SURGE

Analysing The

Bitcoin Scaling Landscape

September 2024

Table of Contents

Executive Summary

- Bitcoin is seeing a wave of innovation with technologies like Ordinals, Inscriptions, BRC-20 tokens, and Runes. These developments are expanding Bitcoin's functionality by enabling metadata attachment and introducing new token standards, drawing comparisons to Ethereum's token ecosystem.

- Ethereum's Layer-2 (L2) solutions account for about 10% of its total value locked (TVL), whereas Bitcoin's L2 adoption remains significantly lower, with only 0.13% of its total value in L2 solutions. This highlights the need for Bitcoin to adopt more scalable solutions to support the increasing demand for its ecosystem.

- State channels, which operate similarly to Bitcoin's Lightning Network, provide off-chain transaction capabilities that can alleviate the burden on the main blockchain. Although the Lightning Network has improved Bitcoin's scalability, its current success rate is around 50%, with issues around routing and liquidity management.

- Sidechains like the Liquid Network offer a promising solution for scaling Bitcoin by enabling faster transactions and asset management without congesting the main chain. Liquid provides features such as confidential transactions and digital asset issuance, making it a valuable tool for enhancing Bitcoin's functionality. However, adoption remains slow due to federal/ centralisation concerns and reluctance from exchanges and wallet providers to integrate it.

- The upcoming Nakamoto Release on the Stacks network is poised to significantly enhance transaction throughput, finality, and security. This release will phase out the need for miner elections and introduce faster, more secure transaction processing, making Stacks more robust for future applications.

- Looking ahead, the adoption of rollups on Bitcoin remains promising but faces several hurdles. While rollups like Optimistic and ZK-Rollups can dramatically increase transaction throughput, challenges such as fraud-proof verification, pricing to verify proofs on Bitcoin, and governance must be addressed before rollups can be fully integrated into Bitcoin's ecosystem.

Introduction

The Bitcoin ecosystem has seen a flurry of innovative developments recently, including the introduction of Ordinals, Inscriptions, BRC-20 tokens, and Runes. Ordinals and Inscriptions allow for the attachment of arbitrary data to individual satoshis, enhancing the functionality and metadata capabilities of Bitcoin. BRC-20 tokens introduce a fungible token standard on the Bitcoin blockchain, similar to ERC-20 tokens on Ethereum, enabling the creation and management of tokenized assets. Runes provides a new scripting language that enhances the programmability of Bitcoin transactions.

These advancements have brought the issue of scalability to the forefront.

The adoption of Ethereum's Layer-2 (L2) solutions accounts for about **10%** of its total value locked (TVL), which translates to $45 billion out of its $450 billion.

In contrast, Bitcoin, with a TVL of $1.4 trillion, has approximately $2 billion in L2 TVL, representing just **0.13%** of its total value. This significant disparity underscores the need for scalable solutions within the Bitcoin ecosystem.

This report analyses the adoption of various solutions that promise to scale Bitcoin to new heights.

State Channels

What Are State Channels?

A channel is a peer-to-peer network allowing two parties to execute multiple transactions directly with each other. Only the final outcomes of these interactions, including the processing and computations, are recorded on the main blockchain. Channels can be categorized as either payment channels or state channels.

State channels, a type of blockchain scaling solution, enable the execution of numerous transactions off-chain. Like other layer-2 scaling methods, state channels aim to minimize interactions with the main blockchain by performing tasks such as processing and computation externally. These channels are similar to payment channels used in the Lightning Network but extend beyond payments by also facilitating public state updates.

In this context, "state" refers to the current condition of the blockchain at a given time, while "channel" represents the communication medium. Simply put, state channels provide a secure, cost-efficient, and private environment where unlimited interactions can take place before they are finalized on the blockchain.

In summary, these channels allow users to engage in direct communication without the need to record every transaction on the main blockchain, thereby alleviating the load on the network.

The technology utilized for building a state channel varies depending on the blockchain platform. For instance, the **Lightning Network** on Bitcoin is an implementation that uses Hashed Timelock Contracts (HTLCs) within bi-directional payment channels, enabling secure transactions across various peer-to-peer channels. HTLCs are a form of payment that leverage features such as hashlocks and timelocks in Script, ensuring the payment receiver confirms receipt by producing cryptographic proof before a specified deadline.

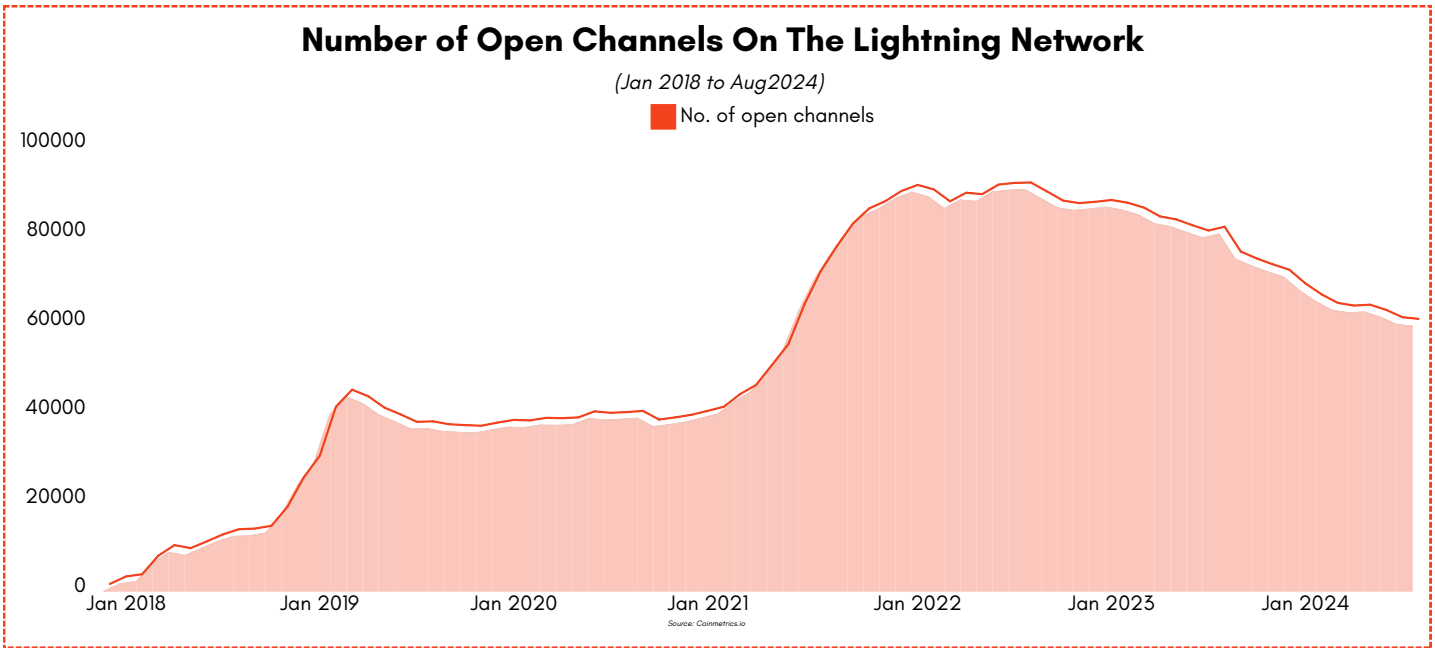
Lightning Network

The Lightning Network is a widely used Layer 2 solution that enables faster and cheaper transactions for BTC micropayments. Major companies like McDonald's and Walmart utilize the Lightning Network as their backend to allow quick Bitcoin payments. Similarly, Bitcoin exchanges like OKX and Binance have realized substantial cost savings by integrating the Lightning Network for inter-exchange transfers, user withdrawals, and other transactions.

If we take a look at a report by **Coingate**, a crypto payment gateway for Bitcoin, the key takeaways from their analysis were:

- The percentage of Bitcoin payments processed via the Lightning Network at CoinGate has more than doubled over two years, increasing from 6.5% in Q2 2022 to 16.6% in Q2 2024.
- CoinGate's Lightning Network order count has also seen significant growth, with orders in Q2 2024 up by approximately 28.4% compared to Q2 2023 and about 74.6% compared to Q2 2022.
- If this growth rate continues, projections indicate that Lightning Network adoption could potentially reach 20% or higher in Q3 2024.

In addition to the Lightning Network, the Liquid Network introduces LBTC, a pegged version of Bitcoin used for faster transactions. BTC is converted to LBTC via a bridge mechanism, where BTC is locked on the Bitcoin mainchain and an equivalent amount of LBTC is issued on Liquid. Similar to a traditional bridging mechanism between L1 chains (like Solana and Ethereum). Hence, this is a double edged sword - enabling faster transfers, but presenting the vulnerability of the bridging mechanism.



The graph above shows that the number of open channels on the Lightning Network increased steadily from 2021 until mid-2022, after which there has been a gradual decline.

On the other hand, the total value of all channels has remained relatively flat since 2023, with occasional sharp drops and increases.

With the emergence of newer solutions, there has been a decline in the usage of the Lightning Network.

Challenges Faced

Early demonstrations of the Lightning Network were promising, presenting Bitcoin as a viable medium of exchange. However, since late 2023, adoption appears to have stalled, with critics pointing to several concerning trends that suggest the Lightning Network may be in a precarious position:

- **Dwindling Capacity:** The total amount of Bitcoin available on the network has fallen below 5,000 BTC, a minuscule portion of Bitcoin's circulating supply, raising doubts about the network's scalability.

- **Bugs and Vulnerabilities:** The Lightning Network has been plagued by issues such as frozen funds and 'jamming' attacks. In October 2023, a developer-introduced bug led to funds being trapped within the network for hours, severely undermining trust in its reliability.

- **Key Developers Departing:** Prominent figures in the Lightning community have expressed doubts about its future. Co-creator Tadge Dryja admitted the network's potential had been overhyped, and other developers like Rene Pickhardt have ceased their involvement, citing fundamental limitations, which raises concerns about the project's long-term viability.

- **Initial Costs:** To use the Lightning Network, users must first make an on-chain Bitcoin transaction to open a channel, which introduces significant friction and upfront costs.

- **Receiving Costs:** Receiving additional Bitcoin via Lightning requires another on-chain transaction, adding further expense and delay, complicating the user experience compared to traditional financial systems.

- **Centralization Concerns:** While custodial Lightning wallets help mitigate some of these issues, they introduce centralization, which compromises Bitcoin's core principle of decentralized, self-sovereign finance.

Current State of the Lightning Network

The Lightning Network's reliability, though improving, remains a key focus for developers. New users' first impressions hinge on this, yet the current success rate is around 50%, far from the ideal 99.9%. Christian Decker suggests enhanced routing algorithms could significantly boost this.

Lightning transmits "onions" — lightweight messages representing payment attempts. If one fails, the network retries until successful. A parallel approach could speed transactions but risks overpaying without Point Time Locked Contracts (PTLCs), now possible with Taproot integration.

Currently, the network centers around a few major hubs, simplifying routing but increasing centralization. Managing liquidity is inefficient, and misallocating it could lead to channel closures and on-chain fees. If usage grows, frequent liquidity reallocation could fill blocks, making the system unsustainable despite solutions like transaction batching. Limited block space remains a challenge.

In summary, managing liquidity on the Lightning Network can be inefficient. Misallocating liquidity may result in needing to close channels and paying on-chain fees. If Lightning sees widespread use, liquidity will need to be reallocated frequently. This could eventually lead to full blocks, making the system unsustainable as liquidity diminishes. Moreover, limited block space presents challenges, even with solutions like transaction batching, because block capacity is finite.

One way to address this challenge is by creating a decentralised intermediary layer - with the sole purpose of improving Bitcoin’s functionality. Surge is building this intermediary layer where Rollups, dApps, and metaprotocols interoperate. Surge achieves this by using zk proofs and zk-aggregation and decentralized verification mechanisms. This creates an environment for builders to create app-specific rollups while inheriting the security and liquidity of Bitcoin.

Sidechains

The idea of sidechains was first introduced in a 2014 whitepaper by Blockstream, a blockchain technology company, which aimed to facilitate innovation and scalability without altering the Bitcoin mainchain. Over the years, developers worked on refining the concept, leading to the formalization of BIP 300 and BIP 301 by Paul Sztorc in 2017.

A sidechain is a scaling mechanism designed to operate alongside the primary blockchain. It functions autonomously, with its own native currency and consensus algorithm, distinguishing it from the parent chain. "Despite this independence, the sidechain remains connected to the mainchain through a bridge, allowing users to transfer assets between the two chains. However, this process typically involves additional steps and may incur fees."

The primary objective of sidechains is to enhance the scalability of Layer 1 blockchains by offloading transactions, thereby reducing congestion on the main chain.

In a metaphorical sense, a sidechain is like a service road running parallel to a busy highway, offering drivers an alternative route to avoid heavy traffic.

The two prominent sidechains in the Bitcoin ecosystem are **Rootstock (RSK)** and **Liquid Network**

Liquid Network

Launched by Blockstream in 2018, the Liquid Network is a layer-2 sidechain designed to enhance the performance and functionality of Bitcoin. Liquid enables users to conduct fast, secure, and confidential transactions on the Bitcoin blockchain.

Liquid serves as an additional layer on top of Bitcoin, enabling the development of technologies and applications without altering Bitcoin's base protocol. Operating independently, Liquid has its own global ledger and consensus mechanism.

The Liquid Network operates independently of the main Bitcoin network through the Liquid Federation, a consortium of crypto-native organizations responsible for confirming new blocks and securing Bitcoin funds held in the network's multi-signature wallet. Federation members also vote on board representatives who oversee decision-making related to the platform's operations and maintenance.

One of Liquid Network's key features is the use of Liquid Bitcoins (L-BTC), which are pegged one-to-one with Bitcoin.

L-BTC can be quickly and securely transferred on the Liquid Network and later converted back to Bitcoin on the main chain. By transferring BTC to the Liquid Network, both retail and institutional investors can access decentralized finance services that are backed by the Bitcoin blockchain. These services include security tokens, trustless swaps, private peer-to-peer payments, and more.

Since its launch in 2018, the Liquid Network has experienced steady growth, with major exchanges and institutions adopting it for its fast and private transactions. The capability to issue new assets on Liquid further enhances its potential within the expanding DeFi sector.

Although specific user numbers are not widely disclosed, the addition of new members to the Liquid Federation, such as Bitmatrix and GMO Coin in early 2022, indicates ongoing growth and deeper integration within the cryptocurrency ecosystem. Liquid is also working towards greater interoperability with other blockchains, facilitating easier transfer of assets across different networks.

Drawbacks

While the Liquid Network offers several advantages, it also has some notable drawbacks.

Custodial Concerns:

One key concern is that the Liquid Network can be considered custodial to some extent, depending on how peg-in and peg-out transactions are handled by federation members. The Liquid Federation uses an 11-of-15 multisig wallet to manage these transactions and secure the Bitcoin held in the federation's wallet. As a result, the network is not entirely permissionless, and users must place a degree of trust in the federation members to manage funds and operate the network properly.

Liquid Network's Privacy Concerns:

Another potential issue is that some federation members may require mandatory KYC (Know Your Customer) checks before allowing users to peg in or peg out, which could compromise user privacy. Additionally, in some cases, federation members might convert a user's BTC balance into LN (Liquid Network) liquidity, meaning that users do not have full control over their BTC while it is on the Liquid Network.

However, alternatives exist to mitigate these issues. For example, using Sideswap instead of the traditional peg-in and peg-out process can offer a non-custodial option for utilizing the Liquid Network.

Due to its federation structure, the Liquid Network is also considered more centralized compared to the classic Bitcoin main chain, where decisions are made by consensus across the network's miners and users.

In summary, while the Liquid Network may be seen as custodial and less decentralized in certain aspects, understanding its workings and the available alternatives is crucial for users who wish to utilize its features while minimizing potential drawbacks.

Current State of Liquid Network

The Liquid Network, despite high potential, remains underused. This is due to several reasons. For instance, Liquid relies on a federated custody system which requires 15 functionaries to maintain trust in the system. This does not stand well with Bitcoiners who value decentralization. Further, Liquid's pegged token LBTC faces trust issue on its 1:1 peg with Bitcoin, due to the potential centralization of management of funds by the functionaries.

While the Liquid Network presents valuable opportunities for enhancing the Bitcoin ecosystem, it also encounters several obstacles to broader adoption. Addressing these challenges and developing strategies to increase adoption are essential for tapping into the network's full capabilities.

At present, the adoption rate of the Liquid Network among exchanges remains relatively slow. This sluggish uptake is due to multiple factors, such as a general lack of awareness about its benefits, resistance from established systems, and potential technical and regulatory issues. Additionally, smaller exchanges may lack the resources or technical know-how to successfully integrate the Liquid Network into their existing systems.

Rootstock (RSK)

Rootstock (RSK) is a Bitcoin sidechain developed by Rootstock Labs, designed to enhance Bitcoin's scalability by offering a 30-second transaction confirmation time and supporting EVM-compatible smart contracts.

RSK aims to address the limitations of Ethereum by leveraging Bitcoin's unparalleled stability, security, and economic power. By porting Ethereum's smart contracts to RSK, the platform ensures that all Ethereum applications can be compatible with the Bitcoin blockchain.

Currently, the RSK sidechain boasts over 70,000 active accounts and has more than 40 protocols building on it. One notable protocol, Sovryn, a DeFi platform built on Rootstock, has processed over $2 billion in trades. This level of user activity reflects the growing adoption of the Rootstock protocol as a whole.

Compared to Ethereum, RSK provides transaction speeds that are about 10 times faster and gas fees that are 50 times cheaper.

As a sidechain, RSK operates adjacent to the Bitcoin blockchain and connects to it via a two-way bridge.

The RSK sidechain design has a few unique mechanisms compared to other Bitcoin layers:

Merged Mining

RSK utilizes the same Proof-of-Work (PoW) consensus algorithm as Bitcoin, but allows miners to generate blocks significantly faster than Bitcoin's base layer.

Through merged mining, miners can simultaneously mine on both the Bitcoin and RSK blockchains using the same mining power, which increases profitability without requiring additional resources. This process ensures that RSK can validate transactions, create blocks, and benefit from the robust security of the Bitcoin blockchain.

Powpeg

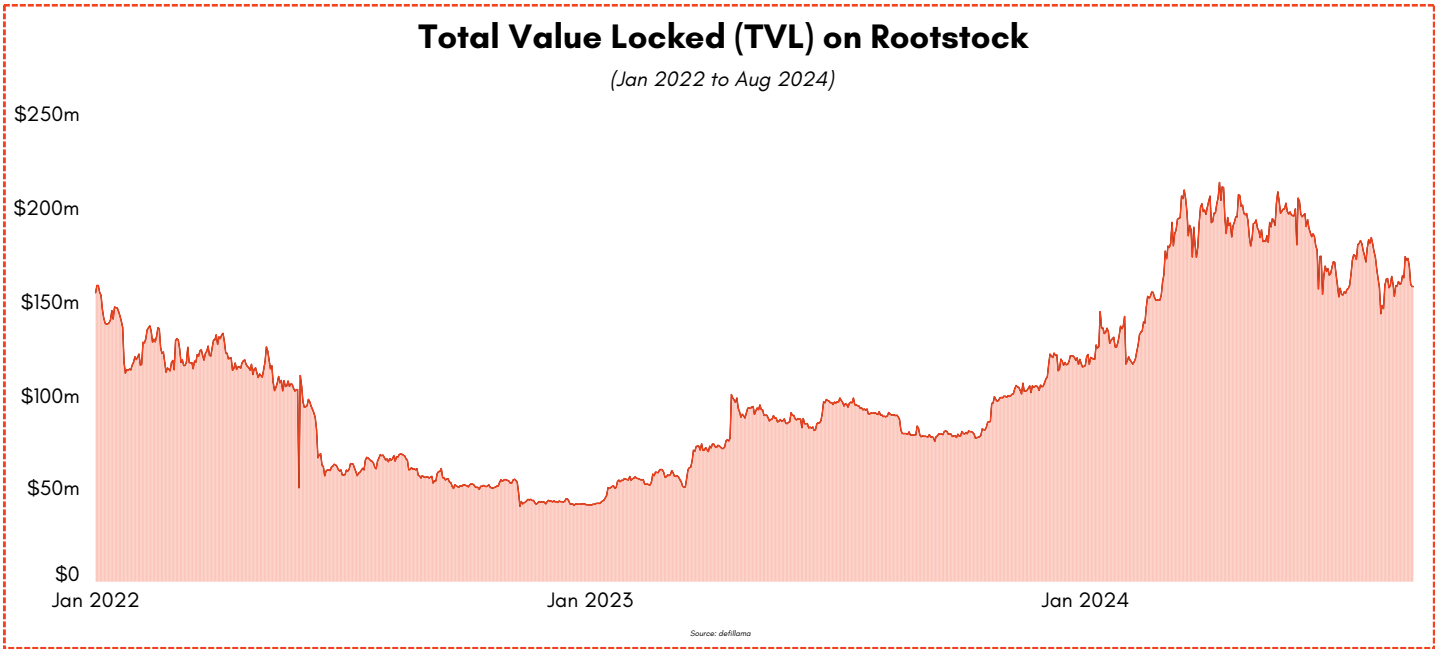
Powpeg is the two-way bridge that facilitates the transfer of Bitcoin to and from the RSK blockchain.

This protocol relies on RSK's asset, smartBTC (RBTC), which is pegged 1:1 with BTC. RBTC, which maintains the same value as BTC, is used to pay transaction fees on the RSK network.

Source: https://defillama.com/chain/Rootstock?stables=false&tvl=true

As of September 2024, the Total Value Locked (TVL) in the RSK network is approximately $160 million, which is modest compared to the leading Ethereum Layer 2s.

However, RSK's TVL has demonstrated resilience during the bear market, suggesting better sustainability compared to many other blockchains. This resilience can be attributed to the fact that, for a considerable period, RSK was the only smart contract platform available for Bitcoin DeFi



Source: defillama

According to data from the block explorer, Rootstock has surpassed 13 million total transactions, with over 670,000 transactions recorded from April to June of 2024.

This notable increase underscores the growing adoption of the sidechain, which provides a secure and reliable environment for building on Bitcoin. With over 60% of Bitcoin's hash rate securing the network and 100% uptime since its launch in January 2018, Rootstock has established itself as a premier destination for development on Bitcoin.

In the past few months, more than 25 dApps and protocols have joined the Rootstock ecosystem, offering users innovative ways to interact with the platform. Key integrations include Artoshi, Bitget, SushiSwap, Uniswap, and others, further expanding the possibilities for use and development on Rootstock.

Drawbacks

Centralization Concerns:

The federated peg system used to transfer BTC to RBTC (and vice versa) involves a federation, which may be perceived as a centralization point and a potential vulnerability within the network.

Development and Integration Challenges:

Integrating RSK's advanced features with the existing Bitcoin infrastructure can be complex for developers, potentially limiting innovation or delaying the deployment of new applications.

Stacks

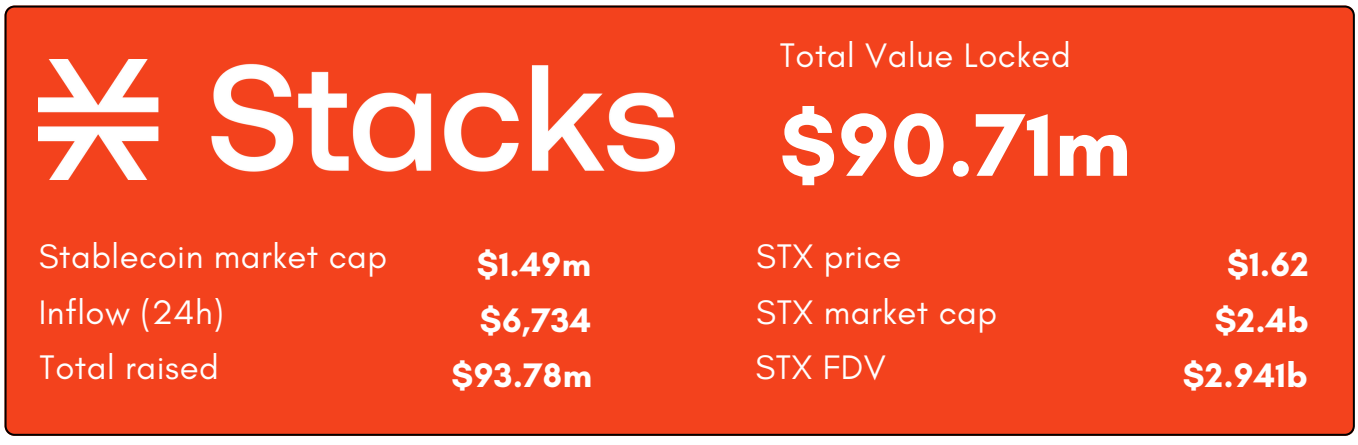
Stacks is not a sidechain, state channel, or rollup; instead, it functions as an abstraction layer or software stack built on top of the Bitcoin blockchain. Stacks connects to Bitcoin through the Proof-of-Transfer (PoX) consensus mechanism, which works alongside Bitcoin's Proof-of-Work by processing transactions on the Bitcoin chain and anchoring Stacks block metadata to Bitcoin blocks.

This dual security model involves both BTC miners and STX holders, with STX holders participating in consensus and earning BTC through a process known as "stacking."

While Stacks enhances Bitcoin's functionality, it does not involve transaction confirmations directly on the Bitcoin chain.

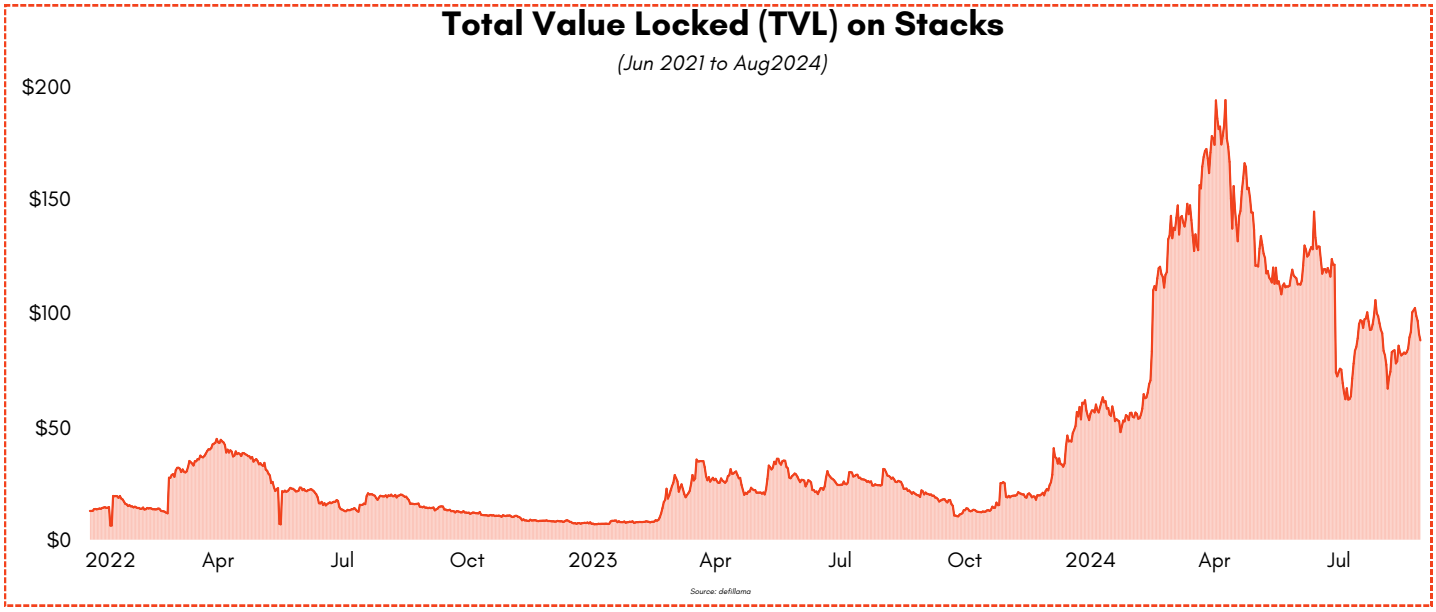
Stacks enables the creation of smart contracts using a coding language called "Clarity." Specifically designed for Stacks, Clarity is optimized for predictability and security.

One of the key advantages of Clarity smart contracts is their ability to read the Bitcoin state, allowing Stacks smart contracts to be triggered by transactions on the Bitcoin base layer. This integration enhances the functionality of Bitcoin by enabling more complex interactions and automation based on Bitcoin's blockchain data.



Source: https://defillama.com/chain/Stacks

As of September 2024, the Total Value Locked (TVL) on Stacks currently sits at around $91 million and has taken a considerable hit from its all-time high value of $190 million at the beginning of April 2024.



Since the launch of Stacking DAO, a liquid staking platform on Stacks, over 55 million STX of liquidity has been unlocked through stSTX, which can be deployed in DeFi. Approximately 40% of this liquidity has flowed into platforms like Zest, Bitflow, Hermetica, Velar, and Arkadiko.

The introduction of Stacking DAO led to rapid Total Value Locked (TVL) growth for Stacks. However, the recent market downturn and the ALEX hack caused a significant drop in TVL.

Critique

- The Stacks consensus protocol is complex, unproven, and lacks sufficient documentation.
- There is a risk of collusion between stackers and block producers, potentially turning Stacks into a de facto PoS system without slashing.
- Stacks advertises smart contracts on Bitcoin but lacks a token representing Bitcoin. (The Nakamoto Upgrade will resolve this)
- Clarity language may hinder scalability and increase transaction costs due to slower execution compared to bytecode.
- Learning curve, leading to lack of dev motivation to learn new language
- The average block interval is 10 minutes, with microblocks every 30 seconds, but this feature is poorly documented and not shown on block explorers.

Nakamoto Upgrade

The Nakamoto Release is an upcoming hard fork on the Stacks network, aiming to provide significant benefits, particularly enhanced transaction throughput and full Bitcoin finality.

The Nakamoto mainnet rollout began with Bitcoin block 840,360 and is being implemented in multiple phases.

With this release, Stacks block production will no longer depend on miner elections. Instead, blocks will be produced at a steady rate, while the PoX Stackers will use miner elections to decide when the current miner should stop and a new one should begin. The blockchain can only fork with the approval of 70% of Stackers, and chain reorganizations will become as difficult as they are on Bitcoin.

The Nakamoto Release introduces several new features and improvements to the Stacks blockchain, including faster transaction speeds, stronger finality for transactions, reduced opportunities for Bitcoin miner extractable value (MEV) in PoX, and enhanced resistance to chain reorganizations.

Rollups / Layer 2

Rollups are a promising layer-2 scaling solution designed to increase the throughput and reduce the transaction costs of blockchains. While originally pioneered on Ethereum, the concept of rollups is now gaining traction within the Bitcoin ecosystem. Rollups work by bundling multiple off-chain transactions into a single, compressed transaction, which is then settled on the base layer. This drastically reduces the amount of data that needs to be processed on-chain, thereby improving network efficiency without compromising the security guaranteed by the underlying Bitcoin blockchain.

There are two primary types of rollups: Optimistic Rollups and ZK-Rollups (Zero-Knowledge Rollups).

Optimistic Rollups

Optimistic Rollups assume that all transactions are valid unless challenged. Users can challenge a transaction within a defined window using a fraud-proof mechanism. This approach allows for high throughput, but transactions can take longer to finalize due to the possibility of disputes and challenge periods.

ZK-Rollups

ZK-Rollups, on the other hand, rely on cryptographic proofs (zero-knowledge proofs) to ensure the validity of every transaction. These proofs are submitted to the blockchain, and transactions are immediately considered valid, offering faster finality and additional privacy. However, ZK-Rollups require more complex computation, which has historically been a challenge for deployment on Bitcoin.

Although rollups were initially designed for Ethereum, the appeal of enhancing Bitcoin's scalability has prompted researchers and developers to explore how similar solutions can be adapted to Bitcoin’s architecture. Given Bitcoin's conservative development philosophy, incorporating rollups poses unique technical challenges, such as ensuring compatibility with Bitcoin's UTXO model and its relatively limited scripting capabilities compared to Ethereum’s account-based system.

To address these challenges, innovative approaches like BitVM (Bitcoin Virtual Machine) have emerged. BitVM introduces a way to execute complex contracts and proofs without requiring a soft fork, thereby preserving Bitcoin's strong focus on decentralization and security. BitVM opens the door to implementing rollup solutions such as zk-proofs on Bitcoin while maintaining the integrity of the Bitcoin protocol.

The adoption of rollups on Bitcoin could represent a major breakthrough in its scaling roadmap. By leveraging rollups, Bitcoin could significantly enhance its transaction throughput, making it more suitable for everyday micro-transactions, decentralized applications (dApps), and even cross-chain interoperability, without sacrificing the security and decentralization that have been central to its identity.

As the development of rollup technology on Bitcoin accelerates, it is becoming an important area of focus for Bitcoin developers and the broader blockchain community. This section will explore the current landscape of rollups on Bitcoin and provide insights into their potential to shape Bitcoin's future.

Current State of Rollups on Bitcoin

The Bitcoin 2024 conference in Nashville showcased significant advancements in Bitcoin rollups, notably with two teams—BitcoinOS and BitVMX—verifying zk proofs on the Bitcoin mainnet. Both approaches rely on BitVM (Bitcoin Virtual Machine), enabling Turing-complete contracts on Bitcoin without the need for a soft fork. This marks a milestone for Bitcoin, opening up the potential for complex smart contracts previously seen on other blockchains like Ethereum.

A key difference between BitcoinOS and BitVMX is the level of trustless execution. While both rely on BitVM, BitcoinOS, through its BitSnark protocol, showcases an optimistic rollup-like design, where trust is placed on multi signature schemes, whereas BitVMX leans towards a more complex zk-proof verification model. L2 Iterative Ventures' Weikeng Chen points out that the addition of OP_CAT in Bitcoin's future could remove the multisig trust assumption, but BitVM's current approach remains cheaper and more feasible for on-chain implementation.

The introduction of these frameworks signals a shift in the Bitcoin ecosystem. For example, the Spiderchain project by Botanix Labs is using BitVM to build a decentralized proof-of-stake layer-2, showing how BitVM can serve as a base for more advanced systems.

The challenge-response model used by BitcoinOS, however, brings up questions of scalability, as its settlement process can involve multiple challenge iterations. Early tests on Bitcoin's mainnet with BitcoinOS demonstrated this with 52 small transactions, but whether it will scale efficiently remains uncertain.

Future Outlook for Rollups on Bitcoin

The future of rollups on Bitcoin hinges on several factors, from the potential activation of OP_CAT to the further refinement of BitVM and zk-proof verification processes. StarkWare's Circle STARKs present a promising path toward higher efficiency in zk-proofs, enhancing scalability and security for rollup solutions. If solutions like these become production-ready, Bitcoin could see the implementation of rollups that allow advanced use cases like Ethereum-style smart contracts, bridging the gap between Bitcoin and other more flexible blockchains.

Optimistic Rollups and ZK-Rollups both promise to increase Bitcoin's transaction throughput significantly. Optimistic Rollups could potentially boost Bitcoin's capacity to over 2000 transactions per second (TPS), a significant leap from its current average of 4.6 TPS. ZK-Rollups, with even higher throughput and privacy benefits, present a scalable and secure alternative.

The adoption of rollups could reduce transaction fees, enhance Bitcoin's usability for micro-transactions, and foster broader adoption. However, it is still too early to predict how and when these technologies will be integrated into Bitcoin Core. Challenges around fraud-proof verification, state management in challenge-response protocols, and governance will need to be addressed before rollups can be fully operational at scale.

Despite these challenges, the potential for rollups to drive Bitcoin's next wave of growth is immense. Rollups could transform Bitcoin's infrastructure, making it more efficient and unlocking new possibilities for decentralized applications (dApps), interoperability with other chains, and broader usage beyond a store of value.

The age of programmability on the Bitcoin blockchain is upon us. This evolution will use core learnings from the EVM programmability space, like zk-verification. Surge is spearheading this with zk-aggregation and decentralized verification mechanism which allows developers to build app-specific rollups. Further, this method of scaling will not rely and be disrupted by soft-forks or core level updates on Bitcoin.

Key Challenges in Layer 2 Adoption

One of the core challenges in developing a Layer 2 solution is the concern over centralization. Users must trust that the sidechain and its associated bridge are secure and reliable. To gain broader adoption within the crypto community, Layer 2 solutions must address these centralization concerns.

While Rootstock offers a partial solution to this issue, the broader blockchain space urgently needs to establish standardized protocols and improve interoperability to facilitate smoother integration across various platforms.

Bibliography

- What is RSK
- The State of L2 Adoption in 2024
- Everyone Wants to Build a Bitcoin Rollup
- What Is a Sidechain?
- The Liquid Network
- The Bitcoin Rootstock sidechain
- Cons of Rootstock (RSK)
- What is the Nakamoto Upgrade?
- Stacks DeFi TVL

PYOR

The Ultimate Metalayer To Scale Bitcoin

A Decentralised Network for Modular Rollups and dApps to Unlock the New Bitcoin Economy

Check out at → surge.build

This report is created by **PYOR** a digital assets data company for institutional investors and hedge funds.
Our investors include – Castle Island Ventures, Hash3 Capital, Coinbase Ventures, and Balaji Srinivasan, among others.