Consenso, fork e compagnia cantante

👤 Valerio Vaccaro

₿ Satoshi Spritz Monza

📅 2025-10-02

👤 Chi sono? 👀

- 💻 Sviluppatore Bitcoin ed Esperto Hardware
- 🐙 Contribuisco a Progetti Open Source Bitcoin
- ⚠️ Appassionato di Sicurezza Hardware
- ₿ Ingegnere presso Blockstream

👤 https://www.linkedin.com/in/valeriovaccaro/

🐙 https://github.com/valerio-vaccaro/

Meme

⚠️ **Not your keys, not your Bicoins!**

Summary

- 🔒 Consenso
- 💻 Regole fuori consenso
- 🔥 Soft-fork
- 💀 Hard-fork
- 🙏 Luke forkerà Bitcoin?

Consenso

Il **consenso** in Bitcoin si riferisce all'insieme di regole condivise che tutti i nodi della rete seguono per validare le transazioni e i blocchi, garantendo che la blockchain rimanga coerente e sicura.

Queste regole definiscono come i nodi raggiungono un accordo sullo stato della blockchain, senza la necessità di un'autorità centrale.

Regole di Consenso in Bitcoin

Le regole di consenso sono quelle che devono essere seguite da tutti i nodi per mantenere la compatibilità con la rete. Se un nodo viola queste regole, i suoi blocchi o transazioni vengono rifiutati dagli altri nodi.

Le principali regole di consenso includono:

- 🕵️ Validità delle transazioni:Ogni transazione deve avere input validi (fondi spendibili).
  - La somma degli input deve essere maggiore o uguale agli output (nessuna creazione di Bitcoin dal nulla).
  - Le firme crittografiche devono essere valide.

Regole di Consenso in Bitcoin

- 📦 Struttura dei blocchi:I blocchi devono rispettare il limite massimo di dimensione (attualmente circa 4 MB con SegWit).
  - Ogni blocco deve includere un riferimento valido al blocco precedente (hash).
  - La difficoltà del proof-of-work deve essere rispettata (l'hash del blocco deve soddisfare il target di difficoltà).
- 🔨 Emissione di nuovi Bitcoin:La ricompensa per i miner (coinbase) deve rispettare il programma di dimezzamento (halving) ogni 210.000 blocchi.
  - Non possono essere creati più di 21 milioni di Bitcoin in totale.

Regole di Consenso in Bitcoin

- ⏰ Validazione temporale:I timestamp dei blocchi devono essere coerenti con l'ordine cronologico.
    - Le transazioni devono rispettare il locktime, se presente.
- 💵 Regola del doppio spesa:Una transazione non può spendere lo stesso output (UTXO) più di una volta.

Se esco dal consenso avviene una biforcazione della catena

💻 Regole fuori consenso

Le regole fuori consenso sono quelle che non influenzano la validità della blockchain per l'intera rete.

I nodi possono scegliere di implementarle senza compromettere la compatibilità.

Esempi includono:

- 🔧 Politiche di mempool:Ogni nodo può decidere quali transazioni accettare nella propria mempool (ad esempio, transazioni con commissioni minime).
- 🕸️ Regole di rete:Regole come il numero massimo di connessioni tra nodi o il formato dei messaggi di rete.
- 🗑️ Validazione aggiuntiva:Alcuni nodi possono applicare filtri personalizzati (es. rifiuto di transazioni non standard), ma queste non sono obbligatorie per la rete.

Se le modifico non avviene alcuna biforcazione della catena

Fork

I fork sono modifiche al **consenso** di Bitcoin che possono essere di due tipi: soft fork e hard fork.

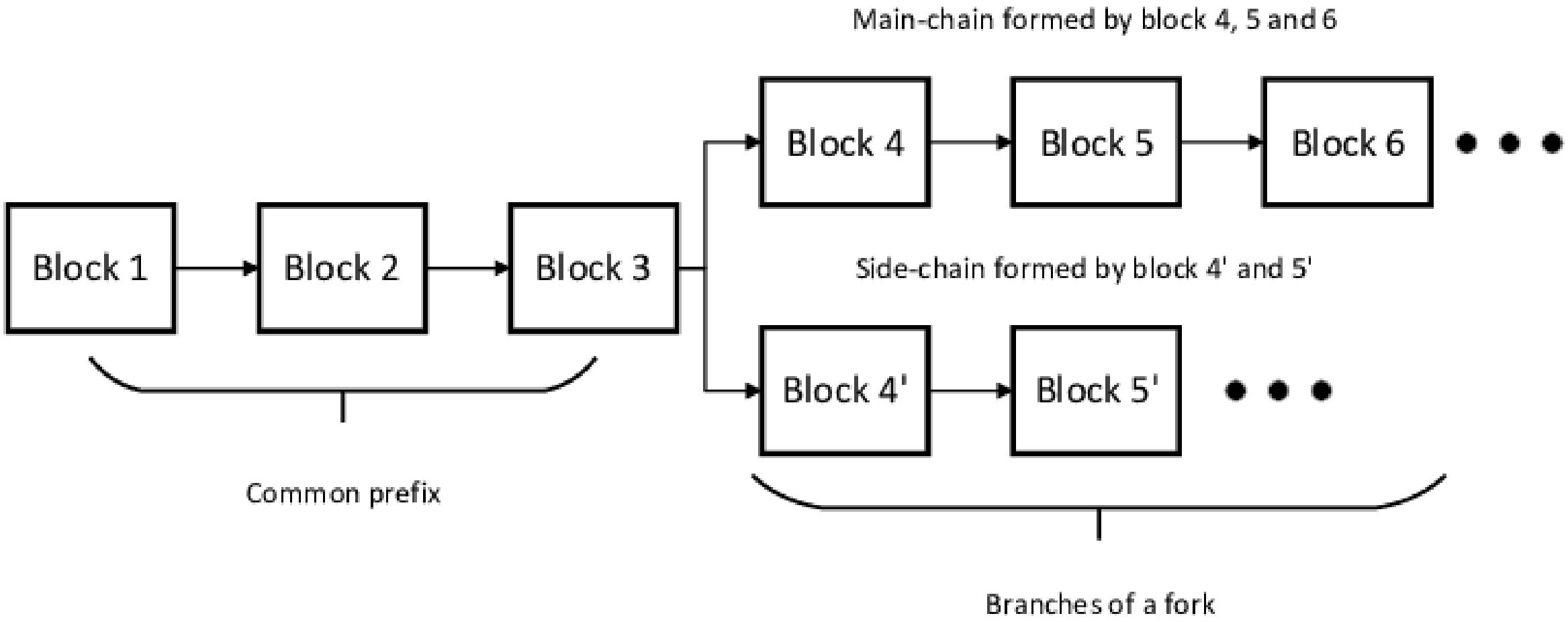
🔥 Soft-fork

Un Soft Fork è una modifica retrocompatibile al protocollo: i nodi non aggiornati possono ancora validare i blocchi prodotti dai nodi aggiornati, ma con alcune limitazioni.

💀 Hard-fork

Un Hard Fork è una modifica non retrocompatibile: i nodi non aggiornati non possono validare i blocchi prodotti dai nodi aggiornati, portando potenzialmente a una divisione della blockchain in due reti separate.

Fork


Main-chain formed by block 4, 5 and 6
Block 1
Block 2
Block 3
Block 4
Block 5
Block 6
Side-chain formed by block 4' and 5'
Block 4'
Block 5'
Common prefix
Branches of a fork

🔥 Soft-fork

Soft Fork:Un soft fork è una modifica retrocompatibile al protocollo: i nodi non aggiornati possono ancora validare i blocchi prodotti dai nodi aggiornati, ma con alcune limitazioni.

Introduce regole più restrittive rispetto a quelle esistenti.

Richiede il consenso della maggior parte dei miner per essere attivato (spesso tramite meccanismi come BIP 9).

✅ **Vantaggi**: Minore rischio di divisione della rete, poiché i nodi non aggiornati rimangono compatibili.

❌ **Svantaggi**: Può introdurre complessità nel codice e ridurre la flessibilità per i nodi non aggiornati.

Esempi

- Soft ForkBIP 66 (2015):Ha introdotto regole più rigide per la validazione delle firme (DER encoding), igliorando la sicurezza contro attacchi di malleabilità delle transazioni.
- BIP 34 (2013):Ha aggiunto l'altezza del blocco nell'header del coinbase, migliorando la tracciabilità.
- BIP 65 (2015):Ha introdotto l'opcode OP_CHECKLOCKTIMEVERIFY, consentendo transazioni con vincoli temporali.
- SegWit (Segregated Witness, BIP 141, 2017):Ha separato i dati delle firme dal resto della transazione, aumentando la capacità del blocco (fino a ~4 MB) e risolvendo la malleabilità delle transazioni.
- Taproot (BIP 340-342, 2021):Ha introdotto firme Schnorr e un nuovo schema di scripting (Tapscript).

💀 Hard-fork

Un **Hard Fork** è una modifica non retrocompatibile: i nodi non aggiornati non possono validare i blocchi prodotti dai nodi aggiornati, portando potenzialmente a una divisione della blockchain in due reti separate.

Introduce regole più permissive o completamente diverse.

Richiede un consenso più ampio e coordinato, spesso controverso.

✅ **Vantaggi**: Permette innovazioni significative e miglioramenti radicali.

❌ **Svantaggi**: Può causare una scissione della comunità e della blockchain, creando una nuova criptovaluta.

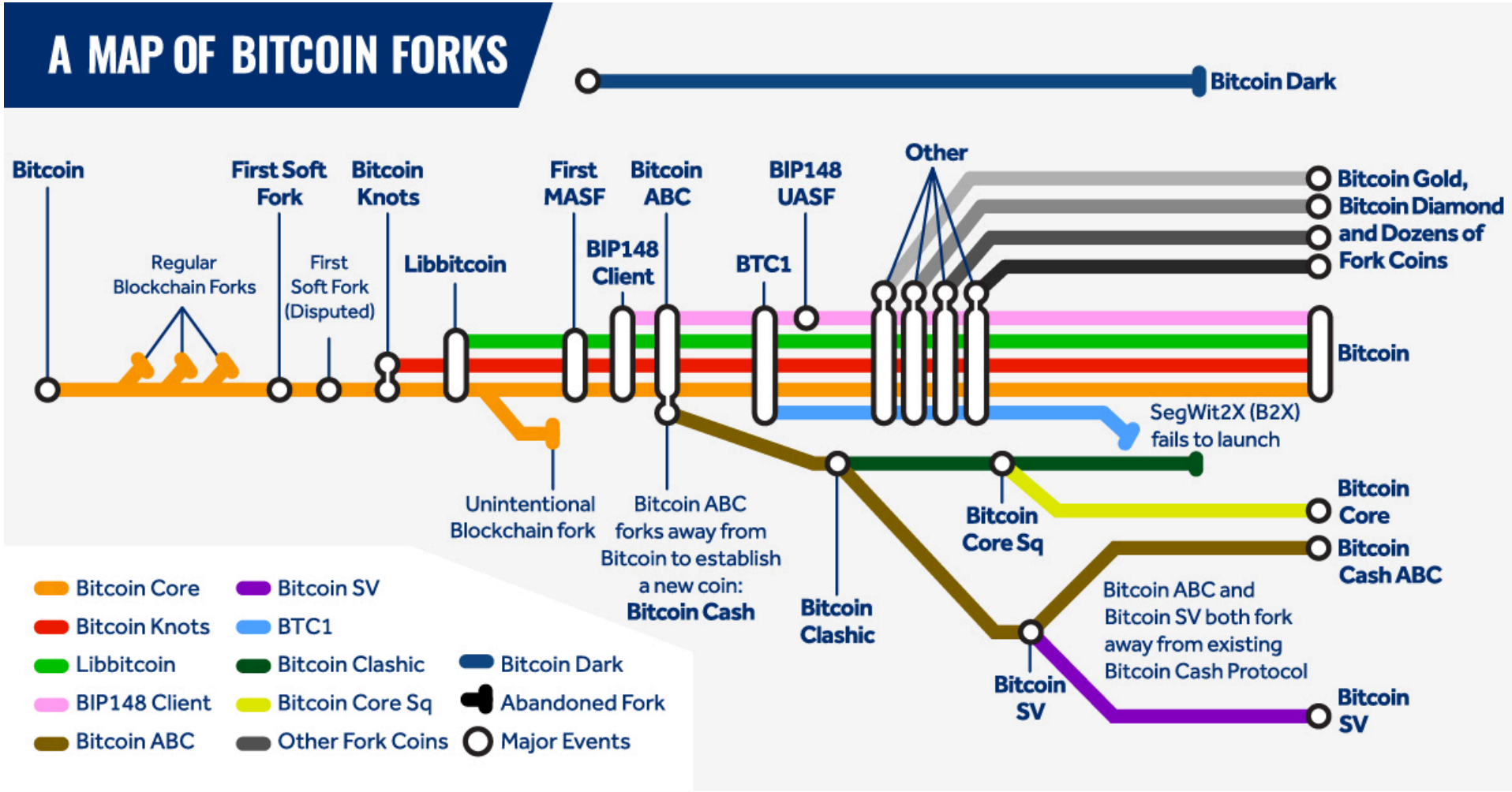
Esempi

- 💩 Bitcoin Cash (BCH, 2017):Creato a causa di disaccordi sulla scalabilità (aumentata la dimensione del blocco a 8 MB, poi fino a 32 MB).
- 💩 Bitcoin SV (BSV, 2018):Derivato da Bitcoin Cash, ha aumentato ulteriormente la dimensione del blocco (fino a 2 GB).
- 💩 Bitcoin Gold (BTG, 2017):Ha modificato l'algoritmo di mining (da SHA-256 a Equihash) per favorire il mining con GPU anziché ASIC.
- 💩 Bitcoin Diamond (BCD, 2017):Ha aumentato l'offerta totale a 210 milioni di monete e introdotto blocchi più grandi.

Sono tutte shitcoin

⚠️ Ma ci sono stati anche Hard fork di emergenza (e.g. inflation bug)

Fork


A MAP OF BITCOIN FORKS
Bitcoin Dark
Bitcoin
First Soft Fork
Bitcoin Knots
First MASF
Bitcoin ABC
BIP148 UASF
Other
Bitcoin Gold, Bitcoin Diamond and Dozens of Fork Coins
Regular Blockchain Forks
First Soft Fork (Disputed)
Libbitcoin
BIP148 Client
BTC1
Bitcoin
SegWit2X (B2X) fails to launch
Unintentional Blockchain fork
Bitcoin ABC forks away from Bitcoin to establish a new coin: Bitcoin Cash
Bitcoin Clashic
Bitcoin Core Sq
Bitcoin Core
Bitcoin Cash ABC
Bitcoin ABC and Bitcoin SV both fork away from existing Bitcoin Cash Protocol
Bitcoin SV
Bitcoin SV
Bitcoin Core
Bitcoin Knots
Libbitcoin
BIP148 Client
Bitcoin ABC
BTC1
Bitcoin Clashic
Bitcoin Core Sq
Other Fork Coins
Bitcoin Dark
Abandoned Fork
Major Events

I Non-fork

I **Non Fork** sono discussioni tecniche che:

- non toccano il consenso
- non sono ne hard fork ne soft fork
- sono drammatizzate da non tecnici
- danno visibilità a gente che non la merita
- la gente vive meglio senza
- alla fine non concludono nulla

e.g. la discussione su OP_RETURN

Conclusione

- I Soft-fork vanno preferiti.
- Richiedono comunque una soglia di attivazione.
- Non toccano la catena.

Conclusione

- Gli Hard-fork vanno evitati il più possibile.
- Portano spesso ad una biforcazione.
- Cambiano il consenso in modi difficilmente prevedibili.

🙏 Luke forkerà Bitcoin?

NO

Contesto:

- Luke non vuole OP_RETURN (di altri)
- Luke dice che in tali spazi può nascondersi il demonio 😈 (solita narrativa fallimentare)
- Luke propone (?) un hard fork per rendere prunabile il contenuto di OP_RETURN (favorendo le iscriptions)
- Luke si rimangia la parola
- Viviamo tutti felici e contenti (fino alla prossima idiozia)

Domande

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

https://satoshispritz.it

https://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
  - ... e molto altro

https://officinebitcoin.it