An Analysis of Bitcoins Security and the Feasibility of Stacks Smart Contract Layer

Luca Cordova Stuart

University of Southern California

February 18th, 2023

ABSTRACT

This research paper explores the strengths and limitations of the blockchain technology used in Bitcoin and Stacks. It examines how Bitcoin's Proof of Work consensus mechanism provides a secure and decentralized peer-to-peer network while also limiting its scalability. The paper then delves into how Stacks' Proof of Transfer consensus mechanism can provide a solution to Bitcoin's scalability issues. The paper discusses Stacks' potential to serve as a building block for a more advanced user-owned internet, enabling individuals to earn Bitcoin through active participation in consensus.

The study finds that the Stacks blockchain has low activity volume and is relatively small in scale compared to other blockchains such as Ethereum. The paper highlights several more limitations which may hinder the mass adoption of Stacks while recognizing its innovative programming language and consensus mechanism.

OUTLINE

I. Introduction

II. How Bitcoin is Secured

III. Limitations of Bitcoin

IV. Understanding Stacks Blockchain

V. Limitations of Stacks

VI. Feasibility of Stacks

I. INTRODUCTION

There are an increasing number of reasons for an individual to enter the blockchain landscape. One of the fundamental components of the most popular thesis is building a decentralized peer-to-peer network, using a blockchain secured by consensus to remove the intermediary and empower individuals. Bitcoin is regarded as one of the most secure blockchains through its mining hash rate distribution, supported by its Proof of Work (PoW) consensus mechanism and the longevity of its blockchain. Per the Lindy effect, the future life expectancy of a non-perishable is proportional to its current age.[i] Meaning because Bitcoin is the longest-lasting blockchain it should continue to exist. This is not to say Bitcoin is without its limitations, although some argue Bitcoins limitations are by design, such as Bitcoin block sizes or the low number of transactions per second (tps) to reduce forks. The largest of these limitations is Bitcoins scaling problem. Other blockchains such as Ethereum were inspired by Bitcoin, born to create an infrastructure more suitable for scaling the future of the internet powered by smart contracts. The Stacks blockchain, founded by Muneeb Ali and Ryan Shea, sought to combine all the strengths of Bitcoin and Ethereum, leaving out the shortcomings.[ii] Stacks achieves this through its unique Proof of Transfer (PoX) consensus mechanism, verified by the Stacking algorithm, and written by the Stacks programming language Clarity. Just like Bitcoin and Ethereum, solutions to existing problems often introduce new ones. The Stacks blockchain has been critiqued for its false advertisement of PoX and the lack of decentralization. This paper seeks to highlight why Bitcoin is a secure base chain for future scaling solutions and analyze Stacks' efforts at solving Bitcoin’s limitations through the PoX consensus mechanism.

II. HOW BITCOIN IS SECURED

To properly illustrate the Stacks value proposition, Bitcoin's shortcomings and its systems architecture must be examined. Introduced in Satoshi Nakamoto’s 2008 whitepaper, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin was proposed as a peer-to-peer electronic cash transfer system that secured transactions without the use of any centralized intermediary.[iii] Satoshi introduced a decentralized chain of blocks secured by the PoW consensus mechanism, in which network participants utilize the SHA-256s hashing algorithm to yield a 256-bit hexadecimal deterministic and random hash. The winning network participant, or miner, wins the reward if their nonce falls under the target difficulty, which programmatically shifts every 2,016 blocks to ensure an average 10-minute block processing interval. Successful miners receive blocks of transactions from the mempool. The mempool, short form for "memory pool," is a component of blockchain networks that stores unconfirmed transactions until they are picked up by miners. Miners essentially engage in trial and error, earning the block reward from the coinbase transaction, the first transaction in the block, and the sum of the transaction fees from the mined block. PoW was integral in coining the term “blockchain,” which consists of a chain of blocks linked via a block header with each block's previous hash, the first being the Genesis Block.

While miners compete to secure the blockchain, another node works to validate it. This node is a validator, also known as a full node or light node.[iv] Validator nodes rely on the Bitcoin blockchain's immutability and public ledger to batch individual transactions into a block and validate transactions per the rules of the Bitcoin software. To accurately validate Bitcoin transactions, a full node must first store the entire blockchain history for reference. Once the transaction is validated, the nodes post the transaction to other network participants and the process is repeated until the nodes reach consensus, adding the valid transaction to a pool with other validated transactions. Light nodes are another Bitcoin validator node, instead of storing the entire blockchain history, a light node relies on full nodes, demonstrably decreasing necessary resources. Bitcoin cannot be generalized, it represents a network, a protocol, and software. Understanding Bitcoin's technicalities are integral to why Stacks believes it is an excellent, secure base layer blockchain.

III. LIMITATIONS OF BITCOIN

Bitcoin's trustless peer-to-peer system is the foundation for a global economy, yet its practical applications sometimes appear one-dimensional. Many investors view Bitcoin as "digital gold" and attribute its success to its store of value proposition. Others believe it is the most secure and decentralized form of electronic payments without borders, sacrificing scalability from the blockchain trilemma. The blockchain trilemma states the three options blockchain serves to solve are security, scalability, and decentralization, yet no blockchain can have all three. Bitcoin notably imposes capacity constraints on processing transactions to maintain decentralization.[v] Theorists claim larger block sizes may lead to the centralization of miners as the barrier to entry becomes more expensive to process larger blocks. Bitcoin processes on average seven tps, which fairs extremely poorly to centralized payment systems such as Visa which can process up to 24,000 tps.[vi] Bitcoin cannot become the world's currency while operating at its current network throughput.

As a result, in 2015 the Bitcoin community proposed BIP141, the SegWit soft fork, a Bitcoin scalability solution.[vii] A soft fork is a backward-compatible way to update the software of a blockchain, as opposed to a hard fork, which permanently diverges the blockchain's latest version. SegWit, or segregated witness, updated the transaction format of Bitcoin, freeing block space for more transactions by separating the witness and transaction data, the former of which took up to 65% of the network's available block space. SegWit introduced new capabilities for layer 2 Bitcoin scaling solutions by removing transaction malleability, which put transaction hashes at risk of manipulation. The Lightning Network was a layer 2 that began development post-BIP141, yet its use-case only scales Bitcoin currency systems by creating an off-chain payment channel that functions like a ledger. Client-side validation technology like RGB is working to develop smart contract evolution through off-chain schema, yet that requires an additional layer, therefore a Bitcoin layer 3.[viii] The Lightning Network is excellent for small payment peer-peer transactions via payment channels to transact BTC off-chain, later posting the ending balance back on Bitcoins layer 1. However, some Bitcoin maximalists had larger aspirations for Bitcoin and looked towards Ethereum's scale of smart contracts as a testament to what true scalability could look like.

IV. UNDERSTANDING STACKS BLOCKCHAIN

The Stacks thesis states, "that successful experiments from various blockchains will eventually get created on Bitcoin.[ix]" Moreover, its network effects provide smart contracts with access to more cryptocurrency capital and enhanced security. Bitcoin has the potential to serve as a fundamental building block for a more advanced user-owned internet, akin to the role of TCP/IP in the traditional internet. The innovative approach of Stacks enables individuals to earn Bitcoin through active participation in Stacking, a Stacks staking scheme. Stacks believes that this approach brings a new value proposition to Bitcoin by deploying previously idle Bitcoin capital and expanding the scope of applications and smart contracts within the Bitcoin ecosystem.

Due to Bitcoin's limited scripting language, Bitcoins blockchain functions as a settlement layer and source of truth, enabling the opportunity for Stacks to integrate smart contract support. Stacks layer 1 blockchain solves Bitcoin’s scalability problems through its general-purpose smart contracts, without modifying Bitcoin’s main chain. Stacks offers far more applications than the layer 2 lightning network, establishing a foundation for a decentralized on-chain ecosystem much like Ethereum’s. Containing faster peer-peer payments and a plethora of applications, including but not limited to DeFi, NFT, Social, Data, and DAOs. As previously mentioned, Bitcoin's poor programming language and the SegWit soft fork only introduced the capability for simpler payment scaling solutions. To combat this, Stacks utilizes the Proof of Transfer (PoX) consensus mechanism, relying on the security of Bitcoin to secure the Stacks layer 1 blockchain.

Designed by Iain Stewart in 2012, PoX takes inspiration from another consensus mechanism known as Proof of Burn (PoB).[x] PoX and PoB are very similar, though the key difference is where the tokens go when they are “burned” or transferred. Instead of using computational power to secure the chain, PoB miners destroy the chain's native cryptocurrency. PoB was regarded as the “holy grail” of consensus mechanisms. Similar to PoW, the cost for bad actors attacking the network is paid upfront, yet PoB may be more effective when built on more nascent base chains.[xi] An explanation for this is miners and network participants in the PoB chain are rewarded in a new cryptocurrency. However, in the early days of the PoB chain, this cryptocurrency may not have as much value or security as the base cryptocurrency, Bitcoin. If the base chain is more valuable and stable than the currency on the PoB chain, there is little incentive for network participants. During PoX, miners send the sacrificed BTC to Stackers who participate in consensus by staking STX. This omits the need to send tokens to a burn or dormant wallet like the PoB consensus mechanism. PoX can help to solve the bootstrapping problem for new blockchains, participants receive rewards in a separate, potentially more stable, base cryptocurrency.[xii] These BTC rewards may be a better incentive for initial participation than rewards in the new cryptocurrency itself, STX.

Stacks carefully chose Bitcoin as the underlying chain in support of their hypothesis, given Bitcoin is the longest-standing, most valuable blockchain by market capitalization. Through PoX, Stacks' blockchain reaps the security of Bitcoins PoW while minimizing environmental impact by proving cost was exerted via the PoX consensus mechanism rather than the computational cost through PoW. The Stacks PoX consensus mechanism uses a verifiable random function (VRF) to select the winning miner. This miner gets the opportunity to write the next block on the Stacks blockchain, being rewarded by minting new Stacks tokens (STX) and the transaction fees from the block. Instead of transferring the tokens to a burning wallet, Stacks miners send the Bitcoin to a set of specified addresses corresponding to other Stacks network participants. The Stacking algorithm determines the specified addresses in which STX holders can participate in consensus and earn Bitcoin token (BTC) rewards. To participate, stakers lock their STX in a reward cycle pertinent to Bitcoin blocks, roughly two weeks, and run full nodes. Stackers post transaction data on the network and work in consensus to validate the Stacks chain. Once the stacking cycle commences, the addresses of actively participating STX holders become the "specified addresses" referred to above. They are then sent the BTC reward in return for their consensus. PoX proposes a greater economic incentive for participating in consensus, whereas PoW uses slashing mechanisms to threaten valid consensus participation.

Every smart contract blockchain is written by its unique programming language, Stacks blockchain is powered by Clarity. Clarity was created as a safe, transparent, decidable programming language. A program is decidable if one can know with certainty the outcome of the program by the code itself.[xiii] This doesn’t just advantage programmers, it empowers non-technical individuals by offering an easier onramp to understanding the open-source nature of blockchains and smart contracts. To further Stacks security, Clarity is interpreted, meaning the source code is published and executed directly via Stacks blockchain nodes. Removing any compiled representation of the source code minimizes the surface area for bugs such as reentrancy attacks. Most importantly, Clarity has visibility into Bitcoin’s state, therefore the contract logic triggers based on pure Bitcoin transactions. If Bitcoin forks, the Stacks blockchain will fork alongside Bitcoin, preventing any edge cases and ensuring no future forking adjustment.

The most exciting current use-case of Stacks’ blockchain is CityCoin. Each CityCoin is unique to a specific city or community and is designed to represent the economic, social, and cultural value of that community. CityCoins are designed to introduce new crowdfunding mechanisms for the cities, the first being MiamiCoin launched in August 2021[xiv]. These mechanisms fund public goods and services and therefore take a partial load off of ordinary taxation. CityCoin introduces new incentives to miners, a potential solution to the lack of Stacks miners, incentivizing miners to forward STX into the smart contract in a given Stacks block, then are later rewarded with new CityCoins tokens. In October 2021, roughly three months after the launch of MiamiCoin, Miami's “city wallet” held ~$20 million worth of STX at present value. CityCoin later launched tokens in New York City and Austin.

V. LIMITATIONS OF STACKS

Stacks popularized the PoX consensus mechanism and successfully identified a product market fit, recognizing the immense security of Bitcoin and its scalability limitations. Yet skeptics challenge one of Stacks’ fundamental principles–PoX's utilization of Bitcoin to secure the Stacks blockchain. During Stacks’ PoX mechanism, the Stacks miners participate in securing its chain to Bitcoin’s blockchain using OP_RETURN during the transfer of BTC. OP_RETURN is a special type of transaction output in the Bitcoin protocol that allows data to be embedded in a transaction, analogous to other programming languages' return functions. This data is stored in the Bitcoin blockchain's unspent transaction output (UTXO) database and is immutable and transparent. One of the use cases of OP_RETURN in Stacks’ blockchain is to store the hash of a deployed Stacks smart contract onto the Bitcoin network. Referencing the UTXO data allows the Stacks network to verify the integrity of the contract and ensure that it has not been modified. Therefore, it is more accurate to claim Stacks uses Bitcoin as an additional availability layer, meaning the Bitcoin blockchain now broadcasts concurrent and past Stacks blocks, allowing for the storage of additional data through the Bitcoin blockchain.

The leading applications on Stacks by activity are by and large NFTs and DeFi. Stacks prides itself in empowering developers through its transparent, open-source agenda seen in most of Stack’s applications. The NFT marketplaces on Stacks serve their function, however not without significant limitations. First, the Bitcoin Naming Service btc.us offers .btc domains, analogous to Ethereum’s ENS domains. These domains are limited to one name per Stacks address, leading to an excess of dormant Stacks addresses. Furthermore, Stacks has low transaction volume across all its applications. The leading decentralized application (dApp) by transaction activity is ALEX, which stands for Automatic Liquidity Exchange, the most popular decentralized exchange (DEX) on the Stacks blockchain. Across the past month, the ALEX DEX facilitated ~12,000 transactions. Uniswap V3, the most popular multi-chain DEX, processed ~1,650,000 transactions on Ethereum the previous month. The disparity of the two DEXs is further illustrated by ALEXs volume traded in USD amounting to over one-millionth of Uniswap V3s month over month.

While Decentralization is relative, there is a consensus that Bitcoin is one of the largest most decentralized blockchains. Stacks aims to build on top of Bitcoin's successes, simply introducing an application layer to an already secure, decentralized base chain. However, due to the PoX consensus mechanism, new qualms of true decentralization have arisen within the Stacks community. Observable through Stack's on-chain data, the previous 100 blocks as of February 20th have been mined by only 8 miners.[xv] Unlike Bitcoin mining, a reported individual Stacks miner does not represent a pool of miners who aim to reap a shared yield rather than gamble to win the block reward. These shortcomings are largely due to the incentive structure of PoX which leads to more lucrative mining yields if paired with the Stacking mechanism, a strategy called "discount-mining.[xvi]" The mining discount is designed to incentivize miners to hold STX tokens and participate in the network, as it allows them to acquire additional tokens at a discounted price. The discount is calculated using a formula that uses the total amount of Bitcoin locked up in the Stacks protocol, the total amount of STX tokens in circulation, and the mining difficulty level. The formula ensures that the discount is proportional to the amount of Bitcoin locked up in the protocol. The associated risk stems from the price volatility of STX and the miner's sacrifice of BTC for STX. Miners have adapted their game theory to participate in an attack against the consensus protocol, to receive as much BTC back post "burn" through the Stacking algorithm. The aforementioned design of Stacks is to be held responsible. Founder

Muneeb Ali recognizes that “Even with 100 unique miners (not counting pools who pool behind a single on-chain miner) you’d be taking up approx 10% of the total Bitcoin transaction bandwidth per block.[xvii]” Taking up too much Bitcoin bandwidth is a topic of hot debate thanks to the recent rise of Ordinals, a data inscription project which is attributed to the recent largest block sizes ever recorded on the Bitcoin blockchain. Ali is not interested in the Stacks layer taking up more than 10% of the Bitcoin bandwidth for mining, therefore establishing a current upper bound for the max number of miners that can be supported with the current Bitcoin on-chain mining approach.

VI. FEASIBILITY OF STACKS

From a pragmatic perspective, Stack is a functional blockchain with a strong developer

community, therefore, the future development of Stacks is in safe hands. Nonetheless, these developers need incentives to continue building. In the Stacks fee market problem, which is the general concern miner incentives will falter as the block reward continues halving, and incentive across the ecosystem is regressing. There are many factors influencing this, however, the overarching barrier is that Stacks blockchain lacks innovation.

The Stacks thesis is ambitious and warranted, demonstrated by the overwhelming initial support Stacks experienced. In early 2022, the Stacks ecosystem was rated the #1 Web3 project on Bitcoin.[xviii] A thriving time for the ecosystem, with over $1 billion in TVL with over 350 million monthly API requests by developers. Since its peak, Stacks TVL has undergone a ~90% decrease, a ~23% greater decrease than Ethereum’s TVL. Suffice it to say, Stacks has lost its momentum and its losses have been perpetuated by mempool congestion. High levels of network activity can lead to a backlog of unconfirmed transactions in the mempool, resulting in longer confirmation times and higher transaction fees. In the past, dApps on Stacks have had to shut down functions as a result of this congestion, seeming to stem from the Bitcoin Naming Service btc.us. Protocols like ALEX halted their collateral rebalancing pools due to failure to rebalance frequently enough, resulting in a material discrepancy between the actual and target weights of the two tokens.[xix] Some users not only experienced failure within ALEXs lending and borrowing mechanisms, but any individual transaction interacting with the ALEX protocol.

The longevity of the Stacks blockchain, much like Bitcoin, is reliant on its coinbase reward supply schedule. A Stacks coinbase transaction is a miner-created transaction that pays the STX block reward to miners for securing the network. The current block reward for miners is 1,000 STX, roughly equivalent to $500 USD in February 2023, yet the STX price action is extremely volatile due to the Bitcoin NFT narrative stemming from Ordinals. Stacks follow Bitcoins halving schedule, with the next occurrence in 2024 where the miner block reward will be lowered to 500 STX. Mining on Stacks rewards very few active participants, mainly the 8 current miners as stated above. The Stacks fee market problem can be resolved; however, given the next halving will be Stacks second and Bitcoins fourth, the STX halvings are steeper per percent change relative to the initial block reward. Stacks runs the risk of losing network participants to secure its blockchain which would lead to further mempool congestion, a negative feedback loop.

The narrative Bitcoin maximalists entertain leaves little room for scaling Bitcoin in the direction Stacks intended, which may be another factor influencing Stacks' demise. Recall the Stacks position, to deploy previously idle Bitcoin capital and expand the scope of applications within the Bitcoin ecosystem. It contradicts the simplicity of Bitcoin to scale on its main chain directly, thus disregarding that future vertical. Stacks functions more closely to an additional availability layer than an inherent property of Bitcoins mainnet, therefore user retention. Historic Bitcoin figures may reject the potential for introducing complexity to the already “perfect” Bitcoin protocol, smart contract enthusiasts may look towards Ethereum where innovation is fruitful, and scalability aficionados may be better suited working with optimistic or ZK rollups. Stacks introduced an innovative consensus mechanism, however abroad collection of limitations within its ecosystem has influenced its demise, negatively influencing the feasibility of the Stacks blockchain.

[i] Cook, John. "The Lindy Effect," John D. Cook (blog), December 17, 2012, accessed February 18, 2023, https://www.johndcook.com/blog/2012/12/17/the-lindy-effect/.

[ii] Chavez-Dreyfuss, Gertrude. "Blockstack's digital currency 'Stacks' to be tradable in U.S. once new blockchain arrives." Reuters, December 7, 2020, accessed February 21, 2023, https://www.reuters.com/article/crypto-currencies-blockstack/blockstacks-digital-currency-stacks-to-be-tradable-in-u-s-once-new-blockchain-arrives-idUSKBN28H22O

[iii] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008, accessed February 21, 2023, https://bitcoin.org/bitcoin.pdf.

[iv] Izatt, David. "What Are the Different Types of Bitcoin Nodes?" Decrypt, last modified September 22, 2021, accessed February 15, 2023, https://decrypt.co/resources/what-are-the-different-types-of-bitcoin-nodes-how-the-bitcoin-network-is-maintained.

[v] Divakaruni, Anantha, and Peter Zimmerman. 2022. "The Lightning Network: Turning Bitcoin into Money." Working Paper No. 22-19. Federal Reserve Bank of Cleveland. https://doi.org/10.26509/frbc-wp-202219.

[vi] "Retail Small Business Tools." Visa USA accessed February 15, 2023, https://usa.visa.com/run-your-business/small-business-tools/retail.html.

[vii] Tan, Eli, Noelle Acheson, John Biggs, and Hoa Nguyen. "Can the Bitcoin Network Scale?" CoinDesk, February 23, 2018, accessed February 21, 2023, https://www.coindesk.com/learn/can-the-bitcoin-network-scale/.

[viii] https://www.rgbfaq.com/faq/what-is-rgb

[ix] Ali, Muneeb. "Stacks 2.0: Apps and Smart Contracts for Bitcoin." Whitepaper Draft v0.1, December 2020, accessed February 17, 2023, https://gaia.blockstack.org/hub/1AxyPunHHAHiEffXWESKfbvmBpGQv138Fp/stacks.pdf

[x] "Proof of burn." Bitcoin Wiki, created January 15, 2018, accessed February 21, 2023, https://en.bitcoin.it/wiki/Proof_of_burn.

[xi] Levine, Andrew. "Inside the Blockchain Developer's Mind: Proof-of-Burn Blockchain Consensus." Cointelegraph, November 3, 2014, accessed February 15, 2023, https://cointelegraph.com/news/inside-the-blockchain-developer-s-mind-proof-of-burn-blockchain-consensus.

[xii] Muneeb, Ali et al. "Proof of Transfer Whitepaper v1.0." Blockstack PBC, May 2020, accessed February 15, 2023, https://assets.website-files.com/5fcf9ac604d37418aa70a5ab/60072dbb32d416d6b3806935_5f1596b12bcc0800f3dcadcd_pox.pdf

[xiii] Ali, Muneeb. "Stacks 2.0: Apps and Smart Contracts for Bitcoin." Whitepaper Draft v0.1, December 2020, accessed February 17, 2023, https://gaia.blockstack.org/hub/1AxyPunHHAHiEffXWESKfbvmBpGQv138Fp/stacks.pdf

[xiv] Newbery, Emma. "Miami to Launch Its Own Cryptocurrency, MiamiCoin." The Ascent, updated November 7, 2022, accessed February 21, 2023, https://www.fool.com/the-ascent/cryptocurrency/articles/miami-to-launch-its-own-cryptocurrency-miamicoin/.

[xv] https://app.onstacks.com/

[xvi] jcnelson, "Cap the Upside of Discount-mining." Stacks Forms, June 2022, accessed February 22, 2023, https://github.com/stacks-network/stacks-blockchain/issues/3095

[xvii] Ali, Muneeb. "Miner Centralization." Stacks Forms, June 2022, accessed February 17, 2023, https://forum.stacks.org/t/miner-centralization/13217/47

[xviii] Sun, Zhiyuan. ”Stacks Ecosystem Becomes #1 Web3 Project on Bitcoin.” Cointelegraph, January 14, 2022, accessed February 18, 2023, https://cointelegraph.com/news/stacks-ecosystem-becomes-1-web3-project-on-bitcoin.

[xix] Alex, ALEXLab. "Temporary Halting Collateral Rebalancing Pool (CRP)." Twitter, October 2, 2022, https://twitter.com/ALEXLabBTC/status/1576537438977073153