandro Sinibaldi, senior security expert CERT-PA
Graphic designer
Daniela De Blasis, visual designer, UX/UI designer at AgID