Bitcoin: in cryptography we trust

Renato Budinich

2013-26-10

I Bitcoin in due parole

Sono una nuova valuta elettronica creata nel 2009 da Satoshi Nakamoto. Per l'utente finale è come Paypal, ma con alcune differenze fondamentali:

I Bitcoin in due parole

Sono una nuova valuta elettronica creata nel 2009 da Satoshi Nakamoto. Per l'utente finale è come Paypal, ma con alcune differenze fondamentali:

- Rete decentralizzata p2p (come i torrent) - non c'è autorità centrale

I Bitcoin in due parole

Sono una nuova valuta elettronica creata nel 2009 da Satoshi Nakamoto. Per l'utente finale è come Paypal, ma con alcune differenze fondamentali:

- Rete decentralizzata p2p (come i torrent) - non c'è autorità centrale
- Transazioni non reversibili

I Bitcoin in due parole

Sono una nuova valuta elettronica creata nel 2009 da Satoshi Nakamoto. Per l'utente finale è come Paypal, ma con alcune differenze fondamentali:

- Rete decentralizzata p2p (come i torrent) - non c'è autorità centrale
- Transazioni non reversibili
- "Impossibili" da falsificare

I Bitcoin in due parole

Sono una nuova valuta elettronica creata nel 2009 da Satoshi Nakamoto. Per l'utente finale è come Paypal, ma con alcune differenze fondamentali:

- Rete decentralizzata p2p (come i torrent) - non c'è autorità centrale
- Transazioni non reversibili
- "Impossibili" da falsificare
- Creati secondo curva prestabilita, e sono limitati (quindi deflazionari)

I Bitcoin in due parole

Sono una nuova valuta elettronica creata nel 2009 da Satoshi Nakamoto. Per l'utente finale è come Paypal, ma con alcune differenze fondamentali:

- Rete decentralizzata p2p (come i torrent) - non c'è autorità centrale
- Transazioni non reversibili
- "Impossibili" da falsificare
- Creati secondo curva prestabilita, e sono limitati (quindi deflazionari)
- L'utente deve riporre fiducia solo nella crittografia (è più facile criptare che decriptare)

Caratteristiche di una buona valuta

Prendendo l'oro come esempio di buona valuta:

Caratteristiche di una buona valuta

Prendendo l'oro come esempio di buona valuta:

- Scarso

Caratteristiche di una buona valuta

Prendendo l'oro come esempio di buona valuta:

- Scarso
- Uniforme

Caratteristiche di una buona valuta

Prendendo l'oro come esempio di buona valuta:

- Scarso
- Uniforme
- Trasportabile

Caratteristiche di una buona valuta

Prendendo l'oro come esempio di buona valuta:

- Scarso
- Uniforme
- Trasportabile
- Facilmente identificabile

Caratteristiche di una buona valuta

Prendendo l'oro come esempio di buona valuta:

- Scarso
- Uniforme
- Trasportabile
- Facilmente identificabile
- Difficilmente falsificabile

Caratteristiche di una buona valuta

Prendendo l'oro come esempio di buona valuta:

- Scarso
- Uniforme
- Trasportabile
- Facilmente identificabile
- Difficilmente falsificabile
- Non deteriorabile

Caratteristiche di una buona valuta

Prendendo l'oro come esempio di buona valuta:

- Scarso
- Uniforme
- Trasportabile
- Facilmente identificabile
- Difficilmente falsificabile
- Non deteriorabile
- Prodotto a un rate abbastanza prevedibile

Firme crittografiche e la rete p2p Bitcoin

Firme crittografiche e la rete p2p Bitcoin

- Una firma crittografica di un messaggio certifica che è stato scritto dal possessore di una certa chiave privata, la cui chiave pubblica è nota a tutti

Firme crittografiche e la rete p2p Bitcoin

- Una firma crittografica di un messaggio certifica che è stato scritto dal possessore di una certa chiave privata, la cui chiave pubblica è nota a tutti
- Nella rete p2p Bitcoin ogni utente ha delle chiavi private

Firme crittografiche e la rete p2p Bitcoin

- Una firma crittografica di un messaggio certifica che è stato scritto dal possessore di una certa chiave privata, la cui chiave pubblica è nota a tutti
- Nella rete p2p Bitcoin ogni utente ha delle chiavi private
- Per ricevere dei bitcoin basta rendere pubblico il proprio indirizzo, tipo `1BTCorgHwCg6u2YSAWKgS17qUad6kHmtQW`

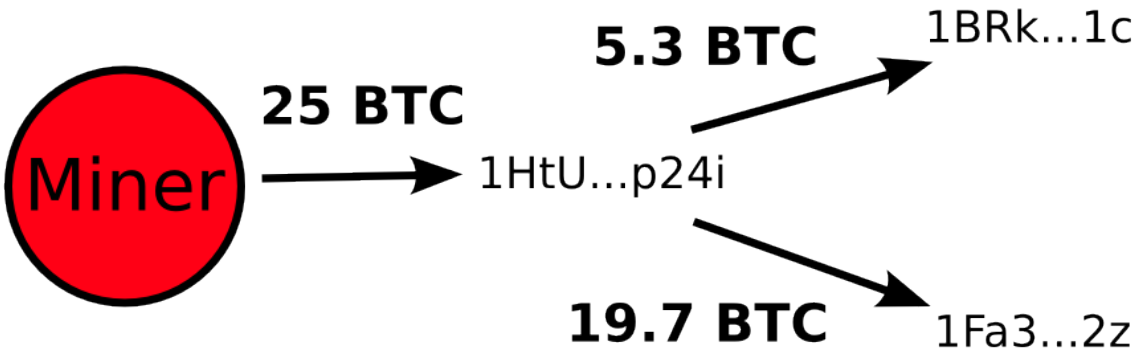
Firme crittografiche e la rete p2p Bitcoin

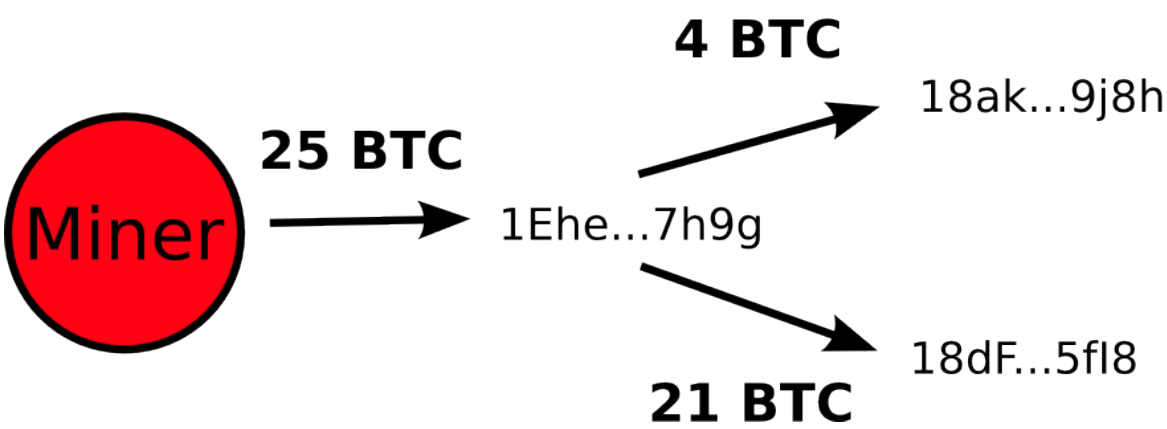
- Una firma crittografica di un messaggio certifica che è stato scritto dal possessore di una certa chiave privata, la cui chiave pubblica è nota a tutti
- Nella rete p2p Bitcoin ogni utente ha delle chiavi private
- Per ricevere dei bitcoin basta rendere pubblico il proprio indirizzo, tipo `1BTCorgHwCg6u2YSAWKgS17qUad6kHmtQW`
- Solo il possessore della chiave privata di quell'indirizzo può spenderli nuovamente

Firme crittografiche e la rete p2p Bitcoin

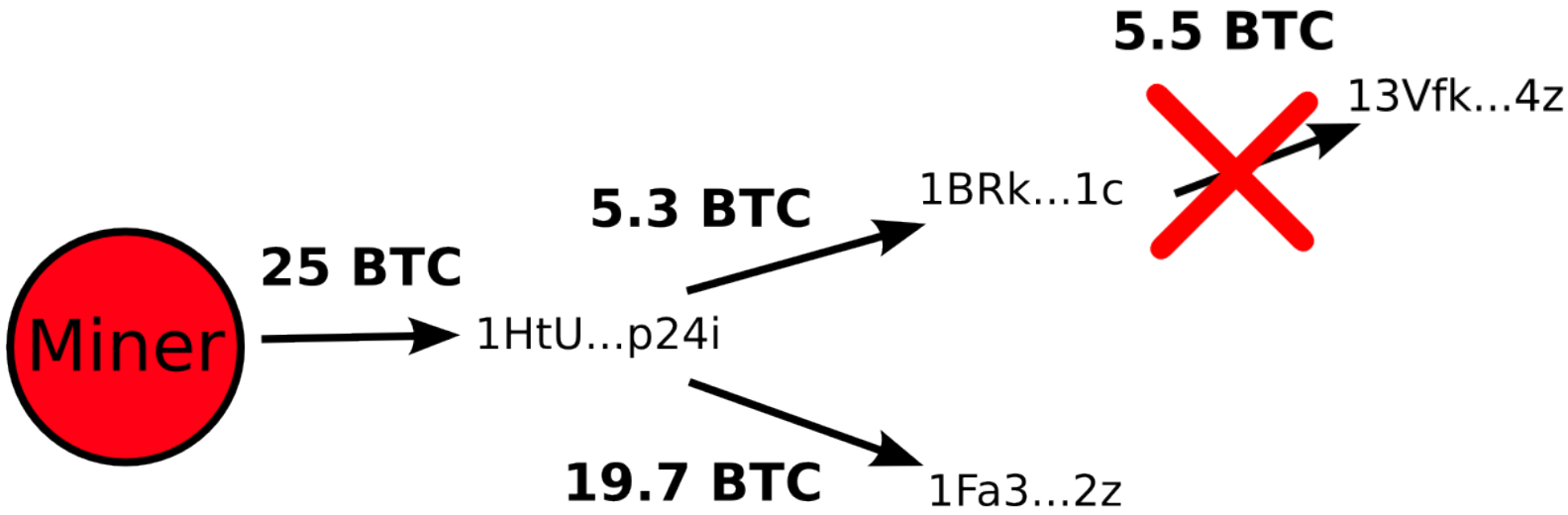
- Una firma crittografica di un messaggio certifica che è stato scritto dal possessore di una certa chiave privata, la cui chiave pubblica è nota a tutti
- Nella rete p2p Bitcoin ogni utente ha delle chiavi private
- Per ricevere dei bitcoin basta rendere pubblico il proprio indirizzo, tipo `1BTCorgHwCg6u2YSAWKgS17qUad6kHmtQW`
- Solo il possessore della chiave privata di quell'indirizzo può spenderli nuovamente
- Quindi "non esistono" i bitcoin come entità, ma solo una lista di transazioni

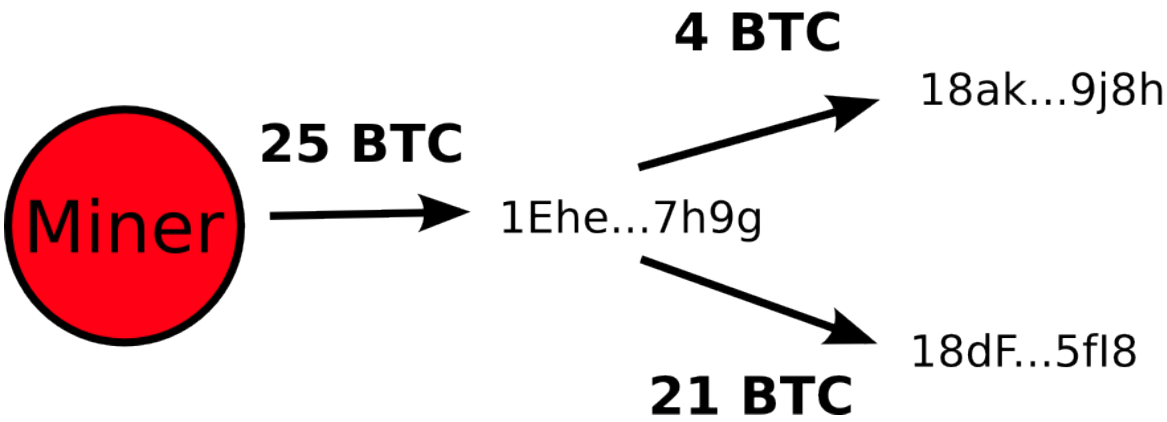
Transazioni





Transazioni





Il problema del double spending

Se creo due transazioni, una in cui mando tutti i miei bitcoin a un indirizzo, una in cui lo mando ad un altro, quale delle due è valida?

Il problema del double spending

Se creo due transazioni, una in cui mando tutti i miei bitcoin a un indirizzo, una in cui lo mando ad un altro, quale delle due è valida?

Si decide di accettare solo la prima transazione in ordine temporale; ma senza un'autorità centrale serve un sistema che permetta ai nodi di accordarsi su una storia comune

La Blockchain

La Blockchain

- Le transazioni vengono trasmesse sulla rete p2p

La Blockchain

- Le transazioni vengono trasmesse sulla rete p2p
- Vengono raccolte in un **block** che contiene un hash di quello precedente

La Blockchain

- Le transazioni vengono trasmesse sulla rete p2p
- Vengono raccolte in un **block** che contiene un hash di quello precedente
- La catena così formata è detta **blockchain**

La Blockchain

- Le transazioni vengono trasmesse sulla rete p2p
- Vengono raccolte in un **block** che contiene un hash di quello precedente
- La catena così formata è detta **blockchain**

E' impossibile cambiare un blocco della catena senza cambiarne anche quelli successivi

La Blockchain - Proof of Work

La Blockchain - Proof of Work

- Per creare un blocco serve dimostrare di aver fatto una certa quantità di lavoro computazionale (esibire dei bit che hashati assieme al block proposto diano una stringa che inizi con n zeri)

La Blockchain - Proof of Work

- Per creare un blocco serve dimostrare di aver fatto una certa quantità di lavoro computazionale (esibire dei bit che hashati assieme al block proposto diano una stringa che inizi con n zeri)
- In questo modo per cambiare un block bisogna rifare tutto il lavoro computazionale per quel blocco e tutti quelli successivi

La Blockchain - Proof of Work

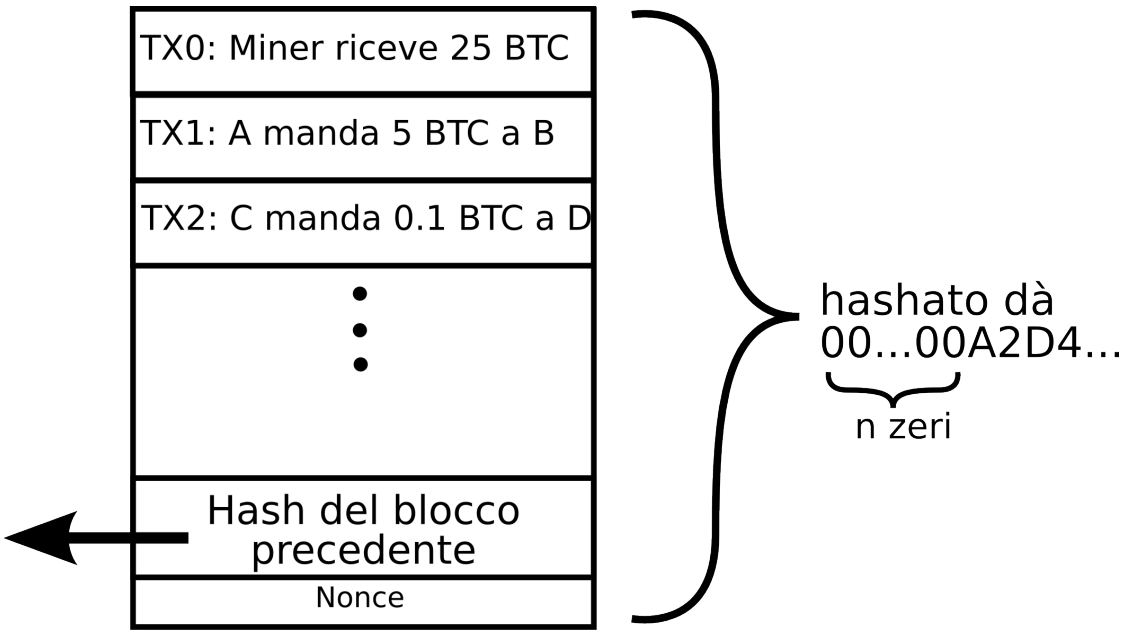
- Per creare un blocco serve dimostrare di aver fatto una certa quantità di lavoro computazionale (esibire dei bit che hashati assieme al block proposto diano una stringa che inizi con n zeri)
- In questo modo per cambiare un block bisogna rifare tutto il lavoro computazionale per quel blocco e tutti quelli successivi
- Come incentivo, chi fa il lavoro computazionale (i **Miners**) è ricompensato con 25 bitcoin per ogni block creato

La Blockchain - Proof of Work

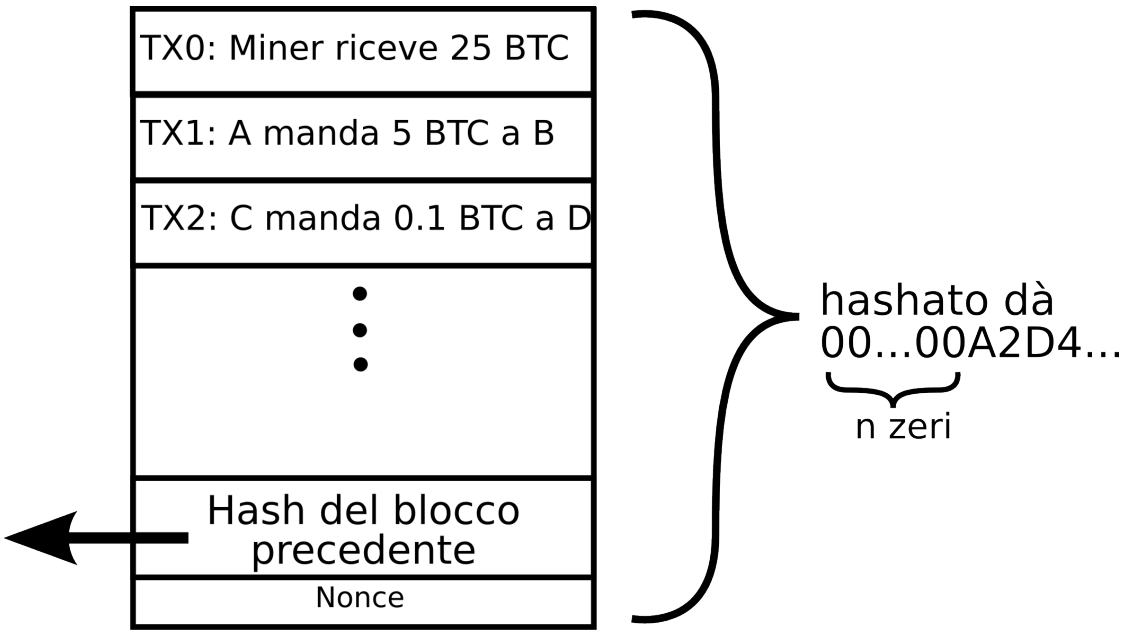
- Per creare un blocco serve dimostrare di aver fatto una certa quantità di lavoro computazionale (esibire dei bit che hashati assieme al block proposto diano una stringa che inizi con n zeri)
- In questo modo per cambiare un block bisogna rifare tutto il lavoro computazionale per quel blocco e tutti quelli successivi
- Come incentivo, chi fa il lavoro computazionale (i **Miners**) è ricompensato con 25 bitcoin per ogni block creato

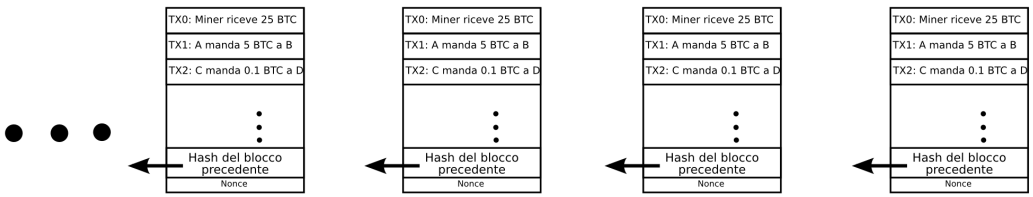
I Miners offrono un servizio (rendono sicura la rete) e sono incentivati dalla ricompensa in bitcoin.

La Blockchain



La Blockchain





Soluzione al double spending

Soluzione al double spending

- Il double spending corrisponde a una biforcazione; in tal caso i Miners aggiungono i block successivi al block contenente la transazione che loro ritengono valida.

Soluzione al double spending

- Il double spending corrisponde a una biforcazione; in tal caso i Miners aggiungono i block successivi al block contenente la transazione che loro ritengono valida.
- Il ramo più lungo viene riconosciuto come quello valido

Soluzione al double spending

- Il double spending corrisponde a una biforcazione; in tal caso i Miners aggiungono i block successivi al block contenente la transazione che loro ritengono valida.
- Il ramo più lungo viene riconosciuto come quello valido
- Per fare double-spending dovrei avere più potenza di calcolo del resto della rete, in modo da aggiungere blocchi al mio ramo "disonesto" più velocemente di quanto ne aggiungano gli altri all'altro

Caratteristiche di una buona valuta

- Scarso
- Uniforme
- Trasportabile
- Facilmente identificabile
- Difficilmente falsificabile
- Non deteriorabile
- Prodotto a un rate abbastanza prevedibile

Referenze e links

- http://bitcoin.org/bitcoin.pdf
- http://en.bitcoin.it/wiki/Main_Page
- https://bitcointalk.org/
- http://bitcoin.reddit.com/
- http://bitcoin.stackexchange.com/
- http://evoorhees.blogspot.it/2013/05/bitcoin-2013-role-of-bitcoin-as-money.html