



Bitcoin

Mattia Monga

Cos'è

Come si usa

Come  
funziona

Transazioni

Firme

Ordinamento  
temporale

Mining

Protocollo

Conclusione

Riferimenti

Bitcoin: "... pagando di moneta senza conio."<sup>1</sup>

Mattia Monga

Dip. di Informatica  
Università degli Studi di Milano  
mattia.monga@unimi.it

Milano, 5 maggio 2014



Si tratta di una moneta scritturale.  
L'obiettivo del progettista (Satoshi Nakamoto, 2008):

## Bitcoin

Due soggetti possono **direttamente** concordare una transazione, *senza la necessità di una terza parte fidata.*

- La transazione non può essere annullata/ripudiata
- Il sistema funziona correttamente nell'ipotesi che gli "onesti" controllino collettivamente più potenza di calcolo dei potenziali disonesti.



Bitcoin

Mattia Monga

Cos'è

Come si usa

Come funziona

Transazioni

Firme

Ordinamento temporale

Mining

Protocollo

Conclusione

Riferimenti





Bitcoin stabilisce un protocollo per mantenere un “log” distribuito di tutte le transazioni, in modo che sia possibile sapere se lo stato di ogni “moneta”, garantendo che non venga spesa piú volte simultaneamente.

Le scritture contabili sono mantenute coerenti senza un'autorità centrale:

- Crittografia asimmetrica (firme digitali)
- Catene di hash-crittografici
- Timestamp garantiti da computazioni onerose
- Pubblicità totale (sincronizzata tramite bittorrent)

Bitcoin

Mattia Monga

Cos'è

Come si usa

Come funziona

Transazioni

Firme

Ordinamento temporale

Mining

Protocollo

Conclusione

Riferimenti



Bitcoin

Mattia  
Monga

Cos'è

Come si usa

Come  
funziona

**Transazioni**

Firme

Ordinamento  
temporale

Mining

Protocollo

Conclusione

Riferimenti

Un transazione è un messaggio che dice:

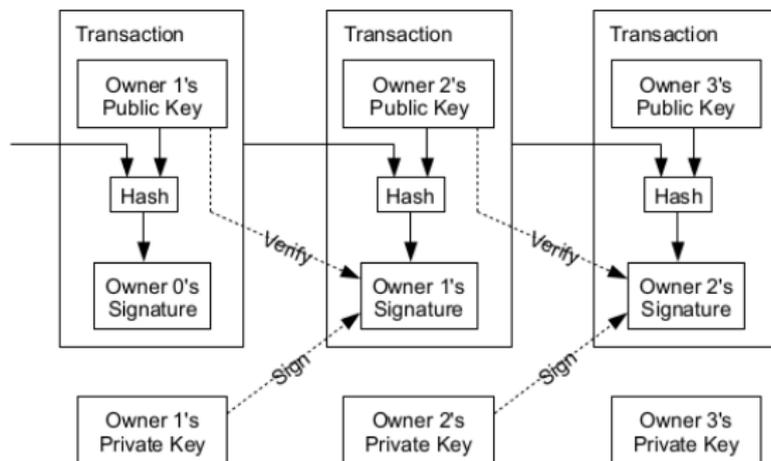
- Il soggetto  $A$  cede  $x$  bitcoin
- Il soggetto  $B$  riceve  $y$  bitcoin
- $f$  bitcoin servono come premio per chi collabora alla validazione della transazione (*transaction fee*)

Naturalmente:  $x = y + f$

# Transazioni firmate

Ogni soggetto ha una coppia di chiavi asimmetriche: una (**privata**) serve per garantire l'autenticità (firma), l'altra (**pubblica**) per verificare le firme.

Owner 1  $\rightsquigarrow$  Owner 2



Bitcoin

Mattia  
Monga

Cos'è

Come si usa

Come

funziona

Transazioni

**Firme**

Ordinamento

temporale

Mining

Protocollo

Conclusione

Riferimenti

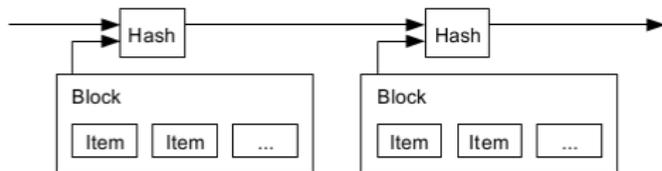


# Hash chain

Ogni transazione (in realtà un **blocco** contiene generalmente molte transazioni) è collegata a quelle precedente perché include uno **hash** (256 bit che “riassumono” l’informazione in una maniera difficile da falsificare) di quelle precedenti: P.es.:

Hash SHA256 della Divina Commedia curata da G. Petrocchi →  
5b57a696ac3bdb48cb09b1d0998f9d582660f5cbd9463e2ef5d5ea4e0f6d5671

Al momento non si conosce un metodo per trovare un’altra stringa di caratteri con lo stesso hash più efficiente del provare a caso.



Per calcolarlo devono esistere gli hash precedenti: se  $H_0$  viene pubblicato il 1 gennaio 2014, la transazione che contiene lo hash di  $H_0$  deve essere temporalmente successiva.

Bitcoin

Mattia  
Monga

Cos'è

Come si usa

Come

funziona

Transazioni

Firme

**Ordinamento**

**temporale**

Mining

Protocollo

Conclusione

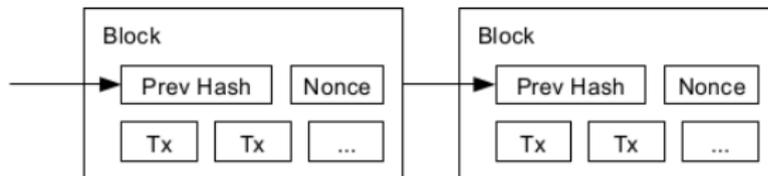
Riferimenti



# Accordo distribuito

Ma come si fa a concordare una singola storia? Un'unica **block chain**?

Il meccanismo con cui si risolve questo problema (in generale insolubile!) è l'introduzione di **proof of work**: non basta calcolare uno hash, lo si vuole anche "particolare":



Bisogna trovare un 'nonce' che dia luogo a uno hash che inizia con un certo numero (parametro di difficoltà) di zeri.

000000000000000001237535293c120a0b9d4d4ac7bac9911c48357bf0f694d26

Se SHA256 mantiene le sue promesse, non c'è modo migliore che quello di provare a caso. . . Siccome però ci provano in molti, il tempo in media col quale lo si trova è 10 minuti.

Bitcoin

Mattia Monga

Cos'è

Come si usa

Come funziona

Transazioni

Firme

**Ordinamento temporale**

Mining

Protocollo

Conclusione

Riferimenti



Ma perché dovrebbero provarci in molti?

Perché c'è un **premio** per chi ci riesce: attualmente 25BTC, dimezzato circa ogni 4 anni.

Chi riesce a trovare un nonce che dà luogo a uno hash opportuno può intestarsi una transazione da 25BTC più i transaction fee di tutte le transazioni nel blocco.

Nel caso (abbastanza improbabile) che ci siano più blocchi validi, si prende il ramo con il maggior sforzo computazionale (la catena più lunga).

*Avendo sufficiente potenza computazionale è possibile accreditare transazioni false, ma l'ipotesi è che: (1) gli "onesti" siano computazionalmente più potenti; (2) "conviene" usare la computazione per ottenere i premi di mining.*

Bitcoin

Mattia  
Monga

Cos'è

Come si usa

Come  
funziona

Transazioni

Firme

Ordinamento  
temporale

**Mining**

Protocollo

Conclusione

Riferimenti



Bitcoin

Mattia  
Monga

Cos'è

Come si usa

Come  
funziona

Transazioni

Firme

Ordinamento  
temporale

Mining

**Protocollo**

Conclusione

Riferimenti

- 1 Firmo una transazione e la annuncio *broadcast*
- 2 Ogni nodo disponibile al mining colleziona gli annunci in un blocco
- 3 Ogni miner cerca un nonce per la *proof of work*
- 4 Chi trova la *proof of work* la annuncia broadcast
- 5 L'annuncio del blocco validato viene confermato e la transazione può essere considerata **genuina**.

- L'anonimato non è un obiettivo di progetto: anche se le transazioni avvengono fra **pseudonimi**
- Il numero di bitcoin è limitato ( $21 \cdot 10^6$  frazionabili fino a  $10^{-8}$ )
- La difficoltà di mining è un parametro del sistema: il tasso di creazione di moneta può essere controllato (fine prevista 2140).
- Le transazioni sono irreversibili: si tutela il venditore, ma non il compratore (il contrario di quanto dovrebbe avvenire con le carte di credito. . . )



SCHMALZER, BERLINSTEIGEL, GORMAN

“È virtuale”.

da Internazionale 1038

Bitcoin

Mattia Monga

Cos'è

Come si usa

Come funziona

Transazioni

Firme

Ordinamento temporale

Mining

Protocollo

Conclusione

Riferimenti



Bitcoin

Mattia  
Monga

- Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008
- Khan Academy: <https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it>
- Esplorare la block-chain: <http://blockexplorer.com>
- Conviene il mining: <http://tpbitcalc.appspot.com/>

Cos'è

Come si usa

Come  
funziona

Transazioni

Firme

Ordinamento  
temporale

Mining

Protocollo

Conclusione

Riferimenti