SOBERIN Research

Stacks (STX)

An Examination of a Promising Bitcoin-Based Ecosystem

Publish date: 21st July 2023

AUTHOR NAME : SOBERIN RESEARCH


SOBERIN

Research Report – Stacks (STX)

Introduction

Bitcoin (BTC) was arguably not the first cryptocurrency. Its theoretical predecessors include electronic money DigiCash launched in 1995 and Bit Gold, a decentralised Proof-of-Work (PoW) virtual currency proposed in 1998 by Nick Szabo. Bitcoin is, however, the first cryptocurrency to integrate blockchain technology at the infrastructure level, and the oldest surviving digital currency. It is also the most widely accepted cryptocurrency, with BTC market capitalisation as of 30th April 2023 45.07% of the total market cap of top 10 largest cryptocurrencies (vs. 18.28% for Ether in second place). At the same time, outside of BTC's role as a store of value, the capital and infrastructure of Bitcoin remain largely untapped. Stacks is the leading protocol aiming to change this, through introducing smart contract functionality and scalability while retaining the security of Bitcoin.

Stacks is a Bitcoin Layer, which enables smart contracts and decentralized applications to utilise BTC as an asset and settle transactions on the Bitcoin blockchain. This paper traces the history of Stacks, discusses the overall vision for the Stacks layer and key upcoming developments such as sBTC and the Nakamoto Release, and considers how its native token could represent one of the most compelling long-term opportunities today.

History

Stacks (then Blockstack) co-founders Muneeb Ali and Ryan Shea didn't start off focusing specifically on Bitcoin, but on developing a decentralised computing platform which affords users greater control over their personal data. In 2016, Blockstack was launched as a comprehensive (i.e., full-*stack*) alternative to traditional cloud computing with data processing run on the client's computers rather than centralised servers, with user controlling what data is shared to the network's *block*chain.

The Blockstack project started in 2017 when Muneeb finished his PhD (his thesis laid out the foundations for the Stacks layer for Bitcoin), released the original whitepaper, and raised $50M. Prior to this, the early team built protocols and apps on Bitcoin L1.

From 2018-2020 the team was heads down building out the Stacks infrastructure and attracted some high-profile strategic investors along the way, such as Union Square Ventures (see their post), Harvard Endowment (which was quite rare), and Winklevoss Capital.

In Jan 2021 Stacks mainnet launched. Leading up to the mainnet launch the project decentralised, and rebranded from Blockstack to Stacks to differentiate the Stacks open-source project from any project/company behind it, with much of the work spearheaded

by the Stacks Open Internet Foundation, a non-profit established in May 2020 with a grant of STX100mn.

The Stacks layer

In December 2022, the sBTC whitepaper was released along with plans for the 2023 Nakamoto Release, which aims to bring faster speeds and transactions backed by 100% of BTC security to the Stacks Layer.

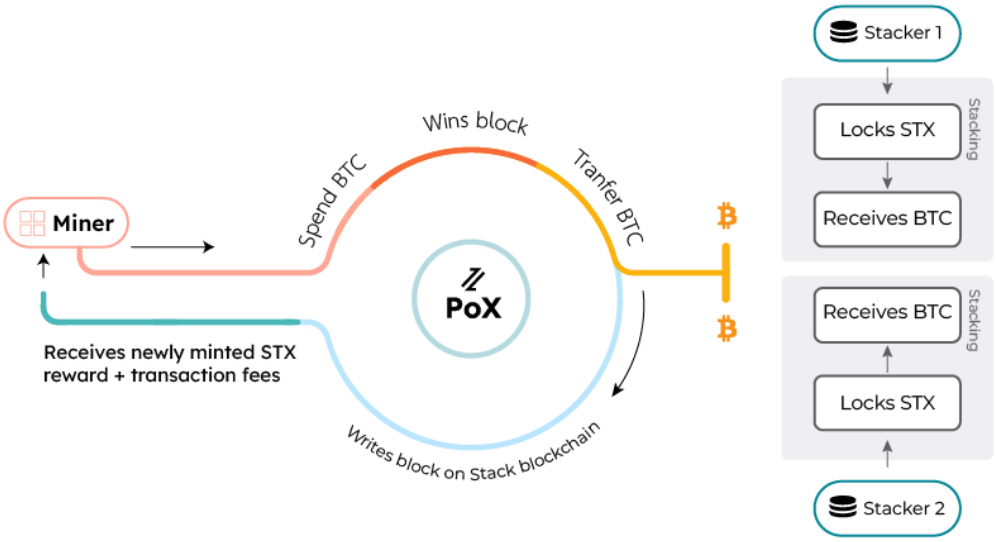
The introduction of sBTC is slated to enable trustless writing to Bitcoin and the movement of BTC in and out of the Stacks Bitcoin layer, unleashing BTC as a fully programmable, productive asset.

In its entirety, this new Stacks platform will comprise of a Stacks blockchain, a PoX consensus mechanism, the sBTC BTC-peg and the STX native token, with the Nakamoto Release upgrades, all powered by the Clarity language. Each component is detailed below:

Stacks blockchain and PoX

The Stacks blockchain is a PoX-secured layer-2 blockchain built atop Bitcoin. Specifically, on the Stacks network transactions initiated by the client are confirmed through decentralised nodes operated by miners. Under PoX, a miner *transfers* BTC to addresses specified by *stackers* – STX token holders who locked up their STX to earn BTC – for a chance to process new blocks for the Stacks blockchain and receive newly-minted STX block rewards and transaction fees.

Figure 1 - The Proof of Tranfer (PoX) mechanism



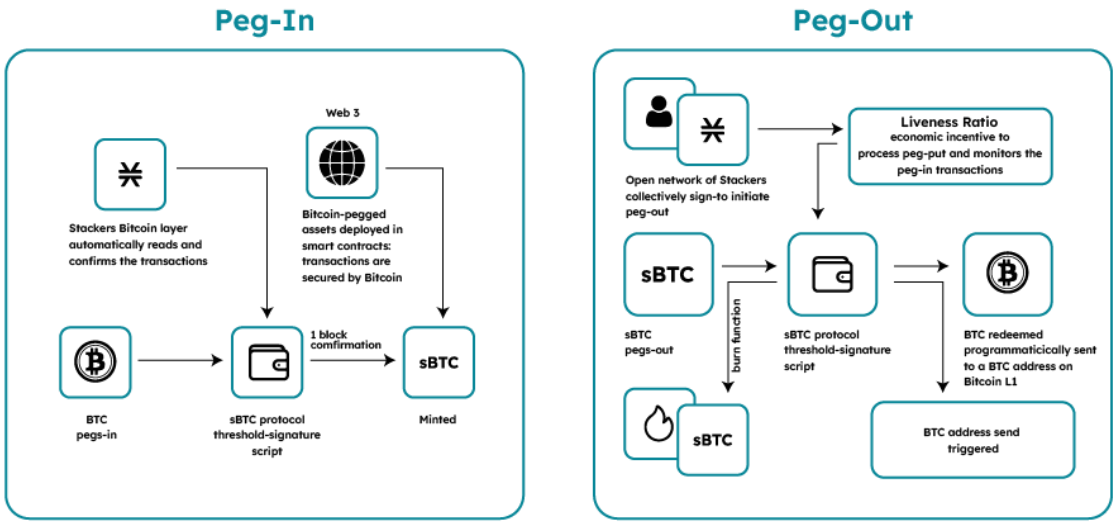
Source: *Proof of Transfer*. Stacks Academy. https://docs.stacks.co/docs/stacks-academy/proof-of-transfer

Impending upgrades to Stacks platform

sBTC

sBTC is a 100% collateralised BTC-pegged-token, minted by locking BTC in a 1:1 ratio on a threshold signature wallet on the Bitcoin mainchain. Specifically, sBTC operates under two modes, the default *Normal Mode* and *Recovery Mode*. Under the former, a user can send BTC to a wallet on the Bitcoin chain (peg-in), the transaction is read and confirmed by the Stacks Bitcoin layer, and the sBTC protocol mints an equivalent amount of sBTC and sends it to an address specified by the sender (Figure 2). To withdraw (peg-out), a user sends his sBTC and the peg-out request to the sBTC protocol, where Stackers operating in the PoX consensus collectively sign to initiate peg-out. Upon receiving the confirmation, the sBTC protocol sends the equivalent amount of BTC to the requested Bitcoin address, and then burns the sBTC it received earlier.

Figure 2 - sBTC peg-in/out mechanism



Source: *sBTC: Design of a Trustless Two-way Peg for Bitcoin*. https://stx.is/sbtc-pdf

Should a liveness failure occur for any reason, the system shifts to Recovery Mode until enough stackers are online to resume signing peg-out requests. In Recovery Mode, a portion of the BTC PoX stackers would have received are redirected to fulfill peg-out requests until all outstanding requests have been satisfied. This process would be considerably slower than Normal Mode, but ensures users can redeem BTC so long as Stacks and PoX continue operating.

A threshold of 70% is planned for the signature wallet, i.e., 70% of all stackers who locked STX in the PoX must approve a peg-out transaction. Conversely, *compromising the peg wallet*

requires at least 70% of stackers to act maliciously. With the launch of sBTC, a stacker would be required to lock up STX *exceeding* the value of BTC in the peg wallet in accordance with the *liveness ratio*, which compels a stacker to remain online and fulfil peg out requests, lest he loses both this larger deposit and BTC rewards from the transition to Recovery Mode.

Stacks's integration into Bitcoin allows BTC/STX price information to be obtained via a decentralised on-chain Bitcoin oracle. By not using an external oracle the Stacks platform avoids a potential point of vulnerability. Indeed, the sBTC white paper argues that an ideal Bitcoin layer needs to have: 1) fully expressive smart contracts, 2) the ability to move BTC in/out of the layer in a decentralised manner, and 3) high security backed by BTC security, but pre-existing layers do not satisfy all such requirements. For example, Lighting does not accommodate fully expressive smart contracts, while Liquid uses a federated peg.

With sBTC, the peg in/out operation is executed through the Stacks blockchain's PoX mechanism and threshold signature wallet, thus *decentralising* the process. Since Stacks is a layer-2 blockchain which ultimately settles on Bitcoin, transactions with sBTC have the finality and *security* of Bitcoin. Finally, since sBTC exists on Stacks which is powered by Clarity, sBTC – and therefore the Bitcoin it is pegged to – could be *utilised via smart contracts*. *It is this Bitcoin write functionality that represents a huge value proposition for Stacks.*

Stacks Nakamoto Release

The Nakamoto Release – slated for Q423 – upgrades the Stacks platform in three major ways. Firstly, it incorporates sBTC. Secondly, it introduces *Bitcoin finality through new forking rules*. Thirdly, it facilitates *faster transaction speed via fast blocks*.

On the second point, the current version of PoX on Stacks does not settle fully on Bitcoin, but rather, on the Stacks blockchain – thus it had a separate security budget from Bitcoin equal to the BTC capital spent by Stacks miner. With the Nakamoto Release, all transactions on Stacks eventually settle on Bitcoin.

Specifically, under Nakamoto Stacks will have the following forking rules:

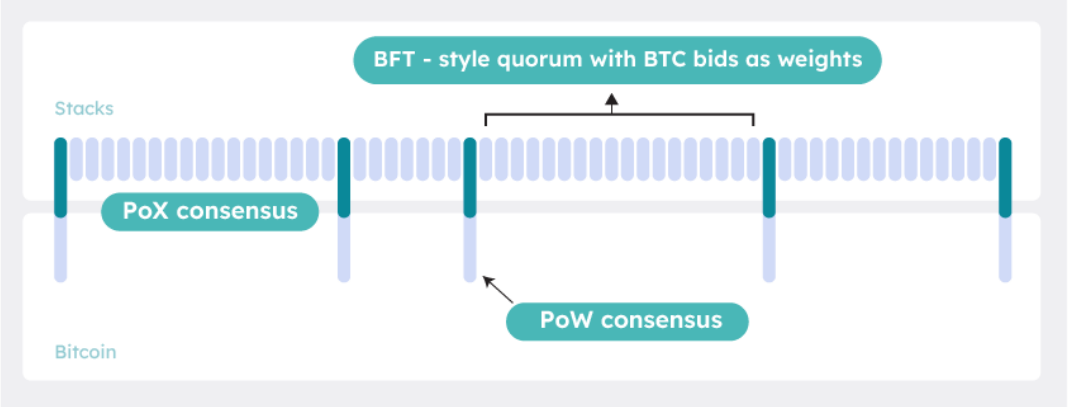
i. Within six Bitcoin settlement confirmations, forks are allowed.
ii. Between six and 150 block confirmations, a fork requires >50% of Stacks mining power and >70% of Stackers supporting it to be executed.
iii. Stacks blocks with 150 or more confirmations on Bitcoin follow Bitcoin finality (i.e., can only fork with Bitcoin) and are secured by 100% of Bitcoin's hash power.

Given Bitcoin's block creation time of 10 minutes, 150 blocks amount to ~25 hours. To alter transactions after this, an attacker would need to successfully change the history on Bitcoin.

In addition to improved security, the Nakamoto Release introduces fast blocks to boost transaction speed. Stacks 2.0 produces blocks at the speed of Bitcoin, or a block every ~10 minutes. With Nakamoto, there will be two types of blocks, *fast blocks* and *settlement blocks*.

Fast blocks will be produced between two Bitcoin blocks at a rate of roughly a block every five seconds. Through an open bidding process on the Bitcoin ledger, a group of Stack miners is elected that can mine for fast blocks between Bitcoin blocks, whereby fast blocks miners use BFT-style quorum signing weighted by their BTC bids to produce the fast blocks (Figure 3). Fast block can contain new transactions and contract calls.

Figure 3 – Fast block mining in-between settlement blocks

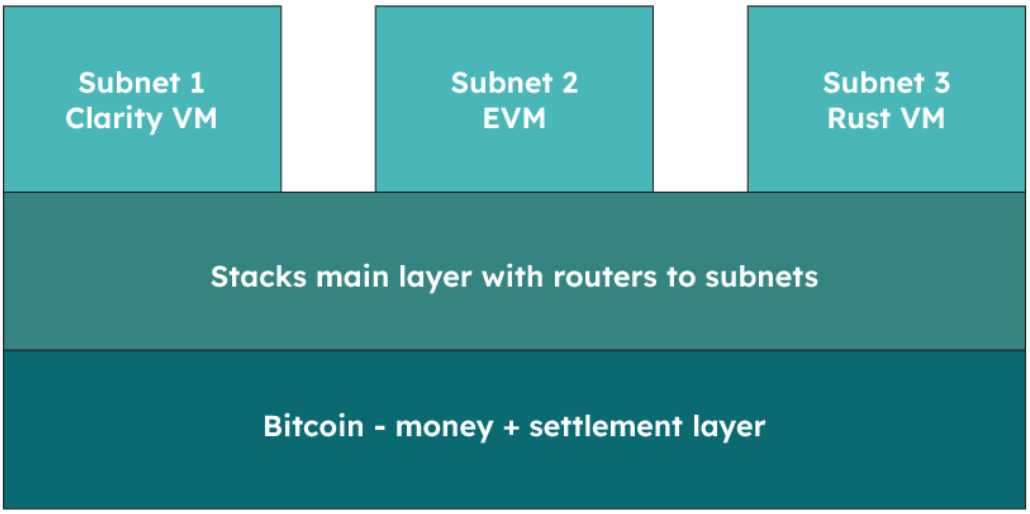


Source: *Proof of Transfer*. Stacks Academy https://docs.stacks.co/docs/stacks-academy/proof-of-transfer

Settlement blocks will be produced at every Bitcoin block, and do not contain any new transaction. Rather, they settle the preceding sequence of fast blocks on the Bitcoin chain. Forks are not permitted with fast blocks, but only possible at the level of settlement blocks, per the rules regarding block confirmation discussed above. *It could be said that Nakamoto is a major step in providing dApps built on Stacks with the proverbial best of both worlds – fast transactions with Bitcoin finality.*

In addition to these key upgrades, the Nakamoto Release will include other features to further boost Stacks performance. For example, Stacks mainnet will support *subnets* – slated to launch in 2023 – that could each host smart contracts in different languages and execution environments. Since Stacks itself is layered upon Bitcoin, some form of Bitcoin finality could be extended to all the subnets. For example, an Ethereum Virtual Machine (EVM) that settles on Bitcoin (Figure 4). *Having subnets makes possible execution environments with higher throughputs (at the expense of reduced decentralisation on the execution layer) while retaining Bitcoin finality*.

Figure 4 - Bitcoin-supported subnets



Source: *Stacks: A Bitcoin Layer for Smart Contracts*. https://stx.is/nakamoto

The Stacks ecosystem

Today there are 30+ companies in the ecosystem, including a non-profit Stacks Foundation, developer tooling company Hiro, and DeFi projects such as ALEX, Arkadiko, as well as other ecosystem builders such as BTC wallet provider Xverse and Daemon Technologies, a software consultancy driving Stacks adoption in Asia. The Stacks ecosystem also benefits from broader projects aiming to boost the adoption of Bitcoin as a L1 infrastructure, notably New Internet Labs and Trust Machines.

Clarity

Clarity is a smart contract language developed by Blockstack and launched via a developer preview on 27th June 2019 as a more intuitive and secure alternative to Solidity used by Ethereum. To this end, Clarity is a *decidable* and *interpreted* language.

Being decidable means that code written in Clarity allows one to determine with certainty what a program running it will do, and that code correctness can by verified by software, which prevents issues like halting problems and allows cost of transactions to be determined beforehand – therefore *unlike with Ethereum, transactions on Stacks cannot fail due to insufficient gas*.

Being an interpreted language means that Clarity code is committed to the chain exactly as it is written, in contrast to *compiled* languages such as Solidity where commands are compiled to bytecode before being submitted to a chain. Eliminating the compiling process

removes a layer of complexity and therefore a source of vulnerability. Moreover, compared to bytecode, which is in binary and thus not human readable, interpreted languages remain in human-readable syntaxes, meaning smart contract codes can be read by humans for verification.

Clarity has also been designed with other security features in mind, which take lessons from past exploits on Solidity. For example, Clarity does not permit reentrancy – when a smart contract calls into another which calls back into the original contract – a feature which could allow an attack to trigger multiple withdrawals before the contract can update its internal balance. Indeed, it was through reentrancy that the infamous Ethereum DAO hack occurred.

Bitcoin Name System

With the Stacks blockchain as its heart, a Stacks ecosystem which extends the functionality of Bitcoin has begun to take shape. One notable case is the Bitcoin Name System (BNS), launched with the Stacks 1.0 blockchain in October 2018, BNS is a decentralised name registry linking human-readable names to nodes on the Stacks blockchain, and in turn, to Bitcoin.

BNS names benefit from three properties: 1) *global uniqueness*, 2) being *human-readable* and 3) having *strong ownership*. In addition to boosting Bitcoin adoption by simplifying transactions, BNS has application in domain name security (making it impossible for hostnames to be hijacked), social media (profiles are tied to private keys) and more. Prior to the Nakamoto update, up to 120 subdomain operations could be broadcasted by a single Stacks blockchain transaction, but *the introduction of fast blocks should further lower the cost of registering/transferring subdomains, aiding BNS adoption.*

Hiro wallet

As mentioned, following the establishment of the Stacks Foundation, Blockstack/Hiro shifted its focus to building dApps and tools for the Stacks ecosystem. Part of this effort is the Hiro wallet, which enables storage and transactions of BTC and BTC layer-2 assets (e.g., STX tokens) and connections to Stacks apps. With over 280,000 downloads, Hiro also enables direct purchase of STX through bank transfer and card, allows stacking participation, and can integrate a Ledger hardware wallet for boosted security. However, unlike most Ethereum wallets, it is currently available only as a browser extension and desktop application.

Ordinals NFT

On 20th February 2023 Hiro wallet added support for ordinals, while the standalone Ordinals Explorer and Ordinals API for developer launched on March 15th 2023. Simply put, ordinals are records of data (e.g., image, text) on the Bitcoin blockchain – colloquially referred to as

Bitcoin-based NFTs, though important distinctions remain. For one, *unlike with the bulk of Ethereum NFTs, an ordinal inscription has all its data on-chain.*

It must be noted that Ord is an independent protocol, which does not need Stacks to operate, though the Explorer and API leave Stacks well placed to capitalise on growing interest in ordinals. Furthermore, *Stacks allows ordinals to be incorporated into smart contracts and DeFi*, with Stacks Accelerator project Deep Lake an example of such a project. Moreover, the enthusiastic adoption of ordinals – daily inscriptions steadily increased through 2023, with 2.7mn total inscriptions as of April 30th – *underscores a general demand for layer-2 solutions built on Bitcoin.*

Valuation of STX

Tokenomics

The Stacks token (STX) is the native token of the Stacks network, used to pay for transactions on the network, reward PoX miners, and facilitate stacking for BTC.

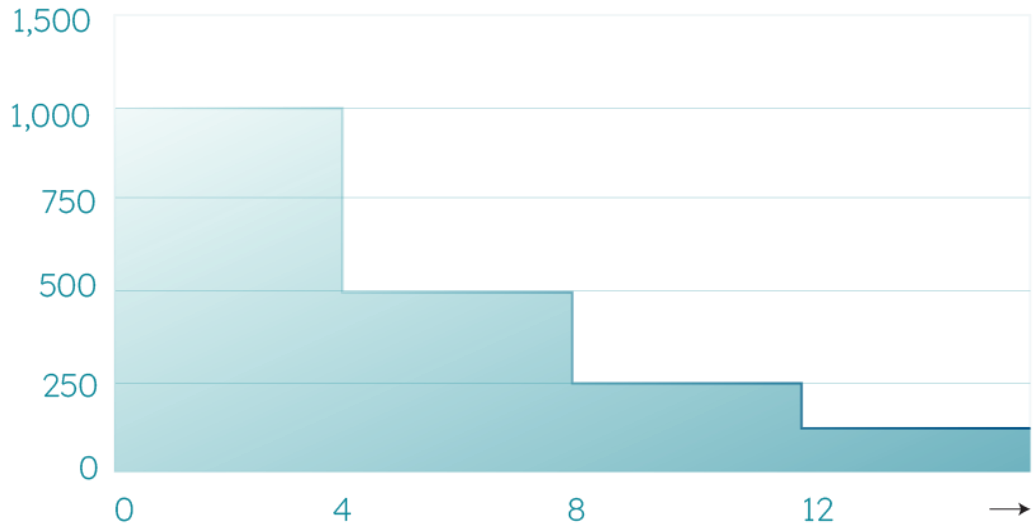
The STX token has a predefined future supply set to reach approximately STX1,818mn by the year 2050, where, per conversation with the Stacks team, the early investors/entities have been allocated less than 5% of total supply.

The initial supply of STX was minted along with the initial block ('Genesis Block') of the Stacks blockchain on October 30th 2018, which introduced 1.32 billion STX tokens. These tokens were allocated through a series of token sales over 2017-2019, as well as other distributions meant to grow the ecosystem. Notably, in 2019, Blockstack PBC sold STX74.98mn and STX30.56mn in SEC-compliant Reg A+ and Reg S offerings, making the company the first to receive SEC approval for token-based fundraising.

While most of the tokens generated in the Genesis Block were subjected to a transfer lock and a time lock – which prevented the tokens from being used for any purposed, including being burned or transferred – all tokens from the Genesis Block are slated be fully released by 2025.

The Stack tokenomics white paper published in October 2019 proposed an adaptive mint and burn mechanism that would specify maximum and minimum values of STX to be minted in a Stacks block, where the specific amount minted would depend upon the average amount of STX burned by the network during an evaluation period (13,149 blocks, ~ three months). However, in October 2020, the Stacks Foundation switched from the adaptive mint and burn to a *decreasing issuance* model, targeting a supply of ~1.82bn by 2050. Specifically, PoX miners now receive coinbase rewards for each settlement block they win per Figure 5 below. Note that STX halvings coincide with Bitcoin halvings every four years, before settling at STX125/block into perpetuity. *An important consequence of this change is to decrease maximum token supply in 2050 by 11.2%, from STX2.05bn to ~1.82bn*.

Figure 5 - Coinbase rewards for STX mining



Source: *Mining*. Stacks Academy documentation. https://docs.stacks.co/docs/stacks-academy/mining

Ratio analysis

While the discounted cash flow (DCF) approach offers valuation more closely tied to a platform's revenue, in the absence of a well-defined mechanism through which revenue feeds into the token – directly or indirectly through a community wallet, etc. – ratio analysis paints a better picture of how the Stacks ecosystem could be valued, which in turn, implicitly dictates a value for the STX token facilitating the functioning of the ecosystem. Specifically, STX is fuel powering the PoX consensus, used to pay transaction fees to PoX miners, and by stackers powering said PoX, each of whom earns BTC by locking up some amount of STX.

Additionally, while the Stacks team has a history of iteratively improving the network and its economics, such that one may be tempted to envision future scenarios where Stacks ecosystem revenue accrues directly to STX holders, such a feed-in mechanism would place STX firmly under the classification of a security token. While STX had been sold through SEC-compliant offerings, on January 20th 2021, as part of its SEC filing, Blockstack/Hiro informed the SEC that it would no longer treat STX as a security. This pivot was to facilitate the token being traded more freely and suggests the Stacks Foundation would avoid any change which would result in STX being classified as a security in the future.

Computing the ratios of market caps of the most prominent Ethereum layer-2 projects – Arbitrum (ARB), Polygon (MATIC) and Optimism (OP) – from project inception through June 29th 2023 gives maximum, minimum, and average values of 6.75%, 0.04%, and 0.93%, respectively (Appendix II). Per Table 1, these ratios yield fair value/token estimates ranging

from USD28.40 to USD0.16, with a mean-based value of USD3.91 vs. the closing price on June 29th 2023 of USD0.68.

Table 1 - L2 to L1 market cap approach

	Max	Min	Average	As of 29th June 2023
STX market cap (USDmm)	39,449.15	219.16	5,432.17	950.80
STX Price (USD/circ. token)	28.40	0.16	3.91	0.68

Source: *Cryptocurrency Prices by Market Cap*. CoinGecko data. https://www.coingecko.com

An intuitively appealing ratio for DeFi platforms is market capitalisation to Total Value Locked (TVL), which could be said to represent how much value a given network could be expected to extract from capital deployed within its ecosystem. Through examining the ratios of market caps to TVL for ARB, MATIC and OP, and assuming Stacks TVL of 2% of BTC-denominated capital, allow implied market caps to be derived and estimates to be made for corresponding fair values. To focus upon market cap as a multiple of capital being utilised in DeFi, TVL figures *exclude* tokens locked up for governance functions. The exclusion is also in line with the fact that STX does not presently offer a governance staking function. Per Table 2, assuming a market cap to TVL ratio of 17.995 yields a fair value per token of USD151.35, while the minimum ratio of 0.159 yields a price of USD1.34.

Table 2 - Market capitalisation to TVL approach

TVL = 2% of BTC cap.	Max	Min	Average	June 29th 2023
Market cap/TVL ratio	25,418.155	0.159	17.995	
STX price (USD/circulating token)	213,785.99	1.34	151.35	0.68

Source: *TVL Rankings*. DefiLlama data. https://defillama.com

An important point raised by the above analysis is that there is presently hardly any BTC TVL to speak of, such that an assumption had to be made regarding the proportion of BTC which would be locked up once Stacks unlocks smart contract functionality for Bitcoin. Conversely, this underlines the fact that unlike Ethereum layer-2 protocols which seek to extend the smart contract utility of Ethereum, Stacks is *introducing* smart contract functionality to Bitcoin, and introducing new use cases for BTC. First-mover advantage

entails that Stacks capturing 2% of BTC capital that it is helping to unlock in the first place is likely not an overly aggressive assumption.

There are two other reasons why Stacks could be reasonably expected to capture a considerable portion of BTC capital. Firstly, unlike Ethereum, for Bitcoin, limited smart contract functionality and slow and expensive transactions are not issues a core team is trying to overcome, but *design features* to preserve the security of the blockchain. This means that the value propositions for layer-2 Bitcoin networks such as Stacks are not vulnerable to material layer-1 upgrades, unlike with Ethereum where planned upgrades to the layer-1 blockchain itself – sharding and Verkle trees in particular – could render off-chain solutions such as Optimism less desirable.

Secondly, through a combination of PoX and sBTC, Stacks provides a *comprehensive* solution to unlocking Bitcoin capital. Using Ethereum as an example, a layer-2 solution offering scalability competes not with just other layer-2 scalability solutions, but also with liquid staking derivative (LSD) providers capitalising on Ethereum's new Proof-of-Stake (PoS) consensus and market demand for greater capital efficiency. Indeed, as of June 29th 2023, LSD provider Lido alone had TVL approximately equal to 52.7% of Ethereum TVL. Given that sBTC would serve as both a smart-contract layer-2 solution for Bitcoin *and* a liquid alternative to holding BTC, this latter consideration should boost its adoption to an even higher percentage of total BTC capital. It should be noted that per the liveness ratio, the value of locked up STX acts as a cap on sBTC supply, and ultimately, how much BTC capital could be utilised. However, to the extent growing adoption of Stacks is reflected in STX price appreciation, this should not pose a problem (e.g., a 100% appreciation doubles maximum sBTC supply).

Assuming a conservative market cap to TVL ratio of 5 yields estimates of fair value shown in Table 3, vs. the closing price on June 29th 2023 of 0.68.

Table 3 - Market capitalisation to TVL approach

% of BTC deployed	Stack TVL (USD)	STX maket cap (USD)	STX price (USD/cir. token)
0.1%	584,187,697	2,920,938,485	2.10
1.0%	5,841,876,970	29,209,384,848	21.03
2.0%	11,683,753,939	58,418,769,696	42.05
5.0%	29,209,384,848	146,046,924,240	105.13
10.0%	58,418,769,696	292,093,848,481	210.27

Source: CoinGecko data, Soberin Research calculations.

There is already evidence that the Stacks ecosystem is growing steadily. Compared to the year prior, the average number of transactions per day on the Stacks network over the first quarter of 2023 grew 70.80% from 6,269 to 10,707, with monthly highs of 13,342 and 26,368, respectively. Moreover, the utilisation of smart contracts has accelerated, with over 40,000 deployed through 1Q23, vs. the 20,755 deployed since the launch of the Stacks blockchain. By way of comparison, as of June 29th 2023, there were roughly 61.8mn smart contracts on Ethereum, suggesting ample room for growth. The impending upgrades to Stack should see its usage grow further as adopters seek STX to pay for transactions and to mint sBTC.

Stacks adoption – and demand for STX – would be aided by dApp developers wishing to benefit from the combination of Bitcoin finality and smart contract functionality Stacks offers. With respect to the valuation approach above, the existence of popular DeFi protocols would facilitate the growth of TVL on Stacks. While there are presently only 32 Stacks dapps, amongst them are notable DeFI projects such as ALEX, Arkadiko Finance and StackSwap. Each stands to benefit from the introduction of sBTC, where the protocols would not only have Bitcoin finality, but also access to BTC capital. Their growth would in turn, spur other developers to turn their attention to Stacks and boost the TVL underpinning STX valuation.

Risks

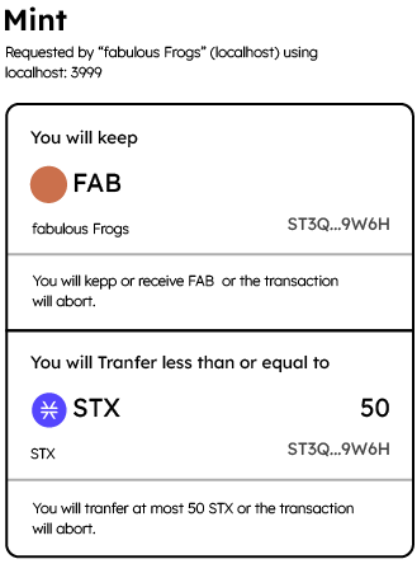
It may be said that Stacks faces *competition risk* from alternative projects seeking to expand the functionality of Bitcoin, notably Ordinals and BRC-20 tokens. However, neither offers smart contract functionality, unlike Clarity-powered sBTC. Moreover, BRC-20 tokens do not accommodate on-chain settlement (i.e., one's 'balance' is simply an inscription that requires an ordinal wallet to read, not an irrefutable unit of currency). This would suggest

that despite their recent popularity, the BRC-20 standard will likelier become a progenitor of meme coins than a long-term competitor to sBTC and Stacks.

Regulatory risk would typically be an important consideration for any blockchain platform with a centralised headquarter, more so for US-incorporated businesses, where more stringent regulations have been introduced following the FTX debacle. However, Stacks has a long-standing working relationship with the SEC, which somewhat mitigates this risk.

More relevant here would be the *technological risk*, which is a primary concern for any blockchain operator. To introduce smart contract functionality for Bitcoin, Stacks adds a blockchain layer which malicious actors could exploit. However, as all transactions on the Stacks layer are automatically hashed and settled on the Bitcoin L1, Stacks blocks are secured by 100% Bitcoin hashpower. In order to re-order Stacks blocks/transactions, an attacker would have to reorg Bitcoin. Moreover, Clarity, the smart contract language for Stacks, has been designed to avoid many vulnerabilities that Solidity has. Offering further protection are *post conditions*. Post conditions are conditions specified on the client side to ensure a transaction does not result in unexpected actions. For example, Figure 6 shows a transaction with the post condition that one side would transfer at most STX50 or the transaction would abort. Notably, post conditions do not live in smart contracts, but are built into the Stacks blockchain and enforced at the protocol level, designed to provide an extra layer of security.

Figuer 6 - Post conditions for extra security



Source: *Post Conditions*. Stacks Academy. https://docs.stacks.co/docs/stacks-academy/post-conditions

For the informed reader, a less obvious, but no less important element of technology risk may be whether Clarity, in its security-minded design, would have limited applicability due to its being a Turing-incomplete language. Its Turing incompleteness means that popular

functions such as loops, recursions could not be written with Clarity, for example. On this matter, a paper by the University of Applied Sciences Ruhr West in Germany analysed 53,757 smart contracts and found that only 35.3% used "for-loops and primitive recursive functions". Moreover, as noted by the authors, many of these functions do not require Turing completeness, and in fact, only 6.9% of the smart contracts analysed required it. This suggests Turing completeness would not materially hinder the adoption of Clarity. Furthermore, the introduction of subnets means that protocols requiring Turing completeness could still be supported by Stacks through subnets built on Turing complete languages (e.g., Solidity).

The last, and arguably most formidable risk is *economic risk*. The liveness ratio specifies a maximum amount of sBTC such that the value of circulating sBTC to the value of locked STX does not exceed the liveness ratio. Given the liveness ratio ( ), the following condition could be derived:

$$\frac{\partial sBTC}{\partial p_{STX}} = \frac{\propto_{LIV}}{p_{sBTC}}\left(STX_{locked} + p_{STX} * \frac{\partial STX_{locked}}{\partial p_{STX}}\right)$$

The above condition shows that as the amount of STX locked up increases, even if the price of STX does not affect how much STX is locked up (i.e., speculative trading is minimal) the effect on sBTC supply from a drop in STX price would be *larger* than when less STX is locked up. This is because when more STX is locked up, even a tiny change in STX price could have a big effect on market cap. A consequence of this is that *the more sBTC is issued, the more sensitive its supply would be to changes in STX price*. While the value of sBTC should be well-supported by the 1:1 BTC collateralisation, this dynamic does mean an ecosystem built around sBTC could have some unexpected vulnerabilities. Given that the Nakamoto Release is slated for 4Q23 however, there remains time for the Stacks community to capably address this issue.

A note on Bitcoin Maximalism

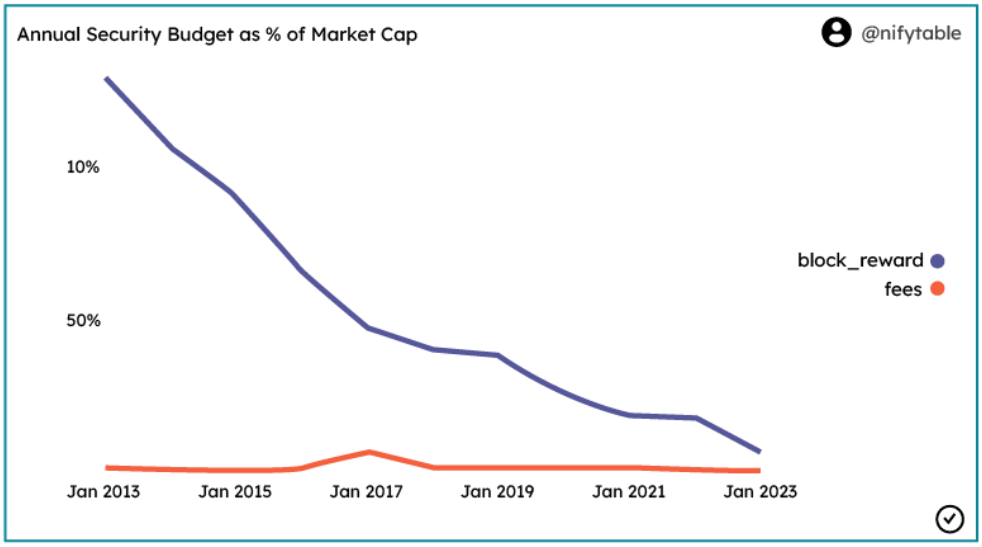
Bitcoin Maximalism could be viewed as a threat specific to Stacks. Coined by Vitalik Buterin in 2014, Bitcoin maximalism is "the idea that an environment of multiple competing cryptocurrencies is undesirable", due in part, to the notion that competing currencies would dilute the network effect around Bitcoin. It has been noted by industry observers that the term has expanded to encompass a fervent and uncompromising advocacy for Bitcoin, e.g., that investing in other cryptocurrencies should be discouraged as a form of consumer protection. Three factors indicate however, that a widespread pushback is unlikely.

Firstly, Bitcoin Maximalism has fallen out of vogue, with reputable industry voices warning against it as at best, counterproductive to innovation and ignoring Bitcoin's limited utility for applications, and at worst, toxic to the point of discouraging crypto adoption. Secondly, Stacks ultimately settles transactions on Bitcoin. As such, it largely preserves the security of Bitcoin. Thirdly, and most importantly, *the Stacks ecosystem increases transaction fees for*

Bitcoin miners. Through PoX STX mining, sBTC transactions, as well as the dApps Stacks enables, the Stacks ecosystem increases the *number on transactions* settling on the Bitcoin blockchain and increases demand for Bitcoin block space – thus *fees* –over a given period.

On the last point, *Stacks's effect on Bitcoin transaction fees may prove to be more than a desirable feature, but an increasingly crucial mean to safeguard Bitcoin's future*. The security budget of Bitcoin – the amount earned by miners comprising of block rewards and transaction fees – has been steadily decreasing over the past decade. This is due to decreases in block rewards from halving events, which occur every 210,000 blocks or roughly four years. Falling block rewards and increasing BTC price have resulted in a steep decline of the ratio of annual security budget as a percentage of market cap, e.g., from 13.2% as of 1st January 2013 to 0.6% on 1st January 2023. Moreover, as can be seen from Figure 7, block rewards continue to constitute the lion's share of the security budget. Through increasing transactions fees on Bitcoin, Stacks creates an avenue through which the security budget could be maintained as block rewards fall further until they eventually reach zero.

Figuer 7 - Block rewards make up the lion's share of a falling security budget



Source: *Bitcoin Security Budget*. Dune Analytics dashboard by @niftytable.
https://dune.com/niftytable/bitcoin-security-budget

The fact that Bitcoin does not presently lend itself well to DeFi also allows greater market fragmentation to persist – that different liquidity pools cannot draw from one another, resulting in distinct BTC prices across them as each pool operator (i.e., exchange) determines BTC price from its order book. The introduction of smart contracts-enabled sBTC could bridge BTC liquidity pools through DEXs and DEX aggregators.

Conclusion

The upcoming Nakamoto Release and introduction of sBTC will allow the Stacks ecosystem to expand the utility of Bitcoin with greater scalability while better preserving Bitcoin's security features, aiding both the adoption and long-term security of the oldest surviving cryptocurrency. Stacks transactions will have Bitcoin finality and share the latter's security budget, while the introduction of fast blocks will make the network more scalable. Through sBTC, Stacks smart contracts will be able to write to Bitcoin, while PoX and Clarity allow Stacks to read from Bitcoin at any time. Together, the read and write capabilities will facilitate applications such as atomic BTC swaps and asset-backed borrowing/lending, unlocking the huge potential of BTC-denominated capital. Finally, the Clarity language used by Stacks arguably represents a safer, yet practical, alternative to Solidity.

Ratio analysis referencing Ethereum layer-2 projects suggests that *assuming Stacks succeeds in unlocking even 2% of BTC-denominated capital – the STX token remains undervalued*.

Appendix

Bytecode – Computer code an interpreter converts into binary machine code that could be read by a computer's hardware processor.

Hash – A mathematical function which converts an input of arbitrary length (letters, numbers) into a fixed-length encrypted output. Regardless of the original amount of the data, the unique hash will be the same size. Hashes cannot be reversed engineered to get the input, but their unique mappings from inputs mean one can validate a set of data is the same as another from its unique hash.

Layer 0/1/2 – Different layers refer to a blockchain's place in the overall data management architecture. Most discussions revolve around layer-1 and layer-2 blockchains. Layer 1 is the underlying blockchain that facilitates data transactions to begin with, and necessarily includes its own consensus mechanism, miners/block producers and network of node operators. Layer-2 solutions may also have some or all these features (e.g., Stacks with its PoX), but being built upon a pre-existing blockchain makes a blockchain a layer-2 solution. Layer 0 refers to the network framework running beneath the blockchain, including the protocols (sets of rules through which nodes can communicate) upon which a blockchain can be built[1].

Opcode – In programming, opcode or operation code is the instruction of operations to be performed by the system.

[1] https://coinmarketcap.com/alexandria/glossary/layer-0; https://coinmarketcap.com/alexandria/glossary/layer-1-blockchain; https://ethereum.org/en/layer-2/

Appendix II

Table AII - L1 to L2 market capitalisations

Platform	Token	Max market cap ratio	Max market cap ratio	Average market ratio	As of29th June 2023
Ethereum	ETH	100.00%	100.00%	100.00%	100.00%
Arbitrum	ARB	0.85%	0.60%	0.70%	0.65%
Polygon	MATIC	6.75%	0.04%	1.89%	2.61%
Optimism	OP	0.43%	0.07%	0.20%	0.36%

Source: CoinGecko data. https://www.coingecko.com

Appendix III

Bitcoin Name System (BNS)

BNS names benefit from three properties: 1) *global uniqueness*, 2) being *human-readable* and 3) having *strong ownership*. Readability comes from names being chosen by their creators, vs. long-form Bitcoin addresses. Property 1) stems from the fact that all well-behaved nodes on a blockchain resolve to the same state (i.e., BNS name), while 3) comes from the fact that a name is tied to an owner's private key.

Specifically, there are three layers in the BNS naming hierarchy. Namespaces (e.g., .btc, .id) and BNS names are stored directly on the blockchain (e.g., muneed.id). The creation of namespaces is on a first-come, first-serve basis, but requires burning BTC to do so, to discourage ID squatters. Moreover, the shorter the namespace, the more BTC needs to be burned. Once a namespace has been created, anyone can create a BNS name linked to it, via a transaction on the Stacks blockchain.

On the contrary, to facilitate faster registration and lower cost, information on BNS subdomains (e.g., intern.soberin.id) are first stored off-chain, with their creation broadcasted to the network in batches by BNS name owners.

Current Stacks platform:

As outlined in its 2017 white paper, Blockstack had three components: 1) a layer-1 blockchain (*virtualchain*), 2) a peer network providing a global index for data discovery (*Atlas*) and 3) a decentralised storage system (*Gaia*). The white paper also discussed a blockchain-based naming system (*BNS*), while seeking to raise money through the sale of a Stacks token (*STX*).

The current Stacks mainnet resulted from a hard fork from the Stacks 1.0 blockchain on January 14th 2021 to introduce PoX and native STX mining – hence the 2.0 moniker. The new Stacks platform will comprise of a Stacks blockchain with 100% Bitcoin finality, a PoX consensus mechanism facilitating this, the sBTC token, the STX native token, as well as EVM-compatible subnets.

Liveness ratio

The liveness ratio is the ratio of the value of circulating sBTC to the value of STX locked in the PoX mechanism, stipulated as a maximum value to limit the circulating supply of sBTC to ensure stackers are sufficiently incentivised to maintain the protocol. E.g., a liveness ratio of 60% (the default value) means that with USD100mn of STX locked, sBTC in circulation must be USD60mn or lower. Should the sBTC/STX ratio exceed the liveness ratio, peg-ins are temporarily disabled until enough peg-outs occur and/or the ratio limit is raised through on-chain voting. Note that the economic security around the peg *decreases* as the liveness ratio *increases*. Also, if STX falls in value against BTC, the permitted sBTC supply also falls. Given the liveness ratio ($\propto_{LIV}$):

$$\propto_{LIV} \equiv \frac{sBTC\ circulating\ value}{STX\ locked\ market\ cap} \geq \frac{actual\ sBTC\ circulating\ value}{STX\ locked\ market\ cap} = \frac{sBTC * p_{sBTC}}{STX_{locked} * p_{STX}}$$

$$SBTC = \frac{\propto_{LIV} * STX_{locked} * p_{STX}}{p_{sBTC}}$$

$$\frac{\partial sBTC}{\partial p_{STX}} = \frac{\propto_{LIV}}{p_{sBTC}} \left(STX_{locked} + p_{STX} * \frac{\partial STX_{locked}}{\partial p_{STX}} \right)$$

Ordinals

The concept of ordinals was spearheaded by Bitcoin core developer Casey Rodarmor, who released an open-source software called Ord in December 2022 enabling the creation and transfer of ordinals, with version 4.0 launching on Bitcoin mainnet on January 21st 2023.

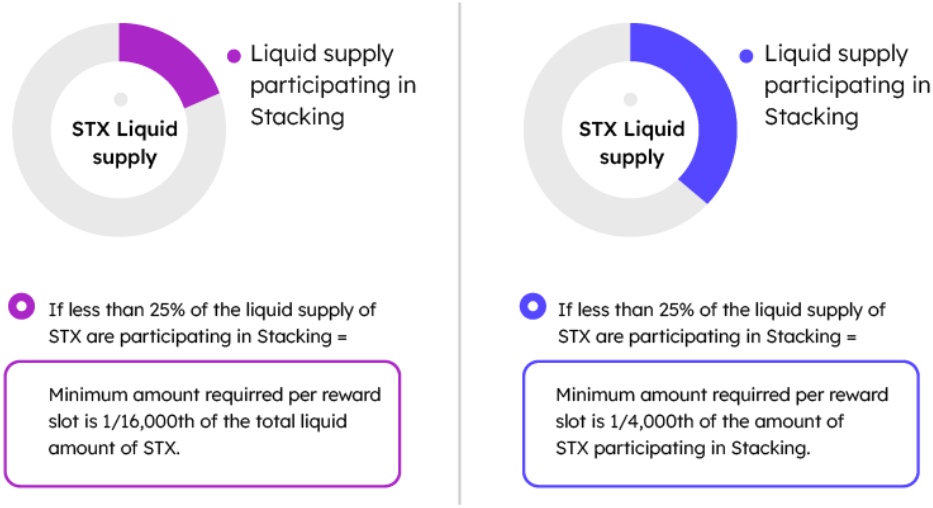
Ord draws from *ordinal theory* – that with a fixed supply of BTC21mn and each BTC containing 100 million satoshis (sats), if there were agreement on the how to *order* all the sats within each BTC, each and every sat could be uniquely numbered and ordered. Ord allows digital *inscriptions* to be made on each such unique sat.

Ord capitalises upon Bitcoin's UTXO accounting model, where every transaction is a set of outputs and inputs (BTC received and sent) and the SegWit and Taproot upgrades to Bitcoin, which together allows for greater flexibility in constructing the 'keys' transactions need to unlock the output received (i.e., so the BTC could be spent). Through including arbitrary data (e.g., an image) in the creation of these keys, one could embed the data onto the Bitcoin blockchain. Notably, through inclusion of the OP_FALSE opcode, the data in the key is not executed.

Proof-of-Transfer (PoX)

The probability of a miner being elected to process a block follows a weighted random function – one's chance of winning is proportional to the amount of BTC transferred vs. that from other miners. On the stacker side, a stacker could stack independently or through pooling with other stackers through a delegation process, whereby stackers receive their STX holdings back after the committed number of cycles has elapsed. Stacker eligibility is determined dynamically, as outlined in Figure 2 below. Notably, as more than 25% of STX in circulation is stacked, the criterion changes from a 1/16,000 share of circulating STX to a 1/4,000 share of stacked STX, which maintains the difficulty level at the threshold limit, while ensuring no more than 4,000 reward slots – the maximum supported by the Stacks blockchain – could be occupied.

Figure AIII: The criteria for stacking



Settlement of Stacks on Bitcoin

As part of PoX mining, a hash (i.e., a math function that encrypts information) of each Stacks block is recorded to the OP_RETURN opcode of Bitcoin – an operational code on Bitcoin which allows up to 40 bytes of arbitrary data to be stored in each Bitcoin transaction. This allows Stacks to record its history to the Bitcoin chain and inherit some of the latter's security – e.g., if one wanted to change the history of the Stacks chain, one would have to modify the OP_RETURN values in each corresponding Bitcoin block, which requires falsifying history on Bitcoin.

Additionally, when PoX is executed, Stack's smart contract language Clarity allows the hash of the Bitcoin header each Stack block is anchored with to be read. Specifically, there is a built-in function ('get-block-info') which returns amongst other information, 'burnchain-header-hash'. Through this feature, Clarity contracts could trigger certain things to occur on Stacks given what occurs on Bitcoin. In turn, through sBTC's peg-out mechanism – which

converts sBTC to BTC – Clarity smart contract could trigger BTC transactions given Bitcoin state.

References[2]

21Shares (2023) *Fundamentals: Bitcoin Key Metrics*. Dune dashboard. Available at: https://dune.com/21shares_research/bitcoin-key-metrics

Ali, M. (2020) *Final Stacks 1.0 Hardfork Successful, Preview Stacks 2.0* Available at: https://blog.blockstack.org/final-stacks-1-0-hardfork-successful-preview-stacks-2-0

Ali, M. (2023) *Is Stacks a Bitcoin L2?* Forum post. Available at: https://github.com/stacks-network/stacks/blob/master/stacks-l2.md

Ali, M. (2021) *Stacks Cryptocurrency No Longer Treated as a US Security by Blockstack PBC*. Available at: https://blog.blockstack.org/stacks-cryptocurrency-securities-filing

Barnette, J. (2021) *FAQ: Delaware Public Benefit Corporations*. Available at: https://www.cooleygo.com/faq-delaware-public-benefit-corporations/

BBC (2023) *Assembly language*. Available at: https://www.bbc.co.uk/bitesize/guides/zbk8jty/revision/2

Benson, J. (2020) *Stacks Foundation Funds Blockstack's Blockchain Expansion*. Available at: https://decrypt.co/40826/stacks-foundation-funds-blockstacks-blockchain-expansion

BitDegree (2023) *What is Liveness?* Available at: https://www.bitdegree.org/crypto/learn/crypto-terms/what-is-liveness#:~:text=In%20blockchain%2Dbased%20distributed%20systems,consensus%20regarding%20the%20block%20value

Blankstein, A. (2019) *Introducing Clarity, a language for predictable smart contracts*. Available at: https://blog.blockstack.org/introducing-clarity-the-language-for-predictable-smart-contracts

Blockstack (2017) *Blockstack Technical Whitepaper*. Available at: https://pdos.csail.mit.edu/6.824/papers/blockstack-2017.pdf

Blockstack (2019) *Stacks Token Economics Whitepaper v 2.0*. Available at: https://uploads-ssl.webflow.com/5e7b1a27d160ce49af1c24e1/5f1596b2f7b9a32ffb25797c_tokenpaper.pdf

Btc.us (2023) Business website. Available at: https://btc.us

[2] Unless otherwise stated, references last accessed May 4th 2023.

Buterin, V. (2014) *On Bitcoin Maximalism, and Currency and Platform Network Effects*. Available at: https://blog.ethereum.org/2014/11/20/bitcoin-maximalism-currency-platform-network-effects

Buterin, V. (2022) Twitter post. Available at: https://twitter.com/VitalikButerin/status/1551603545752870912

Calabro, N (2023) *How Ordinals Are Changing Bitcoin & Web3 Startups*. Available at: https://stacks.org/ordinals-bitcoin-startups

Chainlink (2022) *Reentrancy Attacks and The DAO Hack*. Available at: https://blog.chain.link/reentrancy-attacks-and-the-dao-hack/#:~:text=The%20hacker%20deploys%20a%20smart,sends%20ETH%20to%20the%20hacker

CoinGecko (2023) *Stacks*. Available at: https://www.coingecko.com/en/coins/stacks/historical_data#panel

CoinGecko (2023) *Total Crypto Market Cap Chart*. Available at: https://www.coingecko.com/en/global-charts#:~:text=The%20global%20cryptocurrency%20market%20cap,a%20Bitcoin%20dominance%20of%2044.55%25

CoinMarketCap (2023) *Layer 0*. Available at: https://coinmarketcap.com/alexandria/glossary/layer-0

CoinMarketCap (2023) *Layer-1 Blockchain*. Available at: https://coinmarketcap.com/alexandria/glossary/layer-1-blockchain

Conway, L. (2023) *What Is Bitcoin Having? Definition, How It Works, Why It Matters*. Available at: https://www.investopedia.com/bitcoin-halving-4843769

Cristiano (2021) *It's Time to Stack(s) Bitcoin Up*. Available at: https://messari.io/report/it-s-time-to-stack-s-bitcoin-up

Crunchbase (2023) *Stacks Financials*. Available at: https://www.crunchbase.com/organization/stacks/company_financials

Deeplake (2023) *Bitcoin DeFi*. Available at: https://deeplake.finance

DefiLlama (2023) *Bitcoin TVL*. Available at: https://defillama.com/chain/Bitcoin?tvl=true

DefiLlama (2023) Lido. Available at: https://defillama.com/protocol/lido

Delaware Code Online (2023) *Subchapter XV. Public Benefit Corporations*. Available at: https://delcode.delaware.gov/title8/c001/sc15/

Dgtl_assets (2023) *Bitcoin Ordinals Analysis*. Dune dashboard. Available at: https://dune.com/dgtl_assets/bitcoin-ordinals-analysis

Domo (2023) *brc-20 experiment*. https://domo-2.gitbook.io/brc-20-experiment/

Donnelly, J. (2016) *What is the 'Halving'? A Primer to Bitcoin's Big Mining Change*. Available at: https://www.coindesk.com/markets/2016/06/12/what-is-the-halving-a-primer-to-bitcoins-big-mining-change/

Dylan-Ennis, P. J. (2022) *The Rise and Fall of Bitcoin Culture*. Available at: https://www.coindesk.com/layer2/2022/10/11/the-rise-and-fall-of-bitcoin-maximalism/

Ethereum (2023) *Find a wallet*. Available at: https://ethereum.org/en/wallets/find-wallet/

Ethereum (2023) *Layer 2*. Available at: https://ethereum.org/en/layer-2/

Frankenfield, J. (2023) *What Is a Hash? Hash Functions and Cryptocurrency Mining*. Available at: https://www.investopedia.com/terms/h/hash.asp

Goswami, R. (2023) *SEC proposes rules that would change which crypto firms can custody customer assets*. Available at: https://www.cnbc.com/2023/02/15/sec-chair-gensler-crypto-firms-need-to-register-to-custody-assets.html

Gupta, D. (2023) *What Are Bitcoin Ordinals?* Available at: https://www.hiro.so/blog/what-are-bitcoin-ordinals

Hackernoon (2019) *Should Smart Contracts be Non-Turing Complete?* Available at: https://hackernoon.com/should-smart-contracts-be-non-turing-complete-fe304203a49e

Hendrickson, M. (2023) *Ordinals Are Now Supported by Hiro Wallet*. Available at: https://www.hiro.so/blog/ordinals-inscriptions-hiro-wallet

Hildobby (2023) *Ethereum – The Overview*. Dune Dashboard. Available at: https://dune.com/hildobby/ethereum

Hiro (2023) *About*. Available at: https://www.hiro.so/about

Hiro (2023) *Introducing the Ordinals Explorer and Ordinals API*. Available at: https://www.hiro.so/blog/introducing-the-ordinals-explorer-and-ordinals-api

Hiro Systems PBC (2021) Form 1-U for SEC filing. Available at: https://www.sec.gov/Archives/edgar/data/1693656/000119312521012574/d111554d1u.htm

Hladek, N. (2022) *How many NFTs are actually on the blockchain*? Available at: https://www.rightclicksave.com/article/how-many-nfts-are-actually-on-the-blockchain

Hyatt, J. (2021) *Decoding Crypto: What Was the First Cryptocurrency and Who Created It?* Available at: https://www.nasdaq.com/articles/decoding-crypto%3A-what-was-the-first-cryptocurrency-and-who-created-it-2021-08-18

Hooper, A. (2023) *DeFi's Next Big Thing: Liquid Staking Derivatives*. Available at: https://cointelegraph.com/news/defis-next-big-thing-liquid-staking-derivatives

Jansen, M., Hdhili, F., Gouiaa, R. and Z. Qasem (2019) 'Do Smart Contracts Languages Need to be Turing Complete?', *International Congress on Blockchain and Applications*. Conference Paper March 2019. Available at: https://www.researchgate.net/publication/332072371_Do_Smart_Contract_Languages_Need_to_be_Turing_Complete

Jeon, Y., Samarbakhsh, L. and K. Hewitt (2021) 'Fragmentation in the Bitcoin market: Evidence from multiple coexisting order books', *Finance Research Letters*, Volume 39, March 2021. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1544612320301136

Jha, P. (2023) *Bitcoin BRC-20 token standard becomes new destination for meme tokens*. Available at: https://cointelegraph.com/news/bitcoin-brc-20-token-standard-becomes-a-new-destination-for-meme-tokens

Kimmell, M. (2020) *Blockstack*. Available at: https://www.coindesk.com/company/blockstack/

Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at: https://bitcoin.org/bitcoin.pdf

Nelson, J. (2018) *The Launch of the Stacks Genesis Block*. Available at: https://blog.blockstack.org/the-launch-of-the-stacks-genesis-block

Nibley, B (2022) *What Bitcoin Market Fragmentation Means for Its Future*. Available at: https://blockworks.co/news/what-global-bitcoin-market-fragmentation-means-for-its-future

Niftytable (2023) *Bitcoin Security Budget*. Dune dashboard. Available at: https://dune.com/niftytable/bitcoin-security-budget

Owie, B. (2023) *Arbitrum, Optimism, And Polygon: Which Is The Ultimate Ethereum L2?* Available at: https://www.newsbtc.com/news/ethereum/arbitrum-optimism-and-polygon-which-is-the-ultimate-ethereum-l2/

Rice, J. (2023) *Bitcoin And Ethereum Maximalism: Silly And Self-Defeating*. Available at: https://blockworks.co/news/bitcoin-ethereum-toxic-maximalism

Rieff, N. (2022) *What Was the First Cryptocurrency?* Available at: https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/

Sharma, R. (2021) *Bitgold: Meaning, Overview, Differences From Bitcoin*. Available at: https://www.investopedia.com/terms/b/bit-gold.asp

Sheldon, R. (2023) *What is bytecode?* Available at: https://www.techtarget.com/whatis/definition/bytecode#:~:text=Bytecode%20is%20computer%20object%20code,bytecode%20for%20the%20target%20platform

Shimron, L (2023) *NFTs Are Bloating Bitcoin, Creating Risks And Opportunities For Investors*. Available at: https://www.forbes.com/sites/leeorshimron/2023/02/11/nfts-are-bloating-bitcoin-creating-risks-and-opportunities-for-crypto-investors/?sh=1630b0eb7d77

Stacks (2023) *Bitcoin Name System*. Available at: https://docs.stacks.co/docs/stacks-academy/bns

Stacks (2023) *Clarity Overview*. Available at: https://docs.stacks.co/docs/clarity/

Stacks (2023) *FAQ: Stacks Rebrand*. Forum post. Available at: https://forum.stacks.org/t/faq-stacks-rebrand/11274

Stacks (2023) *Get STX*. Available at: https://www.stacks.co/explore/get-stx#:~:text=STX%20is%20the%20native%20cryptocurrency,to%20earn%20bitcoin%20by%20Stacking

Stacks (2023) *Microblocks*. Available at: https://docs.stacks.co/docs/stacks-academy/microblocks

Stacks (2023) *Mining*. Available at: https://docs.stacks.co/docs/stacks-academy/mining

Stacks (2023) *Post Conditions*. Available at: https://docs.stacks.co/docs/stacks-academy/post-conditions

Stacks (2023) *Proof of Transfer*. Available at: https://docs.stacks.co/docs/stacks-academy/proof-of-transfer

Stacks (2023) *Stacking*. Available at: https://docs.stacks.co/docs/stacks-academy/stacking

Stacks (2023) *Stacks Roadmap*. Available at: https://www.stacks.co/roadmap

Stacks (2023) *Transactions*. Available at: https://docs.stacks.co/docs/stacks-academy/transactions

StacksData (2023) *Contracts*. On-chain data dashboard. Available at: https://stacksdata.info/#contracts

Stacks on Chain (2023) *Transactions per Day*. On-chain dashboard. Available at: https://stacksonchain.com/dashboards/Transactions%20per%20Day/14

Stacks Open Internet Foundation (2022) *Growing the Bitcoin Economy with Bitcoin Layers*: Available at: https://stacks.org/sbtc-nakamoto

Stacks Open Internet Foundation (2021) *Mainnet is Live! What Stacks 2.0 Means for You*. Available at: https://stacks.org/stacks2mainnet

Stacks Open Internet Foundation (2022) *sBTC: Design of a Trustless Two-way Peg for Bitcoin*. Available at: https://stx.is/sbtc-pdf

Stacks Open Internet Foundation (2022) *Stacks: A Bitcoin Layer for Smart Contracts*. Available at: https://stx.is/nakamoto

Thomson Reuters (2023) *Regulation S*. Available at: https://uk.practicallaw.thomsonreuters.com/3-382-3748?transitionType=Default&contextData=(sc.Default)&firstPage=true

Vigna, P. (2019) 'SEC Clears Blockstack to Hold First Regulated Token Offering', *The Wall Street Journal*. Available at: https://www.wsj.com/articles/sec-clears-blockstack-to-hold-first-regulated-token-offering-11562794848

Voight, S. (2021) *Stacks 2.0 Launch Recap*. Available at: https://www.stacks.co/blog/stacks-2-0-launch-recap

Wired (2021) *'Snow Crash' Is a Cyberpunk Classic*' Available at: https://www.wired.com/2021/10/geeks-guide-snow-crash/

YourNfts (2022) Website landing page. Available at: https://yournfts.org/#stats


www.soberin.com


research@soberin.com

IMPRINT

This document is not an investment advice and was not produced in accordance with any legal requirements regarding investment advice or financial or investment research. The document was created on 21st July 2023 by Soberin Research which is currently not licensed or regulated in any jurisdictions.

This document is not intended for distribution or use by any person or entity in any jurisdiction or country where such distribution or use would be in violation of relevant laws and regulations.

IMPORTANT LEGAL INFORMATION

The information and opinions expressed in this document were produced as at the date of writing and are subject to change without notice. This document is intended for information purposes only and does not constitute advice, an offer or an invitation by, or on behalf of, Soberin Research to buy or sell, participate in any particular trading strategy or take any action in regard to any cryptocurrencies, digital assets, cryptocurrencies/digital asset-based derivatives, securities, financial instruments, financial products or other products or services ("**Products/Services**") in any jurisdiction. The authors' opinions and comments in this document represent their own current views, which may not necessarily align with those of Soberin Research. Soberin Research may have issued or may issue in the future other documents that differ from the information presented here and reach different conclusions. Soberin Research is not obligated to bring such documents to the attention of the recipient or reader of this document. We make no commitment to update or revise the information in this document. Although the data in this document is sourced from reliable sources, no specific representation is made regarding its reliability, accuracy, or completeness. It is important to note that this document may not cover all essential information about any Products/Services.

Soberin Research cannot guarantee the accuracy, completeness, timeliness or availability of any information included in this document and is not responsible for any errors or omissions, whether negligent or otherwise, nor for the results obtained from using such content. Soberin Research does not provide any express or implied warranties, including any warranties of merchantability or fitness for a particular purpose or use. Soberin Research shall not be liable for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees or losses, including lost income or profits and opportunity costs, resulting from the use of the content in this document in any way.

SUITABILITY

The Products/Services mentioned in this document may not be suitable for all recipients or readers and may not be legally available in all jurisdictions. Before engaging in any transaction, you should carefully consider the suitability of the transaction to your individual circumstances and objectives. Any investment or trading decision should only be made

after conducting your own research and thoroughly reviewing all relevant documents related to the Products/Services, including white papers, prospectuses, and other materials. Nothing in this document constitutes investment, legal, accounting or tax advice, or a representation that any investment or strategy is suitable or appropriate to individual circumstances, or otherwise constitutes a personal recommendation to any specific reader. Readers should consult with professional advisors to independently assess the specific financial risks and any other risks including legal, regulatory, credit, smart contract, on-chain data, tax, and accounting consequences. If another document is referenced in this document, readers should not read this document in isolation but should instead consult all referenced documents in their entirety.

GENERAL RISKS

The value and price of the Products/Services or any asset class mentioned in this document may fluctuate, and investors may lose their entire investment. Investing in the Products/Services or any asset class mentioned in this document may involve various risks, such as market risks, credit risks, counterparty risks, IT and cybersecurity risks, smart contract risks, on-chain data risks, legal risks, regulatory risks, currency risks, political risks, and economic risks. It is important to note that investing in the crypto market can be highly speculative and volatile compared to other markets. Any past or forecasted performance figures or simulations presented in this document are not a reliable indication of future results. There are several factors that can cause returns to increase or decrease. It is important to carefully consider individual circumstances, risk tolerance, investment needs and objectives before making any investment decisions.

THIRD PARTY INFORMATION

This document may include information obtained from third parties, such as ratings from rating agencies and research from research providers. Some issuers of Products/Services mentioned or included in any documents may be a client of or related to Soberin Research or an affiliated client in any way. Reproducing or distributing third-party content in any form is prohibited without prior written permission from the related third party. Third-party content providers provide no guarantee for the accuracy, completeness, timeliness, or availability of their information, including ratings or research. They provide no express or implied warranties, and shall not be liable for any damages, costs, or losses, including lost income or profits, resulting from the use of their content, including ratings or research. Credit and/or research ratings represent opinions and not factual statements or recommendations to buy, hold or sell any Products/Services. They do not address the market value of any Products/Services or their suitability for investment purposes and should not be relied upon as investment advice.

IMPORTANT DISTRIBUTION INFORMATION

The contents of this document, including any market-related information, are exclusively intended for the personal use of the intended recipient and must not be disseminated to

any third party, unless authorized by Soberin Research or the source of the relevant market data. Soberin Research is not licensed or regulated in any jurisdiction. This document has not been reviewed or endorsed by any regulator in any jurisdiction. This document may not be appropriate for all readers, and it is the recipient's responsibility to ensure compliance with all applicable laws and regulations.

It is crucial to acknowledge that this document is not targeted to or intended for distribution or use by individuals or entities in any jurisdiction where it is unlawful to do so based on their nationality, place of residence, or any other factors.

The information contained in this document is for informational purposes only and should not be considered as investment advice or an offer or solicitation to buy or sell any Products/Services or relied upon by any person. The distribution of this document on social media or elsewhere does not imply any endorsement or recommendation by the author, publisher, or Soberin Research. The recipient of this document should undertake their own independent analysis and should consult with their own advisor before making any decisions. The author, publisher, and Soberin Research are not responsible for any losses incurred by the recipient as a result of relying on the information contained in this document.

This material has not been prepared in accordance with the laws and regulations governing financial research or investment research in any jurisdiction and may not be distributed to or relied upon by any person in any jurisdiction where the distribution would be illegal.