Il Vero Capodanno di Bitcoin

Valerio Vaccaro

Satoshi Spritz Milano

9 Gennaio 2025

Valerio Vaccaro ∞

- 💻 Sviluppatore Bitcoin ed Esperto Hardware
- 🔥 Contributore a progetti Bitcoin open source
- ⚠️ Appassionato di hardware fai-da-te (DIY)
- Ingegnere Bitcoin e Liquid presso Blockstream

Social

- 🤦 **LinkedIn** linkedin.com/in/valeriovaccaro
- 🐙 **Github** github.com/valerio-vaccaro
- **Telegram** t.me/valeriovaccaro

Licenza

May this presentation inspire you to become more self-sovereign!

3 Gennaio 2009: Il Blocco Genesi

Il Blocco Zero

- **Data**: 3 Gennaio 2009, 18:15:05 UTC
- **Hash**: `000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f`
- **Ricompensa**: 50 BTC (non spendibili)
- **Messaggio**: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

Significato Storico

Il messaggio nel coinbase del blocco genesis rappresenta una critica esplicita al sistema finanziario tradizionale, evidenziando il contesto della crisi finanziaria del 2008-2009 che ha ispirato la creazione di Bitcoin.

Analisi delle Tempistiche: Primi Dieci Blocchi

Intervalli tra i Blocchi

Blocco	Data	Intervallo	Note
0 (Genesis)	3 Gen 2009, 18:15:05	-	Blocco iniziale
1	9 Gen 2009	~6 giorni	Primo blocco dopo genesis
2-9	9 Gen 2009	Variabile	Lento avvicinamento ai 10 minuti

Osservazioni

- **Inizio irregolare**: Il secondo blocco è stato minato 6 giorni dopo il genesis
- **Stabilizzazione**: I blocchi successivi si avvicinano gradualmente all'obiettivo di 10 minuti
- **Causa**: Satoshi Nakamoto era probabilmente l'unico miner attivo inizialmente

Stima dell'Hashrate dei Primi Blocchi

Parametri Iniziali

- **Difficoltà iniziale**: 1 (valore minimo possibile)
- **Target**: 1 blocco ogni 10 minuti (600 secondi)
- **Hardware**: Probabilmente un computer personale (CPU mining)

Calcolo Stimato

Con difficoltà = 1 e tempo medio di 10 minuti:

```
Hashrate = Difficoltà × 2^32 / Tempo_target
Hashrate = 1 × 4,294,967,296 / 600
Hashrate = 7,158,278 hash/secondo
Hashrate = 7.16 MH/s (Megahash al secondo)
```

Stima dell'Hashrate dei Primi Blocchi

Confronto Storico

- **Gennaio 2009**: ~7 MH/s (stimato)
- **2010**: ~100 MH/s
- **2011**: ~10 GH/s
- **2025**: ~1 ZH/s (Zettahash = 10^21 hash/s)

Crescita: Da 7 MH/s a 1 ZH/s in 16 anni = aumento di ~140 miliardi di volte!

Spiegazione Avanzata: Calcolo dell'Hashrate

Il Principio Fondamentale

Per avere un blocco ogni 10 minuti in media su Bitcoin quando la **difficulty è esattamente 1** (il valore minimo, come nel genesis block e nelle fasi iniziali della rete), serve un hashrate di rete di circa **7 MH/s** (7 milioni di hash al secondo).

Meccanismo di Bitcoin

Bitcoin è progettato per mantenere un tempo medio tra i blocchi di **600 secondi** (10 minuti), indipendentemente dall'hashrate totale della rete.

- **Difficulty**: quante volte è più difficile trovare un blocco rispetto al caso base (difficulty $= 1$)
- **Difficulty $= 1$**: il target è il massimo possibile (blocco deve avere hash $<$ valore molto grande, circa con 8 zeri esadecimali iniziali)
- **In media servono**: $2^{32} \times$ difficulty hash per trovare un blocco valido
- **A difficulty $= 1$**: mediamente servono $\mathbf{2^{32} = 4.294.967.296}$ **hash per blocco**

Spiegazione Avanzata: Calcolo dell'Hashrate

Calcolo dell'Hashrate Necessario

La formula quindi risulta:

`Network hashrate = (difficulty × 2^32) / target`

Con **difficulty = 1** e per **target = 600** ovvero tempo medio di 10 minuti (600 secondi) otteniamo:

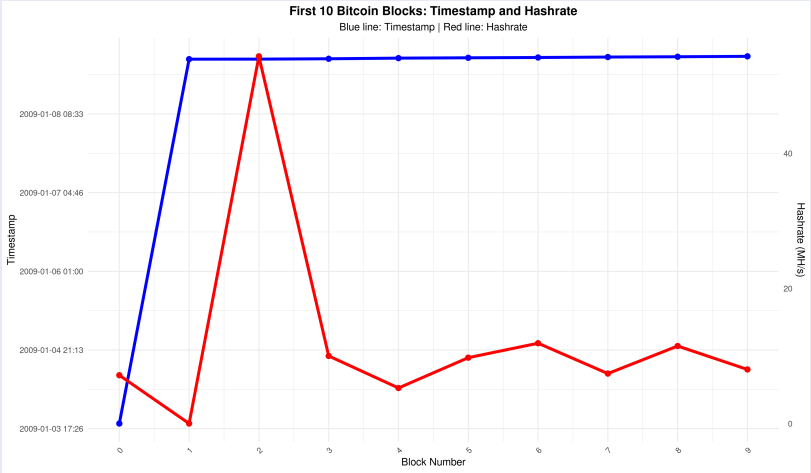
`(1 × 4.294.967.296) / 600 = 7.158 MH/s`

Contesto Storico e Attuale

- **2009**: Satoshi Nakamoto aveva all'inizio ~7 MH/s con la CPU del suo computer
- **Gennaio 2026**:
  - Difficulty: ~148 trilioni
  - Hashrate di rete: ~1 zettahash/s (1.000 EH/s)
- **Principio identico**: più hashrate → difficulty sale per tenere i blocchi a ~10 minuti

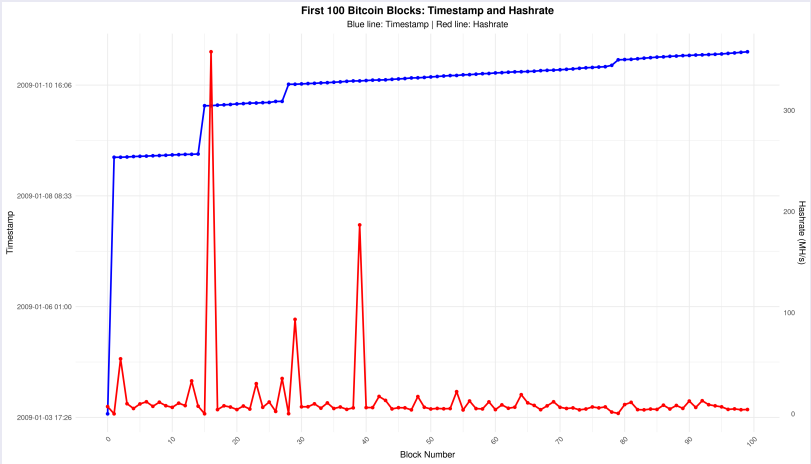
Stima dell'Hashrate dei Primi Blocchi

Grafico: Timestamp e Hashrate dei Primi 10 Blocchi



Primi 100 Blocchi: Analisi Completa

Grafico: Timestamp, Hashrate e Intervalli tra Blocchi



Analisi del Grafico

Analisi Dettagliata: Primi 10 Blocchi

Caratteristiche Tecniche

- **Blocco 0**: Non ha riferimento a blocco precedente (genesis)
- **Blocco 1**: Primo blocco con riferimento al genesis
- **Difficoltà**: Mantenuta a 1 per i primi blocchi
- **Ricompensa**: 50 BTC per blocco (halving ogni 210,000 blocchi)

Implicazioni

- La bassa difficoltà iniziale permetteva il mining con CPU
- L'irregolarità dei tempi riflette la natura sperimentale della rete
- Satoshi ha probabilmente minato i primi blocchi da solo
- La rete si è stabilizzata con l'ingresso di nuovi miner

Caratteristiche del Blocco 1

Dettagli Tecnici

Caratteristica	Valore
Numero Blocco	1
Hash	00000000839a8e6886ab5951d76
Hash Blocco Precedente	000000000019d6689c085ae1658 (Genesis)
Timestamp	9 Gennaio 2009, 02:54:25 UTC
Versione	1
Merkle Root	Hash della transazione coinbase
Nonce	2573394689

Caratteristiche del Blocco 1

Dettagli Tecnici

Caratteristica	Valore
Difficoltà	1
Dimensione	215 bytes
Transazioni	1 (solo coinbase)
Ricompensa	50 BTC

Significato Storico

- **Primo blocco dopo il Genesis**: Collega il blocco genesis alla blockchain
- **Prima transazione spendibile**: La ricompensa del blocco 1 è tecnicamente spendibile
- **Conferma della rete**: Dimostra che il sistema funzionava correttamente
- **Intervallo di mining**: Minato ~6 giorni dopo il blocco genesis (se c'è stato un fork non lo sapremo mai)

Il Significato del 3 Gennaio

Perché questa Data?

- **Contesto storico**: Crisi finanziaria globale 2008-2009
- **Messaggio politico**: Critica al sistema bancario tradizionale
- **Simbolismo**: Inizio di un nuovo sistema finanziario decentralizzato
- **Anniversario**: Ogni 3 gennaio celebriamo la nascita di Bitcoin (o forse no)

Impatto Storico

Il 3 gennaio 2009 ha segnato l'inizio di una rivoluzione finanziaria che continua ancora oggi, dimostrando la resilienza e la sicurezza di un sistema decentralizzato. **Ma è partito tutto proprio il 3 di Gennaio?**

E il 9 Gennaio?

Il primo blocco aggiunto alla blockchain è stato il 9 Gennaio!

E ancora i primi blocchi sono rallentati rispetto allo standard di Bitcoin ma cosa è successo?

- **Fork**: c'è staro qualche problema sulla blockchain? è stata forkata per un errore? non lo sapremo mai ...
- **Performance/bug di mining**: ci sono stati problemi di performance? era buggato il mining?
- **Aggiornamenti di windows**: magari Satoshi ha fatto l'errore di riavviare installando gli aggiornamenti di windows ...

Festeggiamo anche il 9 Gennaio!!!

Evoluzione dell'Hashrate

Crescita Esponenziale

```
2009:  ~7 MH/s      (CPU mining)
2010:  ~100 MH/s    (GPU mining inizia)
2011:  ~10 GH/s     (GPU mining diffuso)
2013:  ~1 TH/s      (ASIC mining inizia)
2016:  ~1 PH/s      (ASIC mining diffuso)
2020:  ~100 EH/s    (ASIC avanzati)
2025:  ~1 ZH/s      (Stato attuale)
```

Implicazioni per la Sicurezza

- **Maggiore hashrate** = Maggiore sicurezza della rete
- **Costo di attacco**: Diventa economicamente impraticabile
- **Decentralizzazione**: Migliaia di miner distribuiti globalmente
- **Resilienza**: La rete è più forte che mai

Conclusioni

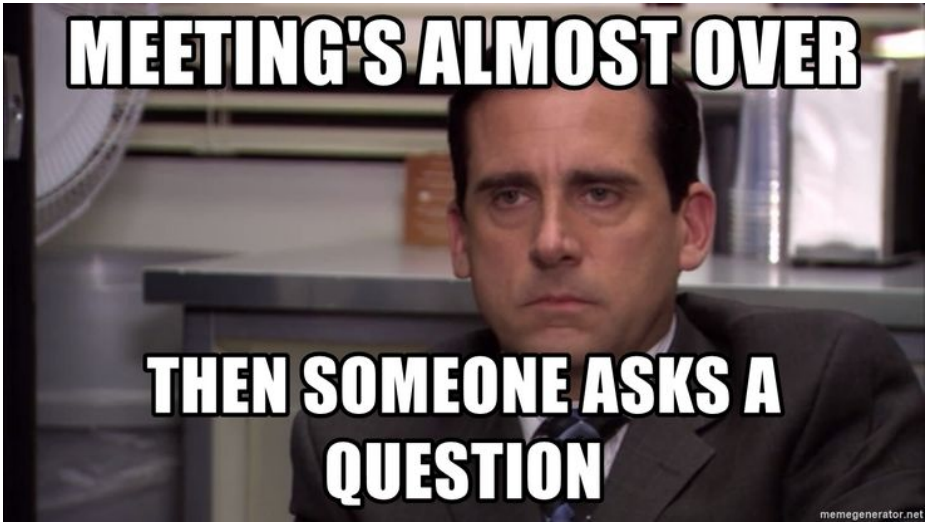
Punti Chiave

- Il **3 gennaio 2009** segna l'inizio della blockchain di Bitcoin
- I **primi blocchi** mostrano l'evoluzione da rete sperimentale a sistema globale
- L'**hashrate iniziale** era estremamente basso (~7 MH/s) rispetto ad oggi (~1 ZH/s)
- La **crescita esponenziale** dell'hashrate dimostra la forza e la sicurezza della rete

Significato per il Futuro

Bitcoin continua a dimostrare la sua resilienza e sicurezza attraverso la crescita costante dell'hashrate e la decentralizzazione della rete. Il blocco genesis rimane un simbolo della visione originale di Satoshi Nakamoto.

? Domande


MEETING'S ALMOST OVER
THEN SOMEONE ASKS A QUESTION
memegenerator.net

Bibliografia

- Bitcoin Whitepaper: “Bitcoin: A Peer-to-Peer Electronic Cash System” - Satoshi Nakamoto (2008)
- Blockchain Explorer: blockstream.info
- Bitcoin Core Repository: github.com/bitcoin/bitcoin
- Genesis Block Analysis: blockchain.info/block/0

Progetto Satoshi Spritz

- 💻 Federazione di gruppi locali di Bitcoiner
- 🎓 Eventi gratuiti e privacy oriented
- 🤖 BITCOIN ONLY
- 🔧 Satoshi Spritz Connect online settimanale
- 📖 Orientato all'apprendimento della self-sovereign
- 🍕 Tutte le settimane un evento online -> Satoshi Spritz Connect

Links

- satoshispritz.it
- t.me/SatoshiSpritzConnect

Officine Bitcoin

- Comunità Italiana di Bitcoiners, totalmente gratuita
- BITCOIN ONLY
- Focus su educazione e sviluppo di progetti
- Progetti:
  - Sviluppo nodi Bitcoin
  - Uso di Hardware Wallet
  - Filosofia open source
  - Installazione di Debian
  - Mnemoniche & Dadi
  - . . . e molto altro

Links

- officinebitcoin.it