Blockchain Focus

BabylonChain: Two Birds with One Stone

Sep 03, 2024
Jaehyun Ha | Research Analyst
jaehyunha@prestolabs.io

Summary

- Currently, Bitcoin holders and PoS chains have their own concerns. Bitcoin holders struggle to utilize their assets efficiently (i.e., generating yields), while PoS chains face security-related issues like bootstrapping, low liveness resilience, and long stake unbonding periods.

- As a two-sided marketplace, Babylon works as a bridge by putting bitcoins to work by staking them to help secure PoS chains. Babylon's remote staking protocol provides strong security guarantee to both the consumer chain (PoS chain) and the provider Bitcoin holders by its novel implementation with Timestamping Protocol, Finality Gadgets, and Bond Contracts.

- Babylon's Bitcoin Staking Protocol can be utilized in a wide variety of consensus protocols used by consumer chains, thanks to its modular design. Any blockchain network that wants to leverage Bitcoin's security and liquidity on top of their protocol can benefit from Babylon. Some promising use cases include DeFi, forkless Layer 2 rollups and oracles.

Introduction

Bitcoin assets sit idle. PoS chains need capital. Why not unlock their combined potential?

Bitcoin, often referred to as “Digital Gold”, stands as the most valuable and secure cryptocurrency in the world. Its strength lies in its primary purpose to serve as a decentralized peer-to-peer digital currency, prioritizing simplicity and security over any other properties. Bitcoin’s scripting language is intentionally limited, preventing it from performing complex computations or creating loops, which significantly reduces the potential for bugs and attack vulnerabilities. The legitimacy of its ledger is secured through the Proof-of-Work (PoW) protocol, which requires miners to use immense computational power, making it infeasible for an attacker to compromise the chain. This unwavering focus on simplicity and security is why Bitcoin is revered as digital gold today.

However, these advantages of Bitcoin come with a trade-off, resulting in **limited programmability and usability**. Unlike newer Proof-of-Stake (PoS) blockchains, Bitcoin is difficult to leverage for yield-generating activities such as staking. As a result, Bitcoin holders (referred to as HODLers, in crypto community) cannot do much other than just rely solely on the appreciation of its spot value as their investments. In today’s financial landscape, merely holding an asset often presents extra opportunities to generate additional yield through reinvestment. Therefore, it is very unfortunate that a digital asset with such a substantial market cap like Bitcoin remains largely untapped in this regard.

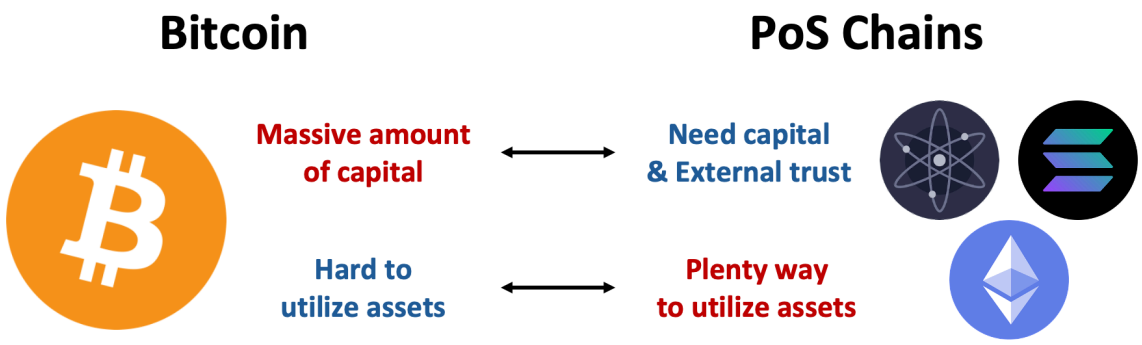
Speaking of which, let’s also talk about **PoS chains**. PoS, adopted by newer blockchains such as Ethereum 2.0 and Solana, secures the network by requiring validators to lock up their cryptocurrency holdings (i.e., staking), which can be slashed if malicious behavior is detected. The more tokens that are staked, the higher the crypto-economic security of the chain. Unlike Bitcoin, PoS provides better opportunities to participate in yield-generating events. Individuals can benefit just by holding (staking) tokens on the chain as validators, and they can also grow their assets through methods such as liquidity provision (LP) or DeFi lending. Moreover, PoS is energy-efficient, as it does not require mining from validators to secure its consensus. Due to these advantages, the mainstream has been shifting from PoW to PoS over the past few years.

However, despite the advantages of PoS, there exists some **security and user experience degradation issues** stemming from the fundamental limitations of the PoS protocol. One of the most apparent problems is the bootstrapping issue. Emerging PoS blockchains (e.g., Cosmos Zones) with low token valuations struggle to attract capital due to a small total staking amount, resulting in weak security, and find it challenging to attract high-value DApp projects. Moreover, due to the inherent limitations of the PoS protocol itself, there are additional security issues, such as low liveness resilience and insufficient resistance against non-slashable long-range attacks without relying on an external trust source.

In a nutshell, Bitcoin has a massive amount of capital, but lacks ways to utilize those assets. PoS chains offer plenty of ways to utilize assets, but they require a sufficient amount of capital and external trust sources for security. Combining these insights, **Bitcoin and PoS chains are perfectly complementary**. So, how about creating a protocol that unlocks their combined potential? This is the key concept of *Bitcoin Staking Protocol* from **Babylon**: leveraging Bitcoin assets to secure PoS chains, and simultaneously generate yields to Bitcoin holders. This sounds very cool, but at the same time, there are a lot of challenges for making a “Good Bitcoin Staking Protocol” with strong security guarantees. Through this full-report, let’s explore what constitutes a “Good Bitcoin Staking Protocol,” what are the challenges

encountered in the implementation process, and how Babylon has addressed these issues through technical advancements.

Figure 1: Bitcoin and PoS chains are Complementary



Source: Presto Research

Problem Statements For PoS Chains

In this section, we dive deeper into the issues associated with PoS chains and Bitcoin as outlined in the introduction, and clearly define the problem statements. We first address the three inherent security limitations of PoS protocols, and then discuss the difficulties involved in incorporating Bitcoin into yield-generating activities.

Statement #1: The BootStrapping Problem

The bootstrapping problem in PoS chains refers to the challenge of attracting capital and validators right after the launch due to inherent security issues. When a PoS chain is newly launched, its native token typically has low value and low market capitalization; this property makes the network susceptible to various attacks that can compromise the integrity of the PoS protocol.

The low token valuation allows individuals or groups to buy a substantial amount of tokens at a relatively cheap price, potentially leading to centralized staking. This centralization increases the likelihood of safety attacks, such as censoring transactions or reverting the chain. Moreover, since the maximum penalty an attacker can face is the amount of tokens they have staked (which the value is relatively low in a newly launched network), attackers might find the potential loss acceptable. They may proceed with malicious activities, even if their stake gets slashed due to protocol violations.

These risks, coupled with the lack of a proven track record for security and reliability, often deter potential validators from committing their funds to new PoS chains. Validators may fear potential losses if the network fails or is attacked. To mitigate this issue, PoS chains often employ strategies such as offering high initial staking rewards or forming partnerships with established entities to bootstrap validator participation. However, these methods can lead to high inflation rates and the centralization of staking power; which may significantly boost chain usage in the short term, but likely to have negative impacts in the long run.

Statement #2: The Low Liveness Resilience Problem

Proof-of-Stake (PoS) protocols face a **liveness resilience problem**, which refers to the ability of the protocol to continue making progress and confirming transactions even in the presence of adversarial validators. Different PoS protocols exhibit varying degrees of resilience to adversarial actions. For instance, protocols like Snow White and Ouroboros have relatively high liveness resilience, tolerating adversarial fractions up to 1/2.

However, PoS protocols with accountable safety, such as Tendermint and Gasper, cannot ensure liveness beyond an adversarial fraction of 1/3. Here, accountable safety means that the protocol not only maintains a consistent state across the blockchain but also identifies and punishes misbehaving validators through mechanisms like slashing (more explanation provided in the following section). This low limitation of 1/3 is rooted in the Byzantine Fault Tolerance (BFT) model, which underpins the security of these protocols. According to BFT theory, a supermajority (typically two-thirds) of honest validators is required to maintain both safety and liveness. When more than one-third of validators are adversarial, they can prevent the formation of this supermajority by either voting for conflicting blocks or withholding their votes, effectively stalling the protocol and preventing it from making progress.

Statement #3: The Long Stake Unbonding Period Problem

The most critical issue in PoS chains (even with accountable safety) is **the long stake unbonding period problem**. Contrary to the advantage of PoS chains, where blocks are finalized within seconds or minutes, stake unbonding usually takes about a few days to weeks. This long stake unbonding period diminishes the user experience, as stakers cannot participate in the PoS protocol, their staked assets remain locked, and are unable to receive staking rewards during this interval. This not only results in loss of potential earnings for the stakers, but also reduces overall liquidity within the PoS system.

Figure 2: Stake Unbonding Period of PoS chains

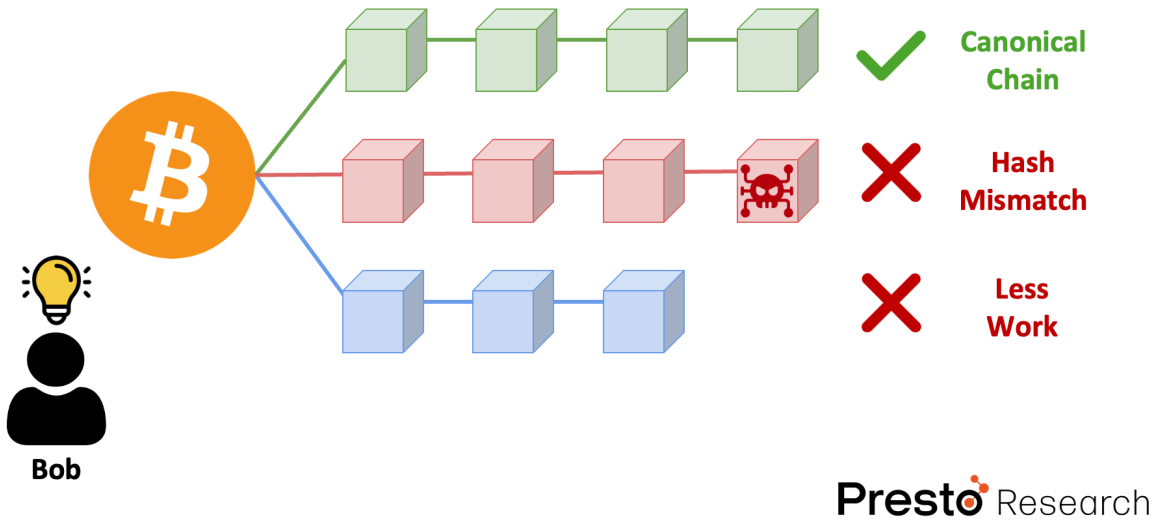
PoS Chains	Stake Unbonding Period
Ethereum 2.0	13 days[1]
Solana	2 - 4 days
Polygon	3 - 4 days
Avalanche	14 days
Cosmos	21 days
Polkadot	28 days

1. According to the authors of the paper "Bitcoin-Enhanced Proof-of-Stake Security: Possibilities and Impossibilities (Oakland '23)", this was calculated for 130K attesters with an average balance of 32 ETH to accurately model the targeted attester numbers on PoS Ethereum using weak subjectivity analysis from D.Park and A.Asgaonkar.

So then, despite the inconvenience, why do most PoS chains maintain a long stake unbonding period? The answer to that lies in the need **to mitigate the posterior corruption attack** (i.e., the long range attack) against PoS chains. To fully understand this, it's necessary to have a certain level of understanding of terminologies like fork-choice rule and weak subjectivity; so let's take a closer look at those concepts.

Let's assume a scenario (Figure 3) where Bob wants to join and participate as a node in a permissionless blockchain protocol that has been operating for a long time. In such blockchains, there isn't a centralized server distributing the legitimate chain to each client. Instead, each peer propagates what they believe as the canonical chain to other peers, and each client determines which chain to follow based on consensus rules. So, if the blockchain that Bob wants to join is the **Bitcoin** network, how would he identify the canonical chain and sync with it? The answer is simple—he would just follow the chain with the most work (i.e., computation), commonly known as the "Nakamoto Consensus" or "The Longest Chain Rule". Even in the case where Bob receives 100 different chains, there's no need to worry. He can independently verify the legitimacy of all those chains by re-computing the hash (since the previous block hash and nonce values are all recorded in the chain), and choose the one he will follow by comparing the amount of work.

Figure 3: Can Bob (a newly joined node) tell which one is the canonical chain? - Bitcoin



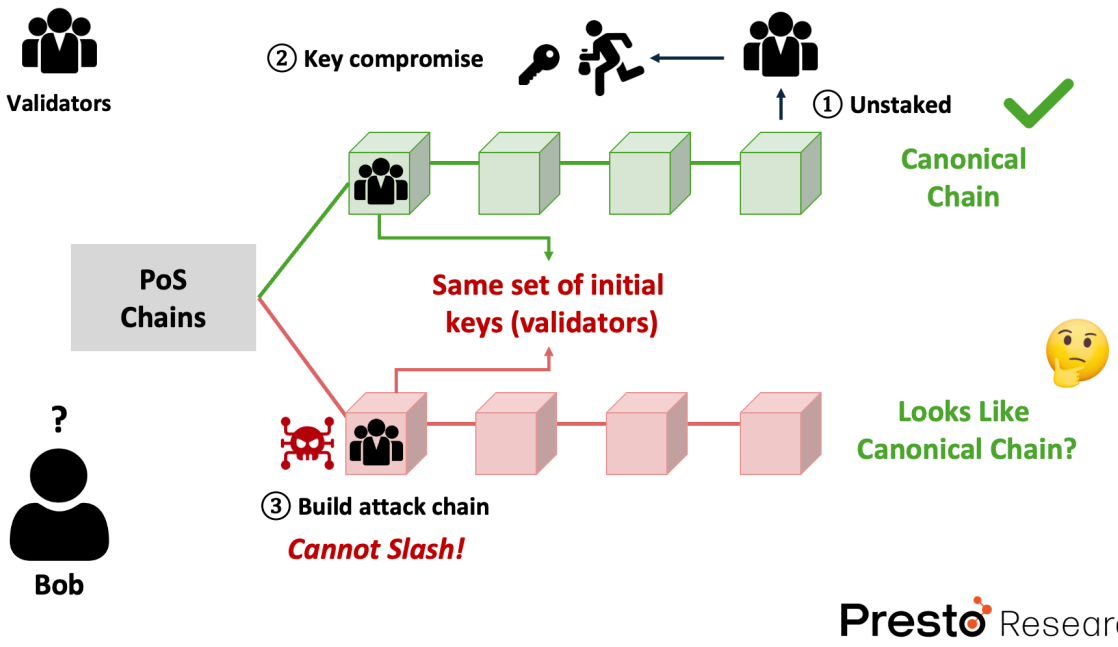
Source: Presto Research

However, if the network that Bob wants to join is a **PoS chain**, the situation becomes more complex. Just like in the previous example scenario, how would Bob choose the canonical chain, if he receives multiple conflicting chains? In PoS chains, a consensus is typically achieved by validators (entities selected based on the amount of cryptocurrency they hold and are willing to "stake" as collateral) who propose and vote on blocks, and the validity of the chain is determined by the collective agreement of these validators. In the case of Ethereum 2.0, validators are incentivized to follow and vote for the chain with the highest cumulative weight based on the most recent votes by receiving attestation awards (i.e., the canonical chain). If a validator makes a contradictory vote, they face penalties (slashing), where a portion of their staked assets is forfeited. Under this system, validators are encouraged to adhere to the canonical chain and maintain proper synchronization with the network. Because of these rules, there shouldn't be forks in PoS chains from the beginning—an attacker attempting a safety attack would only harm themselves. In fact, when we examine Ethereum's reorg depth data, we see that situations where the depth exceeds 1 are extremely rare (i.e., serious forks do not happen).

Despite these rules, there still exists a significant threat to PoS chains, which is the **posterior corruption attack**. In this attack, an attacker compromises historical validators' private keys which they have already participated in the consensus. By doing so, the attacker can potentially rewrite the blockchain's entire history by making a fork from genesis block, and cause significant disruptions in the network. We just said that such an attack will be worthless, because there is slashing in the PoS system. How can this happen?

This attack can happen because **attackers cannot be penalized through slashing since the stake has already been withdrawn.** In this scenario, attackers gain control of an old validators' (who already unbond their stake) private key, either by purchasing it or, even worse, by hacking after they have already unbonded their stake. Using this key, they can create a fraudulent chain (Figure 4) without much effort, as PoS systems do not require much work for generating blockchain. Additionally, since the timestamps of the canonical chain blocks are publicly available, attackers can simply replicate these timestamps in their chain, making it appear more legitimate.

Figure 4: Can Bob (a newly joined node) tell which one is the canonical chain? - PoS chains



Source: Presto Research

When Bob newly joins this PoS chain, he faces a significant challenge: distinguishing which chain is the canonical one. From his perspective, both chains might seem equally valid, as they are signed with keys from legitimate validators, feature consistent timestamps, and show regular validator rotations. In such a situation, Bob has no choice but to rely on external sources (e.g., block explorers, node operator groups) of trust to identify the correct chain. By consulting these sources to identify a reliable checkpoint, known as a **weak subjectivity point**, Bob can synchronize with the chain from that point onward by connecting with other peers.

Weak subjectivity is the key reason why PoS chains often have long stake unbonding periods. Since the weak subjectivity point ultimately depends on social consensus from external trust sources, and this consensus can take time to form, typically through channels like Discord or Telegram, PoS chains are forced to enforce these extended unbonding periods. The authors of the paper "Bitcoin-Enhanced Proof-of-Stake Security: Possibilities and Impossibilities" (foundational paper of Babylon) claim that without help from external trust sources, it is theoretically impossible for PoS chains to completely prevent posterior corruption attacks (i.e., the slashable safety).

Problem Statement for Bitcoin HODLers

Bitcoin has the largest market cap among all existing cryptocurrency assets (approximately 1.2M trillion USD as of Aug 2024) and holds over half of the entire crypto market share, around 56%, making it the leading blockchain in the industry. As a blockchain, Bitcoin demonstrates exceptional performance in decentralization and security, although its scalability is somewhat lacking. In terms of decentralization, unlike emerging PoS chains where a large amount of initially issued tokens are distributed to early investors or foundation members, Bitcoin has been owned by miners dispersed worldwide throughout its long operational history (although this also has miner centralization issues, it is better off than new PoS chains). In terms of security, due to its Proof-of-Work based nature, chain reorganization is economically infeasible. Various studies have shown that exploiting Bitcoin's overlay network and network layer to partition the Bitcoin network is very costly, making it known for being significantly more secure than other chains.

Despite Bitcoin's solid performance as a blockchain, Bitcoin holders face some dissatisfaction. Unlike other mainstream PoS-based blockchains such as Ethereum and Solana, opportunities to participate in yield-generating activities are highly limited, leaving most assets idle. To participate in yield-generating events like DeFi lending with Bitcoin, bridging to another chain in a form of wrapped Bitcoin (i.e., wBTC) is required. However, wBTC is primarily used as collateral, and since collateral assets generally have lower volatility, the yield for holding or lending them tends to be lower than other assets. In fact, the annual percentage yield (APY) for wBTC on DeFi platforms such as Aave, Compound, and Blockchain.com often remains below 1%, making it challenging to achieve significant returns. Even so, wBTC currently maintains a market cap of about $9 billion as of Aug 2024, which is approximately 0.77% of Bitcoin's market cap, leaving most Bitcoin assets idle.

To recap, the problems statements for PoS chains and Bitcoin holders can be summarized as below.

Three problems for PoS chains:

1. **The bootstrapping problem** in PoS chains arises when a newly launched network, with low token value and market capitalization, becomes vulnerable to attacks due to potential centralization of staking power and insufficient deterrents for malicious activities, which in turn deters validators from participating.

2. PoS protocols with accountable safety face the **low liveness resilience problem**, which ensures liveness of the protocol only if less than one-third of the validators are mallory.

3. **The long stake unbonding period problem** in PoS chains exists because they rely on external trust sources to prevent posterior corruption attacks, and those trust sources need time to reach a social consensus.

Problem for Bitcoin holders:

1. Bitcoin holders face **limited yield-generating opportunities**, often requiring the use of wrapped Bitcoin (wBTC) for DeFi activities, which offers low returns—typically below 1% APY—leaving the majority of Bitcoin assets idle.

Implementing “A Good Bitcoin Staking Protocol”

Reflecting on the problem statement we just discussed, it can be said that PoS chains require capital and external security guarantee for their sake, while Bitcoin needs a good playground to generate yield. The most straightforward way to solve the respective issues of both is simple: to create a Bitcoin staking protocol.

How Can We Define “A Good Bitcoin Staking Protocol”?

Then, how are we going to implement such a Bitcoin staking protocol? A naive approach is utilizing a cross-chain bridge; where each Bitcoin holder sends their Bitcoins to the trusted third-party bridge owner’s Bitcoin address, lock it, then use the issued wBTC as the staking asset in the PoS-based blockchain.

This approach, however, falls short of being “a good Bitcoin staking protocol”. One significant drawback is that when Bitcoin holders wish to redeem their wrapped Bitcoin for actual Bitcoin, they are forced to depend on a trusted third party to facilitate the transfer. The recent surge in cross-chain bridge exploits further exacerbates concerns (*Cross-chain Bridge Exploits: There Are More Risks Than You Know*, Jaehyun Ha, 03Jun24), making Bitcoin holders wary of such protocols.

The same goes for PoS chains. The fundamental security problems of PoS chains, as mentioned in the problem statement section, remain unresolved. For example, such a naive approach does not provide any defense against posterior corruption attacks or offer a solution to the long stake unbonding period problem (as the stake unbonding process still relies on external trust assumptions).

Considering these points, a naive Bitcoin staking protocol that simply leverages bridging cannot be called a good Bitcoin staking protocol. **A good Bitcoin staking protocol must be able to provide strong security for both the Bitcoin holders and PoS chains**. Then, what security properties are essential to implement such a good Bitcoin staking protocol?

Security properties of “a good Bitcoin staking protocol”:

1. The first is **slashable security**. To mitigate safety attacks like posterior corruption attacks, the Bitcoin stakes of those who violate the protocol must be slashable before they can unbond their stakes.

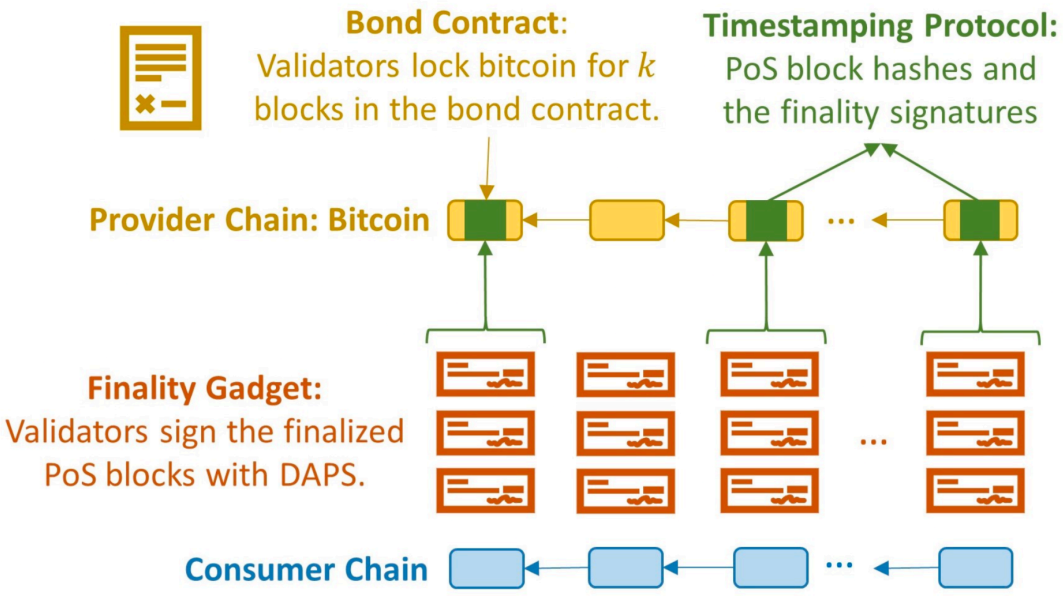
2. The second is **staker security**. If a Bitcoin staker follows the PoS protocol honestly, they should be able to withdraw their funds or unbond their stake whenever they want. This requires the system to be resistant to withdrawal censorship and support trustless stake unbonding.

3. Finally, there’s **staker liquidity**. Given that the stake unbonding period in current PoS protocols can be lengthy due to the need for social consensus, a fast and secure unbonding process is required, without having to go through this prolonged procedure.

How Does Babylon Implement Such a Good Bitcoin Staking Protocol?

Babylon implements "a good Bitcoin staking protocol" with **remote staking**. Remote staking is a concept where assets from one blockchain (i.e., the provider chain) are used to secure a different blockchain (i.e., the consumer chain), without requiring the assets to leave the provider chain. In the context of Babylon, Bitcoin serves as the provider chain, to enhance the security of PoS consumer chains. Babylon's approach to creating a good Bitcoin remote staking protocol is centered around the integration of three following core components: **the Timestamping Protocol, the Finality Gadget, and Bond Contracts.**

Figure 5: Babylon's Remote Staking Protocol

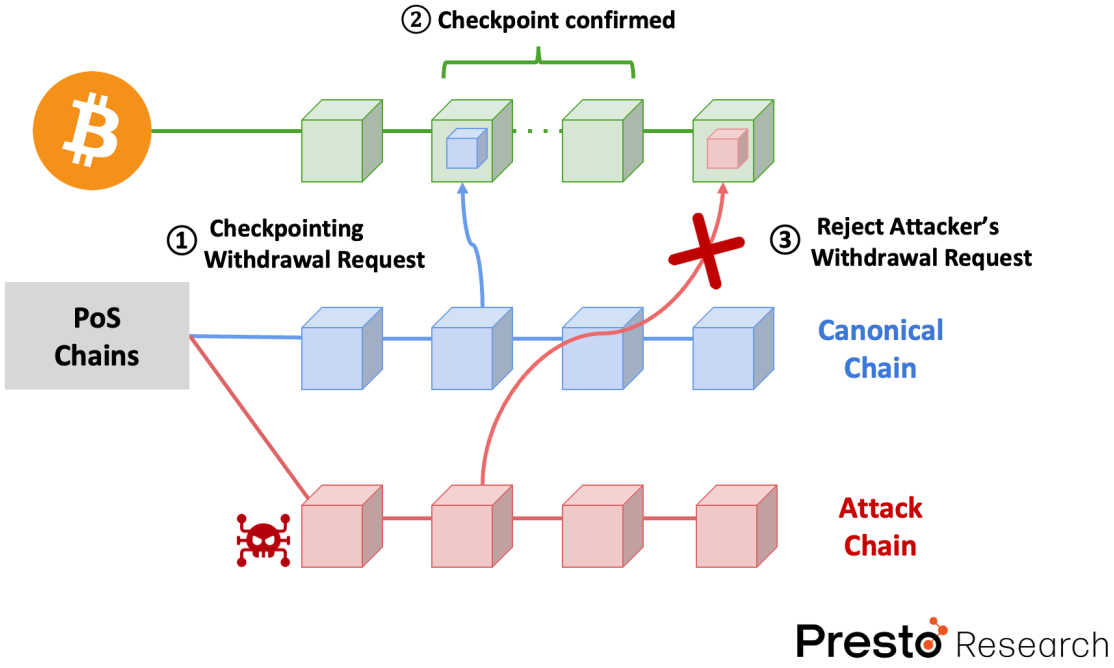


Source: "Remote Staking with Economic Safety", X.Dong et al,.

The Timestamping Protocol (Figure 6) is essential for ensuring the consistency of the blockchain data across both the Bitcoin and the PoS chain during the Bitcoin staking process. Simply explained, it is a process where the Bitcoin network is used as a timestamping server (i.e., external trust source) to checkpoint updates from the PoS chains. It involves recording the hashes of the PoS consumer chain blocks onto the Bitcoin blockchain chain, along with the confirming signatures from validators.

The main purpose of this timestamping protocol is to **improve slashable security and staker liquidity**. As mentioned in the previous section, every PoS chain must rely on external trust sources, for mitigating posterior corruption attacks (i.e., slash before the attackers unbond their stake). Here, Babylon chose Bitcoin, the most secure blockchain, as its external trust source. Once a checkpoint of a PoS chain is embedded deeply enough in the Bitcoin blockchain (i.e., 6 blocks deep), it becomes probabilistically irreversible. This ensures that any checkpoints from an attack chain, recorded later on Bitcoin, are regarded as fraud and simply ignored; thus a posterior corruption attack can be easily mitigated. In other words, if an attacker launched an attack before they unbonded their stake, they would be slashed. If they already unbonded their stake, there's still no problem, since their attempt will be easily identified and blocked by Bitcoin Timestamping protocol.

Figure 6: Timestamping Protocol



Source: Babylon, Presto Research

Not only enhancing the security against safety attacks; the protocol also helps reduce the delay of stake unbonding. Unlike existing solutions rely on social consensus, in Babylon's timestamping protocol, it's only necessary for the PoS block containing the request to be checkpointed on Bitcoin before any conflicting checkpoints and confirmed deeply enough (6 blocks) to approve withdrawal requests. Since this process takes hours instead of weeks, the withdrawal delay can be significantly reduced.

Furthermore, the timestamping protocol also requires the timestamping of the provider chain blocks within the consumer chain blocks to help the clients to track changes in the validator set over time. As the validator set evolves due to staking and unstaking activities, the timestamped data allows validators and clients to verify the eligibility of the current validator set.

The Finality Gadget is another crucial component in Babylon's design; it introduces an **additional layer of finality** to the consensus process of the consumer chain. In standard PoS chains, blocks are considered final after they receive enough validator votes, but this process can be vulnerable to attacks if a majority of validators act maliciously. The Finality Gadget addresses this vulnerability by requiring each validator to sign a single block at each height with a double-authentication-preventing signature (DAPS).

If a validator attempts to sign multiple conflicting blocks, their private key can be extracted and exposed, leading to the automatic slashing of their stake. This mechanism ensures that once a block is finalized using the Finality Gadget, it is impossible to revert without severe consequences for the validators involved. By ensuring that only one block can be final at each height, the Finality Gadget provides a strong deterrent against equivocation during the staking process.

The **Bond Contracts** are the final key component that facilitates secure Bitcoin staking without relying on complex smart contracts. Babylon's design acknowledges that Bitcoin, the provider chain, does not support Turing-complete smart contracts, which limits the complexity of operations that can be performed directly on the Bitcoin blockchain. To address this limitation, Babylon implements a novel bond contract mechanism using Bitcoin's existing scripting capabilities, specifically multi-signatures and timelocks.

A bond contract first requires validators to lock a portion of their Bitcoin as a deposit. This deposit is held in a bond contract on the Bitcoin blockchain for a predetermined period, measured in Bitcoin blocks. During this period, the validator is obligated to perform its duties on the consumer chain—such as participating in consensus mechanisms or validating transactions. The locked Bitcoin serves as collateral, ensuring that the validator has a financial stake in acting honestly and responsibly. This simple locking mechanism ensures that the Bitcoin cannot be spent until a certain number of Bitcoin blocks have passed, providing a secure exit option for the staker. Even if everything else fails, Alice can always retrieve her Bitcoin once the time lock expires, as long as the Bitcoin network is operational (i.e., **the staker security**).

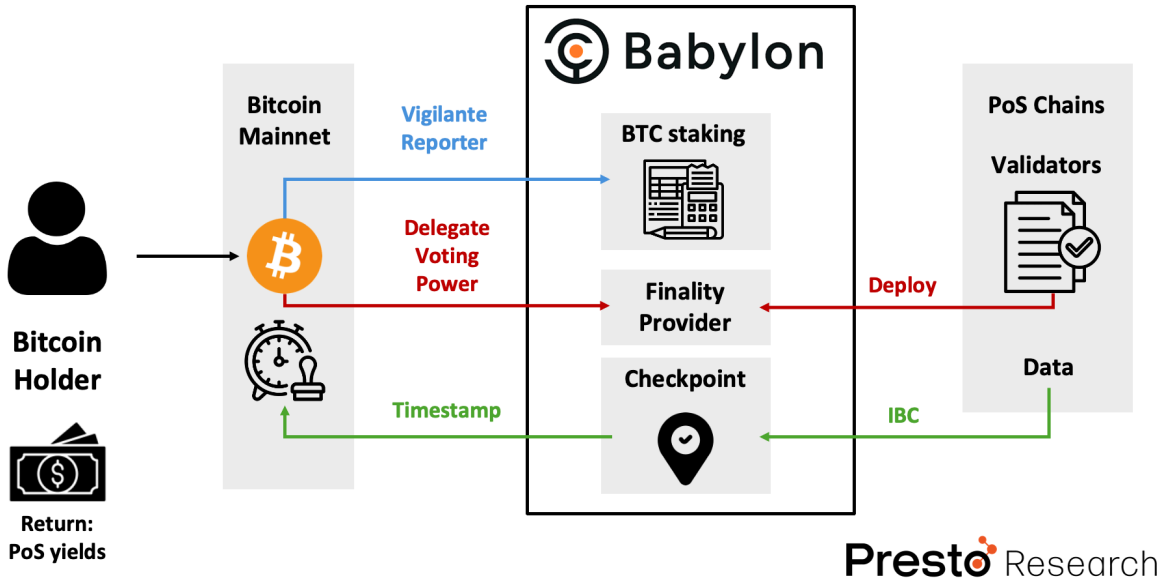
To enforce slashing, the bond contract leverages Bitcoin **covenants**, which restrict how and when the locked funds can be spent. If a validator fails to fulfill their duties or their secret key is compromised, a slashing transaction can be initiated. This slashing transaction sends the locked Bitcoin to an unspendable output, effectively destroying the funds. This is accomplished using a covenant that specifies an unspendable address, enforced by the OP_CHECKTEMPLATEVERIFY opcode in Bitcoin Script. The unspendable output is typically an OP_RETURN output, making it impossible for the validator or anyone else to reclaim the slashed funds.

The covenant mechanism is critical for enforcing slashing, but until covenants are natively supported in Bitcoin Script, an emulation approach is used. This emulation involves a covenant committee composed of multiple members. The bond contract is structured as a multi-signature scheme, requiring the signatures of the validator and the covenant committee to spend the deposit before the validator's duties end. The committee pre-signs a slashing transaction when the bond contract is created, ensuring that anyone can execute this transaction if the validator's secret key is exposed. This emulated covenant relies on an existential honesty assumption, where at least one committee member must remain honest and keep their signing key private, ensuring that the slashing transaction can be executed if needed.

In practice, the emulated covenant using a multi-signature approach, such as MuSig2, ensures that the contract remains lightweight and space-efficient on the Bitcoin blockchain. The MuSig2 scheme allows the committee to generate a single aggregate signature from the participating members, which can then be used to authorize transactions. However, if any member of the committee becomes unresponsive or refuses to participate, the partial signatures can be published on-chain, allowing the community to identify and exclude the uncooperative members. This approach ensures that the slashing mechanism is robust and can be enforced even in the absence of full support for covenants in Bitcoin Script, thus providing a strong deterrent against dishonest behavior by validators.

Babylon: Remote Staking with Economic Safety

Figure 7: Babylon's Bitcoin Staking Protocol Overview



Source: Babylon, Presto Research

Now, let's explore how Babylon's Bitcoin staking Protocol operates as a two-sided marketplace, building on the technical foundations we've discussed so far.

From the **perspective of Bitcoin holders**, they can participate in yield-generating events through the Babylon protocol. As previously explained, each Bitcoin holder can lock their BTC through a self-custodial bond contract. This information is then relayed to Babylon nodes by a standalone program called the Vigilante reporter. Within the Babylon node, the BTC staking module acts as a bookkeeper, verifying and activating the BTC staking request. Once this initial staking process is complete, the next step for the Bitcoin holder is to choose a finality provider to whom they will delegate their voting power. Delegating voting power means granting the right to cast finality votes to entities known as finality providers, who participate in the finality gadget as explained earlier. In return, Bitcoin holders receive yield rewards from PoS chains they choose and share a certain commission to the finality providers (ranging from 3% to 10% of the yield points in Babylon Mainnet Phase-1).

On the other hand, **each PoS chain** can receive enhanced security guarantees from participating in Babylon protocol, by paying staking yields to Bitcoin holders. In addition to generating and validating blocks as in their own PoS protocol, they also deploy a finality provider module and sign finality signatures on the finality gadget. By doing this, they can benefit from Babylon's Timestamping Protocol, as the validators of each PoS chain will post their blockchain data to BabylonChain through Inter-Blockchain Communication protocol (IBC), and those data will be checkpointed in Bitcoin chain by checkpointing module of Babylon node. Under Babylon's remote staking protocol, this whole process is secured by **Economic Safety**: whenever there is a safety violation on the PoS chain, at least one third of the Bitcoin stake securing the consumer PoS chain is slashed (robust against censorship in PoS chains).

Babylon Ecosystem

Babylon's modular design makes it adaptable to a wide variety of consensus protocols used by consumer chains. By integrating Bitcoin through the Babylon Bitcoin Staking Protocol, these consumer chains can tap into Bitcoin's security and liquidity, addressing the limitations of relying solely on native tokens for staking. Potential use cases for this approach include DeFi, Layer 2 rollups and oracles.

DeFi

One important aspect of Babylon's ecosystem is its support for liquid staking tokens (LSTs), which provide Bitcoin holders the opportunity to earn yields with BTC staking while maintaining liquidity. Projects like Bedrock, Nomic, and Solv have developed their own LSTs—uniBTC, stBTC, and SolvBTC, respectively—on top of the Babylon protocol. Users can receive these LSTs by staking their BTCs to Babylon through these services, and simultaneously make extra yields with it.

The Babylon ecosystem also includes more projects focused on enhancing Bitcoin's role in other parts of DeFi. For instance, the Lorenzo Protocol integrates with Babylon to build a scalable Bitcoin application layer, facilitating the use of Bitcoin assets for both data storage and network security. Persistence One, another participant in the ecosystem, focuses on maximizing yield and security through liquid staking and restaking, utilizing Babylon to bolster its staking capital and security.

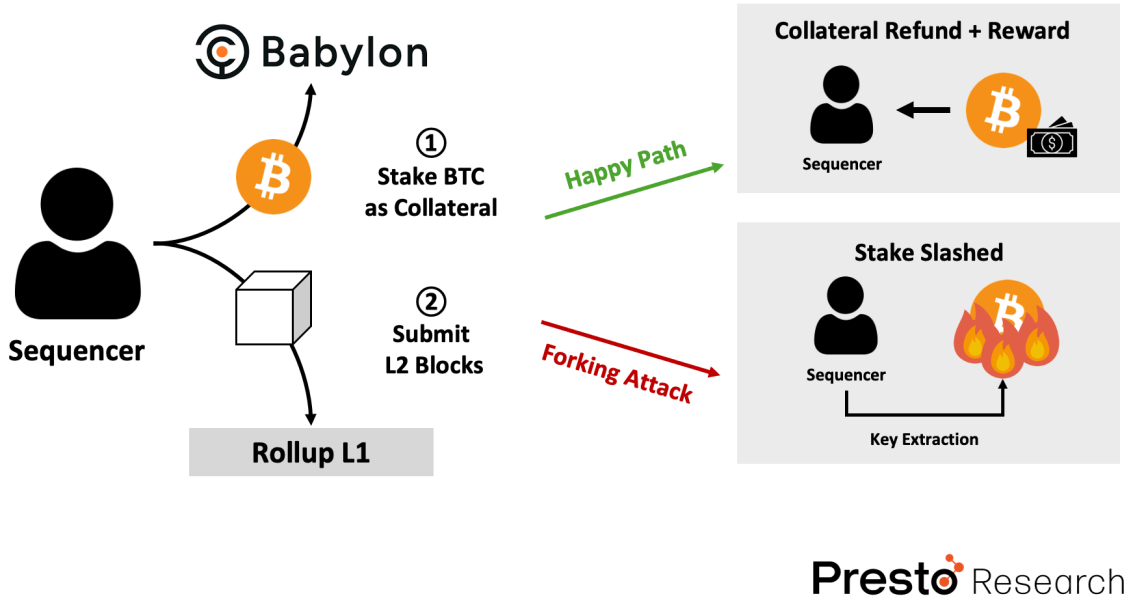
Layer 2 Rollups

Another important aspect of Babylon's ecosystem is its support for **forkless rollups**. The biggest bottleneck for rollups now is the sequencer problem; where the users have to rely on a centralized sequencer for submitting L2 blocks to L1. However, this reliance introduces significant security risks, particularly the threat of forking attacks, where the sequencer could submit different block versions to users and L1, enabling double-spending and other malicious activities. Existing mechanisms, like ZK proofs and dispute periods, are insufficient to prevent such attacks, and users requiring fast finality are forced to just trust a centralized sequencer, which reintroduces the risks of theft and censorship.

Here, Babylon proposes forkless rollups (Figure 7) by using Bitcoin staking as collateral to address the sequencer problem. The sequencer locks Bitcoin as collateral and adds a finality signature to each L2 block. If the sequencer publishes conflicting blocks, a secret can be extracted from the finality signatures, leading to the sequencer's collateral being slashed. This mechanism is enforced by the rollup smart contract on L1, which verifies the finality signature before accepting an L2 block, thereby economically disincentivizing malicious behavior.

Additionally, the protocol also proposes decentralizing the sequencer role by introducing a committee of Finality Providers (FPs) that validate each L2 block. If FPs sign off on conflicting blocks, they too are slashed, ensuring that at least one-third of honest FPs can prevent forking and invalid blocks. This decentralized validation process provides strong security guarantees without significantly increasing latency, making it suitable for high-stakes applications requiring rapid finality. The solution thus mitigates key vulnerabilities in the current rollup architecture, particularly for those needing fast transaction confirmation. Projects like AltLayer, Chakra, Merlin and B² Network are currently trying to integrate Babylon for securing their rollups.

Figure 8: Forkless Rollups with Babylon



Source: Presto Research, Babylon

Moreover, Babylon is currently expanding its ecosystem with more collaborations aimed at improving security, accessibility, and research. Projects such as Glacier Network, Automata Network, Yala, and Hana Network have integrated Babylon to strengthen their security protocols, enhance validator networks, and facilitate seamless Bitcoin staking across various platforms.

ICYMI: Phased Launch of Babylon Bitcoin Staking Mainnet

The launch of the Babylon Mainnet is structured in three major phases, beginning with the Phase-1 update on August 22nd, 2024. In this initial phase, the process of Bitcoin staking is established, but not yet activated, meaning that staking rewards are not available. This phase is primarily preparatory, allowing Bitcoin holders, or stakers, to lock their Bitcoin and delegate their PoS voting power to a chosen finality provider by submitting a Bitcoin staking transaction to the Bitcoin network.

Stakers can lock their Bitcoin for a maximum duration of 64,000 Bitcoin blocks (i.e., about 15 months), while also having the flexibility to unbond their stakes on-demand, with a mandatory unbonding period of 1,008 Bitcoin blocks (i.e., about 7 days) before they can withdraw their funds. An initial total staking cap of 1,000 Bitcoins is set for Phase-1, where limits are placed on individual staking transactions with a minimum stake of 0.005 BTC and a maximum of 0.05 BTC. Stakes are accepted on a first-come, first-served (FCFS) basis, with no queuing system for overflow stakes once the cap is reached.

One thing to note is that **there is no slashing mechanism and staking rewards during Phase-1**. Stakers are not at risk of losing their staked Bitcoin due to network penalties, as there is no requirement to sign a consent to PoS slashing. Instead of traditional staking rewards, a point system is implemented. Stakers earn points based on their active stakes, with 3,125 points allocated per Bitcoin block during the initial staking cap. These points are distributed proportionally among active stakes, with both the staker and their finality provider receiving a share. Point system serves as a measure of staking activity and may be subject to adjustments as Phase-1 progresses, but these points have no monetary value and cannot be traded, sold, or redeemed for any form of currency or asset.

After the launch of Phase-1, two more updates are planned. Phase-2 marks the activation of the Babylon PoS chain, where finality providers with delegations from Phase-1 begin participating in the chain's consensus, determining block finality while enabling the Bitcoin timestamping protocol for cross-chain time synchronization. Moving into Phase-3, the Babylon Bitcoin staking protocol will allow Bitcoin holders to stake the same bitcoins across multiple PoS systems simultaneously, thereby earning multiple staking rewards.

Conclusion

The BabylonChain emerges as a groundbreaking solution that addresses the challenges faced by both Bitcoin holders and Proof-of-Stake (PoS) blockchains. By leveraging the security and liquidity of Bitcoin, BabylonChain creates a unique marketplace where Bitcoin's idle capital can be utilized to enhance the security of PoS networks. This synergy not only unlocks yield-generating opportunities for Bitcoin holders but also provides a robust security layer for PoS chains, particularly in overcoming issues like bootstrapping, low liveness resilience, and long stake unbonding periods.

BabylonChain's approach to remote Bitcoin staking is distinguished by its novel use of the Timestamping Protocol, the Finality Gadget, and Bond Contracts. These elements collectively ensure that the protocol maintains high security standards, offering slashable security, staker security, and staker liquidity. The Timestamping Protocol, by anchoring PoS chain checkpoints in Bitcoin's blockchain, significantly reduces the risks associated with posterior corruption attacks, and shortens the stake unbonding period. The Finality Gadget further strengthens the consensus process by enforcing a strict one-block finality at each height, preventing malicious behavior among validators. Meanwhile, Bond Contracts secure Bitcoin staking without relying on complex smart contracts, using Bitcoin's inherent capabilities to ensure the safety and liquidity of staked assets.

Beyond securing PoS chains, BabylonChain's modular design paves the way for diverse applications across the blockchain ecosystem, including decentralized finance (DeFi), Layer 2 rollups, and oracles. By integrating Bitcoin staking, these applications can benefit from enhanced security and liquidity, fostering innovation while addressing some of the most pressing vulnerabilities in existing blockchain architectures.

To summarize, BabylonChain represents an advancement in blockchain technology, bridging the gap between Bitcoin's unmatched security and the dynamic, yield-generating opportunities of PoS networks. Its implementation not only enhances the utility of Bitcoin but also provides a security layer for the broader blockchain ecosystem, positioning BabylonChain as a vital infrastructure for the future of decentralized finance and beyond.

About Presto

Presto is a Singapore-based algorithmic trading and financial services firm founded in 2014. Presto focuses on delivering exceptional value for clients through a rigorous research-driven approach to investment and trade execution. With more than a 100 million trade executions in a day, Presto is a leading financial services firm in both digital assets and traditional finance markets. Presto Research is a research unit within Presto.

Find out more at https://www.prestolabs.io.
Follow Presto for more content: X, LinkedIn
Follow Presto Research for latest research : X, Telegram

Authors

Jaehyun Ha, Research Analyst
X, Telegram, LinkedIn

Required Disclosures

Any expression of opinion (which may be subject to change without notice) is personal to the author and the author makes no guarantee of any sort regarding accuracy or completeness of any information or analysis supplied. The views and opinions expressed herein are those of the author(s) and do not necessarily reflect the views of Presto Labs or its affiliates. This material by itself, is not and should not be construed as an offer or a solicitation to deal in any investment product or to enter into any legal relations. This material is for informational purposes only and is only intended for sophisticated investors, and is not intended to provide accounting, legal, or tax advice, or investment recommendations, or an official statement of Presto Labs or its affiliates. Presto Labs, its affiliates and its employees make no representation and assume no liability to the accuracy or completeness of the information provided. Presto Labs, its affiliates and its employees also do not warrant that such information and publications are accurate, up to date or applicable to the circumstances of any particular case. Certain statements in this document provide predictions and there is no guarantee that such predictions are currently accurate or will ultimately be realized. Prior results that are presented here are not guaranteed and prior results do not guarantee future performance. Recipients should consult their advisors before making any investment decision. Presto Labs or its affiliates may have financial interests in, or relationships with, some of the assets, entities and/or publications discussed or otherwise referenced in the materials. Certain links that may be provided in the materials are provided for convenience and do not imply Presto Labs' endorsement, or approval of any third-party websites or their content. Any use, review, retransmission, distribution, or reproduction of these materials, in whole or in part, is strictly prohibited in any form without the express written approval of Presto Labs. Presto Research and related logos are trademarks of Presto Labs, or its affiliates.