La Rete Bitcoin

Valerio Vaccaro

Monday 26th February, 2024

1 Introduzione a Bitcoin

2 Architettura Peer-to-Peer e consenso decentralizzato

3 Bitcoin Full Node: verifica indipendente delle transazioni e utilizzo dedicato

4 Nodi di Simplified Payment Verification (SPV)

5 Cosa sono e come funzionano i Bloom Filters

6 Tor Transpor, Autenticazione e Crittografia Peer-to-Peer (BIP-150 e BIP-151)

7 Mining

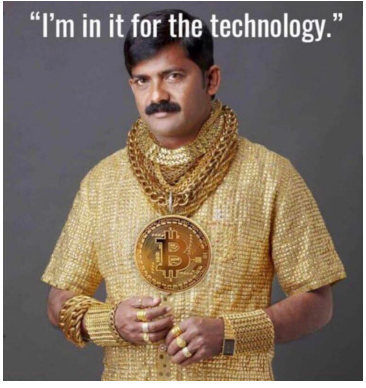
8 Mempool

9 Bibliografia

Chi sono?

- Valerio Vaccaro
- C64
- Laureato al Politecnico ...
- ... poi ci ho anche lavorato per 9 anni
- Hoya
- ...
- ...
- Eternity wall
- EU Blockhackathon 2018
- Blockstream
- Satoshi Spritz
- Officine Bitcoin

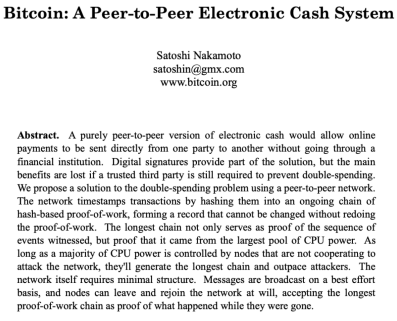
Meme



* entro la fine del corso capirete tutti i meme.

Da dove tutto ha avuto inizio

31 Ottobre 2008



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

La partenza della blockchain di Bitcoin avviene il 3 Gennaio 2009.

Caratteristiche di Bitcoin

"Bitcoin è una raccolta di concetti e tecnologie che formano le basi per un ecosistema di denaro digitale. Le unità di valuta chiamate bitcoin vengono utilizzate per immagazzinare e trasferire valore tra i partecipanti del network Bitcoin."
– Mastering Bitcoin
(tutta questa presentazione sarà fortemente basata su questo libro)

Caratteristiche di Bitcoin

- Denaro programmabile
- Totalmente distribuito
- Supply limitata (e no premine)
- Pseudo-anonimo
- Open-source
- Founder anonimo
- First-mover
- Grande e forte community
- ...

Unico nel panorama.

Reti Peer-to-Peer

Bitcoin è una rete peer-to-peer che non ha server centrali o architetture gerarchiche di controllo.
Tutti i nodi sono uguali e contribuiscono a formare l'infrastruttura di rete di Bitcoin.
Ritengo valide solo le informazioni che provengono dal mio nodo.

Consenso

Le regole di validazione delle informazioni provenienti da altri nodi sono il consenso, il mio nodo controlla il rispetto di tali regole.

Rete Bitcoin

I nodi sono pensati per funzionare in ogni contesto e specialmente nelle situazioni più critiche.

- Minimo consumo di risorse (o quantomento compatibile con hardware "casalingo")
- Minimo consumo di banda (funzionamento anche con reti mobili)
- Ridondanza della rete
- Robustezza del software
- ...

Grazie e queste sue caratteristiche è possibile mettersi un nodo in casa ed usarlo direttamente.

Rete Bitcoin

Le funzionalità base dei nodi sono:

- Network Routing Node
- Full blockchain
- Wallet
- Miner

Reti Bitcoin

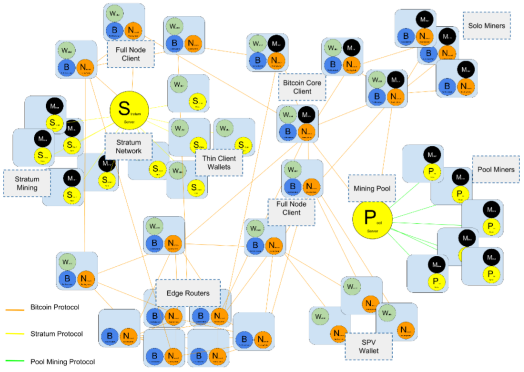
Ma ci sono anche software aggiuntivi che permetto tanto altro.

- Indicizzatori
- Timestamping
- Colored coin
- Second layer
- Sidechain

Opentimestamps

Ad esempio Opentimestamps è una architettura di server pubblici per l'attribuzione di una data certa ed immodificabile a qualsiasi documento digitale (anche a questa presentazione).

Reti Bitcoin



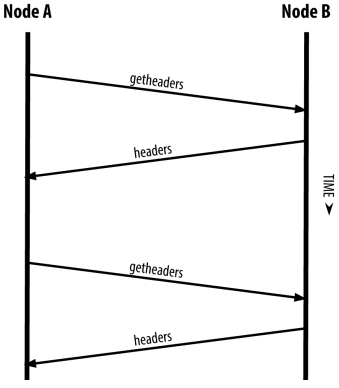
Reti Bitcoin

Protocollo P2P

Il protocollo P2P alla base di Bitcoin ha subito varie trasformazioni al fine di incrementare le performance (soprattutto temporali) della rete.
Il protocollo di discovery si basa su alcuni nodi noti (contattabili tramite specifici DNS) e da un protocollo di propagazione dell'identità ad altri nodi.
Il nostro nodo quindi si connetterà ad un subset di tutti i nodi della rete.

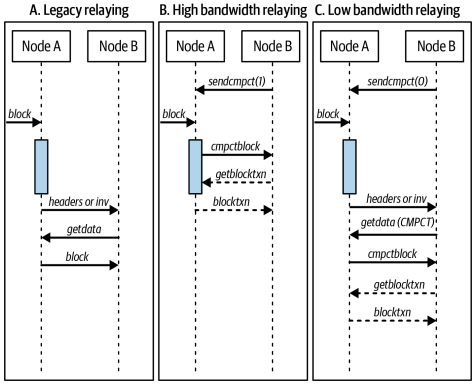
Protocollo P2P

Prosegue poi scaricando gli header dei blocchi e poi il contenuto dei blocchi stessi.



Fino ad aver scaricato e validato tutti i blocchi.

Protocollo P2P



Full node

I full node sono i nodi che contengono la copia completa di tutte le transazioni effettuate su Bitcoin.
Questo consente di:

- identificare le transazioni ricevute
- verificare l'esistenza dei fondi ricevuti

Ma non tutti i wallet sono capaci di avere a bordo un fullnode.

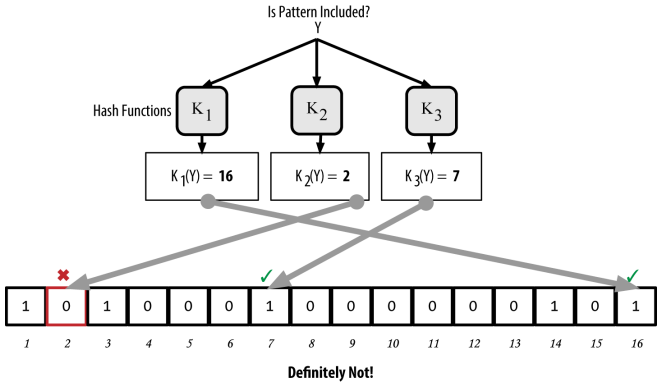
SPV

Simple Payment verification è un protocollo che consente di validare le transazioni senza avere copia delle blockchain completa.
I nodi SPV scaricano solo la lista degli header e poi chiedono ad altri full node una prova matematica della presenza di una certa transazione in un certo blocco.

Bloom Filters

I Bloom Filter sono una modalità per chiedere informazioni su un transazioni senza rivelare troppe informazioni su di essa.
Consentono di richiedere informazioni ad un nodo SPV senza dire esplicitamente cosa si stà cercardo, i nodi hanno indici basati su questi filtri e possono rispondere più velocemente (ma ovviamente riveleranno più informazioni di quelle necessarie).

Bloom Filters



Tor

"Tor (acronimo di The Onion Router) è un software libero, rilasciato su licenza BSD 3-Clause, che permette una navigazione anonima sul Web ed è basato sulla terza generazione del protocollo di rete di onion routing: tramite il suo utilizzo è molto più difficile tracciare o intercettare l'attività che l'utente compie su Internet, sia da parte di società commerciali che da parte di soggetti potenzialmente ostili."

DDOS

Tor è sotto un lunghissimo attacco DDOS! Potrebbe essere estremamente lento.

BIP-150, BIP-151, ...

BIP-150 e BIP-151 sono proposte per autenticare e crittare la comunicazione tra diversi nodi Bitcoin.
BIP-324 ha proposto ed implementato (a partire da Bitcoin Core 26) un protocollo di crittazione delle comunicazioni tra peer.

Mining

Il mining è il processo con cui viene creato un nuovo blocco ed aggiunto in cima alla catena.
Il miner sceglie le transazioni da inserire (tra quelle più remunerative) e prova al risolvere il puzzle crittografico associato.

Lezione sul mining

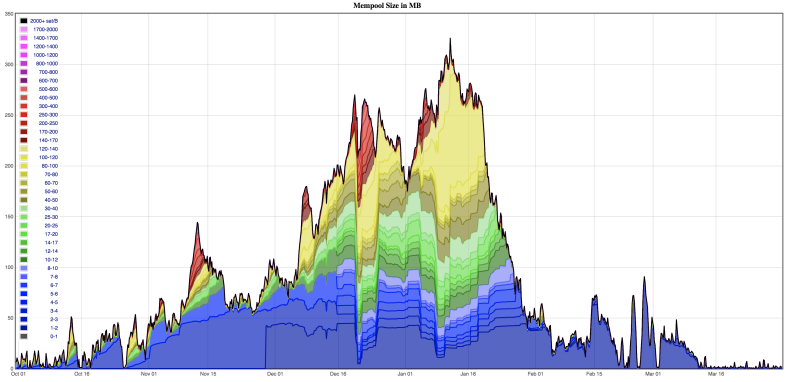
La terza lezione sarà dedicata esclusivamente al mining.

Mempool

La mempool è una area di memoria in cui vengono parcheggiate le transazioni non confermate mie o ricevute da un altro peer.
La mempool non è in consenso quindi ogni nodo può fare come gli pare.

- Mantenere tutte le transazioni non confermate
- Mantenere la lista delle transazioni non confermate fino ad un massimo di 100Mb e per un massimo di due settimane
- Non mantenere nessuna transazione in mempool
- Mantenere in mempool le sole transazioni effettuate il venerdì e con un numero di 7 dispari nella codifica esadecimale ... (inutile ma possibile)

Mempool


Mempool Size in MB
2000+ sat/B
1700-2000
1400-1700
1200-1400
1000-1200
800-1000
700-800
600-700
500-600
400-500
350-400
300-350
250-300
200-250
170-200
140-170
120-140
100-120
90-100
80-90
70-80
60-70
50-60
40-50
30-40
25-30
20-25
17-20
14-17
12-14
10-12
8-10
7-8
6-7
5-6
4-5
3-4
2-3
1-2
0-1
350
300
250
200
150
100
50
0
Oct 01
Oct 16
Nov 01
Nov 15
Dec 01
Dec 16
Jan 01
Jan 16
Feb 01
Feb 15
Mar 01
Mar 16

Mempool

Le transazione in mempool NON vanno considerate come confermate.

Bibliografia

- Andreas M. Antonopoulos, "Mastering Bitcoin", 2015
- Adam Back, "Hashcash-a denial of service counter-measure", 2002
- Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008
- Hal Finney, "Reusable Proofs of Work", 2004

Altre risorse

Tra le altre risorse utili mi piace citare:

- Ovviamente BitPolimi che ha organizzato queste lezioni.
- Satoshi Spritz - eventi serali a scadenze regolari per parlare di Bitcoin (a Milano ci incontriamo ogni mercoledì dalle 18).
- Ventuno - Podcast, raccolta di libri e materiali su Bitcoin.
- Officine Bitcoin - lezioni su telegram da 30 minuti per la risoluzione di problemi pratici.

Domande


BEH... EHM... SAREBBE A DÌ... CHE RISPETTO A STA COSA, CIOÈ, NE LA MISURA IN CUI... EHM... SE ANNAMO, SE FA PE' DÌ, A SVILUPPÀ UN DISCORSO SU LE STRUTTURE, CIOÈ, SUL CONTENUTO, TRA VIRGOLETTE...
AHO', MA CHE VOR DÌ?


"That's all Folks!"