

Bitcoin Blockchain Wars and Its Evolution: Implications for Decentralisation, Economics, and Governance

The Bitcoin Blockchain War (2017): A Turning Point

The Conflict:

As Bitcoin's popularity surged, its scalability was questioned. The network's 1 MB block size limit, introduced in 2010, restricted transaction throughput to 3-7 transactions per second, leading to delays and high fees during peak demand.

Two factions emerged:

1. **Block Size Increase Advocates:**

- Believed Bitcoin should scale on-chain by increasing the block size, enabling more transactions per block.
- Argued that larger blocks would reduce transaction fees and support Bitcoin's use as a peer-to-peer electronic cash system, consistent with Satoshi Nakamoto's original vision.
- Viewed concerns about centralization as overstated, asserting that technological advancements in storage and bandwidth would mitigate increased node costs.
- Criticized second-layer solutions like the Lightning Network as overly complex and potentially centralizing due to the reliance on custodial hubs.

2. **SegWit and Lightning Supporters:**

- Proposed keeping the block size small to preserve Bitcoin's decentralization.
- Emphasized that larger blocks would increase the cost of running a full node, reducing the number of participants and risking centralization.
- Advocated for Segregated Witness (SegWit) to optimize block usage and enable second-layer solutions like the Lightning Network for off-chain scaling.
- Argued that a decentralized network was essential to Bitcoin's resistance to censorship and long-term viability.

The Split:

The disagreement culminated in a hard fork in August 2017, resulting in two chains:

1. **Bitcoin (BTC):**

- Retained the 1 MB block size, adopted SegWit, and shifted toward a "store of value" narrative akin to digital gold.

2. **Bitcoin Cash (BCH):**

- Increased the block size to 8 MB (and later 32 MB), focusing on low-cost, high-speed transactions to maintain Bitcoin's usability for payments.

Implications:

- By limiting block size, BTC ensured decentralization by keeping the requirements for running a full node accessible. However, this choice constrained Bitcoin's capacity as a global currency.
- BCH sought to enhance usability for everyday payments but sacrificed some decentralization, as larger blocks demand more resources, potentially centralizing the network over time.
- BTC's approach also facilitated second-layer scalability solutions like the Lightning Network, designed to handle microtransactions off-chain while maintaining the integrity of the base layer.

The Bitcoin Cash Fork (2018): Further Fragmentation

Dispute Over Direction:

Bitcoin Cash itself split into Bitcoin Cash (BCH) and Bitcoin SV (BSV) in November 2018.

- **Bitcoin SV (Satoshi's Vision):**

- Championed by Craig Wright and Calvin Ayre, this chain implemented massive block size increases (eventually 2 GB) to support high transaction volumes and data-heavy applications, asserting it adhered more closely to Satoshi Nakamoto's original vision.

Implications:

- **On-Chain Scalability:**

- BSV's ability to handle large-scale transactions and applications demonstrated the potential of a high-capacity blockchain but raised concerns about network centralization, as fewer entities can afford to run nodes.

- **Fragmentation Risks:**

- Each fork diluted the community's resources and focus, potentially slowing adoption and development compared to a unified approach.

The Evolution of Bitcoin's Role

Original Vision vs. Reality:

Satoshi Nakamoto's white paper described Bitcoin as a decentralized, peer-to-peer electronic cash system. However, BTC's trajectory has focused on becoming digital gold—a store of value rather than a daily-use currency.

- High fees and limited scalability on the base layer shifted BTC's usability to long-term investment and large transactions, relying on Layer 2 solutions like the Lightning Network for smaller, faster payments.

Economic Implications of the Shift:

- **Inability to Replace Fiat Currencies:**
 - With its current design, BTC cannot handle the transactional volume required to function as a global currency.
 - This leaves the fiat system intact, maintaining the monopoly of central banks and governments over monetary policy and capital controls.
- **Regulatory Leverage:**
 - By not directly competing with fiat for everyday transactions, Bitcoin avoids triggering aggressive regulation aimed at preserving state control over money. This strategic positioning could be deliberate or a by-product of internal disagreements.

Centralisation Concerns:

While Bitcoin is decentralized in protocol, its ownership distribution and rising price challenge its founding ideals:

- **Ownership Concentration:**
 - Studies reveal that 2% of wallets hold over 90% of Bitcoin's supply. While some belong to exchanges holding BTC on behalf of users, the concentration among "whales" (large holders) raises concerns about market manipulation and influence.
- **Corporate and Government Accumulation:**
 - Corporations like MicroStrategy and countries like El Salvador hold significant amounts of Bitcoin. If governments or other centralized entities acquire substantial holdings, they could:
 - Influence the market price by coordinating buying or selling strategies.
 - Use Bitcoin holdings as a tool to control or manipulate economies.
 - Undermine Bitcoin's decentralization by concentrating ownership in fewer hands.
- **Impact on Retail Investors:**
 - With BTC prices exceeding \$90,000, owning a full Bitcoin is out of reach for most individuals, exacerbating economic inequalities and reinforcing its image as a "rich man's asset."
 - Fractional ownership (satoshis) helps, but the psychological barrier of owning "just a fraction" may deter widespread adoption.

Long-Term Risks:

- If a small number of entities control the majority of Bitcoin, they could limit its use as an alternative to fiat by:
 - Hoarding supply, reducing circulation.
 - Using their holdings to impose transaction restrictions or fees, undermining Bitcoin's decentralized ethos.

A Hypothetical Alternative: Bitcoin as Scalable Electronic Cash

Had the community agreed to increase block sizes to enable on-chain scalability, Bitcoin could have developed as a global, decentralized payment system with implications such as:

- **Governments Losing Control Over Money:**
 - Bitcoin could bypass traditional banking systems, enabling global transactions without government oversight.
 - This would challenge the ability of governments to:
 - Collect taxes on income or transactions.
 - Enforce capital controls, such as limiting money movement across borders.
 - Implement monetary policy, as citizens and businesses could opt out of fiat entirely.
- **Financial Inclusion:**
 - With low transaction fees and high scalability, Bitcoin could serve as a practical payment method for the unbanked and underbanked, particularly in developing countries with unstable currencies.
 - This could reduce reliance on remittance services and create economic opportunities.
- **Marketplace Integration:**
 - Scalable on-chain solutions could support decentralized marketplaces, where users buy and sell goods directly using Bitcoin without intermediaries like banks, credit cards, or centralized payment processors.

Challenges to Scalability:

- Larger block sizes increase centralization risks by making node operation more resource-intensive.
- Governments might aggressively regulate or ban Bitcoin if it competes directly with fiat.

Concluding Thoughts

The evolution of Bitcoin reflects the tension between decentralization, scalability, and adoption. While BTC's shift toward digital gold ensures its survival as a store of value, it limits its potential as a peer-to-peer electronic cash system. Meanwhile, the rise of institutions and governments in Bitcoin ownership raises concerns about its decentralization and ability to challenge traditional financial systems.

A scalable Bitcoin could have profound implications, including reducing government control over money and enabling financial freedom. However, achieving this vision would require balancing technical feasibility, decentralization, and geopolitical realities—an ongoing challenge for the cryptocurrency community.

Revision #4

Created 17 November 2024 08:22:22 by coolbaron

Updated 27 December 2024 23:45:28 by coolbaron