Dogoshi Whitepaper

v1.0

Table of Contents

Abstract

The Proof-of-Stake (PoS) blockchain networks rely heavily on capital for their security. However, generating capital can be an expensive process. Bitcoin, although a Proof-of-Work chain, constitutes a $600 Billion asset, with a significant portion of it being idle capital.

In light of this, we propose a novel concept known as Bitcoin staking. This concept gives Bitcoin holders the opportunity to stake their idle Bitcoins and in doing so, enhance the security of the PoS chains. Additionally, this proposition also presents an opportunity for Bitcoin holders to earn yield.

We have developed a Bitcoin staking protocol that enables Bitcoin holders to stake their Bitcoins in a trustless manner, without the need to bridge them to the PoS chain. This protocol, despite not requiring any bridging, equips the chain with complete slashable security guarantees.

One of the key features of this protocol is that it supports quick stake unbonding, thereby maximizing liquidity for Bitcoin holders. Furthermore, the protocol has been designed as a modular plug-in which can be used on top of various PoS consensus algorithms. It also serves as a primitive upon which future restaking protocols can be built.

To cater to the needs of several stakers and multiple PoS chains, we propose a system architecture that scales the protocol. This architecture features a Bitcoin-staked Babylon chain that acts as a control plane, synchronizing between Bitcoin and the PoS chains.

In conclusion, Bitcoin staking not only provides a new use case for Bitcoin but also represents a significant step towards integrating Bitcoin into the broader Proof-of-Stake economy.

1. Proof-of-Stake Security Requires Capital

In recent years, the blockchain industry has seen a shift from Proof-of-Work (PoW) to Proof-of-Stake (PoS) as a Sybil resistance mechanism.

A key event in this trend is the September 2022 merger, the transition of Ethereum from his PoW consensus to PoS consensus. PoW blockchains are secured by miners who solve difficult mathematical puzzles, while PoS blockchains are secured by validators who hold shares.

A validator's staking acts as a deposit that is cut if the validator violates the protocol.Slash Ability is a feature that PoW chains lack and is a key motivation for Ethereum's transition from PoW to PoS.The larger the market capitalization of the security share, the higher the cost of attacks on the chain and the stronger the economic security of the chain.

Therefore, PoW chains are protected by labor, whereas PoS chains are protected by capital. Such capital is often difficult to attract, especially for small or early-stage chains.Attracting this capital requires high inflation rates for high returns.

For example, in the Cosmos ecosystem, which consists of more than 60 application-specific chains, initial annual inflation rates of 20% to 100% are very common.Such high inflation hinders long-term development chain growth.High costs also threaten the safety of the chain's utilities. Inflation may have been used to encourage on-chain applications.
Cosmos SDK chain that operates a distributed AI computing platform and provides an excellent case study solution.The extremely high initial inflation rate of 100% for the AKT token pays dividends in both security and incentives for vendors to rent high-quality computing hardware. As inflation rates decline over time, the tension between security and the public interest becomes more acute.

2. Bitcoin $600 Billion Assets

Despite moving to PoS, Bitcoin remains the largest crypto asset, accounting for more than half of all crypto assets as of this writing. Protected through chains.

There are some important differences between Bitcoin assets when compared to PoS assets.

1. No burden. Bitcoin assets themselves are not used to secure the Bitcoin chain, as Bitcoin is secured by work. In contrast, each PoS asset is used to secure its own chain.

1. Be more idle. Most Bitcoin assets remain unused and out of supply.Most revenue-generating activities such as DeFi lending and security staking occur on PoS chains, so you can generate revenue by bridging your Bitcoin to other chains or to a centrally managed third-party custodian. You need to send it.Such bridges and central custodians are considered too risky for many Bitcoin holders.For example, wBTC, one of the largest wrapped Bitcoin assets, has a mark capitalization of less than $5 billion, which is less than a percentage of Bitcoin's market capitalization.

2. More decentralized. Bitcoin, the oldest blockchain, has perhaps the most decentralized group of token holders.4,444 miners, early adopters and developers, project founders, individual investors, institutional investors, exchanges, and more.In contrast, the assets of many of his PoS chains are at least concentrated.In the early stages of a project, it is in the hands of early investors, founders, team members, and foundations.Concentrated assets expose the network to centralization when assets are staked to validate the network.

3. Low volatility. Bitcoin, the largest crypto asset, has significantly lower volatility than most PoS assets. Volatility of PoS assets is a critical issue for the security of PoS chains.This is because security directly depends on the market capitalization of the assets being staked, and a sharp drop in asset value provides an opportunity for attackers.

3. Bitcoin Staking

Considering these characteristics, why not take advantage of staking and leveraging Bitcoin to secure PoS chains?This concept of using Bitcoin is the focus of this research .
Bitcoin staking is a two-sided market (Figure 1).On the other hand, there are PoS chains that require security and are willing to pay a return for it.On the other hand, there are also Bitcoin holders who have capital and want to profit from it.

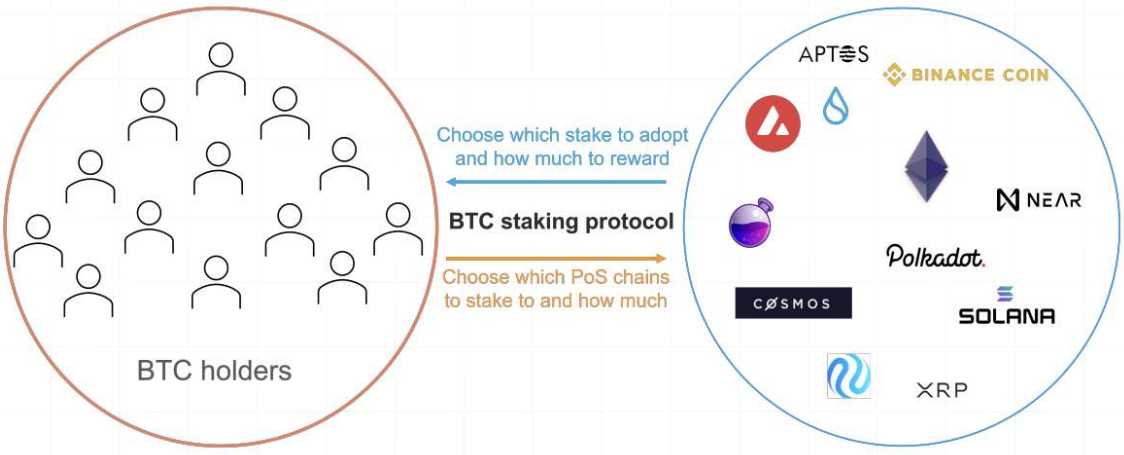

Figure 1: Bitcoin staking is a two-sided market place.

4. Babylon Bitcoin Staking Protocol: Security Properties

Here we introduce a Bitcoin staking protocol that has three important security properties when used in conjunction with commercial consumer PoS chains.

1. Fully slashable PoS security. In the event of a security breach, 1/3 of your Bitcoin stake is guaranteed to be reduced. As long as 2/3 of the Bitcoin stake is following the PoS protocol, the PoS chain is active.
2. Staker Security. Bitcoin stakers are guaranteed the ability to withdraw or unbind their funds as long as they faithfully follow the PoS protocol.
3. Staker liquidity. The release of used Bitcoins is guaranteed to be secure and fast, without the need for social consensus.

Property 1 indicates that protocol violations are truncated. Property 2 states that only protocol violators lose their bets. In summary, properties 1 and 2 reflect perfect slashability, the gold standard for PoS security advocated by Buterin and Griffith.

In fact, the full thrashability is based on Tendermint, one of the most widely used consensus engines for building PoS blockchains, including PoS Ethereum as well as Cosmos SDK chains, Polygon, BNB chains, etc. In fact, Property 2 is even more powerful than standalone PoS protocols.

A staker can still disengage even if all other stakers in the PoS chain are fraudulent. Withdrawal censorship is not possible with our Bitcoin staking protocol. Therefore, our protocol enables reliable staking. PoS Standalone PoS chains, such as Ethereum and Cosmos SDK chains, suffer from long delivery times on the order of several weeks because they use social consensus to defend against long-range attacks. It is the basic “nothing goes wrong” attack vector in PoS chains. In contrast, our Bitcoin staking protocol is immune to such widespread attacks as it maintains the distribution of Bitcoin staking on the Bitcoin chain. We can see that property 3 is achievable by properly designing the staking protocol.

5. Challenges

We consider two basic approaches to Bitcoin staking. Each has their own challenges.

5.1 Bridge to PoS chain

This one approach to Bitcoin staking is to first bridge Bitcoin from the Bitcoin chain to the consumer's PoS chain and apply the slash rule there. Although this approach can add dramatic security to her PoS chain (property 1), the fundamental limitation is the security of the bridging solution itself. The security of most existing Bitcoin bridges is based on the trust of a central administrator (e.g. Bitcoin Bridge, Bitgo for wBTC) or the Multisig Bridge Committee. Even an ideal Bitcoin bridge depends on the trust of stakers in the target chain. Therefore, the bridging solution requires Property

5.2 Trusted Staking, Remote Staking from the Bitcoin Chain

An alternative approach to avoiding Bitcoin bridging is remote staking, locks the staked Bitcoin into a contract on the Bitcoin chain and cuts the staking in the event of a protocol violation on the consumer's PoS chain. This is the approach used in security sharing solutions such as Eigenlayer's Ethereum restaking protocol and the Cosmos ecosystem's mesh security.

In both cases, the provider chain, or security source, has a Turing-complete smart contract layer. This allows evidence of protocol violations to be sent back from the consumer chain to the provider chain, making it technically easier to implement thrash in the provider chain, as it is executed through smart contracts in the provider chain. However, the provider chain in this case is Bitcoin, which does not support smart contracts and only has a scripting language with limited expressive power.

Therefore, the fact that Bitcoin remains on the Bitcoin chain gives us reliable staking (property 2), but the key challenge now is how to do slash to achieve Property 1 fully slashable PoS security.

Our Bitcoin staking protocol follows a remote staking approach, but combines advanced cryptography, consensus protocol innovation, and optimized use of the Bitcoin scripting language to overcome the lack of smart contracts. Before getting into the details of these technologies, let's first explain the high-level functionality of the Bitcoin staking protocol through the staking process.

6. System Architecture

Based on the above basic elements, the underlying infrastructure of the Bitcoin staking protocol represents the control layer between Bitcoin and PoS chains. This control plane is responsible for several key functions, including;

- Provides the Bitcoin timestamp service for PoS chains to ensure they are synchronized with the Bitcoin network.
- Acts as a trading platform, matching Bitcoin stakes and PoS chains, and tracking staking and verification information such as EOTS key registration and updates;

Write finality signatures for PoS chains; On the other hand, the validators of each PoS chain not only sign blocks like in a regular consensus protocol, but also finality signatures on the finality device. Together, these validators control the data layer of the architecture.

The control plane is implemented as a chain to ensure that it is decentralized, secure, censorship-resistant and scalable. For example, the limited and expensive block space of the Bitcoin network makes the immediate timestamp for each PoS chain unstable and unscalable, preventing the adoption of Bitcoin staking. To solve this problem, the Babylon team developed a secure Bitcoin timestamp protocol and implemented it as Babylon Chain based on the Cosmos SDK.

This chain enables efficient timestamp aggregation for any number of Cosmos SDK chains via the standard IBC (Inter-Blockchain Communication) protocol. Its testnet, first launched in February 2023, has integrated with more than 30 Cosmos SDK chains across multiple industries.

This creates a three-layer architecture in which the Babylon chain acts as a control layer and enables the interaction between Bitcoin and the data layer, i.e. the PoS chain. This architecture can also provide network effects and interoperability potential. For example, it is possible to conduct transactions between PoS chains on the Babylon Chain based on the final status of the two PoS chains on the Babylon Chain.

7. Related Works

7.1 Cross-chain staking, re-staking and mesh network security

Each existing PoS chain is secured by its own asset stored in the chain's ledger. For example, Ethereum PoS is secured by ETH, Cosmos Hub is secured by ATOM, and BNB chain is secured by BNB. However, using the native token alone limits the economic security of the PoS chain to the market capitalization of the native token. Placing remote crypto assets instead of or in addition to one's own assets on the PoS chain offers the opportunity to improve the security of the chain by increasing the total market capitalization staked.

One approach that is emerging in the blockchain industry can be called cross-staking: the staked foreign asset remains on its own chain, but on chains is tied to a staking contract intended for the preferred validator of the chain it protects. The asset stake is only reduced if the validator commits serious violations. This idea formed the basis of the concept of network security proposed for the Cosmos ecosystem [11, 4].

An asset from one Cosmos application chain (supply chain) can be cross-hosted to provide security to another Cosmos application chain (consumer chain). This cross-stake protocol is in turn inspired by the restaging concept of Eigenlayer Ethereum [36]. The idea is to take ETH on PoS Ethereum and reuse it to secure middleware (called AVS, active verified systems) such as data availability layers, bridges, oracle services, etc. Emerging from these projects is a generalized form of PoS, where a cryptocurrency asset can be used to secure chains and services other than its own chain.

Our Bitcoin staking protocol can be viewed as an example of a cross-chain staking protocol, but there are two important differences between the security of the Cosmos grid and Ethereum re-staking. First, in the relaunch of Ethereum and Mesh Cosmos security, the asset is already deployed to protect the supply chain. In contrast, Bitcoin is protected by PoW, not the Bitcoin asset itself, so the Bitcoin asset is not encumbered.

This reduces the risk of excessive leverage resulting from re-staking [17, 36]. Secondly, there are no smart contracts in Bitcoin that enable interest rate reductions. Instead, we optimize the use of the Bitcoin scripting language and use an advanced cryptographic engine to achieve the same goal.

7.2 Accountability and reducibility

An important characteristic of many PoS chains is their ability to hold protocol violations accountable in a verifiable manner [18, 20, 33]. This property is not present in PoW chains because miners do not have an ID on the chain. In fact, the property of responsible security, i.e. the ability to hold a third of validators accountable in the event of security breaches, is central to the design of Ethereum PoS [18, 20].].

However, there is a gap between accountability and on-chain pruning, i.e. effectively removing perpetrators of their stake on the chain based on evidence of protocol violations. Especially in the event of a security breach, more than a third of validators are already hostile and may censor evidence of the security breach, preventing it from entering the chain and making a cut. In such a case, the complex process of social consensus must occur off-chain so that violators can be cut and removed from the set of validators and the remaining honest validators can restart the chain [35].

In contrast, our Bitcoin stake protocol does not suffer from this problem because the Bitcoin stake is on the Bitcoin chain and not on the PoS chain and is automatically slashed if a security breach occurs on the PoS chain.

7.3 Responsible Statements and Stakechain

In this work, the deposit must be time-locked to the Bitcoin chain as a requirement for a party to make accountable statements in the distributed protocol. Whenever two different statements are made in the same context, the party's private key is leaked and anyone can use the private key to obtain the deposit. [24] builds on this concept to create a Bitcoin-backed proof-of-stake sidechain.

However, the proposed Proof-of-Stake protocol only includes one voting phase on each blockchain height. While this allows security breaches to be modeled directly as contradictory responsible statements (with the block height as the context and the security breach as the ambiguity for two blocks of the same height), the protocol will fail even if the attacker has very low stakes.

In contrast, all known BFT protocol designs include multiple levels of tuning to ensure liveness. In contrast, in our work, we do not attempt to design a PoS protocol from scratch, but instead use the Bitcoin staking protocol in conjunction with any PoS consensus protocol as an additional end product.

This ensures that the entire protocol works as long as the underlying consensus protocol is in effect, but still achieves shortcuts since all security breaches represent ambiguities at the same block height when using EOTS to sign the finality gadget. Furthermore, the deposit contracts in our protocol allow funds to be withdrawn on demand (after a certain delay), while the contracts in [32] only allow term deposits.

7.4 Finality Gadgets

In general, a finality gadget can be thought of as an overlay protocol that is used in addition to an existing consensus protocol to provide additional security guarantees. The first finality gadget is Casper FFG [18], which is used in addition to the longest chain protocol to ensure security in a section of the network (a security property that the longest chain protocol does not have).

Another finality gadget is GRANDPA [34], which is used in Polkadot. Ethereum's PoS beacon chain consensus protocol, Gasper [19], uses Casper FFG as a finality device in addition to the LMD (Latest Message Driven) GHOST protocol. However, [27] shows that Gasper is vulnerable to live attacks.

The first final gadget design officially proven to be secure is the Snap and Chat protocol [27]. The accountability gadget proposed in [28] allows adding accountability properties to the longest chain protocol. The design of the EOTS finality gadget in our Bitcoin staking protocol follows a similar philosophy. It adds Bitcoin's equity reducibility property to the existing BFT consensus protocol.

7.5 Bitcoin merge mining

Merge mining is the first technology invented by Satoshi Nakamoto in 2010 to secure Bitcoin. It is used to secure Bitcoin's first sidechain, Namecoin. Currently, Rootstock is the largest Bitcoin sidechain supported by merge mining [5]. Using the merge mining technique, Bitcoin miners can mine Bitcoin and another PoW chain simultaneously without consuming additional energy.

However, as a security sharing protocol, merge mining is threatened by the "nothing at stake" problem: in principle, miners can attack the sidechain while honestly mining the Bitcoin chain. Since Bitcoin is the main source of income for miners, there may not be sufficient deterrence against malicious behavior on the sidechain. In contrast, with Bitcoin staking everything is at stake: malicious behavior on the PoS chain can be reduced. Therefore, Bitcoin staking is a much more reliable method of sharing collateral than merge mining.

7.6 Bitcoin timestamps

Another method for securing Bitcoin is timestamping [35]: The hashes and signatures of PoS blocks are transmitted as transactions and recorded on the Bitcoin chain. This provides an additional level of ordering for PoS blocks that can be used to break ties in the event of forks in the PoS chain. This method is the basis of the Babylon Bitcoin time-stamped testnet. Because Bitcoin takes a long time to confirm transactions, securely recording these timestamps on the Bitcoin chain is a slow process.

Therefore, Bitcoin timestamps are effective for long-term security, such as against long-range attacks. In contrast, the use of Bitcoin increases the economic security of the PoS chain, thereby protecting it from close-range attacks. In addition, as mentioned earlier, the Bitcoin timestamp is also an integral part of the Bitcoin staking protocol and serves as a synchronization between the PoS chain and Bitcoin.

7.7 Proof-of-Transfer and Stacks

Stacks develops a Proof-of-Transfer (PoX) consensus mechanism in which miners compete with each other to become the next block applicant by sending Bitcoins to specific addresses on the send bitcoin chain. , the higher the amount sent, the greater the chance. This is a fundamentally different mechanism than Proof-of-Stake protocols, and therefore the separability and security properties of stakers do not apply to PoX stacks.

However, in order to connect Bitcoin to Stacks and allow Stacks smart contracts to access the asset, Stacks provides a way to mint and burn a synthetic Bitcoin token called sBTC, created by STX token stakers called “Stackers.” is secured. Stackers act as a group of signatures with a 70% threshold and have two responsibilities: 1) minting and redeeming sBTC and 2) approving the fork of the Stacks ledger that has already been completed. Thus, the security of the sBTC bridge is safe when more than 30% of stackers are honest,

and alive when at least 70% of them sign transactions honestly. A key advantage of our work is that we make it possible to stake Bitcoins without having to connect Bitcoins, the security of which is often limited by the total value of the locked assets of the token issued by the bridge project.

Compared to Stacks, our Bitcoin staking protocol does not require spending of bitcoins, but preserves the Bitcoin staked as long as no security violations occur. This enables more efficient and scalable utilization of the asset for security applications.

7.8 Bitcoin bridging

Broadly speaking, there are three categories of Bitcoin bridges today: centralized, security-based, and sidechain-based bridges, as well as potential security improvements through hardware solutions. We are not including atomic swaps in our discussion as they have not been adopted by mainstream Bitcoin bridges, possibly due to issues with usability, latency and liquidity sources.

Centralized bridges are operated by a central party that users trust. A typical example is a centralized exchange that allows users to deposit Bitcoin and its associated tokens from other chains and withdraw funds to any of these supported chains. For example, a Binance user can deposit their own Bitcoins into their Binance account and then withdraw the wrapped Bitcoin token onto the BNB chain. Another example is wBTC, where Bitgo acts as a custodian of its own Bitcoin [37]. These solutions strictly assume that centralized parties will neither intentionally cause harm nor adequately compensate users for their losses in the event of an attack.

Interlay is a solution for transferring Bitcoin into the Polkadot ecosystem through overcollateralized vaults that allow locking (creating a wrapped Bitcoin after receiving one's Bitcoin) and exit (redeeming one's Bitcoin after destroying one's Wrapped Bitcoin) of Bitcoin. [23]. The key trade-off here is security (i.e. a higher collateral ratio in case the vaults go out of control and the Bitcoins are stolen) and capacity (the number of Bitcoins transferred over the bridge is limited by the amount of collateral and the collateral ratio). Similarly, sBTC [6], proposed by Stacks in its update to Nakamoto [7], tasks a collective group of “stacked” STX token holders with performing pegging operations between Bitcoin and the sBTC token in the Stacks -Chain.

Alternatively, Nomic is a Tendermint-based chain that provides the ability to connect Bitcoin to nBTC, which in turn can be used in Osmosis and other Cosmos zones via the Inter-Blockchain Communication (IBC) protocol [3] . A limitation of such bridge solutions is that the overall security of bridge tokens depends on the security of the Nomic chain and is weakly bounded by the overall value of the Nomic token. Similarly, Rootstock runs lightweight Bitcoin clients on its miners and relies on the latter to establish a connection between native Bitcoin and a synthetic Bitcoin token on its chain [5, 31]. Without taking into account the additional security provided by the hardware, as described below, the security of your wrapped Bitcoin token is equivalent to the security of Rootstock's proof-of-work chain.

Additionally, Rootstock's Bitcoin peg mechanism called PowerPeg [31] uses secure hardware to increase the security of the Bitcoin peg. Similar hardware-based security improvements are also used in the Avalanche Bitcoin Bridge with Intel SGX [2]. The use of a hardware root of trust can fundamentally reduce the attack surface of such bridges, especially if the integrity of the code can be checked at runtime.

However, practical software security considerations apply here: a) If the bridge logic executed in the protected hardware is based on critical information from external sources, the security of that bridge is reduced to the security level of the external component; and b) if a vulnerability in the code running in the Protected Hardware is exploited, the security enhancements provided by the Hardware may not be effective.

As we have already mentioned, a key risk with the prevailing Bitcoin bridges is the redeemability of wrapped Bitcoin tokens, which are secured by a chain that is far less secure than Bitcoin. Fortunately, in order to host Bitcoins to protect external chains and systems, we do not require full portability of locked Bitcoins. Our proposed Bitcoin staking scheme circumvents the security and throughput issues associated with prevailing Bitcoin bridges by restricting transactions to issuing locked Bitcoins, thereby reducing security breaches. Therefore, our system provides strong security guarantees as outlined in Section 4.

8 Conclusions

Bitcoin is the first and still the best blockchain in terms of market capitalization. However, aside from being a store of value, its utility is limited by its small block space, high latency, and limited programmability. In particular, previous efforts to scale Bitcoin and expand its use cases through the creation of sidechains and other Layer 2 projects have been hampered by the inability to connect large numbers of Bitcoins to these chains. Bridges are limited by either safety or capacity or both.

Our work opens up a new and important use case for the Bitcoin asset: staking for security in a PoS world. We have shown that, at least for this
use case, connecting the Bitcoin asset to other chains is not necessary, but PoS chains can be deployed with complete economic security. The biggest challenge to achieve this goal is to be able to remediate any security breaches remotely without having a smart contract on the Bitcoin chain.

We achieve this by combining four concepts into a single protocol: 1) accountability statements for sharing private keys in the event of ambiguity, 2) finality tools for converting all security breaches into ambiguity of accountability statements, 3) Bitcoin convention emulation for forced money burning when a private key was leaked and 4) a Bitcoin timestamp to ensure that the shortening transaction can be spent before the stake is canceled. Our design is modular and can be used in addition to all PoS consensus protocols. Implementing our Bitcoin staking protocol does not require any soft or hard forks of Bitcoin.

Thanks to new use cases like sequence numbers, Bitcoin has been enjoying something of a renaissance lately. We believe the Bitcoin staking option will further boost this renaissance and stimulate efforts to find other risk-free uses for the massive Bitcoin asset.

What happens in Bitcoin stays in Bitcoin.