Scalability Constraints of Bitcoin

Tech1k (Cyphertoshi)
hello@tech1k.com
tech1k.com | cyphertoshi.com
June 15, 2025

Abstract. Bitcoin has faced growing scalability challenges due to protocol-level constraints, network congestion, and developer reluctance to modify core consensus rules via hard forks. Layer 2 protocols, such as the Lightning Network, offer temporary relief for scalability, but introduce potential trade-offs in complexity, custody, and accessibility. This paper analyzes the core limitations affecting Bitcoin's scalability and argues that protocol-level scaling remains impractical within the network's current governance and technical model set by core developers.

1. Introduction

Since its inception in 2009, Bitcoin's scalability has been a persistent concern [1]. Satoshi Nakamoto, creator of Bitcoin, designed Bitcoin to evolve through consensus upgrades, but development has increasingly favored ossification. Bitcoin is currently able to process approximately 7 transactions per second (TPS), limited primarily by its 10-minute block interval and maximum block size. As of 2025, blocks are consistently filled several blocks in advance, revealing significant usage, but also exposing critical protocol-level limitations that restrict Bitcoin's potential as a widely accessible and stable financial system. Layer 2 solutions, such as the Lightning Network, offer increased throughput but introduce additional operational challenges.

2. Protocol Limitations

Bitcoin's protocol enforces a 10-minute average block interval and a maximum block size of 4 megabytes under full SegWit utilization [2], supporting an average of 7 TPS under ideal conditions [3]. Presently, transaction volume frequently exceeds on-chain capacity, leading to significant mempool backlogs. This design limitation is not a technical defect, but an intentional consensus parameter. As Bitcoin's adoption and market value increases, competition for its limited block space drives transaction fees upward, potentially excluding smaller users from transacting economically on-chain.

3. Layer 2 Solutions Are Not Permanent Remedies

Layer 2 networks, particularly the Lightning Network, attempt to relieve base layer congestion by enabling off-chain transactions that eventually settle on-chain [4]. While the Lightning Network is capable of supporting a high volume of transactions, it introduces new trade-offs. Non-custodial Lightning usage requires participants to operate full nodes, maintain continuous uptime, manage channel liquidity, and possess sufficient technical expertise. As a result, many users gravitate toward custodial Lightning wallet services, which undermine Bitcoin's core principle of self-custody and reintroduce users to managed trusted third parties.

4. Network Spam and Non-Financial Use

The emergence of protocols such as Ordinals and Inscriptions has further stressed Bitcoin's limited block space [5]. By embedding arbitrary data within transactions, users have contributed to persistent network congestion. These non-financial uses consume valuable network capacity, reducing the throughput for monetary transactions and raising concerns about long-term sustainability and prioritization of the network as a financial medium.

5. The Hard Fork Governance Barrier

Bitcoin's governance model strongly favors backwards-compatibility via soft forks, which are activated through mechanisms such as BIP 8 [6] and BIP 9 [7]. These mechanisms allow for the tightening of network consensus rules, but not for relaxing the fundamentals of the network such as the block size or block interval. Any modifications to such fundamental parameters would constitute a hard fork, risking network splits and incompatibility with legacy nodes. Despite occasional proposals, community and developer sentiment remains largely opposed to hard forks aimed at increasing on-chain network capacity. As a result, protocol-level scaling efforts remain effectively futile and off-limits.

6. Outlook for Bitcoin's Scalability

Bitcoin's mainnet is nearing its theoretical capacity. Protocol-level scaling solutions face both technical and political obstacles, while Layer 2 solutions require trade-offs that compromise accessibility and sovereignty. As transaction fees rise and non-financial uses proliferate, smaller users may increasingly be priced out of transacting directly on-chain or forced to wait longer for their transactions to confirm. Over time, this dynamic risks non-financial use cases bloating the network, increasing resource demands for sovereign node operators, and contributing to the centralization of node operations, ultimately threatening Bitcoin's decentralization and its security as a trustless network.

7. References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] Bitcoin Core Developers, “consensus.h,” Bitcoin Core v29.0, accessed June 2025. [Online]. Available: https://github.com/bitcoin/bitcoin/blob/v29.0/src/consensus/consensus.h

[3] E. Georgiadis, “How many transactions per second can bitcoin really handle? (Theoretically),” IACR ePrint Archive, Apr. 2019. [Online]. Available: https://eprint.iacr.org/2019/416

[4] J. Poon and T. Dryja, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments,” 2016. [Online]. Available: https://lightning.network/lightning-network-paper.pdf

[5] C. Rodarmor, “Ordinal Theory: Inscriptions on Bitcoin,” 2023. [Online]. Available: https://docs.ordinals.com

[6] BIP 8 – Version bits with lock-in by height. Bitcoin BIPs repository, commit e1def09, accessed June 2025. [Online]. Available: https://github.com/bitcoin/bips/blob/e1def09/bip-0008.mediawiki

[7] BIP 9 – Version bits with timeout and delay. Bitcoin BIPs repository, commit 9a56d35, accessed June 2025. [Online]. Available: https://github.com/bitcoin/bips/blob/9a56d35/bip-0009.mediawiki