What is Stacks and what challenges may this BTC Layer2 Network face?

Beosin · Follow
9 min read · 1 day ago

Since the launch of the Ordinals protocol in February 2023, the minting of BTC NFTs and the FOMO of BRC-20 tokens have led to a highly active BTC network. The consequence was a surge in the network fees and a network congestion. In addition, the fact that BTC network does not support smart contracts limits the development of more complex business services. The market began to focus on BTC layer2 and dapps, hoping to capture the benefits of BTC's ecological growth.

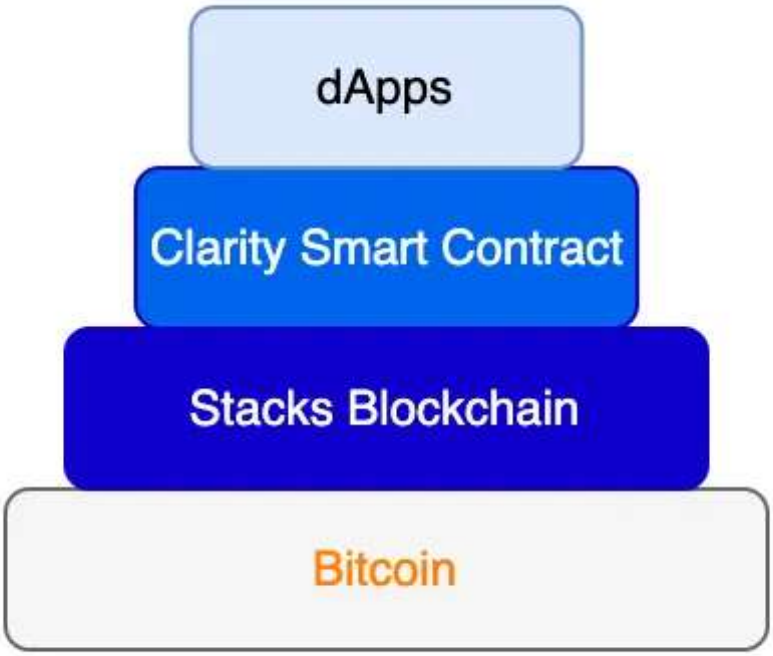
In this article, we will analyze Stacks, a BTC layer2 network. We will discuss its architecture design, its ecosystem, and the challenges it may face.

What is Stacks?

Stacks was founded by Muneeb Ali based on his doctoral thesis, which carefully introduced an Internet framework built around BTC. In the early days, the project was called Blockstack, and it was officially renamed Stacks in 2020. It defines itself as a smart contract layer for BTC.

Architecture design:

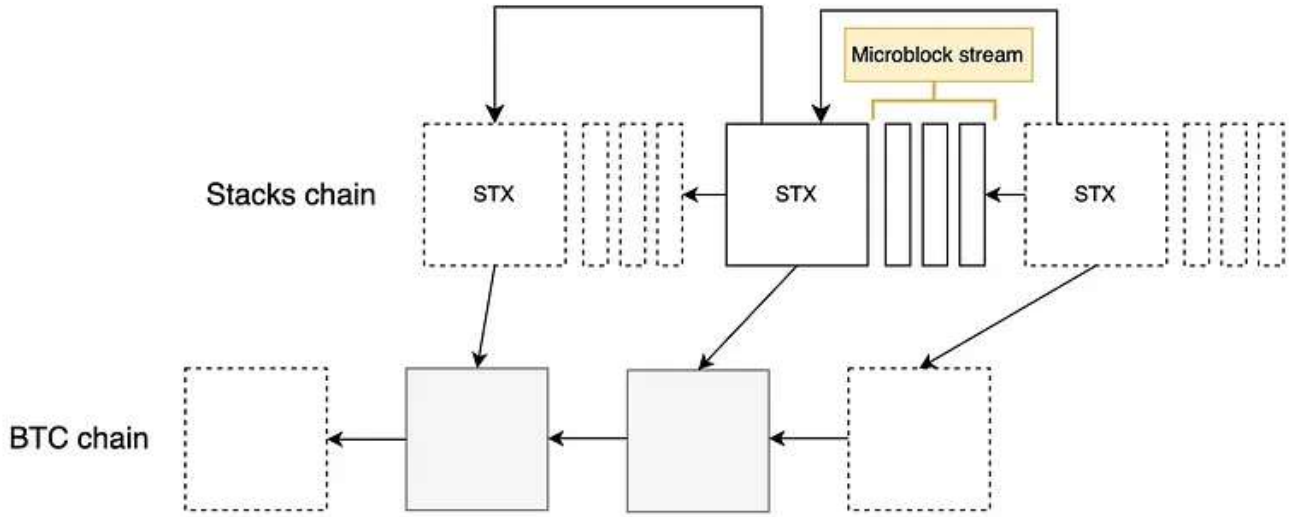
Stacks executes smart contracts written in Clarity on its own blockchain and finalize transactions on BTC network. The two chains interact through the Proof of Transfer mechanism (the details are introduced in the consensus mechanism), so as to use the security of BTC network to ensure the security of Stacks network.



Source: Beosin

Since the transaction data of Stacks need to be confirmed by BTC network, and BTC network generates a new block about every 10 minutes, how can Stacks scale itself and speed up?

First of all, Stacks has designed a special mechanism that **allows multiple small blocks called microblock streams to be generated on Stacks network, allowing the miners responsible for confirming the current block of Stacks to make full use of the time interval of BTC network to generate two blocks to process more transactions. When BTC confirms the current block, these microblocks will also be finalized, and the next Stacks block will be linked to the current last microblock.** As shown below:



Source: Dystopia Labs, Beosin

Mechanism Detail: sips/sip-001-burn-election.md at main · stacksgov/sips · GitHub

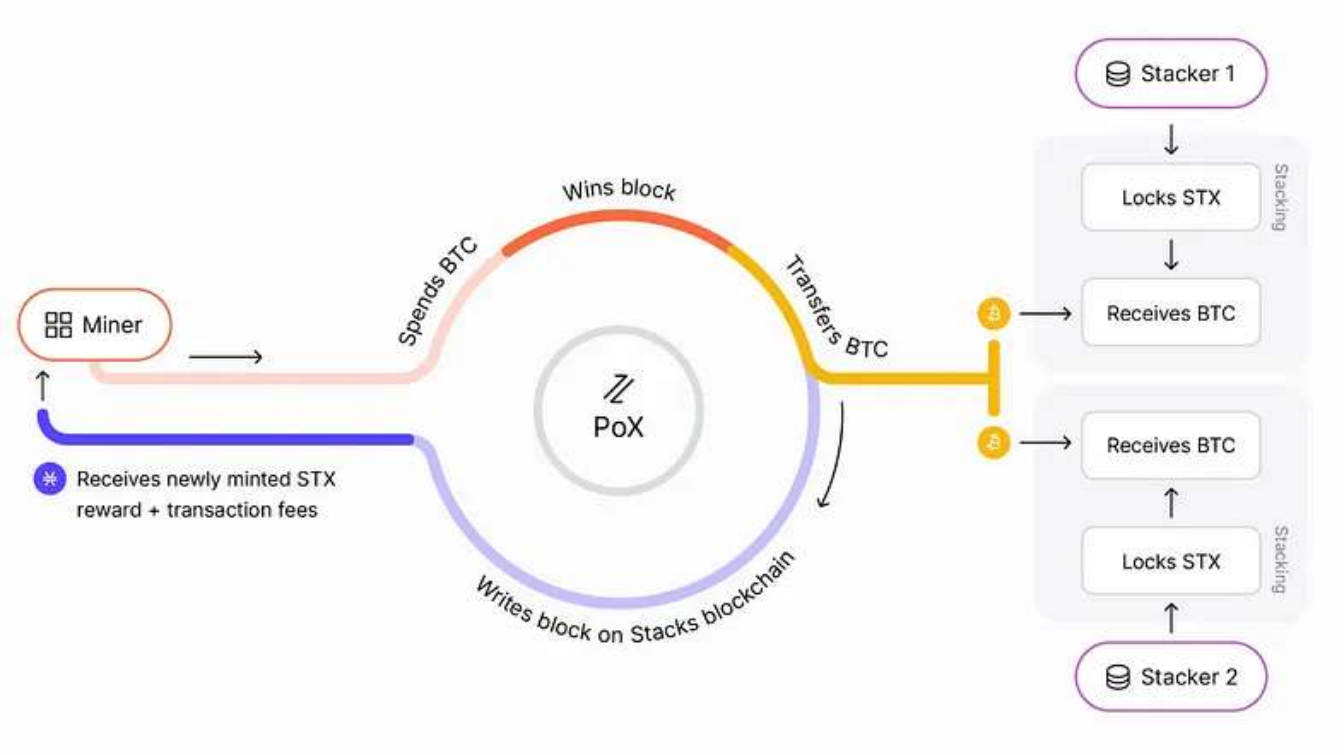
Stacks sets that the miners who confirm the microblocks will get 60% of these micro-block fees, and the nodes that generate these micro-blocks will get 40% of the fees to encourage miners to validate micro-blocks and avoid the abuse of microblocks.

Secondly, Stacks has launched Hiro HyperChains, which can be viewed as layer2 of Stacks, providing developers with a high-performance blockchain development platform to meet low-latency, high-TPS application scenarios. Other types of subnets can also be built on Stacks to meet various needs. These subnets will first confirm transactions on Stacks network, and then confirm the final status on BTC network.

Consensus mechanism: Proof of Transfer (PoX)

Stacks uses a consensus mechanism called Proof of Transfer (PoX). PoX is a consensus algorithm between two blockchains, which can be regarded as Proof of Work + Proof of Burn. Like PoW, PoX requires miners to spend existing resources (BTC) to compete for the opportunity to create the next Stacks block; similar to PoB, PoX requires miners to “burn” BTC to get STX token rewards.

A feature of PoX is that the bitcoins spent by miners are not burnt, but transferred to STX token holders who have locked STX tokens, which is called Stacking. Through the PoX mechanism, miners spend BTC to compete for the right to produce blocks on Stacks, and get STX token rewards and transaction fees for the block; STX holders get BTC rewards by locking STX tokens, and the current APY is about 9%.



Source: Proof of Transfer | Stacks Docs

The Stacks network will use a verifiable random function(VRF) to randomly select block producers (the more BTC spent, the greater the probability of being selected). When miners obtain the right to produce the next Stacks block, they will start packaging the new Stacks block. Each Stacks block contains a hash pointer pointing to the previous Stacks block and a hash pointer pointing to the corresponding BTC block, thus connecting Stacks network and BTC network.

What will happen to Stacks' next important Nakamoto upgrade?

Nakamoto is the next important upgrade of Stacks and is expected to be completed in Q4 of 2023. The upgrade will improve the Clarity language, introduce subnets and sBTC. This upgrade will provide comprehensive basic conditions for the next outbreak of BTC ecosystem.

Subnet:

Stacks will introduce subnets that support other programming languages and execution environments, such as EVM subnets. This will make it easier for projects on Ethereum to migrate to Stacks, allowing Stacks to capture the liquidity of the EVM chains. At the same time, these smart contracts can use Bitcoin as their assets, and finally settle on Bitcoin network.

Subnet is the scaling solution of Stacks, which improves network performance by sacrificing certain decentralization. The subnet can choose miner nodes with high

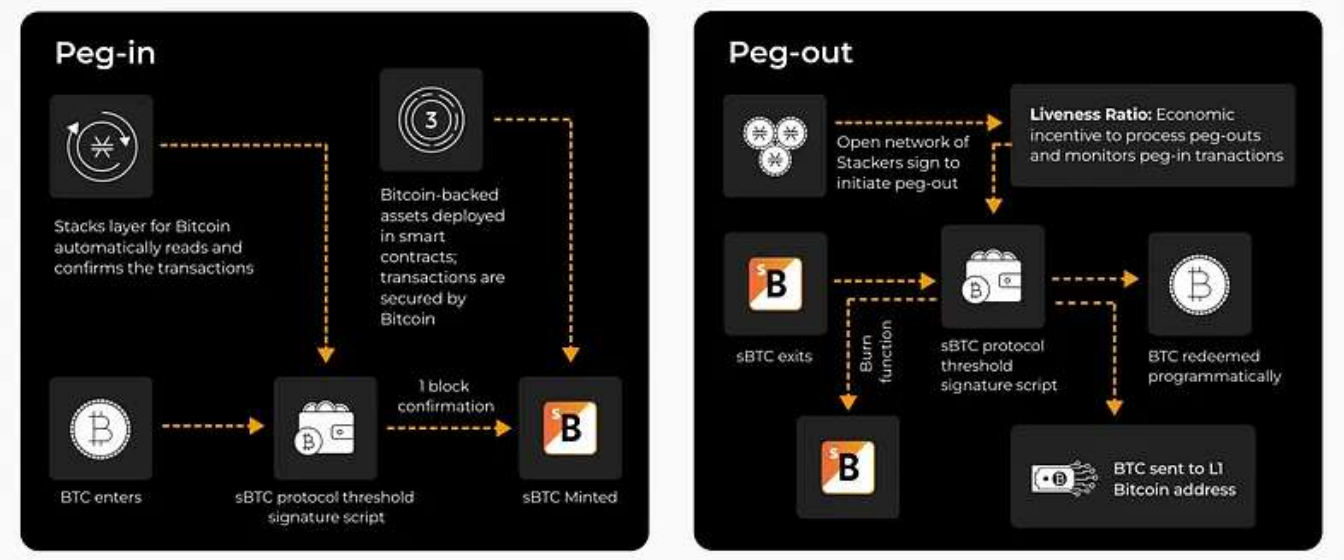
network bandwidth or miner nodes belonging to the subnet whitelist to process subnet transactions to ensure high performance.

sBTC:

sBTC is a decentralized BTC anchoring solution launched by Stacks in the Nakamoto upgrade. The introduction of sBTC will solve the problem of how to use BTC in the BTC layer2 network. Smart contracts on Stacks and Stacks subnets can use sBTC to carry out various DeFi businesses such as lending, exchanging, and minting stablecoins, increasing the TVL of BTC ecosystem.

At present, there are many kinds of BTC-anchored assets in the market, such as Wrapped BTC (wBTC), RenBTC and tBTC that introduce BTC into Ethereum and RBTC that introduces BTC into a BTC layer2, RSK network. The anchoring principle is roughly the same: first lock BTC on BTC network, then mint the same number of anchored BTC on the target network; destroy the anchored BTCs on the target network, and then unlock the same number of BTCs on BTC network. The key lies in the degree of centralization of locked BTC. For example, wBTC is BTC locked by users held by cryptocurrency custodian service providers, and the risk of centralization is relatively high. 3AC and Alameda were the cooperative dealers of wBTC before, and their collapse caused some users to be unable to exchange wBTC back to BTC smoothly. RBTC uses the multi-signature address of the BTC network to lock BTC, and uses the Powpeg mechanism to ensure that the information of locked BTC is correctly delivered to the RSK network, reducing the risk of centralization.

sBTC uses the threshold signature wallet to manage locked BTC in the BTC network, and mints sBTC through smart contracts in the Stacks network, thereby realizing non-custodial and decentralized BTC anchoring. To perform a peg-out operation to unlock BTC, a valid signature must be obtained: at least 70% of the stackers (users who lock STX tokens and get BTC rewards in PoX) signature power. This greatly reduces the centralization risk of asset custody.



Source: Whitepaper | sBTC: A Decentralized Two-way Peg for Bitcoin

Advantages of Stacks

Ecological advantages:

Stacks is currently the most active BTC layer2 network. After the launch of the Ordinals protocol, the market's interest in BTC NFT has gradually increased, and NFT activities on Stacks have also become active. According to Muneeb Ali, the Stacks network has minted over $650,000 worth of NFTs.

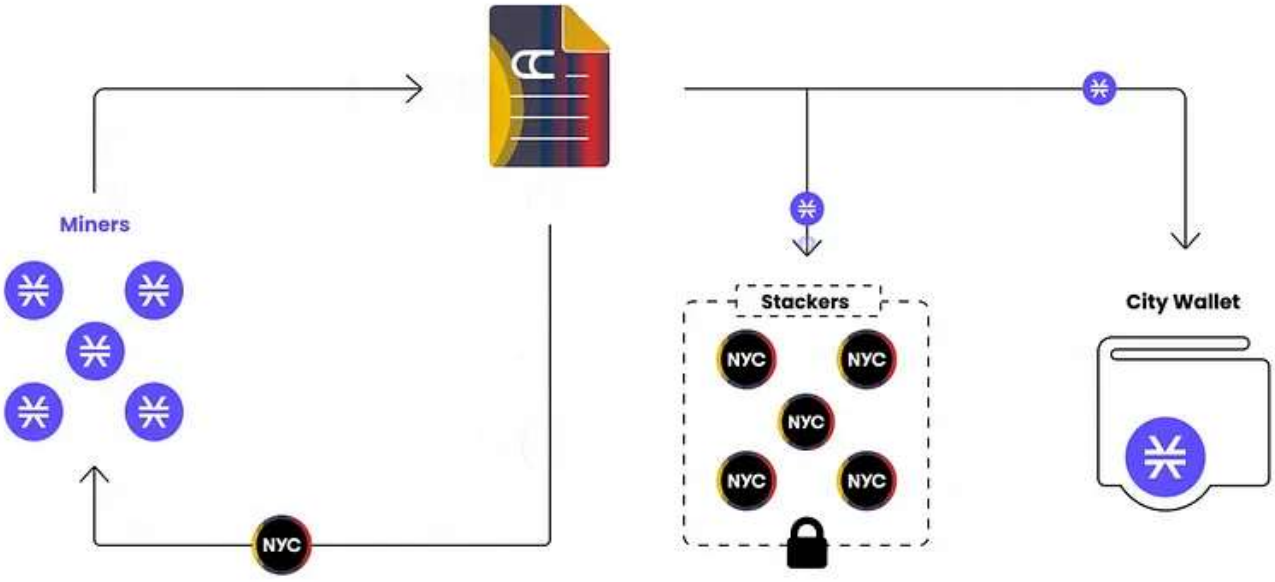
In addition, the TVL of Stacks' DeFi project Alex has increased by 500% in the first half of this year, and the current TVL has reached $24.61M. Alex is the leading Dex of Stacks, with very complete products, providing services such as swap, lending, ido, and perpetual contracts. With the upgrade of Stacks and the growth of the BTC ecosystem, Alex still has great potentials.

Arkadiko built on Stacks is similar to MakerDAO, focusing on minting the decentralized stablecoin USDA to improve the asset liquidity of the Stacks network. Although the protocol has not exploded yet, we can look forward to its performance after sBTC is introduced into the Stacks network.

Source: https://twitter.com/muneeb/status/1456007656305479684

Citycoin:

CityCoin is a protocol built on Stacks that allows the community to contribute to the city's treasury by spending STX tokens to earn rewards in Citycoin. Participants spend STX tokens to become "miners" to mine Citycoin. 30% of the spent STX tokens will be stored in the city treasury, and the remaining 70% will be rewarded as CityCoin Stackers. If you understand the PoX mechanism above, the incentive design of Citycoin is almost the same.



source: Mining CityCoins — CityCoins

Miami was the first city to join the project, launching MiamiCoin (MIA). The total value of the Miami City Vault wallets exceeds $20 million, representing approximately 2 percent of Miami's public budget, which will be used to give back to the local community. New York subsequently joined the initiative, launching NYCCoin. This allows more people to have access to digital assets and wallets, raises funds for public services in the region, and also helps establish the Stacks brand.

Stacks possible challenges

Risks of PoX:

PoX requires BTC miners to spend BTC to participate in the Stacks block competition, so as to obtain STX token rewards. At present, the competition among BTC miners is small, and the income is huge (1000 STX/block, the reward is halved every 4 years, and finally reduced to 125 STX/block), and miners have great motivation to participate in the competition of Stacks. As can be seen from the data in the figure below, miners participating in 7278 competitions spent about 3.56 BTC and obtained 1,337,000 STX tokens (currently about 29.4 BTC)

Address.	Total Spent (sats)	Total Participation	Total Block Won	Total Reward (STX)
bc1q3l89...dkszael4	3200000	18	0	0
bc1qgdq6...m5ggafcr	63570800	4531	388	429000
SP06HBN5...XC5NWJ3P	15000000	50	8	24664
SP0B0EYF...ZZAWEKZE	92704000	212	0	0
SP1000R3...JBE8SKWP	3557543700	7278	1241	1337000

Statistics: Onstacks | Onchain explorer on Stacks

If the Stacks rewards decrease in the future, and the number of miners participating in the competition increases, the STX token rewards miners get are less than the BTC they spend, will miners continue to participate in PoX? According to Onstacks data, there are currently only 6 active miners participating in PoX. Stacks will continue to develop. Assuming that the number of miners only increases by 10 times, and the STX reward is about to be halved to 500 STX/block in about a year, then the STX/BTC exchange rate needs to be increased by 2.5 times to ensure that miners are profitable to be motivated to participate in PoX. Therefore, either the value of STX can continue to increase, or there is an upper limit on the number of miners participating in the competition, in order to

ensure the continued operation of the Stacks network. Can Stacks, like BTC, recover even after miners “give up”?

Vulnerabilities of PoX contract:

On April 19, 2023, Stacks discovered that there was a vulnerabilities in the stacks-increase function in its pox-2 contract, resulting in the bc1qpyjutel6d4gj50dscphjrqcp29ljtfjel7ccap address receiving more BTC rewards than theoretically calculated. **This miscalculation is because the stacks-increase function mixes operations such as database modifications with the logic to determine state changes, and then uses reward-cycle-total-stacked as a global variable to hold the state through successive iterations.** At present, the Stacks team temporarily switches Stacks to the PoB consensus, and then replaces the pox-2 with the pox-3 contract. Some developers in the community called for improving Clarity to a functional, expression-oriented development language to facilitate static analysis and formal verification to avoid such vulnerabilities from recurring on the mainnet in the future.

Summarize

Stacks is undoubtedly the leading project of the BTC layer2 network, with a sustainable development of ecosystem and high-quality brand effect and is about to make an important upgrade: reliable and trustless BTC bridge, sBTC, subnet and the Clarity language improvement. However, **at the same time, the complexity of the PoX mechanism has brought some difficulties to the Stacks team, and the introduction of subsequent subnets will increase the complexity of the entire network. How to ensure the correct operation of the Stacks network and successfully complete the Nakamoto upgrade is a challenge that the Stacks team needs to work hard to solve.**