IL VERO CAPODANNO DI BITCOIN

Analisi Storica e Forense (3 Gen vs 9 Gen)

Satoshi Spritz Cagliari

12 Gennaio 2025

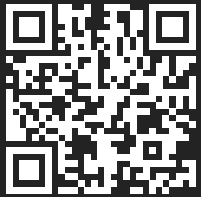
Basato sulla ricerca di Valerio Vaccaro

Intro & Credits

Attribuzione e Licenza

Autore Originale: Valerio Vaccaro

- Sviluppatore Bitcoin ed Esperto Hardware
- Ingegnere Bitcoin e Liquid presso Blockstream
- Founder Satoshi Spritz Milano



Valerio Vaccaro

Licenza CC BY-SA 4.0

3 Gennaio: Il Mito

Il Blocco Zero (Genesis)

Dati Tecnici:

- **Data:** 3 Gennaio 2009, 18:15:05 UTC
- **Hash:** `000000000019d6689c085ae1658...`
- **Ricompensa:** 50 BTC (Non spendibili)

Il Messaggio nella Coinbase

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

Significato Storico

Il messaggio è una critica esplicita al sistema finanziario tradizionale.

- Contesto: Crisi finanziaria 2008-2009.
- Simbolismo: Inizio di un nuovo sistema decentralizzato.

Ma è partito tutto davvero il 3 Gennaio?


THE TIMES

Saturday January 3 2009

£1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Israel prepares to send tanks and troops into Gaza

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Salman Rushdie I won't marry again

Giant killing? Guide to the FA Cup third round

99p

Analisi Tempistiche e Hashrate

Analisi Primi Blocchi: La "Partenza a Razzo"

Blocco	Data (UTC)	Intervallo	Stato Rete
0	3 Gen 18:15	-	Genesis (Hardcoded)
1	**9 Gen 02:54**	**6 Giorni**	**START UFFICIALE**
2	9 Gen 02:55	1 minuto	*Funzionamento Perfetto*
...	...	...	...
14	9 Gen 05:16	$\sim$ 10 min	*Marcia Regolare*

Conclusione: Il 9 Gennaio il software funzionava benissimo. Nessun "inizio lento".

L'Incidente del 9 Gennaio: La "Sosta ai Box"

Analizzando il timestamp dei blocchi, emerge un'anomalia ancora più interessante.

Il Buco di 24 Ore

Blocco 14: 9 Gennaio, ore 05:33 GMT+1

Blocco 15: 10 Gennaio, ore 05:45 GMT+1

Dopo una partenza sprint (14 blocchi in 3 ore),
Bitcoin si ferma per quasi un giorno intero.

Perché?

Coincide esattamente con qualcosa che vediamo più avanti.

STOP OPERATIVO

Mining fermo per 24h

Spiegazione Avanzata: La Matematica del Mining

Il Principio Fondamentale (2^{32})

Per avere un blocco ogni 10 minuti quando la **Difficoltà è 1** (il minimo, come nel 2009), la statistica impone che servano circa **4.29 Miliardi di tentativi** (2^{32}) per trovare l'hash giusto.

Il Meccanismo

Il protocollo Bitcoin aggiusta la difficoltà per mantenere il target di **600 secondi**.

- **Difficoltà 1:** È il livello base. L'hash deve iniziare con circa 8 zeri.
- **Sforzo Richiesto:** 2^{32} hash per blocco.
- **Calcolo:** $2^{32} = 4.294.967.296$ hash.

Ecco perché servivano circa 7 Milioni di hash al secondo (7 MH/s) per trovarne uno in 10 minuti.

Stima Hashrate Iniziale (La Matematica)

Parametri: Difficoltà $= 1$ (Minima). Target $= 600$ secondi (10 min).

Formula Hashrate

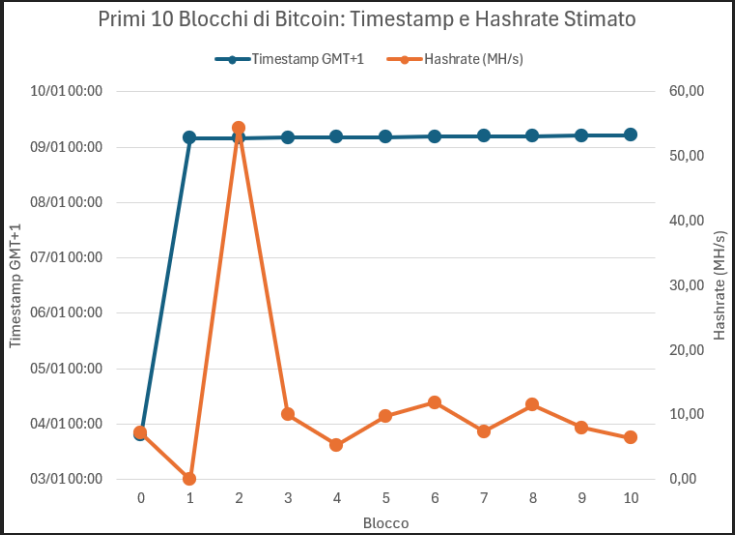
$$\text{Hashrate} = \frac{\text{Difficulty} \times 2^{32}}{\text{Tempo Target}}$$

Calcolo per i primi blocchi:

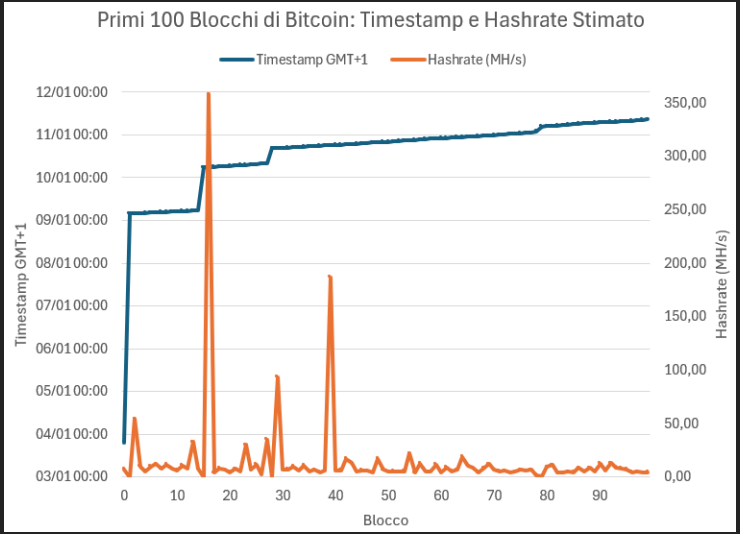
$$\text{Hashrate} = \frac{1 \times 4.294.967.296}{600} \approx \mathbf{7.16}\ \text{MH/s}$$

Questo conferma l'uso di una semplice **CPU** (Computer domestico dell'epoca).

Grafici: Timestamp e Hashrate



Grafici: Intervalli tra Blocchi



Il Mistero dei 6 Giorni

Le Ipotesi sul "Buco" (3-9 Gennaio)

Il primo blocco reale è del 9 Gennaio. Cosa è successo nel mezzo?

1. **Fork?** C'è stato un problema sulla blockchain e una ripartenza nascosta?
2. **Windows Update?** Satoshi ha riavviato per aggiornare il PC?
   (Nota ironica di Valerio... ma forse i crash di Windows erano reali!)
3. **Bug/Sviluppo?** Il software non era ancora pronto?

Le prove forensi puntano all'ultima ipotesi.

La Prova 1: L'Annuncio Ufficiale

Sappiamo per certo che l'annuncio sulla *Cryptography Mailing List* è arrivato l'8 Gennaio.

Bitcoin v0.1 released

Satoshi Nakamoto satoshi at vistomail.com
Thu Jan 8 14:27:40 EST 2009

- Previous message: [tmoore at seas.harvard.edu: [fc-announce] Financ
- Next message: MD5 considered harmful today, SHA-1 considered ha
- **Messages sorted by:** [date] [thread] [subject] [author]

Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.

See bitcoin.org for screenshots.

Download link:
http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar

Windows only for now. Open source C++ code is included.

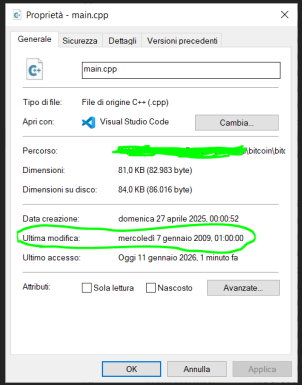
8 Gennaio 2009

"Announcing the first release of Bitcoin..."

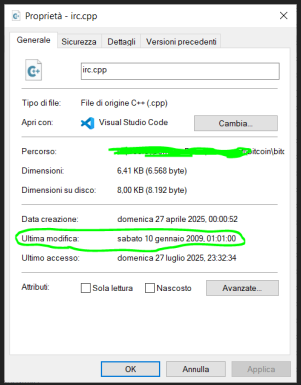
Fino a questa data, il software non era pubblico. Il mining decentralizzato non poteva esistere.

La Prova 2: I File Parlano

Abbiamo analizzato i timestamp dei file sorgente nello zip di `bitcoin-0.1.0`.



7 Gennaio: Il codice è stato finalizzato 4 giorni *dopo* il "Genesis" del 3 Gennaio.



10 Gennaio: I file `irc.cpp` e `.exe` mostrano una "patch silenziosa" post-lancio!

La Prova 3: L'Incidente del 9 Gennaio (23h Stop)

Analizzando i timestamp, emerge un'anomalia (il "Crash") e una prova di isolamento.

Il Buco Operativo:

- **Blocco 14:** 9 Gen, 04:33 UTC
- **Blocco 15:** 10 Gen, 04:45 UTC

La Timeline Forense:

1. **Fix File:** 10 Gennaio (Data file System)
2. **Restart (B.15):** 10 Gen, 04:45 UTC
3. **Mail a Hal:** 10 Gen, 19:52 UTC (11:52 AM PST)

Conclusione

Il Blocco 15 è stato minato **15 ore prima** che Hal ricevesse la mail col fix.

Satoshi stava minando da solo mentre testava la patch.

La Deduzione Finale: L'Isolamento Forzato

Il Paradosso del Blocco 1

Il Blocco 1 è stato minato il **9 Gennaio**. Ma il fix per le connessioni IRC (`irc.cpp`) è del **10 Gennaio**.

La Deduzione:

- Satoshi risponde a Hal il **10 Gen (11:52 AM)**: *"Surprised there was a crash"*.
- Se Hal crashava o aveva il bug IRC, non poteva connettersi.
- Hal twitta "Running bitcoin" solo l'11 Gennaio.

Conclusione

Per circa 24 ore, Satoshi è stato l'unico nodo della rete. Indipendentemente da quando Hal ha ricevuto il codice, **il bug ha isolato Satoshi**.

La Soluzione del Mistero

Combinando Mail, File, timestamp della blockchain e Crash Report:

1. **3-7 Gennaio:** Sviluppo e Code Freeze (Genesis hardcoded).
2. **8 Gennaio:** Rilascio pubblico.
3. **9 Gennaio:** Start (14 Blocchi) $\rightarrow$ CRASH/BUG $\rightarrow$ Stop di 24 ore.
4. **10 Gen:** Satoshi fixa (‘irc.cpp‘) e riparte (Blocco 15).
5. **10 Gen:** Satoshi continua ad indagare con il supporto di Hal.
6. **11 Gen:** Hal riceve la versione 0.1.3 funzionante e twitta "Running Bitcoin".

Bonus: Il Codice "Fantasma" (3-8 Gennaio)

La Teoria

"Satoshi ha inviato il codice privatamente tra il 3 e l'8 Gennaio?"

Indizi PRO:

- **Timestamp:** Il codice era pronto il 7 Gennaio.
- **Precedenti:** Aveva già inviato versioni private nel 2008.

Indizi CONTRO:

- **Nessuna Mail:** Hal Finney ha pubblicato tutte le sue mail con Satoshi. La prima sul crash è del 10 Gennaio. Se ci fosse una mail del 7 Gennaio, perché manca?

In ogni caso, il Punto 3 (Isolamento Tecnico) conferma che il mining è stato solitario.

Bonus: La Teoria del Complotto (Debunked)

C'è un dettaglio ironico sulla patch del 10 Gennaio che smentisce molte teorie.

Il Calendario

10 Gennaio 2009

era un

SABATO

Satoshi $\neq$ Ente Governativo

"Gli impiegati della CIA/NSA non lavorano il sabato per fixare bug su IRC."

Questo dettaglio rafforza la tesi dello sviluppatore solitario (o gruppo cypherpunk) appassionato, che lavora nel weekend per salvare la rete appena nata.

9 Gennaio: La Rete è Viva

Dettagli Blocco 1

Il vero motore si accende il 9 Gennaio alle 02:54:25 UTC.

Caratteristica	Valore
Hash	00000000839a8e...
Nonce	2573394689
Transazioni	1 (Coinbase)
Difficoltà	1

Significato:

- Collega il Genesis alla Blockchain.
- Rende la ricompensa "tecnicamente" spendibile.
- Conferma che il sistema funziona.

Evoluzione Hashrate: 2009 vs 2025

La crescita è stata esponenziale.

- **2009:** ~ 7 MH/s (CPU Mining)
- **2010:** ~ 100 MH/s (GPU Mining)
- **2013:** ~ 1 TH/s (ASIC Era)
- **2016:** ~ 1 PH/s
- **2025:** ~ 1 ZH/s (Zettahash $= 10^{21}$ h/s)

Crescita totale: $\sim$ 140 miliardi di volte in 16 anni.
Maggiore hashrate = Sicurezza economica assoluta.

Conclusioni

Conclusioni

Punti Chiave

- Il **3 Gennaio** è la data simbolica (Manifesto Politico).
- Il **9 Gennaio** è la data operativa (Start della Rete).
- L'analisi forense conferma che il gap di 6 giorni è stato tempo di **sviluppo software**, non di mining.

Buon Compleanno Bitcoin (doppio)!

Risorse e Bibliografia

Le Fonti dell'Indagine

Per chi vuole verificare personalmente i dati presentati:

Fonti Primarie (Prove):

- **Mail 8 Gennaio:** Annuncio Release (Metzdowd Archive)
- **Mail 10 Gennaio:** Segnalazione Crash (The Wall Street Journal)
- **Tweet 11 Gennaio:** "Running bitcoin" (Twitter/X)

Analisi e Codice:

- **Nakamoto Institute:** Archivio versioni storiche
- **Genesis Block Analysis:** Block explorer
- **Analisi Forense:** Screenshot diretti dall'archivio `bitcoin-0.1.0.rar` (Hotfix Version).

Tutti i link sono verificabili pubblicamente per confermare la timeline 3-10 Gennaio.

Rimaniamo in Contatto

SATOSHI SPRITZ

Grazie a tutti per la partecipazione!

SS Cagliari

Sito Web

SS Connect

Officine Bitcoin