Bitcoin Whitepaper

Struttura, contenuto e storia del paper originale di Satoshi

Valerio Vaccaro

Satoshi Spritz Connect

17 Marzo 2026

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

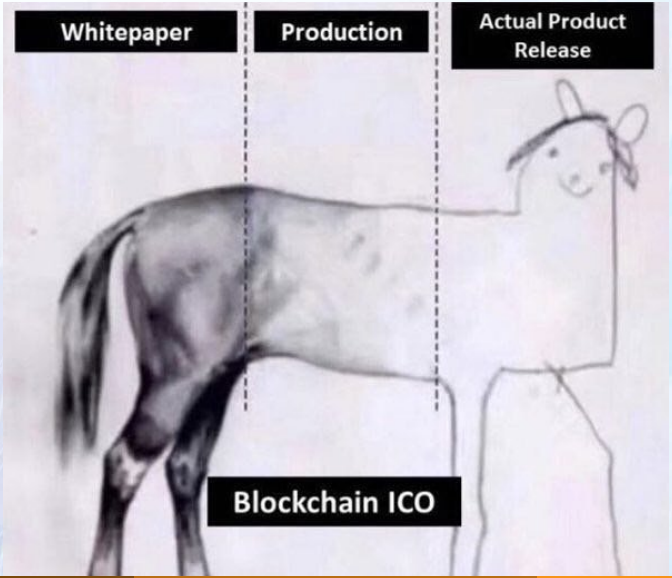
Social

- 🧑‍💼 **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!

Meme


Whitepaper
Production
Actual Product Release
Blockchain ICO

Sommario

- Storia: Satoshi e la nascita di Bitcoin
- Struttura del whitepaper (12 sezioni)
- Concetti chiave: transazioni, proof-of-work, rete
- Incentivi, privacy, verifica semplificata
- Riferimenti e risorse

Storia: Il Whitepaper (2008)

31 Ottobre 2008

- **"Bitcoin: A Peer-to-Peer Electronic Cash System"** pubblicato sulla mailing list di crittografia
- Autore: **Satoshi Nakamoto** (pseudonimo, identità sconosciuta)
- Risolse il **problema del double-spending** che affliggeva le valute digitali precedenti
- Combinò: hashing crittografico, proof-of-work (Hashcash), rete peer-to-peer

Contesto

- Crisi finanziaria 2008: fiducia nelle banche erosa
- Basato su: b-money (Wei Dai), Hashcash (Adam Back), timestamping (Haber & Stornetta)

Storia: Genesis Block (2009)

3 Gennaio 2009

- 🚀 Satoshi minò il **Block #0** (blocco genesi)
- 🪙 Ricompensa di 50 BTC all'indirizzo `1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa` (non spendibile per design)
- 📰 Messaggio coinbase: *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"*

9 Gennaio 2009

- 💻 Bitcoin v0.1 rilasciato su SourceForge
- 🔗 bitcoin.org registrato

Satoshi e la scomparsa

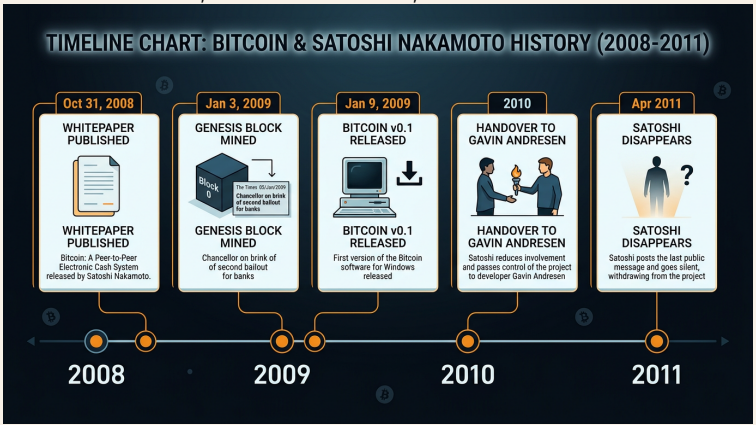
Timeline

- **Ott 2008 – Apr 2011**: Sviluppo e comunicazione attivi
- **Fino a metà 2010**: Controllava tutte le modifiche al codice sorgente
- **2010**: Trasferì il controllo a Gavin Andresen e altri sviluppatori
- **2011**: Ultimo messaggio: *"I've moved on to other things"* — scomparso

Satoshi e la scomparsa

Eredità

- ~1,1M BTC stimati (mai spostati dai blocchi iniziali)
- Nessuna autorità centrale, nessuna azienda, nessun token del fondatore



Struttura del Whitepaper (12 Sezioni)

1. **Introduzione** — Problemi del modello basato sulla fiducia
2. **Transazioni** — Catena di firme digitali
3. **Timestamp Server** — Catena di hash per l'ordinamento
4. **Proof-of-Work** — Voto CPU, consenso
5. **Rete** — Passi per far funzionare la rete
6. **Incentivo** — Ricompensa blocco, commissioni
7. **Recupero spazio disco** — Alberi di Merkle
8. **Verifica pagamento semplificata** — SPV, client leggeri
9. **Combinare e dividere valore** — Input/output multipli
10. **Privacy** — Chiavi pubbliche pseudonime
11. **Calcoli** — Probabilità di successo dell'attaccante
12. **Conclusione** — Riepilogo del sistema

1. Introduzione

Problema: pagamenti basati sulla fiducia

- Istituzioni finanziarie come terze parti fidate
- **Transazioni non reversibili** impossibili (costi di mediazione)
- **Double-spending** richiede una parte fidata per prevenirlo
- **Frode** accettata come inevitabile

Soluzione

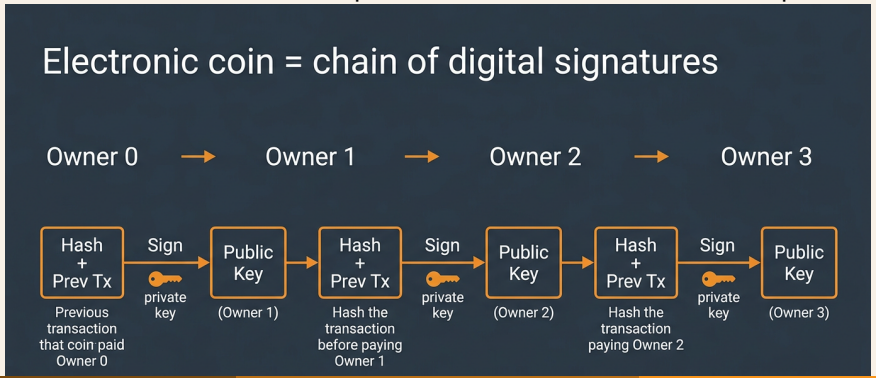
- **Prova crittografica** invece della fiducia
- **Timestamp server distribuito** peer-to-peer
- Sicuro se i nodi onesti controllano la maggioranza della potenza CPU

Moneta elettronica = catena di firme digitali

- Ogni proprietario trasferisce la moneta firmando: *hash(tx_precedente) + chiave_pubblica_prossimo_proprietario*
- Il beneficiario verifica le firme per verificare la catena di proprietà

Problema del double-spending

- ⚠️ Il beneficiario non può verificare che i proprietari precedenti non abbiano fatto double-spend
- 🔑 **Modello mint** (autorità fidata): destino del sistema dipende da un'entità
- ✅ **Bitcoin**: Transazioni annunciate pubblicamente; **ordine** concordato per consenso



3. Timestamp Server

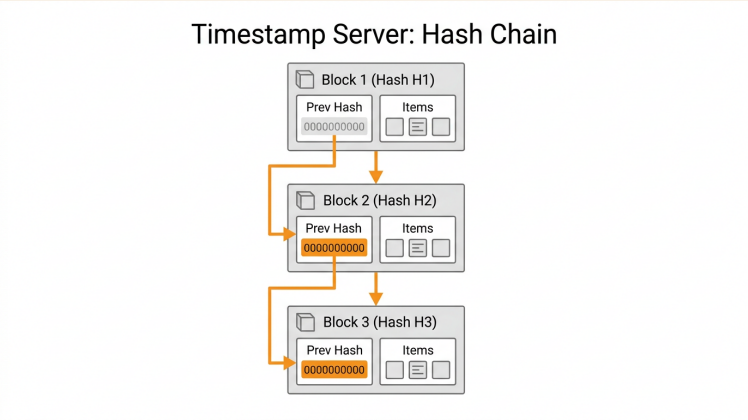
Catena di hash

- Hash del blocco di elementi → timestamp
- Ogni timestamp **include l'hash precedente** → catena
- Ogni nuovo timestamp rafforza i precedenti

3. Timestamp Server

Dal paper

- *"The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash."*



4. Proof-of-Work

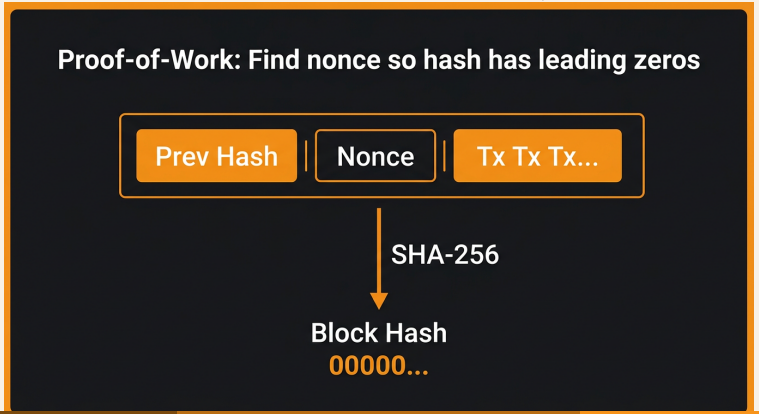
PoW stile Hashcash

- ⚙ Trovare nonce tale che hash(blocco) abbia **bit zero** all'inizio
- 🔑 Lavoro esponenziale nei bit zero; verifica = singolo hash
- 🛡 Il blocco non può essere modificato senza rifare il lavoro

4. Proof-of-Work

Meccanismo di consenso

- 📈 **Un-CPU-un-voto** (non un-IP-un-voto)
- ✅ **Catena più lunga** = decisione della maggioranza
- ⚙ **Regolazione difficoltà**: media mobile, target blocchi/ora

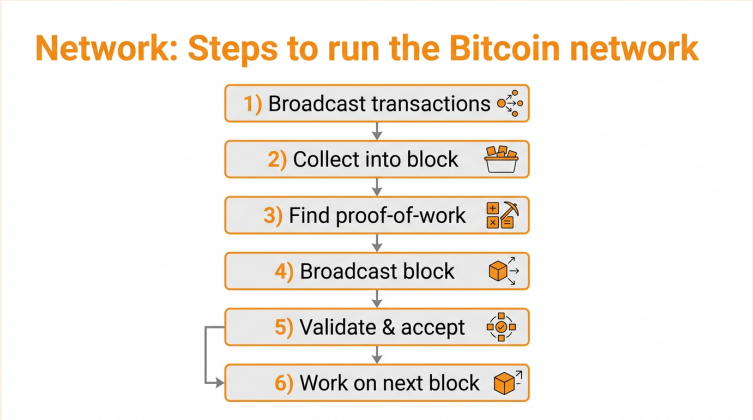


Passi

1. Nuove transazioni trasmesse a tutti i nodi
2. Ogni nodo raccoglie le transazioni in un blocco
3. Ogni nodo lavora sul proof-of-work per il suo blocco
4. Quando trovato $\rightarrow$ trasmette il blocco
5. I nodi accettano se le transazioni sono valide e non spese
6. Esprimono accettazione lavorando sul blocco successivo (hash del blocco accettato come prev hash)

Risoluzione parità

- 🔗 Due blocchi simultaneamente? Lavorare sul primo ricevuto, tenere l'altro ramo
- ✅ Prossimo PoW trovato → un ramo più lungo → passare a quello



6. Incentivo

Ricompensa blocco

- 🪙 Prima tx nel blocco = **nuova moneta** al creatore del blocco
- ⚙ Analogamente ai minatori d'oro che spendono risorse
- 📈 Costante di nuove monete → poi transizione a **solo commissioni** (zero inflazione)

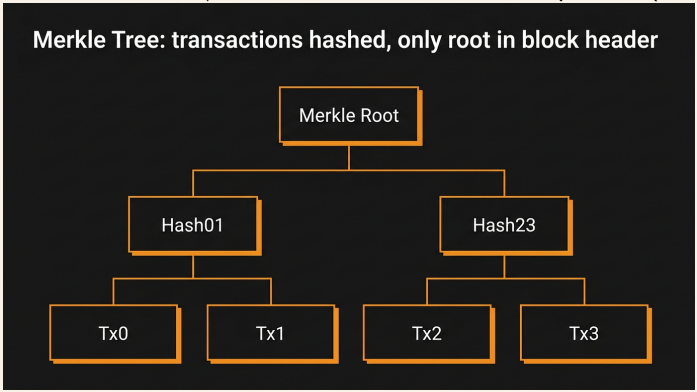
Incentivo all'onestà

- 🛡 Attaccante con più CPU: frodare vs generare nuove monete
- ✅ Più profittevole rispettare le regole

7. Recupero spazio disco

Albero di Merkle

- Transazioni hashed in **albero di Merkle**; solo root nell'header del blocco
- Transazioni spese possono essere potate (rami stub)
- ~80 byte/header blocco $\times$ 6/ora $\times$ 24 $\times$ 365 $\approx$ **4,2 MB/anno** (stima 2008)



8. Verifica pagamento semplificata

Client leggeri

- 🔑 Mantenere solo gli **header dei blocchi** della catena più lunga
- 🔗 Ottenere il **ramo Merkle** che collega la tx al blocco
- ✅ Verificare che la rete l'abbia accettata; blocchi dopo = ulteriore conferma

Caveat

- ⚠️ Affidabile se i nodi onesti controllano la rete; vulnerabile se l'attaccante la sovrasta

9. Combinare e dividere valore

Input/output multipli

- ⚙ Le transazioni hanno **input e output multipli**
- 🔑 Singolo input da tx più grande, o input multipli che combinano importi minori
- ✅ Al massimo due output: pagamento + resto

Nessuna storia completa necessaria

- 🔗 Fan-out (tx dipende da molte) — nessun bisogno di estrarre copia standalone completa

10. Privacy

Pseudonimato

- Tutte le transazioni **pubbliche** — ma le chiavi pubbliche possono essere **anonime**
- Come il “nastro” della borsa: tempo e dimensione pubblici, parti sconosciute

Best practice

- **Nuova coppia di chiavi per transazione** per evitare collegamenti
- Tx multi-input rivelano che gli input appartengono allo stesso proprietario

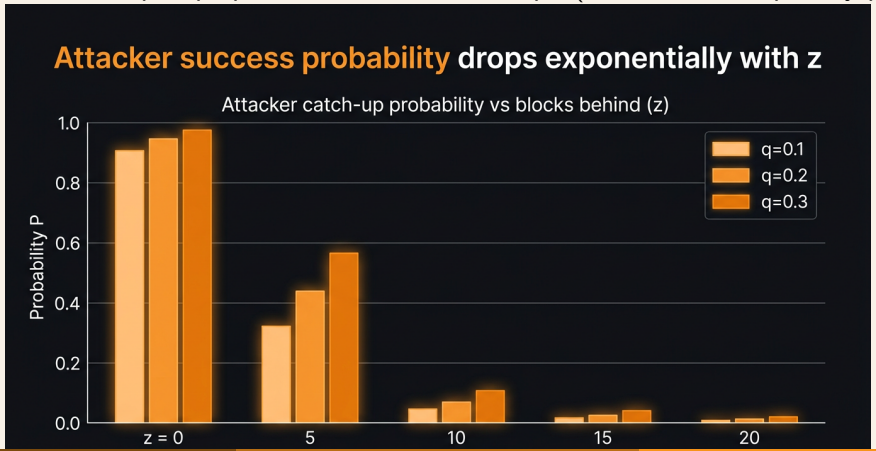
11. Calcoli

Probabilità di recupero dell'attaccante

- **Gambler's Ruin**: probabilità che l'attaccante recuperi da z blocchi indietro
- Cala **esponenzialmente** con z
- P $<$ 0,1%: q=0,10 $\rightarrow$ z=5; q=0,30 $\rightarrow$ z=24; q=0,40 $\rightarrow$ z=89

Attesa conferma

- ⚙ Il destinatario aspetta tx + z blocchi
- 🛡 Il mittente non può preparare la catena in anticipo (destinatario dà pubkey poco prima)



12. Conclusione

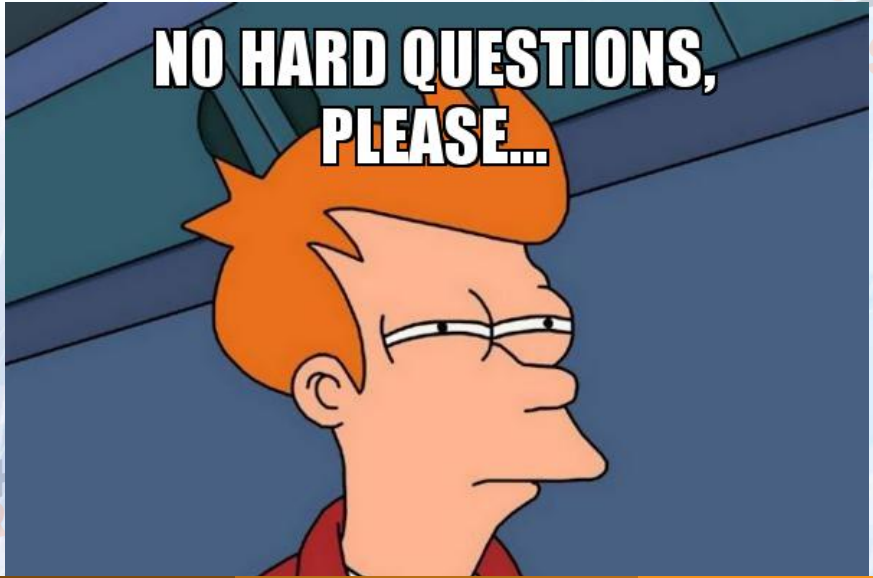
Riepilogo

- Transazioni elettroniche **senza fiducia**
- Monete = firme digitali; PoW previene double-spending
- Peer-to-peer; nodi votano con CPU; struttura minima
- Uscire/rientrare a piacere; catena più lunga = prova della storia

Principi di design

- ✅ Semplicità non strutturata
- ✅ Nessuna identificazione richiesta
- ✅ Consegna messaggi best-effort

? Domande



Riferimenti

Whitepaper

- bitcoin.org/bitcoin.pdf — PDF originale
- bitcoin.org/it/documento-bitcoin — Versione web, traduzioni

Lavori precedenti citati

- Wei Dai: b-money (1998)
- Adam Back: Hashcash (2002)
- Haber & Stornetta: Timestamping (1991, 1993, 1997)
- Merkle: Alberi di Merkle (1980)

Satoshi Spritz

- 💻 Federazione di gruppi locali di Bitcoiner
- 🎓 Eventi gratuiti e privacy oriented
- 🤖 BITCOIN ONLY
- 🔧 Satoshi Spritz Connect online settimanale

Links

- satoshispritz.it
- t.me/SatoshiSpritzConnect

Officine Bitcoin

- 🤝 Comunità Italiana di Bitcoiners, totalmente gratuita
- 🤖 BITCOIN ONLY
- 🎓 Focus su educazione e sviluppo di progetti

Links

- officinebitcoin.it

Bitcoinissimo

- Podcast Bitcoin e statistiche
- Episodi in italiano, inglese, ungherese, cinese, russo, spagnolo, francese
- Statistiche rete in tempo reale, dati di mercato, block explorer

Links

- bitcoinissimo.it