Blockstack

Proof of Transfer Whitepaper v1.0

May 2020

By Blockstack PBC

PoX: Proof of Transfer Mining with Bitcoin

Muneeb Ali Aaron Blankstein Michael J. Freedman[*]
Ludovic Galabru Diwaker Gupta Jude Nelson
Jesse Soslow Patrick Stanley

Blockstack PBC
https://blockstack.org

May 11, 2020

Abstract

Consensus algorithms for public blockchains require computing or financial resources to secure the blockchain state. Mining mechanisms used by these algorithms are broadly divided into proof-of-work, in which nodes dedicate computing resources, and proof-of-stake, in which nodes dedicate financial resources to participate in the consensus algorithm. The high-level idea behind both proof-of-work and proof-of-stake is to make it practically infeasible for any single malicious actor to have enough computing power or ownership stake to attack the network. A variant of proof-of-work is proof-of-burn where miners compete by "burning" (destroying) a proof-of-work cryptocurrency as a proxy for computing resources.

In this paper, we introduce a new mining mechanism, called proof-of-transfer (PoX) that generalizes the concept of proof-of-burn. PoX uses the proof-of-work cryptocurrency of an established blockchain to secure a new blockchain. However, unlike proof-of-burn rather than burning the cryptocurrency, miners transfer the committed cryptocurrency to some other participant(s) in the network. This allows network participants who are adding value to the new cryptocurrency network to earn a reward in a base cryptocurrency by actively participating in the consensus algorithm.

PoX encourages a model where there is one extremely secure proof-of-work blockchain, say Bitcoin. Other new blockchains can be anchored on the secure proof-of-work blockchain instead of introducing new proof-of-work chains. PoX has the interesting property where participants can earn payouts in a separate, potentially more stable, base cryptocurrency while participating in the new blockchain network. This can help solve a bootstrapping problem for new blockchains by providing incentives for early participants. Further, PoX has a potential use case for funding ecosystem developer funds. We present a proposal for using PoX in the Stacks 2.0 blockchain.

[*] Professor of Computer Science at Princeton University and technical advisor to Blockstack PBC.

1 Introduction

Blockstack is an open-source effort to develop software that provides an alternative to traditional (centralized) web applications. We believe that the next chapter for the web is the emergence of a user owned internet, built on top of public blockchains.

Consensus algorithms for public blockchains require computational or financial resources to secure the blockchain state. Mining mechanisms used by these algorithms are broadly divided into proof-of-work (PoW), in which nodes dedicate computational resources, and proof-of-stake (PoS), in which nodes dedicate financial resources. The intention behind both proof-of-work and proof-of-stake is to make it practically infeasible for any single malicious actor to have enough computational power or ownership stake to attack the network.

With proof-of-work, a miner does some "work" that consumes electricity and is rewarded with digital currency. The miner is, theoretically, converting electricity and computing power into the newly minted digital currency. Bitcoin is an example of this and is by far the largest and most secure PoW blockchain.

With proof-of-stake, miners are staking their holdings of a new digital currency to participate in the consensus algorithm and bad behavior can be penalized by "slashing" the funds of the miner. PoS requires less energy/electricity to be consumed and can give cryptocurrency holders who participate in staking a reward on their holdings in the base cryptocurrency. PoS may be less secure than PoW given (a) the trusted channel for new nodes problem [1], and (b) ability of an attacker to create many "fake" histories of the blockchain with minimal cost [2].

By far, the most secure blockchain today is Bitcoin. Blockstack has, since its earliest days, relied on Bitcoin as a mechanism for establishing trust in an open and permissionless network: the Stacks 1.0 blockchain, launched in 2018, operates as a "virtual blockchain" on top of Bitcoin [3]. We continue to believe that Bitcoin can become the "flag of technology" [4], and that most people will be introduced to cryptocurrencies through Bitcoin. The developer ecosystem around Bitcoin continues to grow.

However, adding new features to the Bitcoin blockchain poses a challenge: Bitcoin is secure because it is stable and does not change. While it possesses a scripting language, this language is extremely limited. This is by design— adding complexity increases the attack surface, which reduces the value of Bitcoin as a foundational layer.

Despite this, a user owned internet requires a more complex feature set. The blockchain that powers this next chapter of the web must be designed for this task– it should support the creation of new kinds of digital goods, the management of new kinds of decentralized applications, and be flexible enough to allow developers to build applications that we cannot yet imagine. The Stacks blockchain is an attempt to create this blockchain, and over its lifetime, we have explored the design space for establishing novel, feature-rich blockchains on top of Bitcoin, using it as a trusted foundation.

The Stacks 1.0 blockchain operates as a "virtual blockchain" on top of Bitcoin. Each transaction in the Stacks 1.0 chain *is also* a Bitcoin transaction. All of the data of a

Stacks transaction is encoded within the metadata of a Bitcoin transaction. This design is limited; Stacks transactions must share bandwidth with Bitcoin transactions. Stacks transactions must be separately validated by non-mining blockchain nodes, which do not receive mining rewards for validation.

In SIP-001, we proposed a proof-of-burn (PoB) mechanism for the design of the Stacks 2.0 chain [5]. With proof-of-burn, Stacks miners compete by destroying a cryptocurrency rather than consuming electricity. Proof-of-burn allows miners to participate without special-purpose hardware and provides more transparency for network participants than a normal proof-of-work blockchain. However, like a proof-of-work blockchain, proof-of-burn is destructive, requiring miners to destroy value in order to secure the blockchain.

However, PoB suffers from a potential bootstrapping problem. 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. Before the PoB chain matures, and the new cryptocurrency gains value and stability, miners may be unwilling to destroy Bitcoin in order to participate.

Proof-of-Transfer. In this paper, we introduce a new mining mechanism, called *proof-of-transfer* (PoX) that generalizes the concept of proof-of-burn (PoB). PoX uses the proof-of-work cryptocurrency of an established blockchain to secure a new blockchain. However, unlike PoB, rather than burning the cryptocurrency, miners *transfer* the committed cryptocurrency to some other participant in the network. This allows network participants, who are adding value to new cryptocurrency network, to earn rewards in a base cryptocurrency by actively participating in the consensus algorithm.

PoX can help to solve the bootstrapping problem for new blockchains: participants receive rewards in a separate, potentially more stable, base cryptocurrency. These rewards may be a better incentive for initial participation than rewards in the new cryptocurrency itself. Establishing this initial value for the new cryptocurrency can help improve miner interest, which in turn helps grow the new cryptocurrency ecosystem. By providing a base-cryptocurrency incentive for new-cryptocurrency participants, PoX escapes the spiral of dependent value that may threaten a new blockchain.

PoX can be used not only to incentivize participation from holders of a new cryptocurrency, but it may also be used for establishing developer funds. These developer funds may be funded over the lifetime of a new blockchain. Because the funds would be in a separate cryptocurrency, like Bitcoin, those funds could be used without impacting the value of the new cryptocurrency.

2 Proof-of-Transfer Design

PoX mining can be used with a set of consensus rules to design PoX blockchains. The consensus rules dictate how miners interact with a PoX blockchain and the system

Name	**Acronym**	**Miner action to mint new cryptocurrency**
Proof-of-work	PoW	Consume electricity towards computations to mint units of a new cryptocurrency.
Proof-of-stake	PoS	Dedicate economic stake in a base cryptocurrency to mint units of the same cryptocurrency.
Proof-of-burn	PoB	Destroy a base cryptocurrency to mint units of a new cryptocurrency.
Proof-of-transfer	PoX	Transfer a base cryptocurrency to mint units of a new cryptocurrency.

Table 1: *Comparison of proof-of-work with other mechanisms.*

makes forward progress, i.e., new blocks are written to the blockchain. For the purposes of this paper, PoX mining uses the Bitcoin blockchain as the base cryptocurrency. While any proof-of-work cryptocurrency may be used, we propose using Bitcoin because it is by far the most secure PoW blockchain and its security properties are currently superior to other PoW blockchains.

PoX is a mining mechanism that must be combined with a set of consensus rules for a fully-functional consensus algorithm. PoX mining is a generalization of the proof-of-burn (PoB) proposed for the consensus algorithm for the Stacks blockchain [6, 5]. A similar consensus rule set can be used with PoX as well.

As with PoB, in PoX, the consensus rules select the winning miner (i.e., the leader) of a round using a verifiable random function (VRF). The leader writes the next block of the Stacks blockchain and mints the rewards (newly minted Stacks). However, in PoX, instead of sending Bitcoin to burn addresses, miners send the Bitcoin to a set of specific addresses corresponding to other network participants.

PoX can be used to design different types of blockchains depending on consensus rules and how the base cryptocurrency is distributed. Below we discuss two use cases:

Participation rewards. PoX may be used to reward holders of a new cryptocurrency for adding value to the network. The Stacking mechanism, proposed in SIP-007 [7], is a scheme that rewards Stacks (STX) holders who participate and add value to the Stacks network. STX holders that control some threshold number of STX would be able to issue a signed message that locks their STX tokens for some period of time, specifies a Bitcoin address to receive funds, and signals (votes) on a Stacks chain version/fork as the current one. This information would be useful to (honest) miners on the network. Miners in the protocol would mine in reward cycles, and for each cycle, would send their Bitcoin commitments to the STX token holders that issued such signed messages before the reward cycle begins. Miners that are also STX holders may obtain an advantage over other miners, which could potentially lead to miner consolidation. In Section 4.1 we discuss possible remedies for this potential consolidation.

Developer fund. PoX may be used to fund a developer fund in a blockchain ecosystem. The developer fund would control some Bitcoin wallet (presumably a multi-signature wallet), and would supply the wallet address to the PoX protocol as a protocol constant. Miners would send committed Bitcoin to this address rather than the burn address. The protocol could place some constraints on the developer fund's Bitcoin by using Bitcoin scripts to, e.g., lock funds for some number of blocks, etc. In any event, this reward scheme requires that the network agree that the developer fund should be a trusted participant in the system.

3 PoX Mining Proposal for Stacks 2.0

This section presents a proposal for using PoX mining with participation rewards for the Stacks 2.0 blockchain. For additional details, we refer the reader to SIP-007 [7].

While using PoX to reward a developer fund is more straight-forward, implementation of *participation rewards* require additional validation and mining mechanisms. In addition to the normal operations of PoB mining (see SIP-001 [5]), the requirement to distribute rewards to participants means that the protocol *must* determine the set of addresses to which miners may validly transfer funds. PoB mining does not need to perform these steps, because the address is always the same, i.e., the burn address. However, with participation rewards, the network participants must be able to validate the recipient Bitcoin addresses.

In SIP-007, progression in Stacking happens over *reward cycles*. In each reward cycle, a set of Bitcoin addresses are iterated over, such that each Bitcoin address in the set of reward addresses has exactly one Bitcoin block in which miners will transfer funds to the reward address.

Miners participating in the Stacks blockchain compete to lead blocks by transferring Bitcoin. Leaders for particular Stacks blocks are chosen by sortition, weighted by the amount of Bitcoin sent (for more details, see SIP-001 [5]). Before a reward cycle begins, the Stacks network must reach consensus on which addresses are valid recipients. Reaching consensus on this is non-trivial: the Stacks blockchain itself has many properties independent from the Bitcoin blockchain, and may experience forks, missing block data, etc., all of which make reaching consensus difficult. As an extreme example, consider a miner that forks the Stacks chain with a block that claims to hold a large fraction (e.g., 100%) of all Stacks holdings, and proceeds to issue block commitments that pay all of the fees to themselves. How can other nodes on the network detect that this miner's commitment transfers are invalid?

The consensus algorithm addresses this with a two-phase cycle. Before each reward cycle, Stacks nodes engage in a *prepare* phase, in which two items are decided:

1. An **anchor block** - the anchor block is a Stacks chain block. For the duration of the reward cycle, mining any descendant forks of the anchor block requires transferring mining funds to the appropriate reward addresses.

2. The **reward set** - the reward set is the set of Bitcoin addresses which will receive funds in the reward cycle. This set is determined using Stacks chain state from the anchor block.

During the reward cycle, miners contend with one another to become the leader of the next Stacks block by broadcasting *block commitments* on the Bitcoin chain. These block commitments send Bitcoin funds to either a burn address or a PoX reward address.

Address validity is determined according to two different rules:

1. If a miner is building off of any chain tip *which is not a descendant of the anchor block*, all of the miner's commitment funds must be sent to the burn address (i.e., the funds are burned).
2. If a miner is building off a descendant of the anchor block, the miner must send commitment funds to 5 addresses from the reward set, chosen as follows:
   - Use the verifiable random function (also used by sortition) to choose 5 addresses from the reward set. These 5 addresses are the reward addresses for this block.
   - Once addresses have been chosen for a block, these addresses are removed from the reward set, so that future blocks in the reward cycle do not repeat the addresses.

Note that the verifiable random function (VRF) used for address selection ensures that the same addresses are chosen by each miner selecting reward addresses. If a miner submits a burn commitment which *does not* send funds to a valid address, those commitments are ignored by the rest of the network (because any Stacks node can deduce that the transfer addresses are invalid).

To reduce the complexity of the consensus algorithm, Stacks reward cycles are fixed length — if fewer addresses participate in the reward set than there are slots in the cycle, then for the remaining blocks, all miners must send funds to burn addresses.

For more detail on the prepare phase, how the anchor block would be chosen, and how the Stacks blockchain could recover from missing anchor block data, see SIP-007 [7].

3.1 Participation-Based Reward Threshold Adjustments

Each reward cycle may transfer miner funds to up to 5000 Bitcoin addresses. To ensure that this number of addresses is sufficient to cover the pool of participants (given 100% participation of liquid STX), the threshold for participation must be 0.02% (1/5000th) of the liquid supply of STX. However, if participation is *lower* than 100%, the reward pool could admit smaller STX holders. The protocol specifies **2 operating levels**:

- **25%** - If fewer than $0.25 \cdot STX\_LIQUID\_SUPPLY$ STX participate in a reward cycle, participant wallets controlling x STX may include $floor(x/(0.00005{\cdot}STX\_LIQUID\_SUPPLY))$

addresses in the reward set. That is, the minimum participation threshold is 1/20,000th of the liquid supply.

- **25%-100%** - If between $0.25 \cdot STX\_LIQUID\_SUPPLY$ and $1.0 \cdot STX\_LIQUID\_SUPPLY$ STX participate in a reward cycle, the reward threshold is reduced in order to maximize the number of slots that are filled. That is, the minimum threshold T for participation will be roughly 1/5,000th of the participating STX (adjusted in increments of 10,000 STX). Participant wallets controlling 'x' STX may include $floor(x/T)$ addresses in the reward set.

In the event that a participant signals and locks up enough STX to submit multiple reward addresses, but only submits one reward address, that reward address will be included in the reward set multiple times.

3.2 Submitting Reward Addresses

Reward participants must broadcast signed messages for three purposes:

1. Indicating to the network how many STX should be locked up, and for how many reward cycles.
2. Indicate support for a particular chain tip.
3. Specifying the Bitcoin address for receiving rewards.

These messages may be broadcast either on the Stacks chain or the Bitcoin chain. If broadcast on the Stacks chain, these messages must be confirmed on the Stacks chain *before* the anchor block for the reward period. If broadcast on the Bitcoin chain, they may be broadcast during the prepare phase, but must be included before the prepare phase finishes.

These signed messages are valid for at most 12000 Bitcoin blocks (12 reward cycles, or 3 months). If the signed message specifies a lockup period x less than 12000 blocks, then the signed message is only valid for Stacking participation for $floor(x/1000)$ reward cycles (the minimum participation length is one cycle: 1000 blocks).

3.3 Participant Signaling Delegation

The process of delegation allows a Stacks wallet address (the represented address) to designate another address (the delegate address) for participating in the PoX rewards protocol. This delegate address, for as long as the delegation is valid, is able to sign and broadcast participation messages (i.e., messages which lock up Stacks, designate the Bitcoin reward address, and signal support for chain tips) on behalf of the represented address. This allows the owner of the represented address to contribute to the security of the network by having the delegate address signal support for chain tips. This signaling, like the normal PoX participation signaling, combats potential attacks on the blockchain stability by miners that may attempt to mine hidden forks, hide eventually invalid forks, and other forms of miner misbehavior.

Supporting delegation adds two new transaction types to the Stacks blockchain:

Delegate Funds. This transaction initiates a represented-delegate relationship. It carries the following data:

- Delegate address
- End Block: the Bitcoin block height at which this relationship terminates, unless a subsequent delegate funds transaction updates the relationship. There is no upper limit for this end block.
- Delegated Amount: the total amount of STX from this address that the delegate address will be able to issue Stacking messages on behalf of.
- Reward Address (*optional*): a Bitcoin address that must be designated as the funds recipient in the delegate's Stacking messages. If unspecified, the delegate can choose the address.

Terminate Delegation. This transaction terminates a represented-delegate relationship. It carries the following data:

- Delegate Address

Note that there is only ever one active represented-delegate relationship between a given represented address and delegate address (i.e., the pair $(representedAddress, delegateAddress)$ uniquely identifies a relationship). If a represented-delegate relationship is still active and the represented address signs and broadcasts a new "delegate funds" transaction, the information from the new transaction replaces the prior relationship.

Both types of delegation transactions must be signed by the represented address. These are transactions on the Stacks blockchain, and will be implemented via a native smart contract, loaded into the blockchain during the Stacks 2.0 genesis block. These transactions, therefore, are 'contract-call' invocations.

4 On-going and Future Research

We are actively engaged in further research on several aspects of PoX mining and participation rewards. This section discusses two such topics.

4.1 Addressing Miner Consolidation

PoX when used for participation rewards, as described, could lead to miner consolidation. Because miners that *also* participate as holders could gain an advantage over miners who do not participate as holders, miners would be strongly incentivized to buy the new cryptocurrency and use it to crowd out other miners. In the extreme case, this consolidation could lead to centralization of mining, which would undermine the decentralization goals of the public blockchain. While we are actively investigating additional mechanisms to address this potential consolidation, we propose two mechanisms here:

Time-Bounded PoX. Participation rewards incentivize miner consolidation if miners obtain *permanent* advantages for obtaining the new cryptocurrency. However, by limiting the time period of PoX, this advantage declines over time. In this scheme, a "sunset block" would be set for the participation rewards x years after the launch. At the sunset block, the participation rewards would stop, and all miners would perform commitments by burning Bitcoin. That is, after the sunset block, the PoX system would transition to PoB. This transition could be linear over time, half of the Bitcoin commitment would be burned and the other half would be transfered to holders, and so on. The exact parameters for such a transition can be adjusted and studied in simulations.

This scheme would solve the bootstrapping problem for the new blockchain, providing miners and holders with incentives for participating in the network early on. Then, as natural use cases for the blockchain develop and gain steam, the PoX system could gradually scale down.

Trusted Miner Set. Miner consolidation due to participation rewards is not a threat if miners are prohibited from participating as holders (i.e., miners *cannot* receive PoX rewards). However, in open and decentralized systems, it is not easy to determine whether a given wallet address belongs to another participant. In order to provide the guarantee that miners and holders are separate, a new blockchain could limit the set of potential miners to a trusted set (which could be bootstrapped through some other trusted entity). These miners would have to be vetted by the trusted entity, and would likely require other systems to ensure compliance (e.g., legal contracts). For our purposes, a trusted miner set would undermine our goals of an open public blockchain, and the resulting blockchain would begin to function more like a federated system than our intended system.

4.2 Bitcoin Bandwidth

Because PoX miners must send Bitcoin transactions to participate in the consensus algorithm and send PoX rewards, PoX mining would occupy some Bitcoin transaction bandwidth. Given Bitcoin bandwidth is limited by design, given security requirements, new PoX blockchains need to reduce their bandwidth use requirements. SIP-007 does this by limiting the number of participants, using a STX holding threshold. Other ways to address bandwidth limitations are also possible e.g., lighting channels between Bitcoin and the new blockchain. Optimizations at the Bitcoin transactions layer could also be possible, which would reduce the total size needed for PoX transactions. We're exploring both size reduction at the Bitcoin layer and potential modifications to lightning to enable cross-chain channels.

References

[1] J. Nelson, "PoS Blockchains Require Subjectivity to Reach Consensus," 03 2017. https://forum.blockstack.org/t/pos-blockchains-require-subjectivity-to-reach-consensus/762.

[2] A. Poelstra, "On Stake and Consensus," 03 2015. https://download.wpsoftware.net/bitcoin/pos.pdf.

[3] Blockstack PBC, "blockstack-core: v20.0.8.1," 08 2019. https://github.com/blockstack/blockstack-core/tree/v20.0.8.1.

[4] B. S. Srinivasan, "Bitcoin becomes the Flag of Technology," 1 2020. https://nakamoto.com/bitcoin-becomes-the-flag-of-technology/.

[5] J. Nelson and A. Blankstein, "SIP 001: Burn Election," https://github.com/blockstack/blockstack-core/blob/develop/sip/sip-001-burn-election.md.

[6] M. Ali, J. Nelson, A. Blankstein, R. Shea, and M. J. Freedman, "Blockstack Technical Whitepaper v2.0," 05 2019. https://blockstack.org/whitepaper.pdf.

[7] M. Ali, A. Blankstein, M. J. Freedman, D. Gupta, J. Nelson, J. Soslow, and P. Stanley, "SIP 007: Stacking Consensus," https://github.com/blockstack/blockstack-core/blob/develop/sip/sip-007-stacking-consensus.md.