SIP-0XX: PoX-5 Bitcoin Staking and Emission Schedule Alignment

Stacks Improvement Proposal Framework Draft

PREAMBLE

SIP Number: 0XX

Title: PoX-5: Bitcoin Staking and Emission Schedule Alignment

Authors: Adriano Di Luzio, Alexis Radcliff, Aaron Blankstein, Sam Lee, Tanguy Girault
Consideration: Technical, Economic, Governance

Type: Consensus

Status: Draft
Created: Jun 3, 2026

Layer: Consensus (hard fork)

Discussions-To: SIP forum.stacks.org thread & Whitepaper Forum post

1. ABSTRACT

Stacks exists to activate the Bitcoin economy: to bring Bitcoin into productive use while preserving the security properties that define it. There are several desirable features on other crypto networks that Bitcoin currently lacks, which Stacks aims to build and provide for Bitcoiners without changing Bitcoin itself. One of the longest standing unsolved problems for Bitcoiners is how to deploy BTC as a productive resource and earn yield, while keeping custody of their Bitcoin. Today less than 1% of Bitcoin supply earns yield, against 19% to 67% of supply staked on major proof-of-stake networks **(Appendix 1)**. Closing even part of that gap is the largest capital-formation opportunity available for any Bitcoin layer, and it is the opportunity this proposal is designed to open for Stacks.

The Stacks 2026 roadmap, developed with the Stacks community and the Treasury Committee, addresses key feature requests for Bitcoiners while also building the Stacks economic engine for long term sustainability. The roadmap begins with Bitcoin Staking as Phase 1, the primary mechanism to anchor Bitcoin capital on Stacks. Bitcoin Staking is a proposed upgrade to

Stacks' existing Proof-of-Transfer (PoX) consensus mechanism that enables participants to lock BTC on the Bitcoin blockchain and STX on the Stacks blockchain and earn BTC yield without giving up custody of their coins. This SIP and the companion Bitcoin Staking white paper specify the consensus changes required for Bitcoin Staking. This SIP proposes both the technical and economic implementation of Bitcoin Staking, including an alignment of the STX emissions schedule.

2. INTRODUCTION

2.1 Why Bitcoin Staking, and Why Now

Bitcoin Staking will anchor capital to Stacks by offering Bitcoin-denominated self-custodial yield, something no other product live in production can replicate **(Appendix 2)**.

As more BTC holders enter the Stacks ecosystem, we believe more BTC capital participation will drive economic activity that grows transaction fees on the network. After Bitcoin Staking, the Stacks roadmap details other priorities such as self-custodial lending against locked BTC and a future liquid-staking variant. Capital that arrives to earn native yield is therefore positioned to move into the applications the roadmap describes.

Because STX serves as the capacity asset that BTC positions pair against, participation in Bitcoin Staking creates demand for STX and the need to lock STX, thereby reducing circulating supply. In doing so, participation of Bitcoin capital in Stacks serves to provide long term economic security to the Stacks network: as capital becomes active it generates transaction activity, and activity generates fees. The durable design intent of Stacks is that fees, in addition to emissions, become the primary source of the rewards that fund consensus, including the BTC yield Bitcoin Staking distributes. Bitcoin Staking is the first step toward that end state: it brings in the capital whose activity, over time, is intended to grow the fee base that ultimately sustains the mechanism.

2.2 Design Principles

Bitcoin Staking follows three design principles.

- **BTC holders earn rewards in BTC without giving up custody.** The committed BTC remains on the Bitcoin blockchain under the participant's own keys, held by standard timelocks and secured by Bitcoin's consensus.
- **Bitcoin Staking builds on existing Stacks infrastructure.** Miner competition, block production, and the routing of BTC through PoX remain intact; the mechanism extends the protocol rather than replacing it.

- **Bitcoin Staking works for holders of any size.** The protocol reduces barriers to entry for smaller holders through pooling and provides defined capacity allocation for participants of any size.

3. SPECIFICATION

3.1 Bitcoin Staking Mechanism

This section outlines key specifications for the Bitcoin Staking mechanism. For a detailed overview, please refer to the white paper.

3.1.1 Protocol Bonds

Bitcoin Staking participation is structured through protocol bonds, where participants pair a BTC timelock on Bitcoin with a corresponding STX lock on Stacks for a 6-month bonding period, targeting a fixed yield subject to the risks inherent to the protocol.

The L1 commitment is a timelocked UTXO on Bitcoin, constructed using a P2WSH script that includes OP_CHECKLOCKTIMEVERIFY (BIP-65). The participant locks BTC under their own keys with a timelock expiring at the end of their committed bonding period. The unlock script encodes the participant's Stacks principal address in its metadata, linking the Bitcoin lock to a Stacks identity. The full script format will be specified in subsequent community-refined SIP draft.

The L2 commitment is a call to the Bitcoin Staking smart contract on Stacks. The participant locks STX for the full bonding period and specifies the BTC address at which the L1 lock will appear. The Stacks node monitors and indexes Bitcoin, matching observed timelocked UTXOs against registered L2 commitments to determine eligibility and compute reward allocation.

The Bitcoin side of a protocol bond may be satisfied either as native BTC held under the participant's own keys on Bitcoin L1, or as sBTC held on Stacks. Both forms grant the same bond and the same yield; they differ only in where the Bitcoin sits during the bonding period and which participation flows are available. STX-only staking remains available as a separate path with no BTC commitment, no capacity constraint, and no auction, carrying forward the existing PoX participation model under an updated reward distribution. The participation paths are specified in full in the white paper.

3.1.2 Bonding Periods and Timing

Bitcoin Staking operates on the following time units:

- **Auction Window:** ~1 week before each new bonding period; the protocol publishes the target yield rate and capacity for the period, and participants submit bids.

- **Bonding Period:** 25,200 Bitcoin blocks, ~6 months, the minimum commitment for a paired BTC and STX position.
- **Reward Distribution:** 1,050 Bitcoin blocks, ~1 week; BTC rewards are distributed to all eligible participants once per distribution interval, 24 times over a bonding period.
- **Signer Cycle:** 2,100 Bitcoin blocks, ~14 days; the Stacks signer set updates every cycle as part of Nakamoto consensus. This unit does not directly govern Bitcoin Staking but remains the foundational cadence for STX-only staking and block validation.

Six bonding periods run concurrently in overlapping sequence, with a new period opening every other signer cycle, approximately once a month (every 4,200 Bitcoin blocks). This staggered structure provides regular entry and exit windows without requiring all participants to lock and unlock simultaneously.

Lock renewal differs between the two chains. On L2, STX remains locked until the committed bonding period ends, and a participant may stake continuously by extending before expiry. On L1, automatic re-enrollment is not possible: because a timelocked UTXO cannot be re-committed until its timelock expires, renewal requires a new Bitcoin transaction. The L1 timelock is therefore set to expire approximately 1,400 Bitcoin blocks (10 days) before the bonding period ends, giving participants a window to construct and broadcast the renewal transaction before the L2 lock releases.

An optional Early Exit allows a participant to release the BTC lock before expiry. At the start of the bonding period the participant constructs the timelock with a pre-approved hashed spend option, exercisable through a request co-signed by a designated signer set. Exercising Early Exit forfeits all undistributed yield for the remainder of the period; the paired STX remains locked for the full term and does not convert to an STX-only position.

3.1.3 Capacity Allocation and Auction Mechanism

The target yield rate and capacity for each bonding period are derived from on-chain inputs, including miner economics, reserve fund status, and prior-period participation. The protocol stabilizes yield primarily by adjusting capacity rather than the target rate, anchoring each new period's target to the blended yield of the active bond book.

Capacity is limited. During the initial bootstrap phase of Bitcoin Staking, the Stacks Endowment will manage capacity allocation to approved, whitelisted partners before each bonding period begins. As the protocol gradually decentralizes, capacity will be allocated through an auction mechanism. This SIP ratifies the first phase (bootstrap, PoX-5) only. The auction mechanism will be fully specified as part of PoX-6. The phased rollout is covered in depth in section 3.3.

3.1.4 Yield Distribution and Waterfall Structure

Bitcoin Staking yield distribution follows a three-tranche waterfall:

- **Tranche 1: Active Protocol Bonds.** Confirmed paired BTC:STX positions earn the target yield rate (expressed as APY) on their locked BTC for their respective period. Approximately 10% of Tranche 1 capacity is allocated to pools, open to any participant on a first-come, first-served basis. (Section 3.3).
- **Tranche 2: STX-Only Stakers.** Miner revenue beyond the Tranche 1 obligation, the cycle excess, is split between STX-only stakers and the reserve fund at a proposed initial ratio of 85% to Tranche 2 and 15% to the reserve. The Tranche 2 portion is distributed pro rata among STX-only stakers.
- **Tranche 3: Reserve Fund.** The reserve buffers Tranche 1 payouts when miner revenue falls below total yield obligations.

A paired position is eligible for Tranche 1 yield only if it meets three conditions: it has been allocated capacity through the Stacks Endowment or through an open-access pool; its full BTC amount is locked on L1 before the start of the bonding period; and its paired STX meets the ratio requirement. Detailed scenarios in the event of miner revenue excess and prolonged drawdowns are specified in the white paper.

3.1.5 Coverage Ratio Requirements

The protocol maintains a Coverage Ratio, defined as the reward pool per cycle divided by paired BTC obligations per cycle. A ratio at or above 1.0x indicates that miner revenue covers all Tranche 1 obligations without drawing on the reserve. The protocol targets a coverage multiple of 2.0x (acceptable range 1.5x to 3.0x) and responds across five bands:

- **Excess capacity (≥ 2.0x):** offer new bonds at increased target size (yield and/or capacity).
- **Healthy (1.5–2.0x):** offer new bonds at current target size.
- **Caution (1.0–1.5x):** reduce new bond sizes and monitor closely.
- **Stressed (0.8–1.0x):** halt new bonds; deploy the reserve to cover any shortfall.
- **Distribution failure risk (< 0.8x):** deploy the reserve fully; activate the distribution priority cascade.

The coverage ratio and band-driven responses are computed deterministically on-chain from miner revenue, reserve balances, and active obligations.

3.2 Emission Schedule Alignment

This SIP couples a change to the STX emission schedule with the Bitcoin Staking mechanism. The two are presented together since miners compete for the coinbase block rewards and transaction fees, and that competition funds the BTC reward pool. The yield the protocol can sustainably target therefore scales with the total value miners compete for, of which the coinbase block rewards are currently the dominant part. The proposed emission change is crucial for Bitcoin staking to maintain a competitive APY.

3.2.1 Current State Under SIP-029

Stacks issues a fixed coinbase block reward on each Bitcoin block. Under SIP-029, that reward was scheduled to step down over time. The first reduction took effect in April 2026, lowering the coinbase block reward from 1,000 STX to 500 STX per Bitcoin block, with further reductions scheduled for subsequent periods.

3.2.2 Proposed Change

This SIP makes two changes to the coinbase block rewards, both effective at hard fork activation.

First, it restores block reward to 1,000 STX per Bitcoin block and removes the reduction schedule established under SIP-029. The 1,000 STX rate carries no scheduled reductions. Any future change to the rate would be proposed through a separate SIP, with Bitcoin halving events serving as natural organic milestones at which the community may reassess issuance.

Second, it applies a temporary boost of an additional 500 STX per Bitcoin block, raising the block reward to 1,500 STX per block for the first bonding period following activation. The boost runs for 25,200 Bitcoin blocks (approximately 6 months), matching the duration of one full bonding period, and expires automatically at the end of that window, after which the block reward returns to 1,000 STX per block. The boost is a one-time measure to bootstrap participation during the launch of Bitcoin Staking. It is not renewed by this SIP; any extension would require a separate proposal.

The boost is funded as a new issuance for the duration of the boost window. This SIP does not alter or defer SIP-031 emissions.

3.2.3 Justification

The coinbase block rewards are coupled to Bitcoin Staking through the PoX consensus mechanism. Four considerations motivate restoring the 1,000 STX baseline and a temporary 500 STX booster period.

3.2.3.1. Yield Capacity & Boost

The BTC reward pool that funds staking yield is the BTC that miners spend competing for the coinbase block rewards and transaction fees. The per-cycle reward pool scales with the total value miners compete for, of which the coinbase block rewards are currently the dominant part. At 500 STX per block, the achievable reward pool, and therefore the BTC yield the protocol can sustainably target, is materially constrained. Restoring the 1,000 STX baseline gives the Bitcoin Staking mechanism an adequate reward pool to support the proposed launch parameters (3,000 BTC capacity at a 3% target yield) with adequate coverage. This yield rate is needed for the staking mechanism to be competitive in the broader staking market **(Appendix 5)**, which is

crucial for the roadmap's liquidity-bootstrapping phase and to help anchor the Bitcoin capital the ecosystem's longer-term self-sufficiency depends on. Lastly, the 1,000 STX block reward baseline ensures adequate capacity early on to meet institutional demand.

The proposed 6-month boost adds further Bitcoin liquidity to the waterfall during the protocol's early growth phase, and it benefits non-bonding participants as well. Because the target yield for the bonding period is fixed, any additional Bitcoin yield flows past Tranche 1 to STX-only stakers and the reserve fund. STX-only consensus participants therefore see the larger share of the boost, as the higher residual flows into Tranche 2, conditional on healthy coverage; in a stressed coverage band, those distributions compress (Section 3.1.5).

3.2.3.2. Network Security

Stacks consensus depends on miners committing BTC to compete for blocks; that competition is what produces and secures blocks, and the miner set's size and decentralization scale with how attractive mining is. Block rewards are a primary input to that attractiveness: at a given STX price and fee level, the reduction from 1,000 to 500 STX lowers the expected reward miners compete for and, with it, the incentive to participate. Reducing that incentive at the moment the network is launching a product designed to attract significant new capital to the ecosystem is a risk this proposal avoids. Restoring the 1,000 STX baseline keeps miner participation well-supported through the bootstrap, when a healthy, decentralized miner set matters most.

3.2.3.3. Transition to Fee-Driven Economics

Transaction fees are not yet sufficient to sustain miner economics independently of the coinbase block rewards. The long-term design anticipates fees becoming the primary source of miner revenue as Bitcoin-native activity grows on the network, a transition Bitcoin Staking is intended to accelerate by anchoring productive BTC capital. Until that activity matures, premature reduction of the coinbase block rewards would constrain the economic base the transition depends on.

3.2.3.4. Inflation Alignment & Market Impact

With the proposed emission alignment, the peak emissions rate for 2026-2027 sits near the median emission rate of the 50 largest networks by market capitalization, and below that median in every subsequent year. The schedule remains within single-digit annual supply growth throughout. In terms of liquidity, a detailed analysis found in **Appendix 3** demonstrates the market impact under a deliberately conservative scenario. Inflation impact is modeled in **Appendix 4**.

3.3 Phased Rollout

Bitcoin Staking is delivered in two phases. This SIP ratifies the first phase only. The bootstrap phase, PoX-5, is the operational framework that this proposal activates and specifies. The fully

decentralized phase, PoX-6, is the intended end state and is described here as direction, not as a ratified design. PoX-6 will be proposed and activated through a separate SIP with its own parameters, its own reference implementation, and its own community vote. Approving this SIP does not approve PoX-6 or commit the network to any specific PoX-6 design.

3.3.1 Bootstrap Phase (PoX-5)

PoX-5 operates under Stacks Endowment stewardship for approximately one year from activation. Its purpose is to demonstrate the mechanism's durability, accumulate real participation data, and harden operational processes while limiting the network's exposure during the early phase. The bootstrap phase is a managed operational framework, not a separate protocol design: the consensus mechanism is the one specified in Section 3.1, with a defined set of parameters set by the Endowment rather than computed algorithmically.

During PoX-5 the Endowment sets, for each bonding period, the available capacity, the target yield rate, the BTC:STX ratio, and the capacity allocation. The Endowment computes BTC yield capacity for each period and allocates it to whitelisted partners before the period begins, so that each period launches with committed and known counterparties. Approximately 10% of Tranche 1 capacity is reserved for open access on a first come, first serve basis through selected pooling partners. The proposed initial program conditions are 3,000 BTC capacity, a 5% minimum STX ratio held static for program-management simplicity, and a 3% BTC target APY at launch. Exact values are finalized before activation and may vary with committed partner capacity.

Two guardrails bound the Endowment's role during PoX-5. First, the reserve fund operates in accrual-only mode, held in a contract with no access functions other than those controlled directly by consensus, which lets the reserve build toward a healthy baseline and reduces the risk surface during launch. Second, weekly reward distributions include a built-in delay window during which a designated multisig can pause a distribution as a circuit-breaker. The pause can only halt a distribution; it cannot redirect rewards. In this worst case unwind path, a hard fork would be necessary to distribute rewards. These measures are security, testing, and stability mechanisms with defined limits, not discretionary control over participant funds, which remain self-custodial and recoverable in full at timelock expiry regardless of Endowment action.

3.3.2 Algorithmic Phase (PoX-6)

The intended end state is fully algorithmic, permissionless operation: a consensus-encoded auction open to any participant with no partner preference, dynamic capacity and yield-rate setting derived from on-chain data, and full reserve fund activation under consensus control. The staking-process improvements introduced in PoX-5 carry forward.

The transition to PoX-6 depends on observed performance during the bootstrap phase, infrastructure maturity, and the readiness of the PoX-6 implementation. Because PoX-6 alters consensus-encoded behavior, it will be specified and ratified through its own SIP, informed by

real participation data from PoX-5. This SIP does not commit to a PoX-6 activation date or its parameters, and the community's approval of this SIP is limited to the PoX-5 design above.

3.4. Staking Process Improvements

As part of the PoX-5 contract, this proposal introduces two improvements to the staking process. Both apply across paired and STX-only participation and are independent of BTC participation.

The first improvement removes the cooldown cycle. Under PoX-4, a staker who changes their reward address forfeits eligibility for the following cycle while the change settles, costing a cycle of rewards. PoX-5 allows a staker to update their reward address before the next preparation phase and remain eligible in the upcoming cycle, so an address change no longer requires sitting out a cycle.

The second improvement streamlines solo and pooled staking. Under PoX-4, pool operators must submit a commitment transaction every cycle to register locked STX for rewards, which creates recurring operational overhead and exposes a pool to a missed cycle if the commitment is not resubmitted in time. PoX-5 persists a pool's commitment across cycles until the operator changes it, removing the per-cycle commitment requirement and the missed-cycle risk that accompanies it.

These improvements are encoded in the PoX-5 contract (Section 3.6.1) and carry forward into the algorithmic phase described in Section 3.3.2.

3.5. Burn Mechanism Alignment

Under PoX-4, miner BTC that cannot be matched to an eligible stacker reward address is sent to a Bitcoin burn address and permanently removed from circulation. This occurs in two cases: when the number of participating stackers is fewer than the available reward slots in a cycle, and during the prepare phase, when commitments route to the burn address by default. The burned BTC performs no function beyond proving the miner's commitment.

PoX-5 removes this burn as a now-unnecessary pre-Nakamoto technical artifact and returns the committed BTC to the community via the standard reward mechanism instead. All miner BTC commitments route into the reward pool and are distributed through the yield waterfall (Section 3.1.4) rather than sent to a burn address, so that committed Bitcoin funds network rewards rather than being destroyed.

This treatment carries forward into the algorithmic phase described in Section 3.3.2, where the same waterfall governs distribution under consensus control.

3.6 Smart Contract and Off-Chain Components

3.6.1 PoX-5 Contract

The PoX-5 contract replaces PoX-4 and implements:

- **Protocol bond registration and validation** against paired L2 staking commitments.
- **STX locking** for full bonding periods with BTC address matching.
- **Event emission** enabling the Stacks node to match L1 timelocked UTXOs against L2 commitments.
- **Signer association and pool registration.**
- **Coverage Ratio monitoring** with deterministic state transitions between response bands.
- **Reserve fund tracking** exposing the current coverage ratio, band status, and BTC and USD balances.

During PoX-5 the principal parameters are Endowment-set and the contract records and enforces them; algorithmic computation of yield rate, capacity, and ratio is a PoX-6 capability.

3.6.2 Off-Chain Operational Components

The mechanism requires operational components adjacent to consensus:

- **sBTC autobridging infrastructure** for reward distribution routing and sBTC-based protocol bonds.
- **Early Exit signer set** providing co-signing capability for the hashed spend option during bonding periods.
- **Multisig circuit-breaker** able to pause but not redirect weekly distributions.
- **Auction clearing mechanism**, conducted off-chain during PoX-5 and transitioning to consensus-encoded operation under PoX-6.

Reward distribution moves to sBTC as the network scales, which lets distributions settle on Stacks rather than requiring an L1 Bitcoin transaction per payout and opens the way to later capabilities such as pools distributing rewards trustlessly. The PoX-5 implementation of this shift is autobridging: miner BTC bids route into the contract and are autobridged to sBTC, so weekly distributions can be paid as either BTC on L1 or sBTC on L2 by participant preference. This is the first step toward the broader sBTC-based distribution model that PoX-6 carries forward under consensus control.

4. ACTIVATION

4.1 Voting Parameters

- **Voting threshold for stacked STX:** 80% (recommended based on SIP-021/029 precedent for hard forks)
- **Minimum quorum:** 80M STX recommended
- **Voting window:** The voting window will be identified and shared publicly during the community review period, allowing sufficient time to address critical feedback before a public vote is established.
- **Voting addresses:** Voting addresses will be generated by the voting platform and shared publicly once the voting block height is reached.

4.2 Activation Timeline

- **Snapshot block:** (Bitcoin block height for voter eligibility): Block heights will be determined following the community review period as part of the vote preparation process.
- **Hard fork activation:** Activation block heights will be determined following the community review period.
- **PoX-5 program launch:** PoX-5 program parameters and timeline will be finalized following community review.

4.3 Transition Mechanics

Details will follow after SIP community & core contributor discussion. Current implementation follows:

- At the epoch 4.0 activation height, the pox-5 contract is automatically deployed. Any STX locked in pox-4 gets unlocked at that time for participants to re-stack in PoX-5.
- All stackers continue to receive rewards during that reward cycle. Once the next reward cycle happens, PoX-5 becomes the active PoX contract.

5. BACKWARDS COMPATIBILITY

SIP authors have engaged pool operators, custodians, wallet providers, and core ecosystem app builders ahead of finalization to assess transition impacts. Outreach is ongoing through the finalization phase

This is a hard fork. All PoX-4 stacking locks are released at activation. Operational implications include:

5.1 Pool Operators

Pool operators move to the PoX-5 contract interface and adopt the reference signer manager contract, which is provided so existing signers can resume with minimal customization. PoX-5 persists a pool's commitment across cycles, so the per-cycle commitment transaction required under PoX-4 is no longer needed.

Migration timeline and operator support requirements to be published prior to the voting window, expected in SIP V2.

5.2 Custodians and Wallets

Custodians and wallets integrate the PoX-5 staking interface, which uses one flow for solo and delegated participation. For BTC participation, integrators support constructing the timelocked P2WSH UTXO described in Section 3.1.1 and the renewal transaction described in Section 3.1.2.

Wallet migration timeline and custodian support requirements to be published prior to the voting window, expected in SIP V2.

5.3 Existing Stackers

All locks release at activation, and holders become immediately eligible for any PoX-5 participation path during the re-lock window in Section 4.3. A reward-address change no longer costs a forfeited cycle, since PoX-5 removes the cooldown described in Section 3.4.

6. REFERENCE IMPLEMENTATIONS

- **Sacks-core implementation branch:** ttps://github.com/stacks-network/stacks-core/tree/pox-wf-integration
- **PoX-5 contract (pox-5.clar):** https://github.com/stacks-network/stacks-core/blob/pox-wf-integration/stackslib/src/chainstate/stacks/boot/pox-5.clar
- **Reference signer manager contract:** https://github.com/stacks-network/stacks-core/blob/pox-wf-integration/contrib/core-contract-tests/contracts/signer-manager.clar.
    - Provided so existing signers can adopt PoX-5 with minimal customization

6.1 Security Audits

The PoX-5 implementation undergoes independent security audit ahead of activation, with audit completion a precondition for the activation timeline.

7. RELATED WORK

- **SIP-007:** Original PoX mechanism
- **SIP-015:** Stacks 2.1 upgrade
- **SIP-021:** Nakamoto Release
- **SIP-029:** Current emissions schedule (explicitly superseded for post-activation periods)
- **SIP-031:** Stacks Endowment
- Bitcoin Staking Whitepaper

8. SECURITY CONSIDERATIONS

8.1 Trust Assumptions

The following table enumerates the components of Bitcoin Staking that require trust, the specific assumption made, the consequence if it fails, and the associated mitigation:

Component	Trust Assumption	Failure Mode	Mitigation
Bitcoin L1 timelocks	Bitcoin consensus is secure and OP_CLTV is enforced	Timelocks could be broken or bypassed	Inherits Bitcoin's security model; Users remain in control of their assets and have sole control over their keys
Stacks consensus	Nakamoto consensus is live and producing blocks	The chain may halt or be reorged back to the last PoX anchor block	BTC remains self-custodial on L1; participants can unilaterally exit once timelock expires
Miner bid economics	Miner bids reflect a reasonable approximation of the STX/BTC market price	Manipulated bids distort capacity and yield calculations	ATC-C validation filters outliers; rolling average smoothing dampens single-cycle manipulation
Reward distribution	BTC rewards are distributed to correct reward addresses each cycle	Incorrect or censored reward distribution	On-chain reward set is deterministic and publicly verifiable

Bitcoin Staking does not introduce slashing or protocol-level principal loss. Full access to a participant's locked BTC and STX will be returned in full at timelock expiry regardless of participant behavior, miner behavior, reserve fund availability, or network conditions.

*ATC-C validation refers to Assumed Total Commitment with Carryforward, an MEV mining mitigation strategy.

8.2 Economic Risks

Reflexivity Risk. The economic dependency between STX demand and BTC yield can produce negative reinforcement. If STX price declines, miner bids decrease, the BTC reward pool shrinks, and the system's ability to sustain the target BTC yield rate is reduced. The waterfall structure concentrates residual risk on STX-only stakers in Tranche 2, with drawdown reaching paired BTC participants only if the reserve is depleted.

Concentration Risk. BTC holdings are naturally concentrated with a small number of addresses holding a disproportionate share of total supply. Large BTC positions paired with sufficient STX will receive proportionally large capacity allocations. The auction mechanism ensures competitive allocation but does not remove concentration risk. Post-launch monitoring and potential parameter adjustment may be necessary if rewards become disproportionately concentrated.

Opportunity Cost. Participants face STX price exposure to market fluctuation during the bonding period and the illiquidity of timelocked BTC, both calibrated by the participant's ratio commitment and bonding period selection. The early exit mechanism partially offsets BTC illiquidity: participants can unlock at any time at the cost of forfeiting the BTC yield for the remainder of the bonding period.

8.3 Protocol Risks

Hard Fork Coordination Risk. Bitcoin Staking is a non-backwards-compatible upgrade. At activation, all existing stacking locks from prior PoX versions are released. The transition carries operational risk: a failed activation, for example due to a contract bug, could affect the chain's ability to produce blocks. Mitigations include extensive testnet validation, partner infrastructure audits, and staged activation contingent on minimum participation thresholds. A design property reduces this risk further: Bitcoin Staking does not require BTC participation to function. If zero BTC is committed in a bonding period, the protocol continues to operate as an STX-only staking system, with STX stakers earning the full miner-funded reward pool.

Bootstrap Phase Dependencies. During PoX-5, the Endowment manages capacity allocation and operates the multisig circuit-breaker for weekly distributions. The multisig can pause but not redirect distributions, as a safeguard against unforeseen issues. The transition to PoX-6

removes these dependencies through consensus-encoded operation, as described in Section 3.3.

L1 Scalability and Transaction Cost Exposure. Bitcoin Staking requires one L1 Bitcoin transaction per enrollment, and auto-bridging miner revenue into sBTC requires periodically reconciling each miner UTXO. At scale this introduces exposure to Bitcoin transaction fees and block-space consumption, and during high-fee environments consolidation costs may be material. Batching multiple UTXOs into a single transaction reduces auto-bridging cost.

9. APPENDICES