Bitcoin Staking

A Consensus Mechanism for Self-Custodial Bitcoin Yield on Stacks

Abstract: 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 earn BTC yield without giving up custody of their coins. This mechanism introduces the concept of "protocol bonds" where users lock BTC and STX together in order to receive a target yield rate over a given bonding period.[1] Under Bitcoin Staking, rewards are generated from the BTC paid by Stacks miners competing for STX block rewards and transaction fees, but are distributed according to a waterfall structure that prioritizes paired BTC positions as the primary tranche, buffers yield through a reserve fund, and distributes residual yield to STX-only stakers. Bitcoin Staking builds upon Stacks' long-standing consensus mechanism, which has been live in production and distributed more than 4,200 BTC as consensus yield since January 2021.

The mechanism preserves self-custody of BTC, does not introduce slashing risk, and does not rely on custodial rehypothecation or secondary token payouts to BTC participants. By making BTC participation central to reward eligibility, Bitcoin Staking addresses this gap for self-custodial Bitcoin-denominated yield while creating a stronger economic role for STX within the system, aligning BTC capital formation with Bitcoin-native financial activity on Stacks.

1. Overview

Bitcoin is the largest pool of idle capital in the cryptocurrency economy, currently valued at over $1.3 trillion USD[2], yet BTC holders have limited options for earning yield on their capital. Despite significant market demand for Bitcoin yield, no system live in production, to our knowledge, offers Bitcoin-denominated yield without requiring wrapping, bridging, or custodial rehypothecation.

We propose Bitcoin Staking, an upgrade to the Stacks Proof-of-Transfer (PoX) consensus mechanism, that enables a BTC holder to retain custody of their coins while simultaneously earning BTC-denominated yield on their capital.

Stacks is uniquely positioned to do this because it already operates a live consensus mechanism that yields native BTC for consensus rewards.

---

[1] The terms "bond" and "bonding" are used in this white paper to describe the technical process of locking Bitcoin in an on-chain, permissionless smart contract. Protocol bonds are not financial instruments nor are they any other kind of contractual arrangement promising a contractually-binding rate of return.

[2] as of May 2026

Under PoX in its current form, Stacks miners spend BTC to compete for STX block rewards and transaction fees. The BTC spent by miners is distributed to eligible participants in a process known as “stacking.” Bitcoin Staking is an extension of PoX, which has distributed more than 4,200 BTC since January 2021.

Under the proposed Bitcoin Staking design, the yield generated from PoX operates in a similar manner: BTC is spent by Stacks miners competing for STX block rewards, and then is distributed to eligible staking participants. The primary change is how eligibility is determined for participants. PoX in its current form does not provide yield for locked BTC; only locked STX. Today, BTC is the reward asset, but eligibility for yield is determined by locked STX alone.

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. In this design, BTC becomes the yield-bearing asset, while STX functions as a capacity asset: the native token used for gas, consensus, governance, and as the variable that determines each participant’s share of the reward pool. This creates a direct economic link between STX demand and BTC yield, without exposing BTC stakers to credit risks of centralized BTC lending providers or the operational risks of locking Bitcoin on cross-chain bridges. There still is a participation path for STX-only staking. Both participation paths, protocol bonds and STX-only staking, are equally important to Stacks network security.

For each bonding period, the total BTC yield capacity and the target yield rate for that period are derived based on on-chain inputs including miner economics, reserve fund status, and prior bonding period performance. The system is designed to prioritize yield stability by adjusting capacity first, but the yield rate can also adjust when sustained shifts in underlying conditions warrant it. Capacity is allocated through an auction. Each bid specifies how much BTC the participant wants to lock and the lowest yield they'll accept on it. The auction is the sole mechanism by which BTC yield capacity is distributed, and it is open to any participant who meets the protocol bond (BTC + STX) commitment requirements.

BTC yield is derived from miners' willingness to bid BTC for Stacks blocks, where bids are driven by STX block rewards and network transaction fees. STX demand, in turn, is derived from current and anticipated Stacks on-chain activity. This matters for more than yield alone. A network that can attract meaningful BTC participation in a self-custodial way creates the economic base for broader Bitcoin-native financial activity. If BTC holders can earn yield while retaining control of their assets on Bitcoin, Stacks becomes a more credible venue for additional applications and financial primitives built around that capital base (e.g., lending stables against the locked BTC).

At launch, Bitcoin Staking will operate as a managed whitelisted program with capacity and fixed yield targets allocated by the Stacks Endowment. Over an expected 6-12-month bootstrap phase of progressive decentralization, the mechanism will gradually transition to the fully algorithmic end state described in Section 3. The bootstrap phase of Bitcoin Staking is described in Section 4.

This paper describes Bitcoin Staking and its implications. The sections that follow review the current PoX model, the proposed Bitcoin Staking mechanism, participation paths that govern reward distribution, the economic dependencies and tradeoffs of the design, and known risks.

1.1 Design Principles

Bitcoin Staking is designed to satisfy three design principles.

- **BTC holders earn rewards directly in BTC without giving up custody of their assets.** BTC remains locked, on the Bitcoin blockchain, with Bitcoin's security guarantees, under the participant's own keys using standard timelocks.
- **Bitcoin Staking builds on battle-tested Stacks infrastructure.** Miner competition, block production, and the routing of BTC through PoX remain intact.
- **Bitcoin Staking works for BTC and STX holders of all sizes.** It reduces barriers to entry for small holders (through pools) while providing clear capacity allocation mechanisms for participants of any size.

These principles define the mechanism. Bitcoin Staking is not a Proof-of-Stake system, it does not create a new consensus role for BTC in Stacks governance, nor does it alter Bitcoin L1.

2. Background: Proof-of-Transfer

Bitcoin Staking builds on Stacks' existing Proof-of-Transfer (PoX) consensus mechanism that went live in January 2021 [ref Stacks docs]. This section briefly reviews the current mechanism, PoX-4, to establish the baseline design.

2.1 PoX Consensus Mechanism

Proof-of-Transfer requires miners to transfer BTC in order to compete for block production rights. In each block interval, miners submit BTC bids; the probability of winning is proportional to the BTC committed relative to other miners.

The winning miner produces Stacks blocks and receives the STX block reward and transaction fees. The BTC transferred by all miners in that round forms the reward pool distributed to eligible participants.

STX holders participate in this distribution by locking STX for defined commitment cycles. Locked STX qualifies participants to receive a pro-rata share of the BTC reward pool. Participants who lock STX also serve as Stacks signers — or delegate their signing responsibility to a signer operator — contributing to block validation in Nakamoto consensus [ref SIP-021]. A signer's authority is proportional to the STX locked on their behalf. This role is described in more detail in Section 5.3.

2.2 Current Stacking (PoX-4)

Prior protocol versions used the term "stacking" to describe participant lockup. We propose "staking" to replace this term and reflect the expanded dual-asset mechanism introduced in Bitcoin Staking. Under existing PoX-4, eligibility for BTC rewards is determined solely by STX lockup. Participants commit STX for fixed cycles of 2,100 Bitcoin blocks. At each cycle boundary, eligible STX holders are assigned up to 4,000 reward slots and receive a proportional share of miner-transferred BTC. These reward slots

are the recipients of the PoX payments, two per Bitcoin block, for 2,000 Bitcoin blocks, followed by 100 blocks of "prepare phase," during which the PoX payments are sent to a burn address.

No BTC commitment by participants is required under PoX-4. Bitcoin Staking modifies this eligibility condition and the enrollment cycle while preserving the underlying miner bidding model described above.

2.3 Source of Yield

The source of BTC rewards in Stacks is miner competition for STX block rewards. Miner bidding is economically bounded. Rational miners will not commit BTC in excess of the expected value of the STX block reward and transaction fees. In equilibrium, BTC rewards distributed to participants are therefore a function of:

- The STX block reward schedule
- The market price of STX
- Transaction fee revenue on Stacks

Over time, miner incentives depend increasingly on sustained economic activity on Stacks rather than emissions alone. That activity may come from greater use of Bitcoin-native applications, higher transaction demand, and the expansion of financial activity built around BTC capital positioned on the network. The extent and pace of that transition will depend on ecosystem execution and adoption. We expect transaction fees from economic activity on Stacks to be a major source of consensus yield in the future.

Bitcoin Staking does not introduce a new yield source. It reallocates eligibility for an existing BTC reward pool whose size is determined by STX economics and network activity. The durability of BTC yield depends on the durability of those underlying economics.

Capital attracted by self-custodial Bitcoin yield is positioned to convert into broader economic activity on the network, including borrowing stable loans against locked capital, participating in DeFi strategies to enhance yield, payments, future privacy applications for Bitcoin, and other emerging use cases. To the extent that capital prefers Bitcoin-native, self-custodial infrastructure over bridged alternatives, Bitcoin Staking participation should drive transaction demand and fee revenue over time, resulting in a greater proportion of miner economics derived from transaction fees rather than block rewards alone.

3. Bitcoin Staking Mechanism

This section specifies the Bitcoin Staking mechanism and the technical design of the protocol bonds. It explains the dual-asset commitment model, bonding period structure, capacity allocation, the waterfall yield structure that determines reward distribution, and the activation conditions.

3.1 Protocol Bonds (Dual-Asset Commitment Model)

Participation in a protocol bond requires two cryptographically linked commitments: one on the Bitcoin blockchain and one on Stacks.

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.

An example of the unlock script:

```
None
# first, the stacks address (24 total bytes)
OP_PUSH_22 # 0x16
05${addrVersion}${addrHashBytes} # 22 bytes
OP_DROP # 0x75

# next, the lock (6 total bytes)
OP_PUSH3 # 0x03
${unlockHeight} # 3 bytes, little-endian
OP_CHECKLOCKTIMEVERIFY # 0xB1
OP_DROP #0x75

# finally, the unlock script
# this is arbitrary, up to 255 bytes
```

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 a BTC address where their 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.

Protocol bonds could theoretically exist between STX and other asset commitments such as stablecoins or tokenized real-world assets. Because Bitcoin Staking requires protocol bonds between BTC and STX, we may refer to these commitments as **Bitcoin bonds**.

Participants who prefer not to pair a BTC commitment may still stake STX alone. STX-only staking has no BTC capacity constraint, no whitelist, and no auction; it follows the existing standard signer cycle cadence with a 50,000 STX minimum for solo participation or the option to participate in a STX staking pool. For existing PoX-4 stackers, this path is effectively the same participation model with an updated reward distribution algorithm. This path is described in section 5.2.

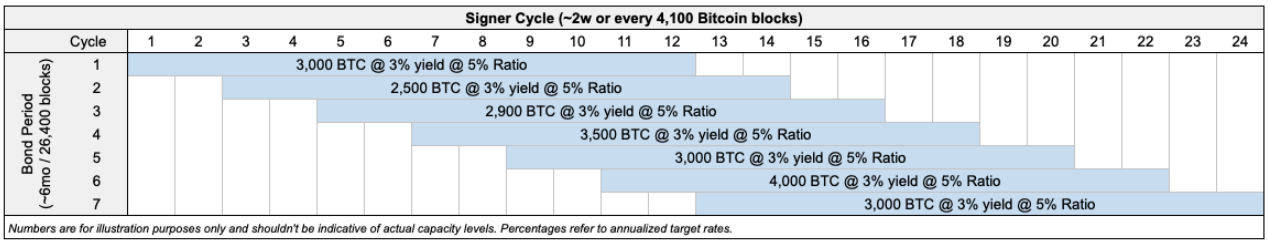
3.2 Bonding Periods and Timing

Bitcoin Staking operates on the following time units:

- **Auction Window:** 1 week before each new bonding period, parameters (target yield rate, bonding period capacity) for the bonding period are set and participants can submit bids to secure allocation.
- **Bonding Period**: 25,200 Bitcoin blocks (~6 months). The minimum commitment for paired BTC + STX staking.
- **Reward Distribution:** 1,050 Bitcoin blocks (~1 week). BTC rewards (self-custodial Bitcoin yield) are distributed once a week for the duration of the bonding period for all eligible participants.

- **Signer Cycle:** 2,100 Bitcoin blocks (~14 days). Stacks signer set updates every two weeks as part of PoX block validation under Nakamoto consensus (SIP-021). This cycle does not directly impact Bitcoin Staking, but it is a foundational time unit for Stacks.

Six concurrent bonding periods run in overlapping sequences, with a new bonding period opening every other signer cycle (approximately once a month, every 4,200 blocks). This staggered structure enables regular entry and exit windows without requiring all participants to lock and unlock simultaneously. Unpaired STX (STX staked without any corresponding BTC) follows the standard signer cycles.



Bonding period timeline

Each bonding period follows the same sequence of events:

1. **~7 days before opening:** Bonding period parameters (capacity and yield rate) are published. The auction window opens for bid submission.
2. **Auction clears.** Successful bidders receive a confirmation window to complete their L1 BTC timelocks.
3. **Day 0 (D0):** All paired assets must be locked ("bonded") by this point to be eligible.
4. **Day 172:** L1 BTC timelock expires (~10 days before the bonding period ends). This gives participants time to re-lock for the next period before the current one closes.
5. **Day 182:** Bonding period ends. STX lock expires on L2.

The specific durations of the auction window, confirmation window, and other phases will be defined in the implementation specification.

Lock renewal differs between L1 and L2

On L2, STX remains locked until the participant's committed bonding period ends. Participants may stake continuously by extending their commitment before expiry, or by setting their position to remain locked until they submit an unlock transaction.

On L1, automatic re-enrollment is not possible. Because timelocked BTC cannot be re-committed until the timelock expires, lock renewals on L1 require a new Bitcoin transaction. The ~10-day gap between L1 expiry (D172) and bonding period end (D182) exists specifically to give participants a window to construct and broadcast that renewal transaction.

Early Exit

Participants may fully exit their L1 BTC lock before expiry without a slashing penalty against their locked BTC by exercising an optional "Early Exit" feature. At the start of the bonding period, the participant constructs their timelock with a pre-approved, hashed spend option that can be exercised through a hashed transaction request co-signed by a designated signer set.

Exercising early exit forfeits all undistributed yield for the remainder of the bonding period. Paired STX remains locked for the full term and is not released early. This mechanism provides liquidity relief in extraordinary circumstances while preserving the STX commitment that anchors the participant's position.

3.3 Auction, Capacity Allocation and Ratio Requirement

The target yield and capacity for each bonding period are determined by mathematical functions derived from observed miner economics, reserve fund status, and prior-period participation data. The number of participants who can earn paired yield in a given bonding period is a function of capacity available and the size of individual positions.

Because capacity is limited, all available capacity is allocated to participants via an auction, where a bid is the lowest annualized yield the participant is willing to accept on a specified amount of BTC, paired with the required STX commitment at the protocol-set ratio for that bonding period. The auction is the sole mechanism by which BTC yield capacity is distributed, and it is open to any participant who meets the dual-asset (BTC + STX) commitment requirements.

Ratio Requirement. To participate in the auction for an upcoming bonding period, each bidder submits a bid specifying the BTC amount they're willing to lock and the yield they require. Bidders must also lock STX equal to a minimum fraction of their BTC commitment's value as a participation requirement. This minimum is set by the protocol, initially it will be set to 5%. The required STX quantity is computed at lock time using a trailing-average STX/BTC exchange rate derived from on-chain miner bid data, so participants know the exact STX amount needed to meet the floor. For example, at a 5% minimum with a computed STX:BTC ratio of 100,000:1, a participant locking 10 BTC must lock at least 50,000 STX to be eligible to bid - the auction itself clears on yield.

At initial launch, bid collection and clearing will be conducted off-chain. Ultimately these functions will be encoded in consensus (PoX-6) but during the bootstrap phase of Bitcoin Staking (PoX-5), they will be set manually by the Stacks Endowment.

The auction design will be finalized and agreed upon as part of the SIP approval process. The core principle of the auction is that capacity in each bonding period is allocated algorithmically through competitive bidding on yield; the specific clearing mechanism may evolve. Protocol activation and phased roll out are discussed in detail in sections 3.5 and 4.

3.4 Yield Distribution and the Waterfall Structure

The yield distribution mechanism determines how the BTC reward pool is allocated across participants in each bonding period. Bitcoin Staking uses a waterfall structure with defined tranche distribution priority.

1. **Tranche 1: Active Protocol Bonds.** All participants who have locked BTC paired with STX at the ratio requirement and whose allocation has been confirmed for the bonding period earn the target yield rate for that bonding period (expressed as APY) on their locked Bitcoin. The target rate applies consistently across all reward distributions within the bonding period.
    - Approximately 10% of the capacity in tranche 1 is reserved for community participation via pools, see Section 4.2 for more details.

2. **Tranche 2: STX-Only Stakers.** The miner revenue beyond Tranche 1 obligations, known as the cycle excess, is split between STX-only stakers and the reserve fund according to the reserve allocation percentage (proposed initial value: 85% to Tranche 2, 15% to reserve fund). The portion not allocated to the reserve fund is distributed pro rata among all STX-only stakers.
3. **Tranche 3: Reserve Fund.** The reserve buffers Tranche 1 payouts when miner revenue falls below the total yield obligations. The reserve is held in two sleeves: a BTC sleeve and a USD sleeve (stables or short-duration treasuries), with new contributions split at deposit time. In a drawdown, the BTC sleeve is drawn first; the USD sleeve is the last line of defense.

Eligibility. A participant's paired position is eligible for Tranche 1 yield if and only if: (a) they have been allocated capacity for the bonding period via the auction mechanism described in Section 3.3, (b) their full BTC amount is locked on L1 before D0 of the bonding period, and (c) their paired STX meets or exceeds the ratio requirement for that bonding period's auction.

Paired STX earns no yield. STX locked alongside BTC earns no yield; only the BTC portion of a protocol bond (ie, the paired BTC:STX position) earns yield. This creates a meaningful opportunity cost for the STX commitment, ensuring that the pairing reflects genuine economic alignment rather than costless ratio optimization. In the event that the paired BTC portion of a position exits the bond commitment early, the paired Stacks portion of that position remains locked for the duration of the bonding period and does not convert to a STX-only Tranche 2 position.

Drawdown Priority. In the event that the reserve fund is exhausted and yield in a given period falls below the target rate, the shortfall is distributed among paired BTC participants based on their market price of STX (in relation to BTC) at lock time. Positions locked when the STX market price was highest absorb losses first, providing greater protection to participants who locked when STX was less expensive. The STX market price at lock time is derived from the same on-chain miner bid data used to compute the minimum ratio floor — specifically, the trailing average implied STX/BTC exchange rate at the time the participant's L2 commitment was confirmed. This ensures the drawdown ordering uses a manipulation-resistant, on-chain price reference rather than an external oracle.

3.5 Protocol Activation and Phased Rollout

Bitcoin Staking requires community governance approval via the SIP process.

At activation, all existing stacking locks from prior PoX versions are released. Participants who wish to continue as either STX-only Stakers or via the BTC + STX protocol bond must re-enroll according to the parameters of their participation mode. This follows the precedent set by prior PoX upgrades.

The activation parameters and associated initialization conditions, including a minimum amount of committed STX sufficient to maintain network security, will be fixed prior to activation and published as part of the final implementation and governance proposal.

Bitcoin Staking will roll out in two phases: the bootstrap phase (PoX-5) and fully decentralized phase (PoX-6). Section 4 describes the bootstrap period, an operational framework rather than a new protocol design where parameters (capacity, ratio, and yield rate) are set through Endowment-mediated processes rather than the fully algorithmic consensus-encoded functions of PoX-6. Sections 5 and onward describe the fully decentralized phase (PoX-6) unless otherwise noted.

4. Bootstrap Phase (PoX-5) Program

This section describes the managed bootstrap phase that precedes the fully decentralized PoX-6 phase of Bitcoin Staking.

4.1 Overview

The initial rollout of Bitcoin Staking is a bootstrapping period, referred to as PoX-5, stewarded by the Stacks Endowment. This period is expected to run for roughly one year from PoX-5 activation. Its purpose is to demonstrate the mechanism at meaningful scale, accumulate real participation data, harden operational processes, and protect the broader Stacks community during the bootstrapping period by limiting exposure to abuse and attacks.

During PoX-5, the principal parameters — available capacity, target yield, BTC:STX required ratio and capacity allocation — are set manually by the Endowment for each bonding period. Bitcoin Staking in the bootstrap phase (PoX-5) will become progressively more automated and decentralized as the system transitions toward PoX-6.

PoX-5 will also include the following improvements to the staking process:

1. Removal of the cooldown cycle, enabling an STX staker to change their reward address before the next prepare phase without having to ‘miss’ a cycle.
2. Streamlining solo and pooled STX staking, e.g. by removing the need for pool operators to *commit* every cycle - this should meaningfully reduce the amount of work for pool operators while also reducing the risk of pool participants losing rewards due to a missed cycle.

4.2 Endowment-Mediated Capacity Allocation

During the bootstrap period, the Endowment computes the BTC yield capacity for each bonding period and then allocates that capacity to approved whitelisted partners prior to the beginning of each bonding period. This ensures the bootstrap period launches with committed, known counterparties. Approximately 10% of the capacity in tranche 1 is reserved for community participation via similarly selected pooling partners, preserving open access during the PoX-5 phase.

In PoX-6 and beyond, both channels converge into a permissionless auction described in Section 3.3, open to any participant with no partner preference.

4.3 Static Ratio Target

During PoX-5, the STX ratio target per bond is fixed for the sake of simplicity of program management. For example, a flat 5% or 8% applied uniformly. A static ratio simplifies partner onboarding and participant communication while the mechanism is earning trust while the program is in its early days.

4.4 Reward Distribution

As part of PoX-5, miner BTC bids are routed into a smart contract, autobridging to sBTC. The smart contract distributes rewards to participants on a weekly basis, either as BTC on L1 or sBTC on the L2 depending on each participant's preference.

Each weekly payout includes a built-in delay window during which a designated multisig can pause the distribution as a circuit-breaker safeguard. The pause cannot redirect rewards; it can only stop them, protecting against unforeseen issues or bugs that could compromise the payout and protocol security.

4.5 Initial Program Conditions

The economic model supports several viable configurations for the bootstrapping launch. The exact parameters will be finalized prior to activation and may vary based on committed partner capacity.

Proposed: *3,000 BTC capacity, 5% minimum STX ratio, 3% BTC APY. The minimum viable ratio-to-APY combination per the economic model.*

4.6 Reserve Fund Behavior

Throughout PoX-5, the Reserve Fund will remain in accrual-only mode in a contract with no access functions other than those controlled directly by consensus. The PoX-6 hard fork transition will specify the precise reserve fund behavior as part of the SIP process. This deferred activation serves a dual purpose of allowing the reserve to build up to a healthy baseline coverage and reducing the risk surface and complexity of the economic calculations during the initial bootstrapping phase.

4.7 Transition to PoX-6

As Bitcoin Staking matures, it will progressively transition from Endowment-mediated operation toward a consensus-encoded, fully decentralized operation. The staking-process improvements introduced in PoX-5 (cooldown removal, streamlined pool commitments) carry forward into PoX-6. The transition timing depends on observed performance, infrastructure maturity, and the readiness of the PoX-6 implementation. Activation parameters for PoX-6 — and any refinements to the algorithmic functions based on real participation data from the bootstrapping phase — will be specified in the corresponding SIP proposals.

5. Participation Paths

Bitcoin Staking supports three participation paths: native BTC paired with STX, sBTC paired with STX, and STX-only staking. The first two are variants of the protocol bond, differing only in the form of the

Bitcoin commitment. The third involves no Bitcoin commitment and functions as the existing PoX staking model with a new reward distribution path.

Specific enrollment flows, script requirements, pooled participation mechanics, and reward distribution details will be defined in a subsequent technical design document.

5.1 Protocol Bonds: BTC or sBTC Paired with STX

Protocol bonds combine a Bitcoin commitment with an STX commitment for one 6-month bonding period. The pairing ratio is set by the protocol, and eligibility is allocated through the auction described in Section 3.3. Participants earn BTC yield on the Bitcoin portion; the STX portion establishes capacity eligibility but does not earn yield directly.

The Bitcoin commitment may be satisfied in one of two forms: native BTC held under the participant's own keys on Bitcoin L1 via a timelocked UTXO, or sBTC held on Stacks.

Both forms grant access to the same protocol bond and the same yield. The choice of form affects where the Bitcoin sits during the bonding period and which participation flows are available. Notably, sBTC enables participation through L2 smart contracts, which opens the door to pooled participation, liquid staking tokens, BTC carry on market-making inventory, and other DeFi integrations.

5.2 STX-Only Staking

Participants may lock STX without a paired Bitcoin commitment. STX-only staking earns residual yield as Tranche 2 of the waterfall (Section 3.4), splitting the post-Tranche-1 excess with the reserve fund. It is uncapped and does not compete in the bond auction.

This path is effectively Stacks-native staking (formerly “stacking”) as it has existed under prior PoX versions, with the reward mechanics adjusted to reflect its new position in the waterfall. It is the default path for STX holders who prefer not to participate in consensus via the protocol bonds.

Every staker — whether participating through a protocol bond or STX-only — must be associated with a Stacks signer responsible for block validation under Nakamoto consensus. Stakers may run their own signer node or delegate to a third-party signer operator. Signer association is specified during enrollment and can be changed before any cycle's prepare phase.

5.3 Types of Weights Across Participation Paths

The Stacks protocol distinguishes three types of weight: reward eligibility, signing weight, and governance weight. Bitcoin Staking modifies only the first.

Reward eligibility determines whether a participant earns BTC yield in a given bonding period. It is a function of capacity allocation (determined by the auction), BTC locked, and whether paired STX meets the ratio requirement. Residual yield for STX-only stakers is determined by locked STX alone. This is the new mechanism introduced by Bitcoin Staking.

Signing weight determines a participant's authority in Stacks block validation under Nakamoto consensus. Governance weight determines voting authority on Stacks Improvement Proposals. Both are pure functions of STX locked; BTC plays no role in either. Participants may run their own signer or delegate to a signer operator in any participation path.

This separation is deliberate. Stacks consensus security depends on signers whose economic interest is aligned with the health of the network. Granting consensus or governance authority based on an external asset whose value is independent of Stacks would weaken that alignment.

6. Economic Model

This section analyzes the economic dynamics of Bitcoin Staking, specifies the yield framework, proposes initial parameters, and health metrics for the system.

6.1 Economic Dependencies

Bitcoin Staking creates an economically significant interaction between STX demand and BTC yield. The mechanism by which miner bids fund the BTC reward pool is described in Section 2.3. Because participants lock STX alongside BTC, participation affects STX supply, which affects STX price, which affects miner bid economics, which affects the reward pool, which affects participation incentives. The implications for yield are specified in Section 6.2. The risk of negative reinforcement during a persistent decline in demand for STX or mining is examined in Section 8.1.

By staking BTC in a protocol bond, participants take on STX price exposure proportional to their required pairing ratio. Over the bonding period, the total-position return is the BTC yield minus any STX price movement times the pairing ratio. This is the economic core of Bitcoin Staking participation.

Feedback loops of this kind produce volatility in both directions. Three design features reduce (but do not eliminate) volatility from the perspective of BTC stakers:

- **Waterfall structure.** The reserve fund absorbs most short-term miner revenue shortfalls before they reach BTC stakers; STX-only stakers absorb the residual as Tranche 2.
- **Bonding periods.** The ~6-month commitment enforces time separation between entry and exit, slowing feedback loops.
- **Capacity constraint.** Total BTC participation is capped at levels the system can sustain at the target yield, preventing oversubscription from compressing yields.

6.2 Yield Framework

Bitcoin Staking structures BTC yield as a target rate (expressed as APY) applied to paired BTC positions for the duration of a bonding period. The target rate is not a guaranteed return; it represents what the protocol expects to pay under normal operating conditions, and actual yield depends on miner revenue, reserve fund coverage, and waterfall distribution (Section 3.4).

Capacity is the primary adjustment variable. The protocol stabilizes yield by sizing each new bonding period through coverage-adjusted capacity rather than by adjusting the target rate. The target yield for a new period is set to the blended yield of the active bond book — the BTC-weighted average clearing yield across bonding periods currently outstanding — anchoring new offerings to what the protocol is already paying.

Yield is market-driven within protocol caps. The clearing yield for each bonding period emerges from auction competition (Section 3.3), bounded by two protocol-level limits: a 2.0x cap on clearing yield relative to target, and a 60% fill cap on allocations above target. Once a bonding period is active, its clearing yield is locked for the life of the term; the blended yield across the book evolves as older bonds roll off and new bonds enter at market-determined rates.

Yield stability is asymmetric. The waterfall (Section 3.4) pays Tranche 1 first, then allocates excess to STX-only stakers and the reserve fund. BTC yield stability for paired positions therefore comes at the cost of yield variability for STX-only stakers.

Yield is backstopped by variables outside any individual participant's control: the STX price (which drives miner bid economics), the capacity allocated for the bonding period, and the reserve fund balance. Bitcoin Staking targets but does not guarantee a fixed yield. Section 6.3 describes how the protocol monitors these backstops and responds when they deteriorate.

6.3 Coverage Monitoring and Health Metrics

The primary system health metric is the **Coverage Ratio**:

$$\text{Coverage Ratio} = \text{reward pool per cycle} \div \text{paired BTC obligations per cycle}$$

A ratio ≥ 1.0x indicates solvency: miner revenue is sufficient to pay all Tranche 1 obligations without drawing on the reserve. The protocol defines five response bands, each with a prescribed action:

Band	**Coverage Ratio**	**Protocol Response**
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 (yield and/or capacity)
Caution	1.0–1.5x	Reduce new bond sizes and monitor closely
Stressed	0.8–1.0x	Halt new bonds; deploy reserve to cover any shortfall
Distribution failure risk	< 0.8x	Deploy reserve fully; activate the distribution priority cascade

The target coverage multiple used in capacity sizing (proposed 2.0x, acceptable range 1.5–3.0x) is the primary governance lever for tuning these band thresholds. The coverage ratio and band-driven responses are computed deterministically on-chain from miner revenue, reserve balances, and active obligations.

7. Security Considerations and Trust Model

This section enumerates the trust assumptions and attack surfaces of Bitcoin Staking. The mechanism inherits the security properties of both Bitcoin (for L1 timelocks) and Stacks Nakamoto consensus (for block production and reward distribution). The focus here is on risks specific to Bitcoin Staking.

7.1 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.*

7.2 Attack Surface Analysis

This section examines the primary attack vectors identified to date. Where precise cost estimates require further analysis, these are flagged. Other unidentified attack vectors may exist.

Auction manipulation via inflated bids. An attacker could submit artificially high ratio bids to crowd out legitimate participants and monopolize BTC yield capacity. Because the auction clears from lowest yield upward, this requires the attacker to actually lock STX at extreme ratios, making the attack self-limiting. Capital cost scales with the BTC capacity sought, and the capacity ceiling bounds total system exposure even in a successful single-period attack. Sustained manipulation across multiple bonding periods would require maintaining inflated STX positions continuously, at significant opportunity cost.

Miner bid oracle manipulation. An attacker could submit artificially high or low miner bids to distort the implied STX/BTC ratio, affecting capacity and yield calculations. ATC-C validation filters outlier bids, and rolling average smoothing reduces the impact of any single cycle's distortion. The cost of sustained manipulation scales with the number of cycles the attacker must maintain artificial bids.

Sybil attacks on ratio distribution. An attacker could create many wallets with optimized BTC/STX splits to attempt to win more capacity in the auction. Because each wallet's ratio is computed individually and the auction ranks by ratio, splitting a position across multiple wallets provides no advantage — the ratio of each sub-position is identical to the ratio of the aggregate position. This attack vector is neutralized by the individual ratio computation.

Auction bid sniping. An attacker could observe other participants' bids during the auction window and submit a last-moment bid calibrated just above the expected required ratio, minimizing STX commitment while securing allocation. This is a form of strategic gaming common to on-chain auctions. Mitigations include commit-reveal submission (encrypted bids revealed simultaneously at clearing) or minimum bid increments. Specific anti-gaming mechanics will be defined in the implementation specification and may be refined based on observed behavior, as described in Section 4.7.

Reward distribution censorship. A signer with more than 30% of the total stacked STX (and therefore very high signing weight), even with a low BTC position (and therefore low reward eligibility), could potentially use their block validation authority to censor or delay reward distribution to other participants. However, there are existing mechanisms to ensure honest signer behavior, including loss of signer yield for misbehavior (enabled in PoX-6), that substantially reduce the likelihood of this risk.

8. Risks and Trade-Offs

This section describes the risks and trade-offs inherent in Bitcoin Staking. These are properties of the mechanism's design, not failure modes to be resolved.

8.1 Reflexivity Risk

The economic dependency described in Section 6.1 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.

This dynamic differs from STX-only stacking in an important way. Under STX-only stacking, if STX price declines, both the value of rewards and the value of the staked position decline proportionally. The yield as a percentage of the staked asset remains relatively stable. Under Bitcoin Staking, the staked position includes BTC, whose value may not decline proportionally with STX. Yield as a percentage of the combined position compresses more sharply because the denominator includes a non-correlated asset.

Three design features dampen this reflexivity: the waterfall, bonding periods, and capacity-constrained enrollment. See Section 6.1 for more detail.

The waterfall structure concentrates residual risk on STX-only stakers in Tranche 2. In sustained downturns, STX-only yield can compress significantly or reach zero, which may reduce STX staking participation and further reduce signing set security. If the reserve is depleted, drawdown reaches paired BTC participants via the priority ordering defined in Section 3.4.

Correlated vs isolated stress. The economic model distinguishes between isolated STX drawdowns (STX falls, BTC flat) and correlated drawdowns (BTC and STX fall together). The isolated case is the pessimistic scenario for the protocol: BTC obligations in USD terms are unchanged, but the STX-BTC ratio rises, compressing the miner-bid-denominated reward pool. The correlated case is softer: falling BTC reduces USD obligations proportionally, and the ratio movement is partially offsetting. Keeping a portion of the reserve fund in USD mitigates this stress. Target coverage (proposed 2x, range 1.5–3x) is sized primarily to absorb isolated STX drawdowns; correlated drawdowns consume less of the coverage buffer.

8.2 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 that capacity is allocated competitively, but does not remove concentration risk. Post-launch monitoring and potential parameter adjustment may be necessary if rewards become disproportionately concentrated.

8.3 Opportunity Cost

The costs are 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 (section 3.2) 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. The paired STX remains locked for the full bonding period in this scenario and does not earn yield (see section 3.4).

8.4 Protocol Upgrade & Transition Risk

Bitcoin Staking is a non-backwards-compatible upgrade. At activation, all existing stacking locks from prior PoX versions are released. Participants who wish to earn BTC rewards must enroll by completing one of the participation paths described in Section 5. This follows the precedent set by prior PoX upgrades; the operational playbook for protocol upgrades is well-established.

The transition still carries operational risk. A failed activation (for example, due to a contract bug) could impact the chain's ability to produce blocks. Mitigation strategies include extensive testnet validation, partner infrastructure audits, and staged activation contingent on minimum participation thresholds (Section 3.5).

A specific design property reduces transition risk further: Bitcoin Staking does not require BTC participation to function. If zero BTC is committed in a given bonding period, the protocol continues to operate as a STX-only staking system, with STX stakers earning the full miner-funded reward pool.

8.5 L1 Scalability & Transaction Cost Exposure

Bitcoin Staking requires one L1 Bitcoin transaction per enrollment. Auto-bridging miner revenue into sBTC requires periodically reconciling each miner UTXO. At scale, this might introduce considerations around Bitcoin transaction fees and block space consumption. During high-fee environments, consolidation costs may be material. Batching multiple UTXOs into a single transaction and handling the frequency of consolidation is possible and can reduce sBTC auto-bridging costs.

9. Future Work

Bitcoin Staking unlocks a range of extensions that become possible once meaningful BTC capital is positioned on Stacks. The system's decentralized, algorithmic design is intended as a foundation for further development through community governance rather than a static endpoint. The most interesting directions identified to date are below.

Liquid staking: Pairing sBTC with STX in smart contracts enables liquid staking protocols. Further development of liquid staking token standards and integration patterns will expand the range of DeFi activity that can be built around staked positions.

Self-custodial lending: The L1 timelocking mechanism used in Bitcoin Staking establishes a foundation for additional self-custodial Bitcoin primitives. A natural extension is self-custodial lending, where users retain custody of their BTC on L1 while borrowing against it on L2.

Algorithmic parameter refinement: The consensus-encoded functions that compute yield rate, capacity, and ratio targets (Section 3.3) should be evaluated against observed participation patterns, concentration metrics, auction clearing behavior, and manipulation attempts. These models may be refined via SIP governance as real-world data reveals opportunities to improve accuracy, responsiveness, or resilience.

Auction mechanism refinement: The auction design may be refined based on observed bidding behavior, including adjustments to the allocation algorithm, bid timing windows, clearing mechanics, and competitive dynamics across bonding periods. Potential improvements include sealed-bid variants and multi-round auction structures to reduce strategic gaming and improve price discovery.

Anti-gaming measures: The auction limits the marginal benefit of custodial aggregation and other known gaming vectors. Additional measures (e.g., a 1:1 mapping rule for wallets participating in bonding auctions) may be required during the bootstrap phase to preserve long-term system stability and will be explored as needed.

10. Conclusion

This paper has described Bitcoin Staking as an extension of Stacks' existing Proof-of-Transfer consensus: one that preserves the core structure of PoX while reallocating BTC-denominated rewards to protocol bonds where BTC and STX are locked together. Rather than introducing a new token incentive layer or a custodial yield scheme, Bitcoin Staking uses a dual-asset commitment model in which BTC remains self-custodied on Bitcoin L1 and STX continues to anchor participation within the Stacks network.

The significance of this design is that it offers a new path to Bitcoin-native yield while building on a proven mechanism that routes BTC through consensus, and has distributed more than 4,200 BTC since 2021. Bitcoin Staking therefore represents the evolution of a live economic system into one better aligned with the needs of BTC holders and the long-term growth of the Stacks network.

Bitcoin Staking is a practical and economically grounded next step for Stacks. In addition to expanding access to BTC-denominated rewards, Bitcoin Staking will make BTC participation a more direct source of capital formation on Stacks, deepen the economic role of STX within that process, and strengthen the foundation for broader Bitcoin-native financial activity on the network. In that sense, its importance lies not only in reward distribution, but in the kind of ecosystem it enables: one where productive BTC, self-custody, decentralized governance, and on-chain economic activity reinforce one another.

Appendix A: Bitcoin Staking Yield Model

This appendix specifies the structural relationships used to compute per-cycle BTC reward flows, coverage, reserve accumulation, residual yield to unpaired-staked STX, and target enrollment capacity. Symbols are defined in *Table A.1*; specific parameter values are set by the SIP and may be set differently for whitelisted PoX5 partners under bespoke deal terms.

Table A.1. Notation. Symbols denoting protocol constants are fixed by the network; market inputs are observed at any moment in time; design levers are set by SIP, governance, or partner deal terms.

Protocol constants (fixed by network)		**Design levers (set by SIP, governance, or partner deal terms)**	
B	STX coinbase per block	α	STX pairing per BTC (fraction of BTC value)
d	blocks per day	y	annual BTC yield. Offered rate before any auction clears; once terms are active, the enrollment-weighted blend of clearing yields across all active terms.
T	cycle length (days)	m	target coverage multiple
N	cycles per year, N = 365 / T. Per-cycle quantities are the default; multiplying a per-cycle flow by N annualizes it.	r	share of cycle surplus contributed to reserve
ρ	miner return on capital	u	USD share of new reserve contributions
φ	protocol transaction fees – additive to coinbase emissions	L	bond term (lock duration)
S	STX total supply		
s	unpaired-staked share of supply		
Market inputs (observed)			
P_{BTC}	BTC price (USD)		
P_{STX}	STX price (USD)		
κ	STX per BTC (= P_{BTC} / P_{STX}); the STX-denominated price of one BTC.		
State variables			
E	BTC currently enrolled		

A.1 Per-cycle waterfall. Each cycle of length T days, miner activity produces a BTC reward pool:

Daily STX miner reward (coinbase + fee):	$B \cdot d \cdot (1 + \varphi)$
Daily BTC bid flow (after miner ROC):	$B \cdot d \cdot (1 + \varphi) \cdot (1 - \rho) / \kappa$
Per-cycle reward pool, R_{pool}:	$B \cdot d \cdot (1 + \varphi) \cdot (1 - \rho) / \kappa \cdot T$
Annualized reward pool:	$R_{pool} \cdot N$

The BTC obligation (A) owed to bond stakers in a cycle is

$$A = E \cdot y / N$$

BTC-denominated and unaffected by USD price moves.

The cycle coverage ratio (C) is

$$C = R_{pool} / A$$

with $C \geq 1$ indicating that the cycle pool covers obligations on its own.

A configurable share r of any surplus is contributed to the protocol reserve,

$$\Delta R = \max(0, R_{pool} - A) \cdot r$$

of which a fraction u of *each new contribution* is converted to USD at the time the contribution is made and the remainder is retained in BTC. This gives the per-cycle sleeve allocations:

USD added to reserve this cycle:	$\Delta R_{USD} = u \cdot \Delta R$
BTC added to reserve this cycle:	$\Delta R_{BTC} = (1 - u) \cdot \Delta R$

The residual after obligations and reserve is distributed to the unpaired-staked STX pool, producing an annualized residual yield:

BTC residual per cycle:	$R_{pool} - A - \Delta R$
USD value of residual:	$(R_{pool} - A - \Delta R) \cdot P_{BTC}$
USD value of unpaired-staked STX pool:	$s \cdot S \cdot P_{STX}$
Annualized STX yield, Y_{STX}:	$(R_{pool} - A - \Delta R) \cdot P_{BTC} \cdot N / (s \cdot S \cdot P_{STX})$

Both s and S evolve over the protocol's life – emission increases S gradually, and s shifts as STX staking expands or contracts. Plugging in current values produces a current-state yield, not a constant. Paired STX is locked collateral and earns no yield during the bonding period.

The protocol must size enrollment such that obligations remain serviceable at the chosen offered yield. Capacity quantities relate to the underlying enrollment (E). The system capacity (E_{sys}), the enrollment level at which $C = 1$, and the target capacity (E_{max}), the safety-adjusted offered supply used in issuance, are:

$$E_{sys} = R_{pool} \cdot N / y \quad , \qquad E_{max} = E_{sys} / m$$

Each unit of BTC enrolled requires STX collateral pairing of value α times the BTC value, so the total paired STX (in tokens) is obtained by valuing the pairing requirement in USD and converting at the STX price:

USD value of pairing requirement:	$E \cdot P_{BTC} \cdot \alpha$
Total paired STX, Q_{STX}:	$E \cdot P_{BTC} \cdot \alpha / P_{STX}$

Appendix B: Bonding Period Schedule

Unit	Interval	Duration	Definition
Signer cycle	2,100 blocks (14d)	2,100 blocks (14d)	Existing PoX unit; signer set updates, STX-only enrollment, block validation.
Prepare Phase		100 blocks (1d)	Last 100 blocks of each signer cycle
Bonding period	25,200 blocks (6mo)	25,200 blocks (6mo)	Full term of a single bond, D0 to D182. Six run concurrently, staggered.
Distributions (aka Payouts)	1,050 blocks (1wk)	At block-height	every 1,050 blocks, 24 per bonding period
Re-lock Phase		1,400 blocks (10d)	final 1,400 blocks in a bonding period D172 → D182, L1 expired, STX still locked; time to construct next L1 lock.
Enrollment Period (PoX-5)	4,200 blocks (1mo)	1,050 blocks (1 wk)	New bonding period opens once a month. During PoX-5, the two principal parameters — available capacity and capacity allocation — are set manually by the Endowment for each bonding period.
Auction period (PoX-6)	4,200 blocks (1mo)	TBD	After PoX-6 activations, new bonding periods open once a month, set by permissionless auction
Bidding Phase		TBD	bid submission, before a bonding period opens.
Confirmation Phase (L1 Lock up)		TBD	PoX-5, issued on a rolling basis, must complete L1 lock up before D0 of bonding period