Una “breve” introduzione ai Bitcoin

@FlavioGiobergia

Bitcoin: cos'è?

Bitcoin è una moneta decentralizzata: non esiste alcun potere centrale in grado di controllarla.

Al suo posto, esiste una rete di “peers” che gestisce tutte le transazioni.

Inoltre, grazie alla crittografia è possibile garantire la sicurezza di tale moneta.

Come funziona?

Ogni utente è in possesso di un “wallet”, un file generato dal client Bitcoin.

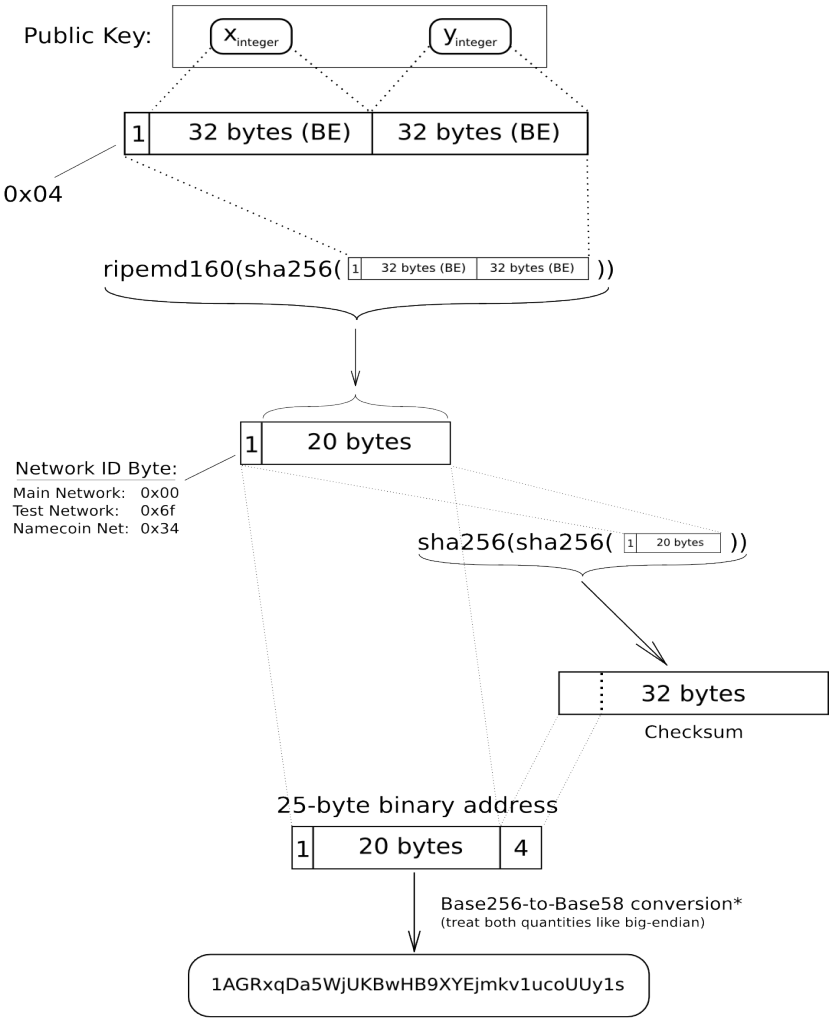
Questo wallet contiene una serie di coppie chiave privata-chiave pubblica.

La chiave privata è nota solo al proprietario, e serve per effettuare i pagamenti.

La chiave pubblica può essere resa nota, e serve per dimostrare a terzi che si è in possesso della chiave privata.

Dalla chiave pubblica viene estratto un indirizzo, una serie di lettere e numeri lungo solitamente 34 caratteri (minimo 27).

Elliptic-Curve Public Key to BTC Address conversion



@FlavioGiobergia

*In a standard base conversion, the 0x00 byte on the left would be irrelevant (like writing '052' instead of just '52'), but in the BTC network the left-most zero chars are carried through the conversion. So for every 0x00 byte on the left end of the binary address, we will attach one '1' character to the Base58 address. This is why main-network addresses all start with '1'

etotheipi@gmail.com / 1Gffm7LKXcNFPrtxy6yF4JBoe5rVka4sn1

Effettuare pagamenti

Per effettuare pagamenti, è necessario avere un wallet, dei soldi da inviare e l'indirizzo del destinatario.

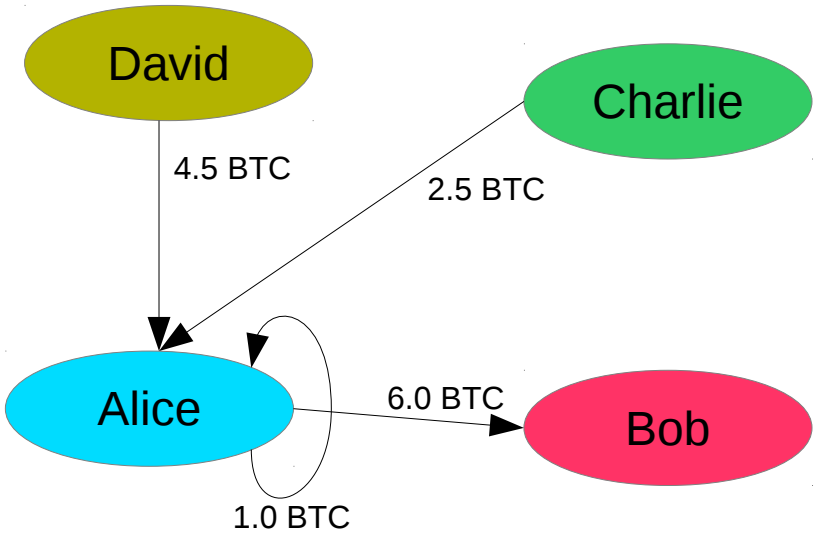
Il client Bitcoin genera una transazione, che viene firmata utilizzando la chiave privata di chi effettua il pagamento.

Questa transazione viene inviata, insieme alla chiave pubblica, al resto della rete. Chiunque può verificare, usando la chiave pubblica, che il messaggio è stato firmato utilizzando la chiave privata.

Dove sono i soldi?

Avere soldi significa essere in grado di dimostrare che qualcuno ci ha mandato bitcoin in precedenza.

Per fare questo, ad ogni pagamento bisogna allegare delle transazioni che abbiano come destinatario l'indirizzo con il quale si mandano i bitcoin. Una volta allegata una transazione, questa si può considerare “spesa”, e quindi non più riutilizzabile.



Double-spending

Il double-spending consiste nello spendere più volte gli stessi soldi.

Per ovviare a questo problema, ogni peer della rete conosce tutte le transazioni effettuate, e può verificare che, fornita una nuova transazione, questa allega tutte transazioni che non sono ancora state “spese”.

Per questo motivo, quando si utilizza per la prima volta un client Bitcoin, questo scaricherà tutte le transazioni effettuate dal 2009 in poi.

Blocchi di transazioni

Le transazioni vengono raccolte in blocchi (blocks).

All'interno di un blocco, le transazioni non hanno un ordine cronologico: vengono tutte considerate come effettuate allo stesso momento.

Le transazioni non ancora inserite in un blocco vengono considerate non ancora effettuate.

Ogni blocco presenta un problema che deve essere risolto. Per i BTC, si tratta di trovare un hash SHA256 con caratteristiche particolari (il sistema utilizzato è detto “Hashcash”). Risolvere questo problema richiede del tempo (e potenza di calcolo).

Inoltre ogni blocco contiene la soluzione al problema del blocco precedente.

Block Chain

I blocchi hanno un preciso ordine cronologico: questa sequenza di blocchi viene chiamata block chain.

L'ultimo blocco aggiunto sarà quindi quello contenente le transazioni inserite più recentemente.

Come aggiungere blocchi?

Ogni peer della rete può proporre un nuovo blocco da aggiungere alla block chain.

Tra tutti quelli proposti, viene scelto il blocco che contiene la soluzione al problema del blocco precedente.

Il blocco viene quindi inviato al resto della rete: è immediato verificare se la soluzione è corretta. Se questo è il caso, la rete accetta il blocco, e inizia a lavorare sul nuovo problema.

Mining

Il processo di ricerca della soluzione del problema viene detto “mining”; chi lo effettua viene invece chiamato “miner”.

Grazie ai miners, le transazioni vengono aggiunte ai blocchi (ossia vengono “confermate”).

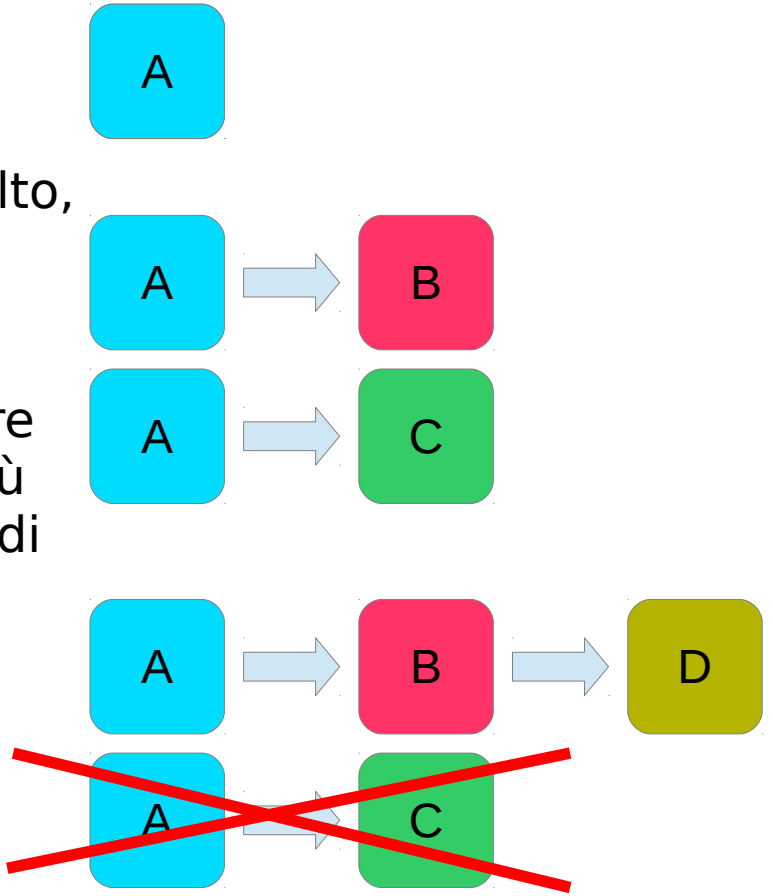
Risoluzione contemporanea di un blocco

Può succedere che un blocco venga risolto in tempi molto vicini da due (o più) miner diversi.

In questo caso, ognuno provvede a inviare il nuovo blocco ai nodi adiacenti della rete.

Ognuno inizierà quindi a lavorare sul nuovo blocco ricevuto: quando uno dei due (o più) nuovi blocchi viene risolto, il blocco successivo viene inviato alla rete.

Per regola, tutta la rete passa a lavorare sulla catena più lunga; quindi quella più corta viene scartata, e tutta la rete ha di nuovo una sola catena su cui lavorare.



Rewards

Ogni volta che il problema di un blocco viene risolto, viene assegnata una retribuzione, in bitcoin, a colui che lo ha risolto.

Questo reward viene dimezzato ogni 210,000 blocchi risolti (circa 4 anni), fino ad arrivare al 2140, quando non verranno più assegnati rewards.

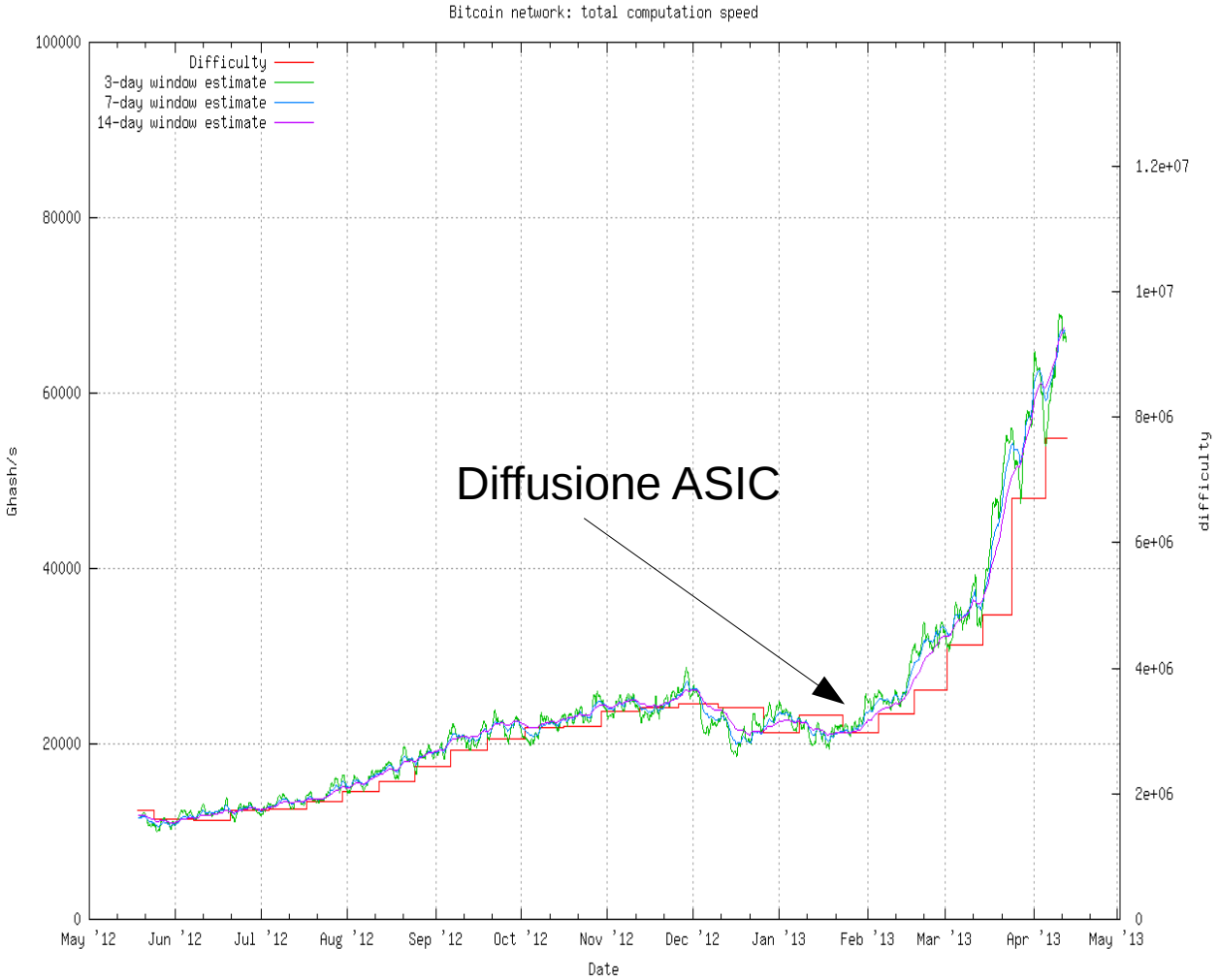
Nel 2140 ci saranno in circolazione 21 milioni di bitcoin.

Difficoltà del mining

La difficoltà dei problemi da risolvere viene aggiustata automaticamente in modo da far passare circa 10 minuti tra un blocco e il successivo.

Il mining avveniva in origine usando la potenza di calcolo delle CPU, in seguito GPU, FPGA e ASIC.

Ad ogni “novità”, la difficoltà incrementa esponenzialmente.



Mining pools

La maggior parte dei piccoli e medi miners raccolgono la loro potenza di calcolo in quelle che si chiamano “mining pools”.

Il lavoro viene diviso fra i vari partecipanti e, quando un blocco viene risolto, il reward viene diviso in base al contributo fornito.

In questo modo si hanno guadagni più modesti, ma più frequenti.

Difetti di Bitcoin

Nonostante i numerosi aspetti positivi, esistono anche alcuni contro dei Bitcoin: si tratta per la maggior parte di “fastidi” o di vulnerabilità che difficilmente si possono verificare.

Nonostante questi problemi, si può affermare che Bitcoin sia un sistema costruito in maniera elegante ed efficiente.

>50% attack

È una vulnerabilità teorica, ma che, con la nascita di pool molto grosse, potrebbe diventare prima o poi una realtà.

L'assunzione di base è che un malintenzionato sia in controllo di più del 50% della potenza di calcolo della rete.

In questo modo è possibile generare una catena di blocchi segreta più lunga di quella pubblica, in modo da rilasciarla quando necessario. In questo modo il resto della rete, ricevendo una catena più lunga, passerà ad utilizzare quella, e tutte le transazioni che erano state convalidate in precedenza ritornano ad essere considerate non effettuate.

L'attacker può a questo punto rientrare in possesso di bitcoin che aveva speso in una delle transazioni contenute nei blocchi più recenti della block chain, che sono stati sostituiti dalla catena da esso creata.

Tracking di un indirizzo

Bitcoin fornisce teoricamente i mezzi per essere veramente anonimi: molti, però, non li usano propriamente.

Se si vuole scoprire l'identità di chi è in possesso di un certo indirizzo (supponendo di conoscere un certo numero di corrispondenze persona-indirizzo), è possibile controllare tutte le transazioni effettuate da quell'indirizzo: si ottiene così una lista di altri indirizzi.

Si può procedere con questa operazione anche sugli indirizzi così ottenuti, finchè nell'elenco di indirizzi non se ne trova uno il cui proprietario è noto: è possibile quindi richiedere a tale persona aiuto per rintracciare a ritroso la persona di partenza.

La maggior parte di questo procedimento può essere automatizzato tramite l'utilizzo di bot e algoritmi per la visita di grafi.

Tempi di attesa “lunghi”

Per avere la propria transazione confermata è necessario aspettare un minimo di 10 minuti, ossia il tempo necessario perchè un blocco venga risolto.

Dato però che esiste il rischio del >50% attack, è consigliabile aspettare che la catena diventi relativamente lunga prima di poter considerare la transazione veramente avvenuta.

Il maggior numero di blocchi consecutivi risolti dalla stessa pool è, per ora, di 6. È quindi consigliabile aspettare almeno 60 minuti per poter considerare la propria transazione come effettuata sicuramente.

Tempi di attesa “lunghi”

Per avere la propria transazione confermata è necessario aspettare un minimo di 10 minuti, ossia il tempo necessario perchè un blocco venga risolto.

Dato però che esiste il rischio del >50% attack, è consigliabile aspettare che la catena diventi relativamente lunga prima di poter considerare la transazione veramente avvenuta.

Il maggior numero di blocchi consecutivi risolti dalla stessa pool è, per ora, di 6. È quindi consigliabile aspettare almeno 60 minuti per poter considerare la propria transazione come effettuata sicuramente.

Fees

Ad ogni transazione è possibile allegare una piccola quantità di bitcoin (un compenso, o “fee”) che verrà consegnata a chi risolverà il blocco in cui viene inserita la transazione.

Al momento non ci sono costi per effettuare transazioni. Questo perchè i miners ricevono un reward quando risolvono un blocco.

Con il passare del tempo, però, i rewards diminuiranno. A quel punto, l'unica fonte di guadagno dei miners saranno le fees.

A causa di ciò, le transazioni alle quali non sono state allegate fees finiranno per non essere mai processate.

Altre cryptocurrencies

Grazie al successo di Bitcoin, molte altre cryptocurrencies sono nate.

Si differenziano da Bitcoin principalmente per numero di monete erogate, algoritmi utilizzati e tempi di attesa tra un blocco e il successivo.

Alcune monete portano qualcosa di innovativo, altre sono copie palesi di altre cryptocurrencies, create con il solo obiettivo di arricchirsi.

Grazie per l'attenzione :-)

@FlavioGiobergia