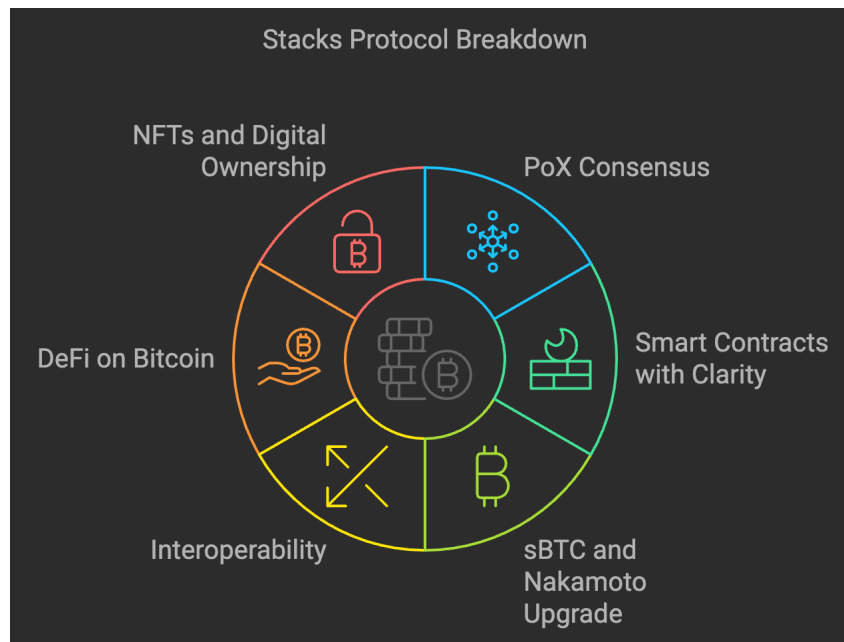




Stacks — Research Document (.10.24)

Project Overview



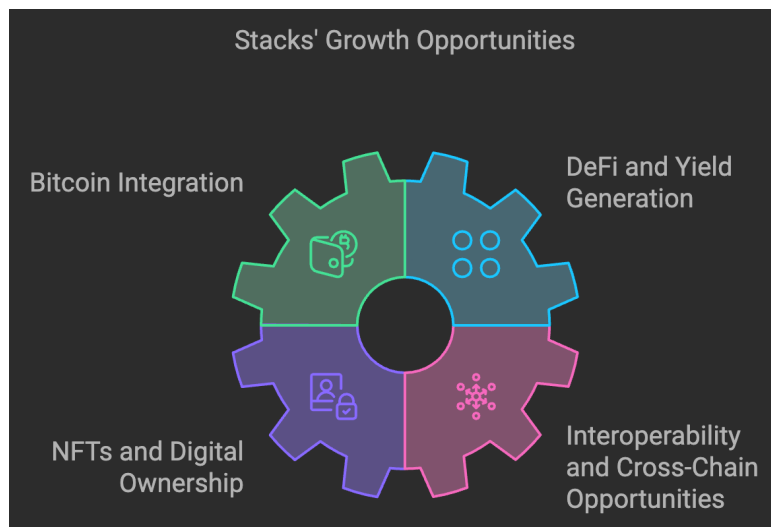
- **Stacks Protocol Overview:** Stacks is a Layer 2 solution that brings smart contracts and decentralized applications (DApps) to Bitcoin, extending its utility while leveraging Bitcoin's security through the innovative Proof-of-Transfer (PoX) consensus. This mechanism links the Stacks blockchain directly to Bitcoin, ensuring the safety and reliability of the Bitcoin blockchain without altering it.
- **Key Features:**
 - **PoX Consensus:** Stacks uses PoX, tying each Stacks block to a Bitcoin block, which ensures the security and stability provided by Bitcoin.
 - **Smart Contracts with Clarity:** The Clarity programming language allows secure and predictable smart contracts, making it suitable for DApps, DeFi, and NFTs.
 - **sBTC and Nakamoto Upgrade:** sBTC will make Bitcoin programmable by allowing non-custodial Bitcoin transactions within Stacks-based smart contracts, opening up Bitcoin DeFi opportunities. The Nakamoto upgrade will also improve transaction speed to about 5 seconds.
 - **Interoperability:** The upcoming upgrades will add support for multiple environments (e.g., EVM and Rust VM), enhancing cross-chain compatibility and liquidity.

- **Use Cases:**

- **DeFi on Bitcoin:** Stacks introduces DeFi capabilities like lending, borrowing, and yield farming for Bitcoin holders.
- **NFTs and Digital Ownership:** By using Clarity smart contracts, Stacks enables secure Bitcoin-backed NFTs, offering enhanced immutability and security.

Market & competitors

Market:



- **Integration with Bitcoin Economy:** Bitcoin is the most well-known cryptocurrency, with over 50 million addresses holding non-zero balances and a market capitalization exceeding \$1.3T. Stacks extends Bitcoin's functionality while leveraging its brand and trust to attract users and developers. Currently, most Bitcoin holders are passive investors; activating even a small fraction of these users for DeFi participation and DApps could lead to significant growth. For instance, converting just 5% of Bitcoin holders into active participants would result in over 2.5 million new users for Stacks' ecosystem.
- **DeFi and Yield Generation (sBTC):** Stacks introduces Bitcoin DeFi, allowing users to lend, borrow, and yield farm using their BTC without moving it off the Bitcoin network. The global DeFi market currently has over \$80 billion in Total Value Locked (TVL), with Ethereum alone accounting for more than 50% of this value. The introduction of sBTC by Stacks enhances Bitcoin's liquidity and enables Bitcoin-collateralized stablecoins, opening new opportunities for Bitcoin holders to directly participate in DeFi activities. Even capturing a small percentage of the DeFi TVL could mean billions of dollars flowing into Bitcoin-native DeFi on Stacks.
- **NFTs and Digital Ownership:** NFTs on Ethereum and other platforms have surpassed \$4 billion in market value in 2023. The Stacks ecosystem with STX20 token standard facilitates Bitcoin NFTs, offering enhanced

security and immutability compared to other platforms. With the Nakamoto upgrade, Stacks will support high-performance NFT marketplaces. By positioning Bitcoin as a trusted and secure platform for NFTs, Stacks could capture a portion of this \$4 billion market, potentially attracting collectors and creators looking for the permanence offered by Bitcoin-backed NFTs.

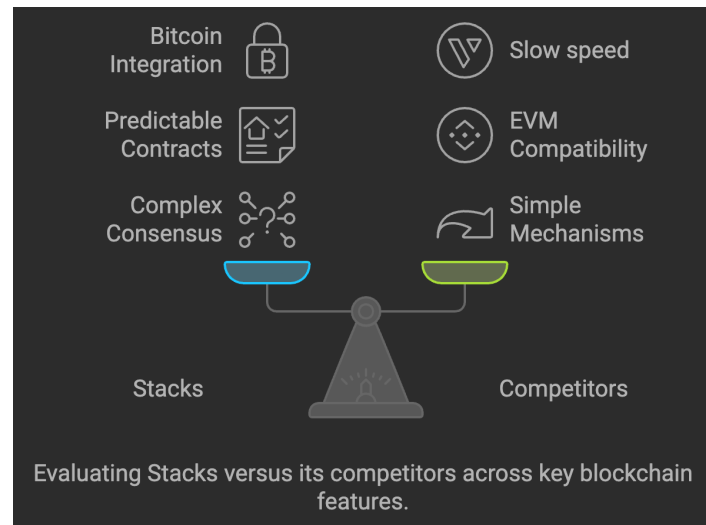
- **Interoperability and Cross-Chain Opportunities:** With the upcoming Nakamoto upgrade, Stacks will introduce subnets, enhancing compatibility with multiple programming environments, including EVM subnets and Rust VM. This provides Stacks with interoperability that could open doors to collaborate with ecosystems like Ethereum, which currently boasts a TVL of over \$27 billion across its L2 networks. Cross-chain applications could enhance Bitcoin's role in decentralized finance and broaden its reach beyond traditional boundaries.
- **Summary of Growth Prospects:** The Stacks ecosystem is well-positioned for substantial growth, leveraging Bitcoin's brand trust, security, and vast user base. The potential market opportunities range from capturing a share of previous mentioned markets, to becoming a preferred platform for enterprises interested in secure, compliant blockchain solutions.

Competitors:

Feature/Aspect	Stacks	Lightning Network	Rootstock (RSK)	Merlin	BOB	Sovryn
Type	Bitcoin Layer 2 with smart contracts	Bitcoin Layer 2 (state channels)	Bitcoin Sidechain (EVM-compatible)	Bitcoin Sidechain	Bitcoin Rollup (Optimism stack)	Bitcoin Sidechain (Rootstock-based)
Consensus Mechanism	Proof-of-Transfer (PoX)	Off-chain channels + Bitcoin finality	Merged mining with Bitcoin (PoW)	PoS-style Validators	Optimistic Rollup (using EVM)	Merged mining with Bitcoin (PoW)
Smart Contract Support	Yes (Clarity language)	No	Yes (Solidity/EVM)	Yes (EVM, zk-Rollup support)	Yes (EVM-compatible)	Yes (Solidity/EVM)
Native Token	sBTC	No separate token	RBTC (1:1 pegged to BTC)	None, uses BTC	iBTC	RBTC (1:1 pegged to BTC)
Primary Use Cases	DeFi, NFTs, smart contracts	Micropayments, instant BTC transfers	DeFi, smart contracts, DApps	Bitcoin scaling, zk-Rollups	Bitcoin DeFi, Ordinals, Lightning	DeFi (lending, trading, liquidity)
Peg Mechanism	sBTC (1:1 BTC)	No pegging required	Two-way peg with Bitcoin	zk-Rollup-based, multisig bridges	Optimistic Rollup, pegged assets	Two-way peg with Bitcoin
Transaction Speed	~5 seconds (after Nakamoto upgrade)	Instant through state channels	10-minute Bitcoin block time (depends)	Fast (zk and rollup-based solution) ~ 3s	Fast (Rollup design) ~ 2s	Bitcoin block time, merged mined
Key Strengths	Bitcoin-backed security, DeFi, NFTs	Micropayment capabilities, low fees	EVM compatibility, BTC-backed assets	zk-Rollup integration, speed	EVM-compatible, multi-chain focus	Comprehensive DeFi services

Feature/Aspect	Stacks	Lightning Network	Rootstock (RSK)	Merlin	BOB	Sovryn
Key Weaknesses	Complex consensus, slower development	Centralization risks, scaling issues	Dependency on federation, complexity	New technology, complexity	Developing ecosystem, complexity	Dependency on Rootstock, federation
Developer Focus	Smart contracts, DApps, DeFi	Payment solutions, merchant tools	Ethereum-compatible DApps	zk-rollups, scalability solutions	Bitcoin/Ethereum cross-chain apps	DeFi-focused (lending, liquidity)
Security Model	Inherits Bitcoin's security	Bitcoin's security + off-chain channels	Bitcoin's PoW + federation security	zk-Rollup, federated multisig	zk and optimistic Rollup	Bitcoin's PoW + federation
Governance	Stacks Foundation, open development	None (open source community)	Federation of multiple companies	Decentralized PoS validators	Community-governed	Sovryn community + Rootstock Labs

Competitors analysis:



• Type and Consensus Mechanism

- **Stacks Advantage:** Stacks has a unique hybrid consensus model (PoX), which tightly integrates with Bitcoin for security while allowing programmability and DeFi.
- **Drawbacks:** The Lightning Network provides a simpler, more intuitive payment solution without the need for a complex consensus mechanism. Moreover, Stacks' PoX mechanism adds complexity, which may slow down development compared to simpler systems like the Lightning Network's state channels.

• Smart Contract Support

- **Stacks Advantage:** Stacks' use of Clarity provides greater predictability and security for smart contracts compared to Solidity-based platforms, which are more prone to exploits.
- **Drawbacks:** The lack of EVM compatibility is a significant drawback for Stacks. Developers familiar with Ethereum may find the learning curve steep, and it may limit the portability of DApps from Ethereum to

Stacks compared to platforms like RSK or Merlin that offer full EVM compatibility.

- **Native Token and Peg Mechanism**

- **Stacks Advantage:** Stacks benefits from sBTC to offer a Bitcoin-like asset within its DeFi ecosystem, bringing programmability while maintaining the value of BTC.
- **Drawbacks:** Not found since two-way peg Bitcoin asset seems to be the most relevant technology right now.

- **Transaction Speed**

- **Stacks Advantage:** The Nakamoto upgrade has positioned Stacks as one of the faster Bitcoin layer solutions compared to traditional sidechains like RSK or Sovryn.
- **Drawbacks:** Lightning Network remains unmatched for instant transactions due to its use of off-chain state channels, which Stacks cannot compete with in terms of speed for simple Bitcoin transfers.

- **Key Strengths and Weaknesses**

- **Stacks Advantage:** Stacks shines in its versatility, enabling both DeFi and NFTs while maintaining strong security. Its integration with Bitcoin and smart contract capabilities make it a versatile option for developers aiming for a secure, Bitcoin-based environment.
- **Drawbacks:** The complexity of the Proof-of-Transfer consensus mechanism, combined with the slower development pace, can make it challenging for Stacks to quickly adapt compared to other solutions like **Merlin** or **BOB**, which are specifically designed for faster scalability.

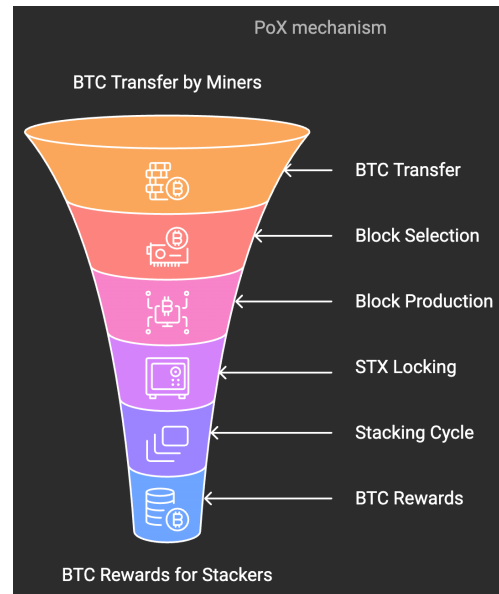
Technical Overview

PoX mechanism:

- **Overview of Proof of Transfer (PoX):** PoX operates by utilizing Bitcoin's existing Proof of Work (PoW) system, allowing Stacks to inherit Bitcoin's security and finality. This mechanism effectively recycles the computational power used in Bitcoin mining, enabling Stacks to secure its transactions without requiring miners to invest in specialized hardware or consume excessive energy.

- **Key Components:**

- **Miners:** Participants who wish to mine new Stacks blocks do so by transferring Bitcoin (BTC) to designated addresses. This transfer does not burn the BTC; instead, it is sent to other network participants known as Stackers.
- **Stackers:** Users who lock their STX tokens (Stacks' native cryptocurrency) for a predetermined cycle. In return for locking their tokens, Stackers earn a share of the BTC that miners transfer during the mining process.



- **Mining Process:**

- **BTC Transfer:** Miners send BTC to specific addresses associated with Stackers. The amount of BTC transferred influences their chances of being selected as the next block producer.
- **Block Selection:** The winning miner is determined through a weighted random selection process, where the probability of winning is proportional to the amount of BTC they have transferred compared to other miners.
- **Block Production:** Once selected, the miner creates a new block on the Stacks blockchain and receives rewards in the form of newly minted STX tokens and transaction fees from that block.

- **Stacking Process:**

- Stackers lock their STX tokens for one or multiple cycles (typically two weeks).
- They can choose to stack independently or pool their STX with others for potentially greater rewards.
- Upon completion of the stacking cycle, their STX tokens are unlocked, and they receive BTC rewards proportional to their locked amount.

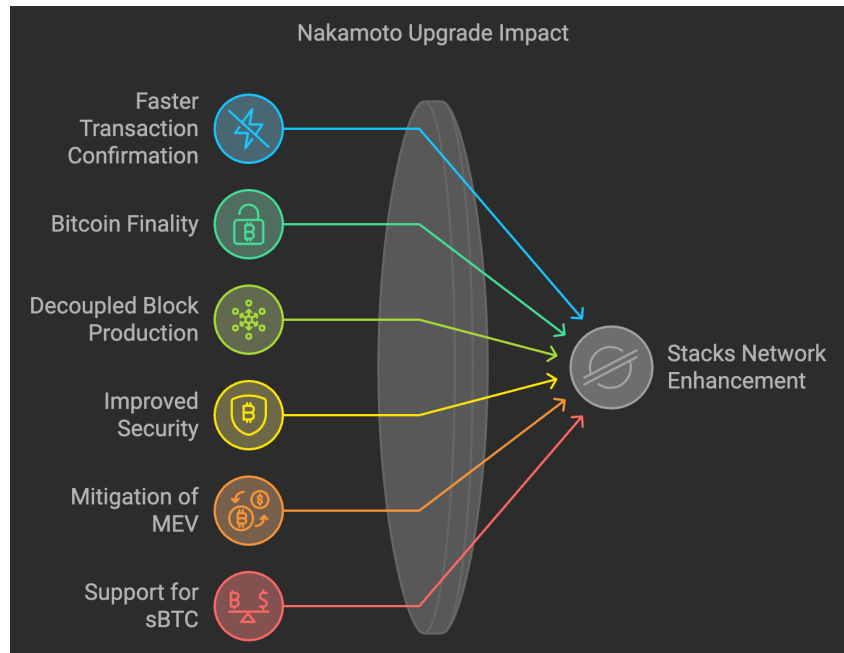
- **Benefits of PoX**

- **Security:** By anchoring Stacks transactions to Bitcoin, PoX ensures that any attempt to alter Stacks' transaction history would also require altering Bitcoin's history, making it highly secure.
- **Energy Efficiency:** Unlike traditional PoW systems that require substantial energy consumption, PoX allows miners to utilize existing Bitcoin resources without additional energy expenditure.
- **Incentivization:** Both miners and Stackers are economically incentivized to participate in the network. Miners earn STX and transaction fees, while Stackers earn BTC rewards, promoting long-term engagement with the ecosystem.

Conclusion: Proof of Transfer is a novel consensus mechanism that effectively combines elements of both Proof of Work and Proof of Stake while introducing unique features tailored for the Stacks network. By

leveraging Bitcoin's security and enabling a user-friendly staking process, PoX positions Stacks as a robust platform for building decentralized applications on top of Bitcoin's foundational layer

Nakamoto upgrade:



- **Key Enhancements from the Nakamoto Upgrade**

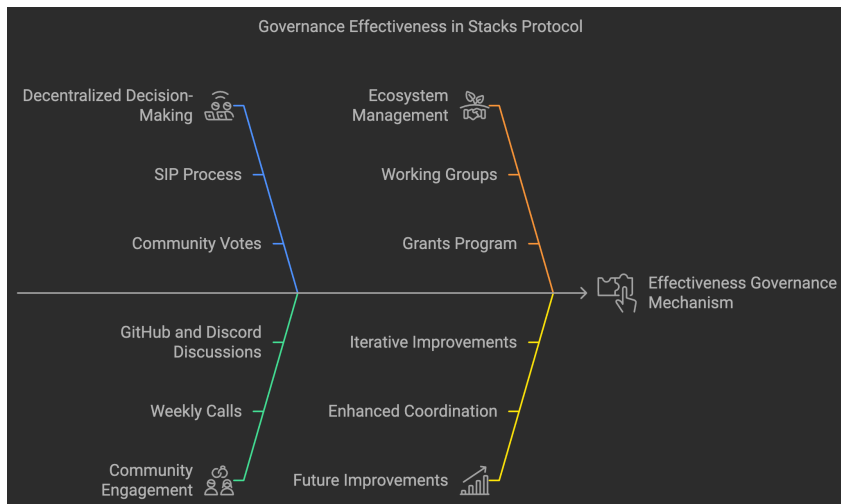
- **Faster Transaction Confirmation Times:** The Nakamoto upgrade introduces a new mechanism for block production that reduces transaction confirmation times dramatically. Instead of waiting for Bitcoin's typical 10-minute block time, Stacks aims to produce blocks approximately every 5 seconds. This change allows user-submitted transactions to be confirmed in under a minute, which is particularly beneficial for decentralized applications (dApps) that require quick interactions, such as those in the DeFi sector.
- **Bitcoin Finality:** With the Nakamoto upgrade, Stacks transactions achieve 100% Bitcoin finality. This means that once a transaction is confirmed on the Stacks blockchain, it is as irreversible as a confirmed Bitcoin transaction. This enhancement is crucial for building trust in the network, as it aligns the security guarantees of Stacks transactions with those of Bitcoin.
- **Decoupled Block Production:** The upgrade decouples the production of Stacks blocks from Bitcoin block arrivals. Previously, Stacks block production was tied to Bitcoin's block times, but now miners can produce multiple Stacks blocks between Bitcoin blocks. This change not only increases throughput but also enhances the responsiveness of the network to user transactions.
- **Improved Security Against Reorganizations:** The Nakamoto upgrade incorporates mechanisms to resist Bitcoin reorganizations (reorgs). Valid Stacks transactions remain confirmed even during Bitcoin reorgs, ensuring that most Stacks transactions retain their validity regardless of changes in the Bitcoin blockchain state. This resilience enhances the overall integrity and reliability of the Stacks network.

- **Mitigation of Miner Extractable Value (MEV):** The upgrade introduces changes to mitigate Miner Extractable Value (MEV) opportunities that could affect Proof of Transfer (PoX) operations. By adjusting how miners are selected and ensuring that they cannot unilaterally orphan confirmed transactions, Nakamoto enhances fairness and security within the mining process.
- **Support for sBTC:** The Nakamoto upgrade sets the stage for **sBTC**, a trust-minimized two-way peg system that allows for seamless transfer of Bitcoin onto the Stacks network. This feature enables developers to create programmable applications using Bitcoin while maintaining its security, unlocking new use cases for BTC within the Stacks ecosystem
- **Stacks subnet:** It's a solutions designed to extend the scalability of the Stacks mainchain by offering high-speed, low-cost transactions while maintaining Bitcoin-backed security. Subnets aim to support applications like DeFi marketplaces and NFT mints by improving throughput and reducing latency. They also plan to integrate EVM compatibility, bridging the Bitcoin ecosystem with Ethereum, which will enable interoperability between Bitcoin-based and Ethereum-based decentralized applications.

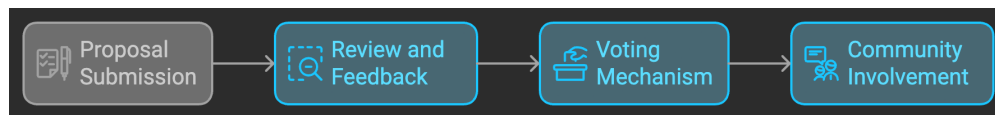
Conclusion: Overall, the Nakamoto upgrade represents a pivotal advancement for the Stacks network by enhancing its integration with Bitcoin and improving performance metrics across the board. With faster transaction speeds, robust security measures, and new functionalities like sBTC, this upgrade positions Stacks as a leading platform for building decentralized applications on top of Bitcoin's foundational layer. The enhancements not only improve user experience but also attract developers looking to leverage Bitcoin's capabilities in innovative ways.

Governance & Decentralization

- **Governance mechanism overview:** The governance of the Stacks protocol is structured to ensure decentralized decision-making, community engagement, and the effective management of the ecosystem. This governance framework is essential for maintaining the integrity and functionality of the Stacks layer, particularly as it evolves with future upgrades. Here's a detailed description based on the provided governance document.



- **Governance Philosophy:** The Stacks Foundation emphasizes decentralization as a core principle, aiming to distribute power and resources in a way that empowers all participants. The foundation recognizes the challenges of effective decentralization, noting that projects can either decentralize too quickly, leading to inefficiencies, or too slowly, resulting in power imbalances. The overarching goal is to create an ecosystem that maximizes utility while minimizing exploitation.
- **Governance Structure:** Governance in Stacks operates through a multi-layered approach:
 - **Stacks Improvement Proposals (SIPs):** The SIP process serves as the formal mechanism for making blockchain-level decisions. It allows community members to propose changes, receive feedback, and review ideas for improvements to the blockchain. SIPs are design documents that outline key features or standards for the Stacks blockchain.
 - **Working Groups:** These are informal groups focused on specific areas of development within the Stacks ecosystem, such as the sBTC working group. While they do not follow a standard decision-making process, their decisions can significantly impact the ecosystem.
 - **Decentralized Grants Program:** This initiative aims to empower community members to make decisions regarding funding for public goods and resources necessary for community growth.
- **Stacks Improvement Proposal (SIP) Process:** The SIP process is fundamental to Stacks governance and consists of several components



- **Proposal Submission:** Community members can submit SIPs outlining proposed changes or improvements.
 - **Review and Feedback:** SIPs undergo a rigorous review process involving SIP editors and a Consideration Advisory Board (CAB), which evaluates proposals before ratification.
 - **Voting Mechanism:** Significant changes that require consensus-breaking alterations may lead to community-wide votes. The last two votes saw increased participation, with nearly 500 community members voting in recent decisions.
 - **Community Involvement:** The SIP process encourages broad participation through weekly calls and discussions on platforms like GitHub and Discord, fostering collaboration between core developers and the wider community.
- **Roles in Governance:** The governance structure includes various roles:
 - **SIP Council:** Comprising editors who assist in drafting SIPs, CAB members who review proposals, and steering committee members who have ratification powers.
 - **Community Contributors:** A broader community of contributors participates in discussions and provides feedback on SIPs, enhancing transparency and inclusivity.

- **Informal Governance Dynamics:** In addition to formal processes like SIPs, informal governance dynamics play a significant role in decision-making within the Stacks ecosystem:
 - **Working Groups:** These groups operate organically to address critical research and development needs. They are instrumental in shaping features that enhance competitiveness among Bitcoin Layer 2 solutions.
 - **Community Collaboration:** There is a growing trend of community members collaborating on decisions outside the formal SIP process, indicating an evolving governance landscape that values open dialogue and cooperation.
- **Future Directions for Governance:** Looking ahead, several initiatives aim to strengthen governance within Stacks:
 - **Enhanced Coordination:** Efforts are underway to improve coordination among working groups to streamline decision-making processes while ensuring community input remains integral.
 - **Decentralized Grants Program Development:** The de-grants initiative will empower community-selected representatives to evaluate grant applications, allowing for more democratic resource allocation.
 - **Iterative Improvements:** The governance framework will continue to evolve based on community feedback and testing, with key improvements expected quarterly.

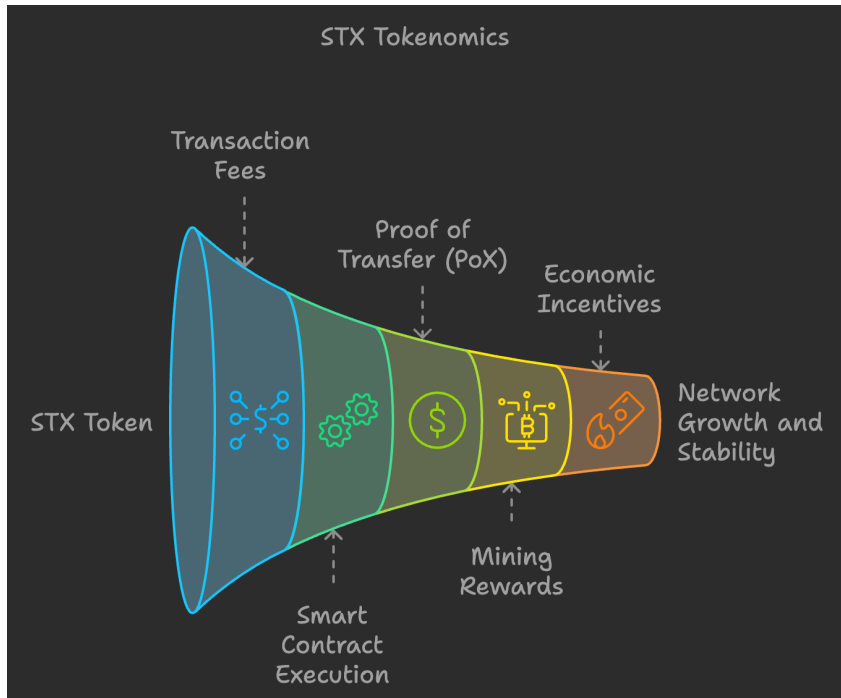
Conclusion:

The governance mechanism of Stacks is designed to foster an inclusive and decentralized ecosystem that encourages active participation from all stakeholders. Through formal processes like the SIP system and informal dynamics such as working groups and community collaboration, Stacks aims to create a balanced governance model that empowers contributors while ensuring effective decision-making. As the ecosystem grows and evolves, ongoing enhancements will be crucial in maintaining alignment with community interests and facilitating sustainable development within the Stacks protocol.

Tokenomics

STX token

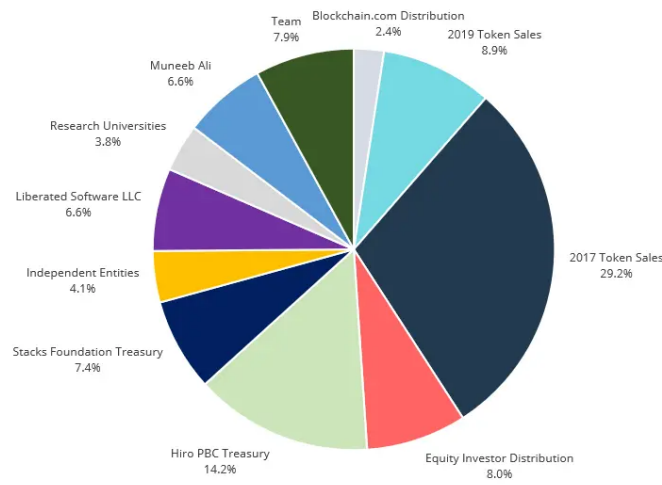
- **Overview of Stacks Tokenomics:** The tokenomics of STX is structured to incentivize network participants, support the protocol's operations, and facilitate the growth of a decentralized economy built on Bitcoin. This overview explores the key components of Stacks tokenomics, including its utility, distribution model, consensus mechanism, and economic incentives.



- **Utility of STX:** STX serves multiple purposes within the Stacks ecosystem:
 - **Transaction Fees:** STX is used to pay for transaction fees on the Stacks network. Every transaction that interacts with smart contracts or transfers assets requires a fee paid in STX, which helps maintain network security and incentivizes miners.
 - **Smart Contract Execution:** Developers must use STX to deploy and execute smart contracts on the Stacks layer. This ensures that only those who are invested in the ecosystem can create and manage contracts.
 - **Proof of Transfer (PoX):** STX plays a crucial role in the PoX consensus mechanism, which allows users to earn Bitcoin (BTC) by locking up their STX tokens. This mechanism aligns incentives across the network by rewarding participants who contribute to its security.
- **Distribution Model :** The distribution of STX tokens has been designed to promote decentralization and long-term growth:
 - **Initial Token Supply:** The total supply of STX is capped at 1.8 billion tokens. The initial distribution included allocations for early investors, team members, and reserves for future development.
 - **Public Sale:** A portion of STX was made available through public sales, ensuring that a wide range of participants could acquire tokens and engage with the network.
 - **Mining Rewards:** Through PoX, miners are rewarded with newly minted STX tokens for securing the network and validating transactions. This mining process encourages active participation in maintaining the integrity of the Stacks blockchain.

MESSARI STX initial distribution

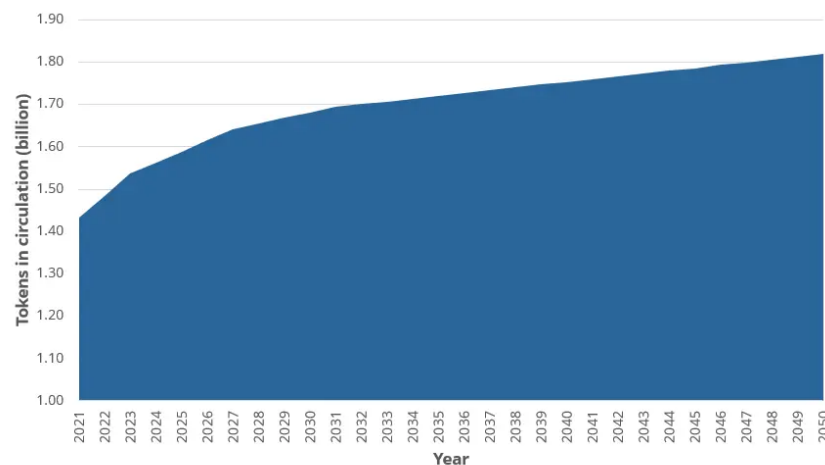
Token sales occurred in 2017 and 2019 account for more than one third of the total supply



Source: Stacks

- **Economic Incentives:** Stacks tokenomics is structured around various economic incentives that promote growth and stability:

MESSARI STX cumulative token release schedule



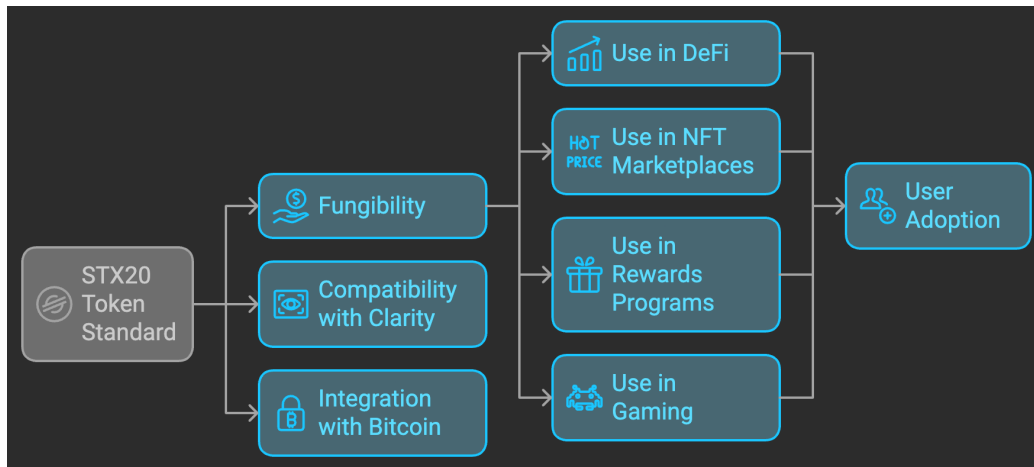
Source: Stacks

- **Staking Rewards:** Users who stake their STX through PoX not only earn BTC but also help secure the network, thus fostering a community-oriented approach to governance and operations.
- **Burn Mechanisms:** Certain transactions may involve burning STX tokens as part of their execution process. This deflationary mechanism can help reduce supply over time, potentially increasing value for existing holders.
- **Community Development Funds:** A portion of the initial token supply is allocated for community development initiatives, grants, and ecosystem projects aimed at expanding the use cases for STX and

enhancing overall network utility.

STX20 standard

The **STX20 token standard** is a significant advancement within the Stacks blockchain ecosystem, designed to enhance the functionality and interoperability of tokens built on the Stacks protocol. This standard allows developers to create fungible tokens that can be easily integrated and utilized across various applications and platforms within the Stacks ecosystem.



- **Key Features of STX20**

- **Fungibility:**

- STX20 tokens are fungible, meaning each token is interchangeable with another token of the same type. This characteristic is crucial for creating currencies or other assets that need to maintain consistent value across transactions.

- **Compatibility with Clarity:**

- The STX20 standard is built on the **Clarity smart contract language**, which is designed for predictable execution and security. This compatibility ensures that developers can leverage Clarity's features to create robust and secure token contracts.

- **Integration with Bitcoin:**

- One of the standout features of the Stacks protocol, including STX20 tokens, is its ability to leverage Bitcoin's security and finality. Tokens created under this standard can interact with Bitcoin, allowing for seamless transfers and transactions while benefiting from Bitcoin's decentralized network.

- **Use Cases for STX20 Tokens**

- **Decentralized Finance (DeFi):** STX20 tokens can be utilized in DeFi applications for lending, borrowing, and trading, allowing users to create liquidity pools or participate in yield farming.

- **NFT Marketplaces:** While primarily fungible, STX20 tokens can also be used in NFT marketplaces as a medium for transactions, facilitating easier buying and selling of non-fungible tokens.
- **Rewards Programs:** Businesses can issue STX20 tokens as part of loyalty programs or rewards systems, allowing customers to earn and redeem tokens for discounts or exclusive offers.
- **Gaming:** In gaming applications, STX20 tokens can represent in-game currencies or assets, enabling players to trade items or currencies seamlessly.

- **Current Adoption and Ecosystem Status**

As of now, the STX20 token standard has gained traction within the Stacks community. Several projects are actively developing on this standard, contributing to a growing ecosystem of dApps that leverage its capabilities. The ongoing enhancements in the Stacks protocol, particularly with the recent Nakamoto upgrade aimed at improving transaction speeds and integrating Bitcoin finality, further bolster the relevance of STX20 tokens.

Product & Ecosystem

- **Core Products and Components:**

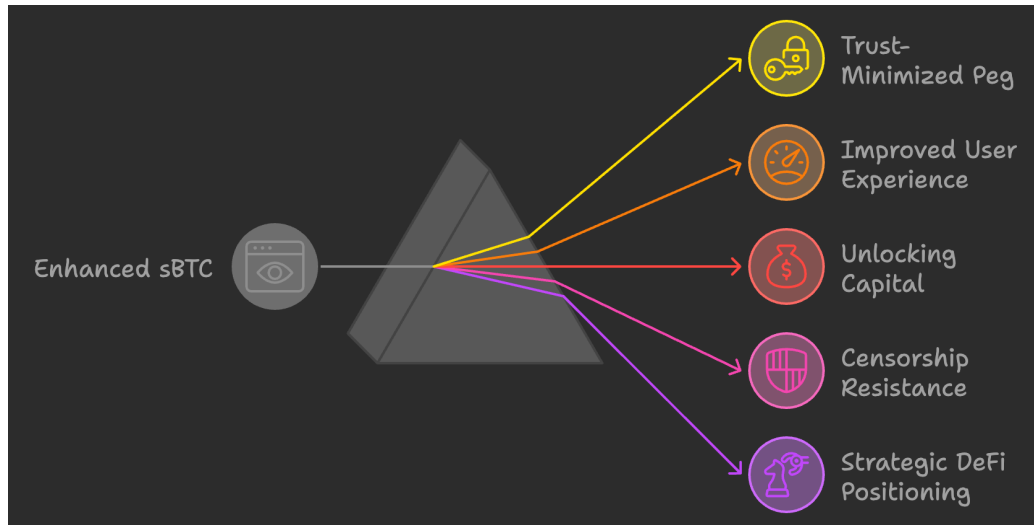
- **Stacks Blockchain:**

- The core of the Stacks ecosystem is its blockchain, which uses the innovative **Proof-of-Transfer (PoX)** consensus mechanism to secure itself with Bitcoin. By linking directly to Bitcoin's blockchain, Stacks ensures that all transactions and operations benefit from Bitcoin's inherent security and decentralization.
- PoX mining allows users to use Bitcoin to mine new Stacks (STX) tokens, which helps connect the two blockchains and aligns incentives between the Stacks network and Bitcoin.

- **Smart Contracts via Clarity:**

- **Clarity** is the programming language used for writing smart contracts on Stacks. Designed for security, Clarity is non-Turing complete, which helps prevent common vulnerabilities seen in other blockchain environments.
- The language prioritizes predictability, meaning developers can know precisely how smart contracts will execute without unexpected behavior. This predictability makes it well-suited for decentralized finance and other applications requiring reliability.

- **sBTC:** The introduction of **sBTC** in the context of the **Nakamoto upgrade** is highly significant for the Stacks ecosystem and the broader Bitcoin community.



- **Significance of sBTC:**

- **Trust-Minimized Two-Way Peg:** sBTC establishes a **trust-minimized two-way peg** between Bitcoin and the Stacks network. This mechanism allows Bitcoin to be transferred onto Stacks without sacrificing the security that Bitcoin is known for. Users can seamlessly move their BTC into the Stacks ecosystem, enabling it to be utilized within smart contracts and decentralized applications (dApps) built on Stacks
- **Enhanced Programmability:** With sBTC, Bitcoin gains programmability, allowing developers to create applications that leverage Bitcoin's security while enabling more complex functionalities typical of smart contracts. This opens up new possibilities for decentralized finance (DeFi), non-fungible tokens (NFTs), and other innovative applications that were previously challenging to implement directly on Bitcoin
- **Improved User Experience:** By decoupling Stacks block production from Bitcoin's block times, the Nakamoto upgrade allows for much faster transaction speeds—approximately every five seconds compared to Bitcoin's ten-minute intervals. This improvement significantly enhances the user experience when interacting with sBTC, making it more practical for real-time applications
- **Unlocking Capital in Bitcoin:** sBTC has the potential to unlock vast amounts of capital currently stored in Bitcoin by allowing it to be used in various DeFi applications on Stacks. This could mobilize hundreds of billions of dollars worth of BTC, facilitating new investments and fostering innovation within the crypto ecosystem
- **Censorship Resistance:** The Nakamoto upgrade allows all sBTC operations to occur directly on the Bitcoin main chain, enhancing censorship resistance. This alignment with Bitcoin's foundational principles promotes user confidence in sBTC's immutability and resistance to external interference
- **Strategic Positioning for DeFi:** As the DeFi landscape grows, sBTC positions Stacks as a leading layer-2 solution for hosting economic activity on Bitcoin. By providing a fully programmable version of BTC, it enables Stacks to compete effectively with other blockchain ecosystems while leveraging Bitcoin's established trust and security
- **Conclusion:** Overall, sBTC represents a transformative advancement for both Stacks and Bitcoin, bridging the gap between traditional cryptocurrency functionalities and modern decentralized applications. The Nakamoto upgrade not only enhances the performance and usability of sBTC but

also solidifies its role in expanding Bitcoin's capabilities into new realms of finance and technology, ultimately driving further adoption and innovation within the crypto space.

• **sBTC vs WBTC:**

	sBTC	WBTC
Design	Collateral secured by smart contract and open membership of validators	Collateral secured by central custodian and a closed federation of merchants (Bitgo)
Protocol	Stacks	Ehtereum
Launch date	Estimated in Q4 2024	January 2019
Circulating supply	N/A	~ 163,000 (1% of BTC supply)
Fees	BTC + STX transactions fees No deposit/withdraw fee	BTC + ETH transaction fees Fee vary by merchant to wrapping/unwrapping
Protocol details	Deposit to sBTC requiere 6 Bitcoin block confirmations, about 1 hour. Withdrawals from sBTC are processed every Bitcoin block	End users purchase and sell WBTC directly from a merchant. Often, the experience is less than 5 minutes. However, the onboarding can take until few days Unwrapping/wrapping can only be processed by authorized merchants
Finality	Settle on Bitcoin through Stacks	Settle on Ethereum
Use cases	<ul style="list-style-type: none"> - Trustless, Bitcoin-collateralized stablecoin loans - On-chain, undercollateralized BTC lending - Trustlessly deploy BTC to earn BTC yield - BTC DAO treasuries - sBTC stacking pools 	<ul style="list-style-type: none"> - lending/borrowing - Liquidity providing - Yield Farming

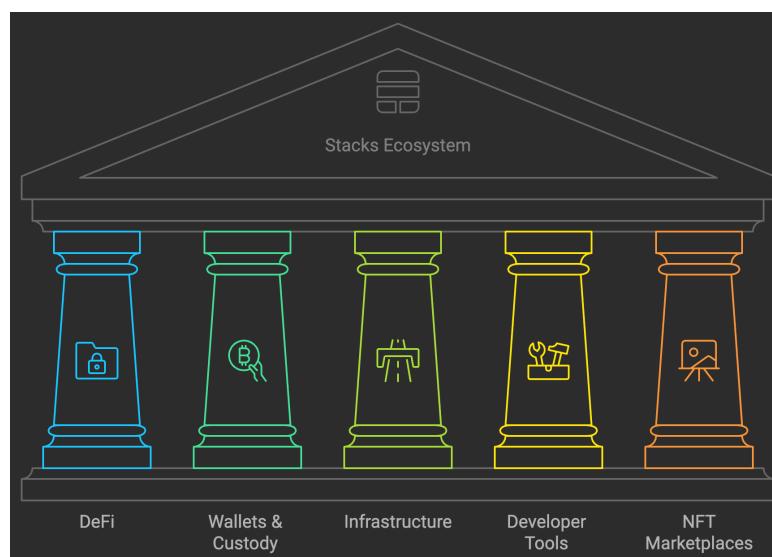
Stacks' Partnerships

Partner	Description	Date	Key Points
BitVM Working Group	Partnership to lead BitVM-related R&D, focused on enhancing the scalability and security of Bitcoin L2 using a computational engine called BitVM.	March 28, 2024	Stacks Foundation allocated \$500,000 initially for the Working Group, with a potential \$2 million more over 12-18 months. The goal is to open-source findings and improve trust assumptions.
Stacking DAO	Partnership for a Liquid Stacking protocol, which surpassed \$100 million in TVL, transforming Stacks from an	April 1, 2024	Liquid Stacking allows Stackers to earn BTC yield while also providing liquidity to DeFi.

Partner	Description	Date	Key Points
	ecosystem "black hole" to a DeFi accelerator.		Stacking DAO collaborates with Bitflow for increased liquidity.
Bitflow	Collaboration with Stacking DAO to provide liquidity to decentralized exchange operations.	December 28, 2023	Bitflow held around 12 million STX (valued at ~\$40M) in pools for trading pairs, facilitating seamless liquidity for its users.
Galxe	Integration to support Bitcoin L2 campaigns and increase community engagement for builders using Stacks.	April 2024	Galxe's integration brings Stacks into a large Web3 community, with over 12 million users, fostering growth through incentivized campaigns and enhancing Bitcoin utility.
Anchorage Digital	Partnership for custody support of Stacks' token (STX), enhancing institutional engagement with Bitcoin L2.	August 29, 2024	Anchorage Digital, the only federally chartered digital asset bank in the US, supports custody for Stacks, enabling institutions to securely hold and use STX.
Bitcoin Frontier Fund & Tokensoft	Collaboration to provide a streamlined legal and fundraising framework for Bitcoin builders.	September 16, 2024	Tokensoft's services, integrated with Bitcoin Frontier Fund's programs, help reduce risks for startup founders by offering compliance and entity setup assistance.
Aptos Foundation	Integration to launch sBTC on the Aptos L1 blockchain, extending Bitcoin's functionality for use in decentralized applications.	September 2024	Stacks' sBTC is a programmable, Bitcoin-backed asset that will be used on Aptos, expanding its use cases for gaming, NFTs, AI, and DeFi.

Stacks Ecosystem

The ecosystem comprises various sectors, including DeFi, wallets, infrastructure, and more, with numerous key players contributing to its growth.

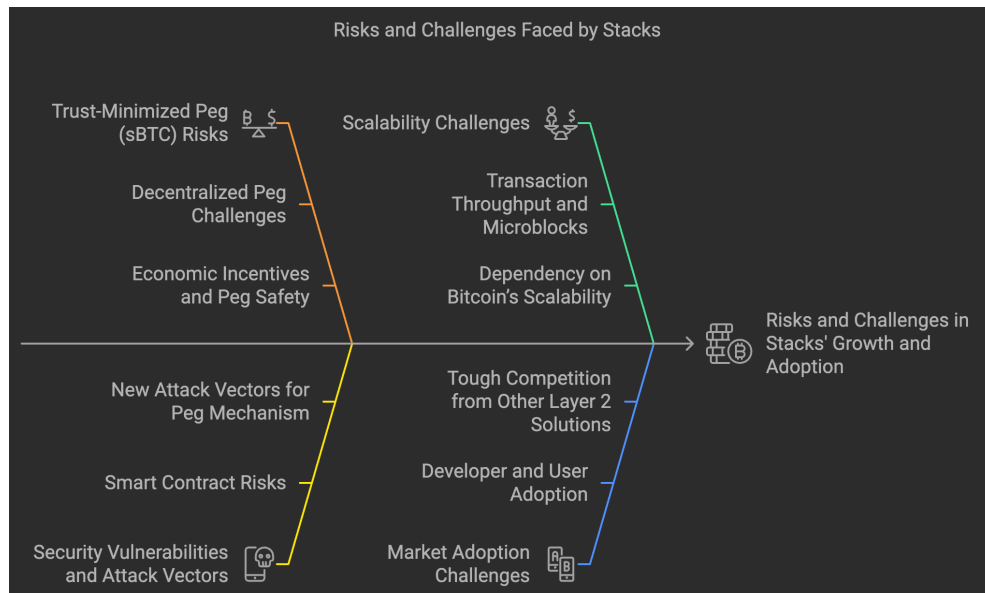


- **Decentralized Finance (DeFi):** DeFi applications on Stacks leverage Bitcoin's security while providing financial services such as lending, borrowing, and trading.
 - **ALEX:** A decentralized exchange (DEX) that allows users to trade STX and other tokens with minimal fees.
 - **Arkadiko:** A lending platform enabling users to borrow against their Bitcoin holdings.
 - **Gamma:** A marketplace for NFTs and digital assets that integrates with the Stacks blockchain.
 - **StackingDAO:** The StackingDAO project is a decentralized organization that optimizes the stacking process in the Stacks ecosystem for earning Bitcoin rewards.
 - **Bitflow:** The Bitflow protocol is a decentralized finance solution that enables efficient trading of Bitcoin and other assets through automated market-making and liquidity provision.
 - **Velar:** Velar is a DeFi liquidity protocol on Stacks that tokenizes and trades Bitcoin, unlocking its value for decentralized finance applications.
- **Wallets and Custody Solutions:** Wallets facilitate the storage and management of STX tokens and other digital assets.
 - **Hiro Wallet:** A popular wallet for managing STX tokens and interacting with dApps.
 - **Xverse:** A mobile wallet designed for easy access to Stacks dApps and services.
 - **BitGo:** Provides regulated custody solutions for institutional investors in the Stacks ecosystem.
- **Infrastructure Providers:** These entities support the development and operational aspects of the Stacks network.
 - **Stacks Foundation:** A non-profit organization that funds projects and initiatives within the ecosystem.
 - **Trust Machines:** Focuses on building infrastructure to enhance the usability of Bitcoin through Stacks.
 - **InfStones:** Offers blockchain infrastructure services to developers building on Stacks.
- **Developer Tools:** Tools that assist developers in creating and deploying applications on the Stacks blockchain.
 - **Clarity:** The smart contract language used in Stacks, designed for security and predictability.
- **Community Engagement:** Organizations that foster community growth and education around the Stacks ecosystem.
 - **DeSpread:** A consultancy that promotes Stacks activity in Korea, focusing on startup growth.
 - **Bitcoin Builders:** A community-led initiative aimed at expanding Bitcoin adoption through educational programs.
- **NFT Marketplaces:** Platforms dedicated to the creation, buying, and selling of non-fungible tokens within the Stacks ecosystem.
 - **NFTY Labs:** Focuses on NFT creation tools that integrate with Stacks.

- **Satoshibles:** An NFT marketplace built specifically for assets on the Stacks blockchain.

Risks & Challenges

- **Risks & Challenges overview:** While Stacks presents a promising solution for building on Bitcoin, there are several risks and challenges that could impact its growth and adoption. Below is a comprehensive overview of these challenges.



- **Trust-Minimized Peg (sBTC) Risks:**

- **Decentralized Peg Challenges:** Stacks employs a decentralized peg for the **sBTC** asset to allow BTC to move into the Stacks layer. However, this mechanism relies on Stackers as signatories to manage peg-outs, creating vulnerabilities to collusion attacks, coordination failures, or other errors that could compromise the peg's safety.
- **Economic Incentives and Peg Safety:** The integrity of the peg relies on aligning incentives for Stackers to behave honestly. If rewards diminish relative to the value at risk in the peg, Stackers may be tempted to behave maliciously. Ensuring that incentives remain aligned under varying market conditions will be an ongoing challenge.

- **Security Vulnerabilities and Attack Vectors**

- **Smart Contract Risks:** Although the **Clarity** language is designed to minimize vulnerabilities by being non-Turing complete, the risks of smart contract exploits still exist. Poorly designed contracts could lead to unintended behavior, resulting in potential financial losses and damage to network reputation.
- **New Attack Vectors for Peg Mechanism:** The novel sBTC peg mechanism introduces new attack vectors, such as collusion among Stackers, that could impact peg safety. Additionally, potential vulnerabilities introduced by integrating new features like **subnets** and **EVM compatibility** could increase the risk of attacks on the system.

- **Scalability Challenges**

- **Transaction Throughput and Microblocks:** As user and transaction numbers grow, maintaining fast transaction speeds and low fees will be crucial. Stacks relies on microblocks for quicker transaction confirmations, but scalability limitations could arise if the transaction volume surpasses the capacity of the network to process them efficiently. In times of congestion, this could lead to delays and increased transaction costs.

- **Market Adoption Challenges**

- **Developer and User Adoption:** Compared to Ethereum, which has a robust developer community, Stacks faces challenges in attracting developers to build on its platform, particularly due to the **learning curve associated with Clarity**. The Clarity language's predictability and non-Turing completeness, while providing security benefits, can limit its adoption by developers accustomed to Turing-complete languages like Solidity or Rust.
- **User Base Growth:** Stacks needs to cultivate a significant user base for its applications. If users do not find sufficient value in using Stacks over other solutions like the **Lightning Network** or **Rootstock (RSK)**, adoption may remain limited.

- **Tough competition from Other Layer 2 Solutions**

- **Established Competitors:** Stacks faces competition from established Layer 2 and sidechain solutions, such as **Lightning Network** for micropayments and **Rootstock (RSK)** for EVM-compatible smart contracts. Additionally, new entrants like **Merlin**, **BOB** and **BitVM** present innovative solutions that could further fragment the Bitcoin Layer 2 market, challenging Stacks to differentiate itself effectively.
- **Cross-Chain Interoperability:** Achieving seamless integration with other blockchain ecosystems remains a complex task. **Cross-chain compatibility** challenges could hinder Stacks' ability to compete effectively in the broader blockchain landscape.

- **Regulatory Uncertainty**

- **Uncertain Regulatory Environment:** As global regulatory frameworks around cryptocurrencies continue to evolve, Stacks may face challenges in adapting to new regulations. Compliance issues around DeFi, NFTs, and pegged assets like sBTC could impact the growth of the network and restrict the use of certain features.
- **Tax Implications:** Changes in tax regulations, particularly for cryptocurrency transactions, could deter potential users from engaging with the platform if they perceive high tax liabilities or regulatory burdens.

- **Conclusion:** The Stacks protocol represents an ambitious effort to bring programmability and DeFi to Bitcoin. However, it must navigate several risks and challenges, including the complexity of the Proof-of-Transfer consensus, scalability limitations, adoption barriers, security vulnerabilities, and regulatory risks. Stacks also faces strong competition from other Layer 2 solutions and challenges in maintaining decentralization. Successfully overcoming these challenges will be crucial for Stacks to establish itself as a leading platform for building on Bitcoin, driving adoption, and fully realizing its vision of turning Bitcoin into a productive and programmable asset.

Traction study paper

Current Maker datas

- Date: /10/2024
- Price: \$
- Current Token Value Locked: \$
- Current circulating marketcap: \$
- Current fully diluted marketcap: \$
- Cumulative fees generated by Stacks over the last 365d: \$

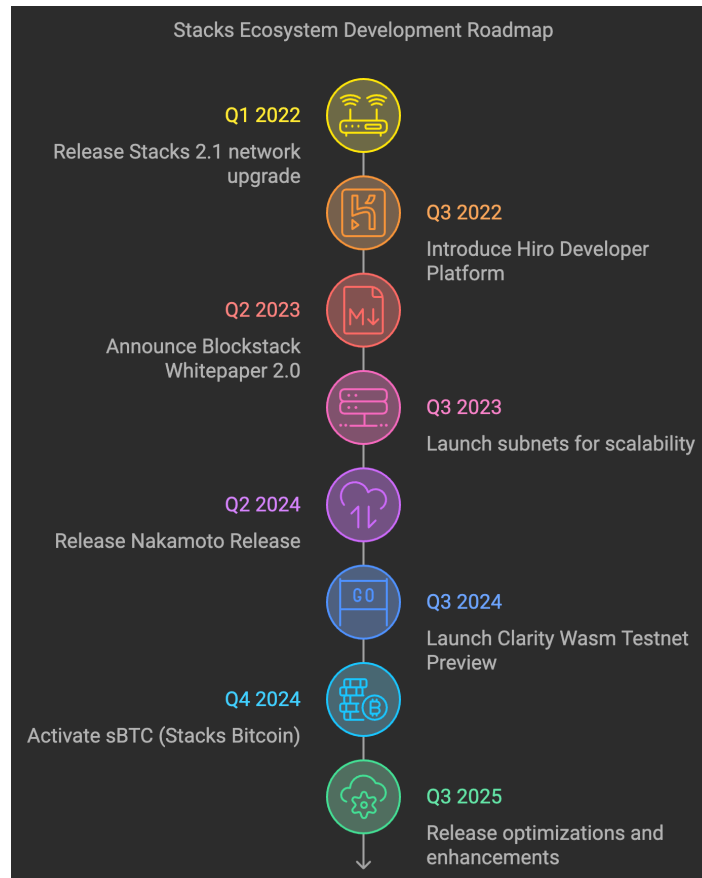
Team / Community

- **Stacks Team Overview:** The Stacks protocol is backed by a team of experienced developers and entrepreneurs who have been instrumental in expanding Bitcoin's capabilities. Since its mainnet launch in 2021, Stacks has significantly decentralized, with over 30 independent entities contributing to its growth. Key team members include:
 - **Muneeb Ali** - Co-Creator of Stacks and CEO of **Trust Machines**, focusing on Bitcoin applications and infrastructure.
 - **Ryan Shea** - Co-Creator of Stacks and advisor to the **Bitcoin Frontier Fund**.
 - **Jude Nelson** - Stacks Core Blockchain Engineer, responsible for core components such as the **Clarity** smart contract language and **Proof-of-Transfer (PoX)** consensus mechanism.
 - **Brittany Laughlin** - Executive Director of the **Stacks Foundation**, overseeing operations, grants, and community initiatives.
 - **Ken Liao** - CEO and Founder of **Xverse Wallet** and early contributor to the Stacks open-source project.
- **Investors:** Prominent investors include **Union Square Ventures** and **Winklevoss Capital**. In 2019, Stacks held the first-ever SEC-qualified offering, involving over 4,500 entities and individuals.

Roadmap

Stacks Roadmap

- **Key Phases of Development:** The roadmap is divided into several key phases, each focusing on different aspects of the ecosystem



- **Foundation Phase (2018 - 2021):**

- **2018:** Stacks was founded, laying the groundwork for a user-owned internet.
- **2020:** Launch of the Stacks 2.0 Testnet, which served as a testbed for smart contracts.
- **January 2021:** Official launch of Stacks 2.0, introducing the Clarity programming language and enabling smart contracts on Bitcoin.

- **Expansion Phase (2022 - 2023):**

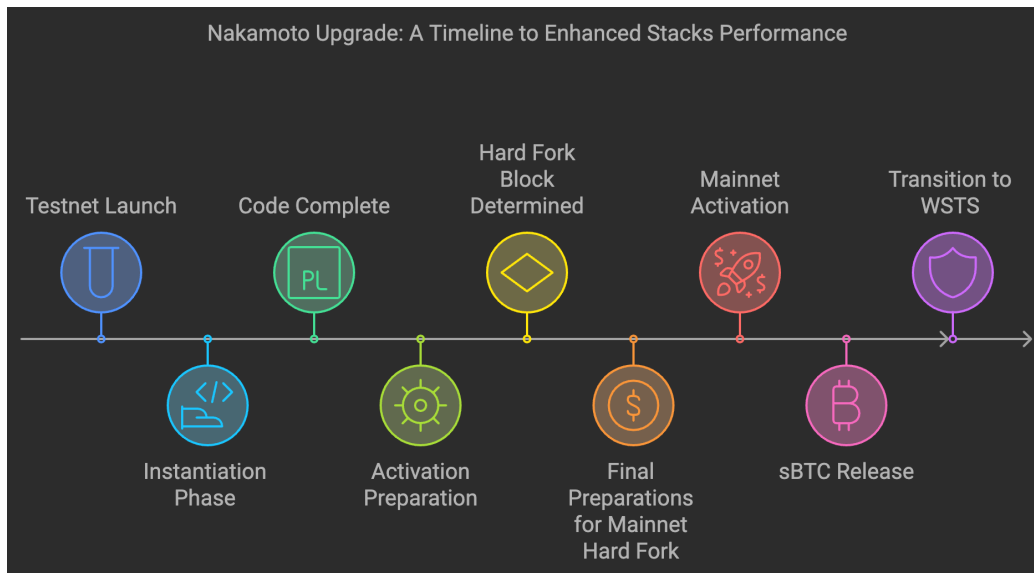
- **Q1 2022:** Release of Stacks 2.1, an important network upgrade.
- **Q3 2022:** Introduction of the Hiro Developer Platform, facilitating dApp development.
- **Q2 2023:** Announcement of the Blockstack Whitepaper 2.0 and SEC filing for a \$50M regulated token offering.
- **Q3 2023:** Launch of subnets to enhance scalability and performance.

- **Optimization Phase (2024)**

- **Q2 2024:** Release of the Nakamoto Release, which aims to provide faster transactions and 100% Bitcoin finality.

- **Q3 2024:** Launch of the Clarity Wasm Testnet Preview, allowing for builder feedback on major features.
- **Q4 2024:** Planned activation of sBTC (Stacks Bitcoin), which will integrate Bitcoin into the Stacks ecosystem more effectively.
- **Maturity Phase (2025 and beyond)**
 - **Q3 2025:** Anticipated release of further optimizations and enhancements based on community feedback and technological advancements.
 - Ongoing focus on establishing governance mechanisms that allow stakeholders to participate in decision-making processes.

Nakamoto upgrade roadmap

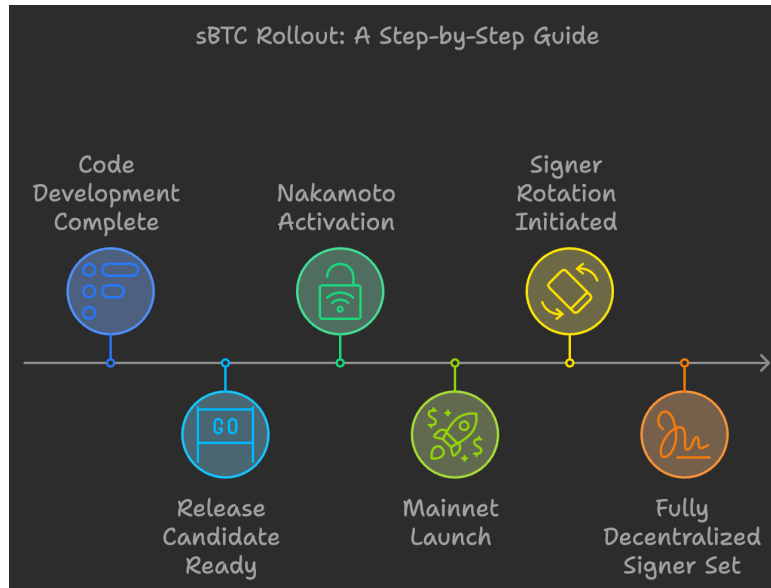


- **March 2024: Nakamoto Testnet Launched**
 - **March 11:** The Pre-Launch Testnet went live, providing a testing environment for developers to prepare for the upcoming upgrade.
 - **March 25:** The Nakamoto Testnet was introduced, allowing developers and Signers to work with a stable network similar to the mainnet's eventual form. Workshops and calls were scheduled to help participants get acquainted with the new features and setup.
- **April 2024: Instantiation Phase**
 - **April 11:** A new block for the Nakamoto "Instantiation" phase was chosen to ensure adequate preparation time for Stackers, pools, and node operators. The new instantiation block was set at Bitcoin block 840,360, scheduled for around April 22, offering more flexibility to network participants.
- **July 2024: Code Complete**

- **July 11:** Core developers announced that the Nakamoto upgrade had reached the "code complete" stage, making the full codebase ready for audit and testing. Key improvements, such as enhanced Signer configurations and a simplified signature scheme under SIP-025, were also implemented to make the upgrade process smoother.
- **July 23:** SIP-025, an addendum to SIP-021, introduced a temporary simplified signature scheme for the initial Nakamoto release. This change was proposed to reduce complexity and speed up the implementation.
- **August 2024: Activation Preparation**
 - **August 28:** The activation window for Nakamoto opened, marking the beginning of the process to bring the Nakamoto consensus rules live. This involved network participants upgrading to the new system, with final binaries delivered to Signers, Miners, and Node Operators.
- **September 2024: Hard Fork Block Determined**
 - **September 16:** The successful handoff from Cycle 92 to Cycle 93 paved the way for the next major step: selecting the Nakamoto hard fork block. The block selection took place during Cycle 93, with all features set to go live during Cycle 94.
 - **September 27:** The Nakamoto Testnet hard fork was successful, setting the stage for a Primary Testnet upgrade and eventually a mainnet upgrade after at least a week of stable operation.
- **October 2024: Final Preparations for Mainnet Hard Fork**
 - The Nakamoto mainnet upgrade is expected to occur in mid-October following stable Primary Testnet testing. Once activated, Nakamoto will bring fast blocks, full Bitcoin finality, and improved network resiliency.
- **Insights for the Future**
 - **Nakamoto Mainnet Activation:**
The mainnet activation began on August 28, 2024. This involves activating all Nakamoto features, including consensus rules, Signer functionalities, and fast block production, to enhance the overall performance and security of the Stacks blockchain.
 - **sBTC Release:**
The release of sBTC is expected to follow approximately four weeks after the Nakamoto mainnet activation, placing the projected launch around October 2024. sBTC will be a significant feature that enables smart Bitcoin transactions on the Stacks network.
 - **Transition to Full Weighted Schnorr Threshold Signatures (WSTS):**
Following the current simplified signature system introduced by SIP-025, the network plans to move to a more sophisticated WSTS signature scheme in a future release (Stacks 3.1). This will be a phased transition aimed at enhancing network security and performance.

sBTC Roadmap

The sBTC roadmap outlines a structured plan for the rollout of sBTC, a token designed to facilitate the secure transfer of Bitcoin (BTC) onto the Stacks Layer 2 blockchain. This initiative aims to leverage scalable and expressive smart contracts while ensuring a safe and efficient launch.



- **Overview of the Rollout Plan:** The sBTC rollout consists of two primary phases: **Bootstrapping** and **Signer Rotation**. This phased approach is designed to enhance security and decentralization progressively.
- **Key Milestones**
 - **July 2024:** Completion of code development.
 - **August 2024:** Release candidate for sBTC mainnet will be ready.
 - **Nakamoto Activation:** Mainnet release of sBTC will follow approximately four weeks after this activation.
 - **Q1 2025:** Initiation of Signer Rotation, transitioning to a fully decentralized signer set.
- **Bootstrapping Phase:** The Bootstrapping phase is crucial for launching sBTC quickly while maintaining security. During this phase, a limited group of Signers, chosen through community voting, will manage the signing of sBTC transactions. This allows for real-world testing and feedback before moving to a more decentralized model.
- **Features During Bootstrapping**
 - **SIP-10 Token:** sBTC will be a SIP-10 token backed 1:1 by BTC in a peg wallet.
 - **Limited Signer Set:** The wallet will be managed by a restricted group of Signers throughout this phase.
 - **Conversion Times:** BTC can be converted into sBTC within three Bitcoin blocks, while conversion back to BTC will occur within six blocks.
 - **Stable Contract Design:** The SIP-10 token contract remains unchanged, ensuring that builders do not need to adjust their applications as the system evolves.