Stacks 2.0: Apps and Smart Contracts for Bitcoin

Muneeb Ali

Whitepaper DRAFT v0.1
Dec 2020

Stacks

Introduction

This paper provides an overview of the Stacks 2.0 blockchain, a layer-1 blockchain that brings smart contracts and decentralized apps to Bitcoin. We introduce the first consensus algorithm between two blockchains. Stacks 2.0 integrates smart contracts and decentralized apps natively with Bitcoin's security, stability, and economic power.

Blockchains are the most significant upgrade to the internet since the Web's creation over 30 years ago. For the first time, you can define and engage with digital assets using open protocols, unlocking new business models and capabilities that were not possible before.

Bitcoin is the earliest and most secure blockchain; it provides a new type of money that cannot be controlled or altered by any single party [1]. The Bitcoin network provides the foundations for not just the Bitcoin cryptocurrency but a general settlement protocol.

Blockchains enable new types of computer programs: (a) smart contracts that can be published on a blockchain to execute in a trustless manner and anyone can verify their outputs, and (b) decentralized apps that are user-owned and avoid centralized servers. Ethereum demonstrated the power of smart-contracts, and Stacks brings these capabilities to Bitcoin.

Our thesis is that decentralized apps and use cases will eventually get built on Bitcoin, the strongest and most widely used blockchain network, instead of disconnected networks. In the early days of the internet, there were several competing protocols. TCP/IP emerged as the winning standard, and everything else was built on it. Bitcoin is that standard for crypto.

Given our thesis of Bitcoin as the standard for value settlement, we have built the first consensus algorithm between two blockchains, called Proof of Transfer (PoX), that connects the Bitcoin and the Stacks blockchains and extends the functionality of Bitcoin. Leader election happens on the base Bitcoin chain, and new blocks are written on the connected Stacks chain.

The Stacks 2.0 blockchain brings (a) scalable transactions and (b) general-purpose smart contracts to Bitcoin without modifying Bitcoin. Stacks miners use Bitcoin (BTC) to mine newly minted Stacks (STX). Stacks holders can lock their STX in consensus to earn Bitcoin, making STX a unique crypto asset that is natively priced in BTC and gives BTC earnings.

Clarity language, a secure and predictable smart contract language, goes live with Stacks 2.0 mainnet launch. It was developed by Princeton and MIT scientists over the last two years. Clarity makes it much harder to have smart contract bugs and allows developers to write logic around Bitcoin state directly. We believe bringing smart contracts directly to Bitcoin can make BTC more valuable as it can be put to productive use instead of being a passively held asset.

The Stacks cryptocurrency was distributed to the general public through the first-ever SEC qualified token offering in 2019. Stacks (STX) is used as fuel for Clarity smart contracts.

Disclaimer: This paper is not an offering for any security or token and is meant only for information purposes. There are certain forward-looking statements in the paper which may not prove to be accurate. Further, the information in this whitepaper may become outdated.

Why Bitcoin

Bitcoin is the strongest sovereign blockchain. Bitcoin is a tamper-proof source of truth; a value settlement protocol. Once you have the ultimate source of truth, other decentralized protocols and use cases can be built on it. On the traditional internet, TCP/IP protocol emerged as the standard and didn't need to change for people to innovate on it. Protocols, once established, are fairly hard to compete with. Bitcoin is sovereign money and a value settlement protocol. The world will likely converge to one standard of value. We believe that this standard of value will be Bitcoin, given the network effects, security, and crypto market dominance.

There is a misconception that Bitcoin is a "one-trick pony" and cannot have use beyond store of value. It is possible to innovate around the Bitcoin settlement protocol and enable general-purpose smart contracts and decentralized apps. Bitcoin does not need to change.

There are two fundamental challenges to building apps and smart contracts on Bitcoin:

1) Scalability: The base Bitcoin blockchain has a limited capacity for transactions.

2) Secure contracts: The Bitcoin blockchain has a limited scripting language and does not allow general smart contracts. This design choice ensures security at the base layer.

The Stacks blockchain addresses the limitations of scalability and secure smart contracts and enables apps and smart contracts for Bitcoin. We do this through a unique consensus algorithm that runs between two blockchains. The Bitcoin blockchain functions as the settlement layer and source of truth while smart contracts execute on the Stacks chain.

Enabling scalable smart contracts directly on Bitcoin has been a long-standing bottleneck, and the Stacks blockchain unlocks that functionality. We enable this without modifying Bitcoin, a critical design requirement for enabling such apps and smart contracts.

Bitcoin is currently used as a (passive) store of value, and the Bitcoin cryptocurrency is the primary use case for the Bitcoin blockchain. Successful use cases presently being tested on other blockchains can simply be ported over or built directly using Bitcoin.

Earning Bitcoin:

The security of the Bitcoin network and access to Bitcoin's crypto capital are benefits of our design. In addition, our design enables a unique economic characteristic for the Stacks cryptocurrency where STX holders can lock their STX to earn BTC rewards from the consensus algorithm.

Bitcoin's fixed, limited supply and adoption as a hedge against inflation makes earning BTC attractive. Further, as smart contract usage increases on the Stacks blockchain, BTC earning rate also increases (see Page 6).

Stacks 2.0 Design

Stacks 2.0 is a layer-1 blockchain that connects to Bitcoin for security and enables decentralized apps and predictable smart contracts. Stacks 2.0 implements PoX mining that anchors to Bitcoin security. Leader election happens at the Bitcoin blockchain and STX miners write new blocks on the connected Stacks blockchain. With PoX there is no need to modify Bitcoin to enable smart contracts and apps around it.

There are two types of participants as part of the PoX consensus mechanism: (a) STX miners, and (b) STX holders.

STX miners can view state on both the Bitcoin blockchain and the Stacks blockchain. STX miners participate in leader election by sending transactions on the Bitcoin blockchain, a Verifiable Random Function (VRF) randomly selects leader of each round (while giving more weight to higher BTC bids), and the leader writes the new block on the Stacks chain. STX miners get newly minted STX (coinbase rewards), transaction fees paid to them in STX, and Clarity contract execution fees of each block also paid in STX. STX miners express the cost of mining in BTC and spend BTC to participate in leader election. The STX miners can model the total value of a new Stacks block as a BTX/STX on-chain trading pair, and will participate in mining if they can get cheaper STX from mining than from outside exchanges.

STX holders can participate in consensus and earn BTC rewards by participating in a process called Stacking. To participate, users lock their STX for a reward cycle (approx two weeks), run or support a full node, and send useful information on the network as STX transactions. STX holders who actively participate in Stacking earn the Bitcoin rewards of that cycle. Unlike proof of stake, there is no risk of slashing (economic penalties by protocol) for STX holders.

Stacks 1.0, an initial design with limited set of functionality, was launched on top of Bitcoin in Fall 2018. Stacks 2.0 is a major upgrade and feature-complete design which is expected to go live on mainnet in Jan 2021. This paper only covers Stacks 2.0 and replaces the previous technical design of Stacks 1.0 [2].

Scalability of Transactions:

The Stacks blockchain transactions can scale independently of Bitcoin; they only depend on Bitcoin for finality. Thousands of Stacks transactions result in a single hash on Bitcoin; Stacks transactions “settle” on Bitcoin automatically every Bitcoin block as part of consensus. Further, Stacks introduces the concept of microblocks that give initial confirmation in seconds. Microblocks are a main venue for future scalability research, where theoretically faster consensus algorithms can run for microblocks that settle data on Bitcoin per Bitcoin block.

Bitcoin is used as a settlement protocol by Stacks. It serves as the source of ultimate truth and archives hashes of Stacks block history. Finality of transactions is currently tied to Bitcoin and we believe that Bitcoin offers a strong notion of finality that our design benefits from.

The Stacks 2.0 blockchain is written in Rust. Protocol details and the open-source code is available in the Stacks GitHub repository [3].

PoX Consensus

Proof of Transfer (PoX) is the first consensus algorithm between two blockchains. Specifically we present an implementation of PoX by using Bitcoin as the base chain and Stacks as the connected chain. In PoX, leader election happens on the Bitcoin blockchain. Instead of burning electricity on proof of work, PoX reuses already minted bitcoins as “proof of computation” and miners represent their cost of mining in bitcoins directly.

STX miners bid for becoming the leader of the next round. The protocol selects the winning miner (i.e., the leader) of a round using a verifiable random function (VRF). The leader writes the new block of the Stacks blockchain and mints the rewards: newly minted Stacks for the block, fees for smart contracts and transactions.

Bitcoins used for miner bids are sent to a set of specific addresses corresponding to Stacks (STX) tokens holders that are actively participating in consensus. Thus, rather than being destroyed, the bitcoins consumed in the mining process go to productive Stacks holders as a reward based on their holdings of Stacks and participation in the Stacking algorithm.

PoX Parameters:

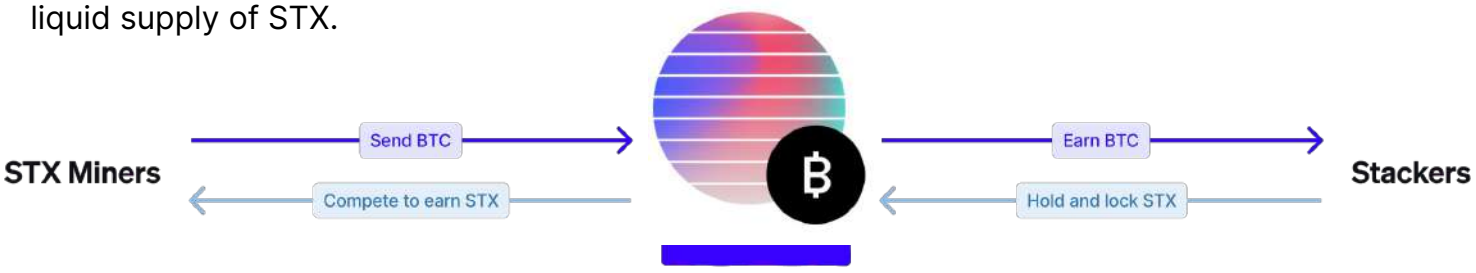
- Block reward: 1000 STX/block for first 4 yrs; 500 STX/block for following 4 yrs; 250 for the 4 yrs after that; and then 125 STX/block in perpetuity after that.

- Block time: Stacks blockchain produces blocks at the same rate as Bitcoin. Bitcoin blocks are produced roughly once every 10 minutes, so that will be the rate for Stacks 2.0 mainnet. However, microblocks can give faster initial confirmation.

- Block reward maturity window: 100 blocks, meaning if a miner wins a block, they will earn the coinbase reward for that block after 100 blocks have elapsed.

- Stacking parameters: 2 reward addresses per block; reward cycle 2000 blocks (~2 weeks) for a total of 4000 reward slots.

- Stacking threshold: the minimum number of STX needed is dynamic based on participation. This threshold is 0.025% of the participating amount of STX when participation is between 25% and 100% and when participation is below 25%, the threshold level is always 0.00625% of the liquid supply of STX.



Proof of Transfer consensus mechanism

More details for PoX consensus are in the PoX technical paper [4].

Clarity Smart Contracts

Clarity is a new programming language for smart contracts. The Clarity language optimizes for predictability and security. Stacks 2.0 anchors clarity smart contracts to Bitcoin making it possible for smart contracts to operate based on actions seen on the bitcoin blockchain.

Well-designed smart contracts can prevent bugs, but poorly designed contracts can exacerbate problems. This is especially important given smart contracts are meant to keep digital money on them. With Clarity, we took the what you see is what you get approach. Clarity makes the behavior, cost, and performance of smart contracts transparent both for developers and for automated verification and introduces post-conditions for added safety.

Decidable Language:

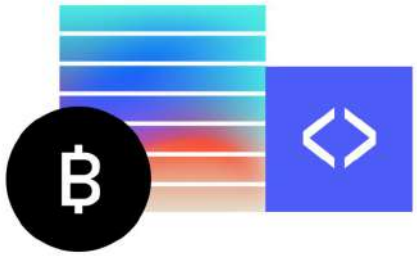
Clarity is a decidable language. A programming language is decidable if one can know, with certainty, from the code itself what the program will do. Clarity is intentionally Turing incomplete as it avoids “Turing complexity.” This allows for complete static analysis of the entire call graph of a given smart contract. Further, support for types and type checker can eliminate whole classes of bugs like unintended casts, reentrancy bugs, and reads of uninitialized values. Finally, Clarity code can be analyzed for runtime cost and data usage. Developers can predict what a given Clarity program will do, and how much it will cost.

Solidity, the implementation language for contracts on Ethereum [], is an undecidable language: it is impossible to know precisely how a contract will behave in certain situations without actually executing it in those situations. There are advantages to both types of programming languages. But when it comes to smart contracts that lock up billions of dollars in code, it’s critical to minimize risks.

No Compiler:
In addition to being a decidable language, Clarity is also interpreted. The contract source code itself is published and executed by blockchain nodes. Removing any intermediate, compiled representation (e.g., EVM byte code for Solidity) further minimizes the surface area for introducing bugs. Publishing the contract source code also improves understandability. Compiler bugs are doubly damaging in blockchains because while the programmed source code may not have an error, the eventual program reaching the blockchain could. Any such errors would require contentious hard forks — which are potentially infeasible — to remedy.

Visibility into Bitcoin State:

Clarity contracts have visibility into Bitcoin state, meaning that contract logic can trigger based on pure Bitcoin transactions. Clarity contracts have built-in SPV proofs for Bitcoin and can make interacting with Bitcoin state much easier for developers. Clarity contracts fork with Bitcoin, so developers don’t have to worry about corner cases where Bitcoin forks and smart contracts need to adjust to the fork.



Stacks (STX) Cryptocurrency

Stacks cryptocurrency (STX) is designed primarily to be used as “fuel” to execute Clarity smart contracts. Stacks are also used for other network functions like registering digital assets, paying for transaction fees, and to publish Clarity contracts on the blockchain.

Stacks can be locked by STX holders to participate in consensus and earn Bitcoin rewards. This process is called Stacking. To participate, STX holders run a full node, lock their STX, and publish useful information periodically on the network. The annual earning rate of Bitcoin rewards depends on several factors. For example, if 50% of the liquid supply participates, along with other assumed parameters, then the earning rate can be approx 9%. See details [5].

Stacks cryptocurrency was distributed to the general public through the first-ever SEC-qualified token offering in US history with 4,500+ people/entities participating.

PoX consensus mechanism establishes a native exchange pair between STX and BTC and makes STX a unique asset in that you can lock it to get earnings in Bitcoin. This is different from traditional proof of stake assets that give a yield in the same cryptocurrency.

Long-term Value:

Stacks cryptocurrency, like other cryptocurrencies, has several risk factors that can negatively impact the value of the crypto asset. Readers should see the Risk Factors section of the 2019 SEC offering for a comprehensive list of these risks [6].

The long-term value of Stacks is generally dependent on the growth of the Stacks network and demand for Clarity smart contracts. To execute Clarity contracts on the network, users need to pay STX as fuel (gas fees). For example, a decentralized exchange built as a Clarity contract requires STX as fees to execute the logic of the exchange contract on each user interaction.

Given the unique property of Bitcoin earnings, we expect a subset of the STX liquid supply to be locked and taken out of the effective liquid supply. Such long-term holders want to earn Bitcoin rewards and actively participate in consensus. The value of the Bitcoin rewards going to STX holders depends on (a) coinbase rewards and (b) network usage. If more Clarity contracts get executed on the network then the Bitcoin rewards for Stacking increase as well. In the initial years, 1000 STX per new block are released as newly minted tokens (coinbase rewards). In addition to coinbase rewards, fees for contracts and transactions also determine how miners value a block. If network usage goes up then the value of the block to miners goes up because of the higher contract and transaction fees. This means higher Bitcoin bids for blocks and more BTC rewards flowing to STX holders that actively participate in consensus.

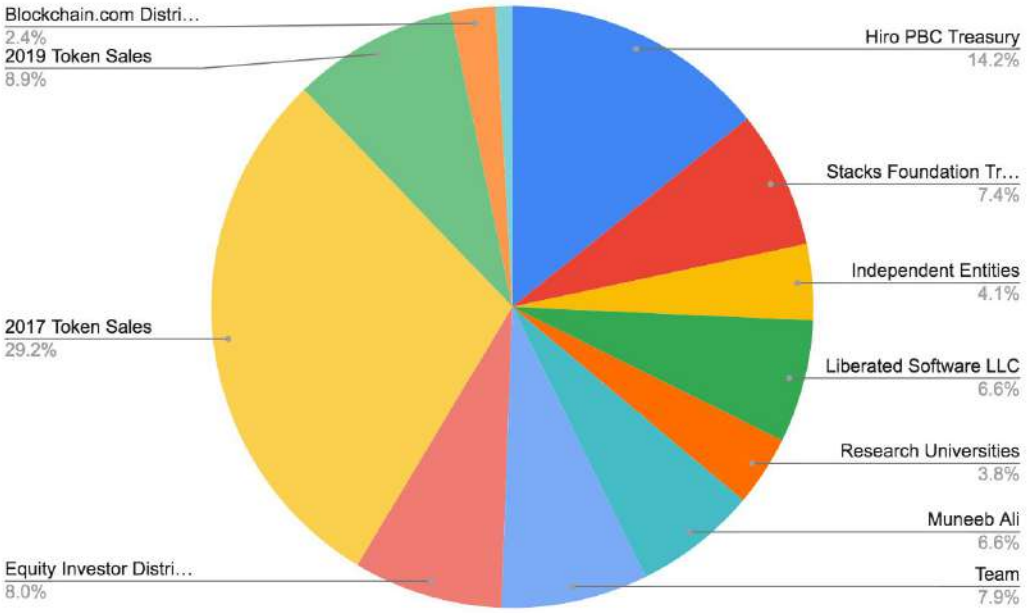
Coinbase STX	Clarity fees	Transaction fees

* Coinbase STX follow a fixed predefined schedule.
* Clarity & transaction fees go up or down with network usage.

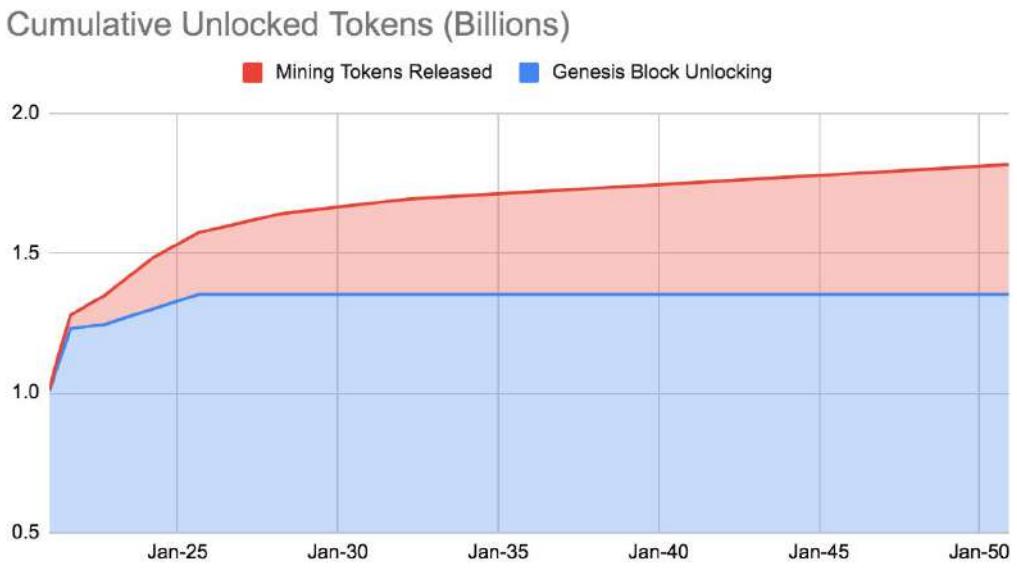
[BTC bids proportional to the value of a STX block]

Token Economics

The Stacks cryptocurrency has 1.32 billion (1,320M) STX in the genesis block [14]. These STX were distributed through various offering in 2017 and 2019. The 2017 offering distributed STX at a $0.12 price, the 2019 Reg S offering at $0.25, and the 2019 SEC qualified offering at $0.30. Figure 1 below gives the breakdown of the genesis block tokens.



The Stacks cryptocurrency has a predefined future supply that reaches approx 1,818M STX by year 2050 (a reduction from the earlier 2,040M number [14]). By end-Jan 2021, approx 1,006M of the 1,320M genesis block STX will be liquid and the remaining will unlock monthly following various locks. For example, STX allocated for founders and employees follow a 3 year unlocking and a subset of these will unlock between Jan 2021 and Nov 2021. Figure 2 shows the increase in total circulating supply of Stacks until 2050. See [7] for more details.



Stacks Ecosystem

The Stacks ecosystem is a collection of independent entities, developers, and community members working to build a user-owned internet on Bitcoin.

Project History:

The project got its start at the Princeton Computer Science Department in 2013 as an effort to build a better internet. Muneeb Ali and Ryan Shea went through Y Combinator in 2014 and recruited other Princeton computer scientists for initial R&D. Early investors include Union Square Ventures, Naval Ravikant, SV Angel and others. Muneeb's 2017 PhD thesis laid the technical foundations of a user-owned internet built on blockchains [8].

The project raised $47M in a token offering for the Stacks cryptocurrency in 2017, and an additional $23M through the first-ever SEC-qualified US Reg A offering and concurrent Reg S offering in 2019. More than 4,500 Stacks holders participated in these offering, including USV, Lux, DCG, Winklevoss Capital, Blockchain Capital, Foundation Capital, Hashkey, Fenbushi, and others.

Decentralized Ecosystem:

Blockstack PBC, a public benefit corp, worked on the early R&D, protocol design, and public infrastructure after raising a Series A in 2017. The public infrastructure building phase completed in late 2020 and Blockstack PBC rebranded to Hiro Systems to narrowly focus on developer tools after the launch of Stacks 2.0.

In 2020, following a path to decentralization, several independent entities emerged in the Stacks ecosystem. These include the non-profit Stacks Foundation, a community focused entity Freehold, a mining and Asia markets focused entity Daemon Technologies, along with New Internet Labs and Secret Key Labs that work on independent user clients. There are 400+ apps in the Stacks ecosystem developed by independent developers and entities.

In Fall 2020, Blockstack PBC released a legal memo summary that details the transition to a non-security status for the Stacks (STX) cryptocurrency in the US [9].

Hiro

Stacks Foundation

地灵科技
DAEMON TECHNOLOGIES

FREEHOLD

New Internet Labs

Stacks 2.0 Mainnet Launch

The Stacks 2.0 launch, currently anticipated on Jan 14th 2021, is closer to the launch of a whole new project than an upgrade from Stacks 1.0. Stacks 2.0 is our master design and solves two long-standing problems with Bitcoin (a) scalability of transactions and (b) enabling smart contracts without modifying the main Bitcoin blockchain itself.

Start of Mining:

The launch of Stacks 2.0 mainnet requires adoption by at least 20 independent miners. The miners need to register themselves in the .miner namespace and follow other steps [10]. With the start of mining, 1000 STX per block will be released as newly minted STX (as incentive for STX miners to package/write new STX blocks). The start of mining may be thought of as a small new decentralized exchange coming online in the ecosystem. Roughly 150K STX per day will be “traded” through mining in the BTC/STX on-chain pair. Like other blockchains, miners will only mine new blocks if it is profitable for them to do so. For Stacks 2.0, this is expected to mean that miners can get cheaper STX through the BTC/STX mining pair exchange as compared to other exchanges that currently support BTC/STX pairs (like Binance). The “trading volume” on the mining exchange pair is expected to be relatively small compared to normal exchanges, given that exchanges like Binance currently do approx millions of STX in trade volume (compared to the 150K STX upper limit on the mining pair).

Earning Bitcoin:

With the Stacks 2.0 mainnet launch, a subset of the liquid STX supply may get locked to actively participate in consensus. If 50% of the liquid supply participates in earning BTC rewards, along with other assumed parameters, then the BTC earnings can be approx 9% [5].

The minimum number of STX required to participate in consensus is dynamic and depends on the percent of liquid supply that is actively participating. If 50% of the liquid supply is participating and 950M is the liquid supply then 120K minimum STX are required to participate in Stacking. However, STX holders can use pooling services and delegation to service providers is supported by the network.

Clarity Contracts:

The ability to publish and execute Clarity smart contracts will go live with Stacks 2.0 mainnet launch. All transaction fees and Clarity contract gas fees will be paid in STX to miners.

Upgrade Guide:

Stacks 2.0 mainnet launch acts as a hardfork from Stacks 1.0 and all STX balances and ownership of digital assets will be automatically transferred to Stacks 2.0. There is no need for any token swap between Stacks 1.0 and Stacks 2.0. STX holders will need to upgrade to Stacks 2.0 wallets [11] and exchanges and other node operators can follow the integration guide [12].

Summary and Future Work

Stacks 2.0 brings apps and smart contracts to Bitcoin. Our thesis is that successful experiments from various blockchains will eventually get created on Bitcoin. The network effects of Bitcoin mean that smart contracts around Bitcoin have access to more crypto capital and benefit from higher security. We believe that Bitcoin can be the foundation for a better user-owned internet much like TCP/IP for the traditional internet.

Stacks 2.0 enables a new way for users to earn Bitcoin by actively participating in consensus. Our work can make Bitcoin more valuable by turning passive Bitcoin capital into actively deployed capital and bringing more apps and smart contracts to the Bitcoin ecosystem.

After the release of Stacks 2.0 certain improvements like auctions for block space, more throughput and speed of microblocks, and advanced Clarity language features [13] can be areas for future work that the Stacks Foundation and the broader community may work on.

References:

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

[2] M. Ali, R. Shea, J. Nelson and M. J. Freedman, “Blockstack: A New Internet for Decentralized Applications”, Whitepaper Version 1.1, Oct 2017.

[3] Stacks GitHub repository. https://github.com/blockstack/

[4] M. Ali, A. Blankstein, M. J. Freedman, L. Galabru, D. Gupta, J. Nelson, J. Soslow, P. Stanley, “PoX: Proof of Transfer Mining with Bitcoin”, Whitepaper v1.0 May 2020. https://blockstack.org/pox.pdf

[5] M. Ali, “Stacking Earnings Model: Projecting Consensus Participation Rewards for STX Holders”, Oct 2020. https://blog.blockstack.org/stacking-earnings-model/

[6] Blockstack Token LLC, SEC Offering Circular, May 2019. https://www.sec.gov/Archives/edgar/data/1719379/000110465919029828/a18-15736_1partiiandiii.htm

[7] STX future supply spreadsheet. https://github.com/zone117x/stx-supply-schedule/

[8] M. Ali, “Trust-to-Trust Design of a New Internet”, PhD dissertation, Princeton University, June 2017. https://muneebali.com/thesis

[9] M. Ali, “Stacks Cryptocurrency Expected To Reach Non-Security Status in the United States”, Dec 2020. https://blog.blockstack.org/stacks-cryptocurrency-expected-to-reach-non-security-status-in-the-united-states/

[10] D. Gupta, “[RFC] Stacks 1.0 → 2.0 Upgrade Process”, Nov 2020. https://forum.stacks.org/t/rfc-stacks-1-0-2-0-upgrade-process/11346

[11] Stacks 2.0 wallet. https://wallet.blockstack.org

[12] Stacks 2.0 Integration Guide, https://docs.blockstack.org/stacks-blockchain/overview

[13] J. Nelson, “After Stacks 2.0: Potential Features for Stacks 2.1”, Nov 2020. https://forum.stacks.org/t/after-stacks-2-0-potential-features-for-stacks-2-1/11376

[14] M. Ali, "Stacks Token Economics and Incentive Mechanisms", Whitepaper Ver 2.0.7, Oct 2019.

[15] V. Buterin, “A next-generation smart contract and decentralized application platform,” Ethereum whitepaper 2013. https://ethereum.org/en/whitepaper/.