Comprehensive Analysis of Babylon

Sumaiia

Mentor: Seungmin Kim

Advisor: Heung-No Lee

Feb. 24th 2025

Objective of the Report

This report aims to provide a comprehensive understanding of Babylon's **business model**, **technical innovations**, **testnet operations**, **Finality Provider mechanism**, and **Total Value Locked (TVL)** metrics. By analyzing these aspects, the study will evaluate Babylon's potential applications in PoS networks and broader Web3 ecosystems.

Table of Contents

Contents: **Page**

1. Introduction: Overview and Importance of Babylon

What is Babylon?

Babylon is a Data Availability Layer (DAL) powered with Bitcoin to enhance the security and finality of Proof-of-Stake (PoS) chains. Native vulnerabilities of PoS networks such as long-range attacks, low liveness resilience and bootstrapping challenges are solved by Babylon by leveraging Bitcoin's security infrastructure. Bitcoin chain acts as an external trust layer, introducing a unique hybrid model that anchors PoS transactions to external chain. Unlike traditional PoS models that rely on internal mechanisms, Babylon ensures robust security to PoS chains, especially for decentralized applications and Layer 2 solutions through external assistance.

The core mechanisms of Babylon are Bitcoin checkpointing and Bitcoin stacking modules. Timestamping model uses Bitcoin's immutability to maintain PoS chain security, this innovative approach ensures slashable safety, liveness, and reliable data availability. Stacking mechanism transforms idle Bitcoins into a dynamic asset capable of powering with high security of PoS transactions. By integrating this process into Bitcoin, Bitcoin holders can actively use their passive coins for active contribution of enhancement of PoS blockchain space.

Objective of the Report

Bitcoin operates on a proof-of-work (PoW) consensus mechanism, which traditionally does not support staking. However, Babylon's founder has made a bold claim:
"There is a way for Bitcoins to tap into this native earning opportunity of staking, even though Bitcoin is a proof-of-work chain. Our solution is the world's first trustless Bitcoin staking protocol. In this protocol, we can enable any Bitcoin holders to lock the Bitcoin on the Bitcoin chain trustlessly and, at the same time, secure any proof-of-stake chain in the world. This is the protocol that we built."
This report aims to analyze and validate this claim by examining Babylon's technical foundations, business model, testnet operations, Finality Provider mechanism, and Total Value Locked (TVL) metrics. Through data-driven analysis and comparison with existing staking mechanisms, this study will evaluate how Babylon's approach integrates Bitcoin's security with PoS chains, ensuring decentralization, economic sustainability, and trustlessness. By providing empirical evidence, this report will determine whether Babylon successfully bridges the gap between Bitcoin's security and PoS scalability, creating a new paradigm in blockchain staking.

2. Babylon's Business Model

Key Stakeholders

To create a highly decentralized ecosystem, Babylon utilizes three primary stakeholders – Bitcoin Stakers, Finality Providers and PoS network operators. Babylon's unique hybrid model is mainly contributed by these stakeholders, leveraging Bitcoin's stability to enhance the security and stability for Proof-of-Stake (PoS) chains.

Bitcoin Stakers are essential to safeguard PoS networks against attacks. By stacking their Bitcoin by Babylon's self-custodial protocol, they can lock their Bitcoin directly on the blockchain without use of third-party thereby minimizing potential risks. By contributing to the safety of the network of PoS chains and active use of passive Bitcoin store of value Babylon transforms Bitcoin into an active economic security asset.

Finality Providers are especially vital for prevention of long-range attacks. They introduce a new PoS block to immutable Bitcoin chain ensuring safety and finality of a transaction. Finality providers are rewarded with network fees and Bitcoin delegations for their contribution to Babylon's mission of delivering unmatched data availability and integrity.

PoS Network Operators are primarily responsible for the collaboration of Bitcoin Stakers and Finality Providers. Their main task is to validate transactions, participate in governance and maintain the decentralization of the network. By integration of Babylon to their ecosystem they benefit from advanced security and scalability, and monetary rewards from stacking and transaction fees.

Value Proposition

Traditional blockchain systems' limitations are addressed and enhanced by Babylon's innovative hybrid approach guaranteeing security and improved scalability for decentralized applications (DApps) and Layer 2 solutions.

Strengthening PoS Network Security is achieved by Babylon's unique checkpointing mechanism, which integrates Bitcoin's stability and immutability into PoS networks. This mechanism anchors PoS network finality to Bitcoin blockchain thereby advancing the vulnerability, reorganizations and long-range attack limitations of traditional PoS chains. By incorporating timestamping mechanism, the secure high-value transactions and increase of adoption is achieved.

Guaranteed Data Availability for DApps and Layer 2 solutions are achieved by the same checkpointing mechanism offered by Babylon. Leveraging Bitcoin's timestamping capabilities data availability is guaranteed, moreover, enhances the scalability and efficiency of decentralized ecosystems. For this highly secure system users also benefit from lower cost.

In short, Babylon's unique combination with secure Bitcoin chain sets it apart from standalone PoS systems offering several advantages such as secure, scalable and interoperable ecosystem.

Revenue Model

Babylon's economic framework is designed to sustain its ecosystem while ensuring alignment of incentives among stakeholders.

Staking Fees and Transaction Fees: Revenue is generated from fees paid by Bitcoin Stakers and PoS network participants. These fees are distributed among Finality Providers, network operators, and Bitcoin Stakers, ensuring equitable rewards and ecosystem sustainability.

Economic Interactions Between Stakeholders: Babylon's model fosters collaboration among stakeholders by aligning their incentives. For instance, staking fees collected from PoS networks to anchor blocks on Bitcoin are shared between Finality Providers and Bitcoin Stakers. This dynamic interplay promotes network health and long-term success.

Liquidity Enhancement: Through partnerships with protocols offering Liquid Staking Tokens (LSTs), Babylon enhances staking liquidity. This allows participants to earn rewards while retaining flexibility, further bolstering economic interactions.

Conclusion

Babylon's business model is transformative for blockchain security and scalability primarily by integrating the most stable Bitcoin chain with PoS network operations. This innovative solution is mainly benefited by Bitcoin Stakers, Finality Providers and PoS network operators.

Babylon's potential to lead the blockchain industry can be demonstrated by their recent achievements in 2024; $70 million funding and 25 Bitcoin Secured Networks (BSNs) included for expansion of Babylon's ecosystem. Looking ahead to 2025, their plan for multi-staking functionality and ecosystem growth will further strengthen its position as a pioneer in the blockchain industry.

3. Testnet Operations and Insights

Structure of Babylon Testnet

Babylon's Testnet environment is significant for analyzing and enhancing the Bitcoin staking protocol that it utilizes for refining the security of Proof-of-Stake (PoS) networks by the help of Bitcoin's robustness. The testnet was launched and evolved through multiple phases, starting from bbn-test-1chain, followed by bbn-test-2, bbn-test-3, bbn-test-4, each with refinements compared to previous chains. The changes were applied based on community feedbacks, and each testnet phase builds upon the last addressing the key concerns such as safety of staked Bitcoin and improving user experience. The latest iteration, which is bbn-test-5, was launched on January 8, 2025. These testing chains are used for introducing the Babylon PoS test chain secured by both Babylon and Signet Bitcoin stakes.

Key Functionalities and Roles:

Validators: In the Babylon testnet validators are in charge of proposing and validating new blocks within the PoS network. The active size for validators specifically in bbn-test-5 chain is capped at 100 slots.

Finality Providers: Different types of validators, finality providers, are responsible for anchoring PoS blocks to the Bitcoin blockchain, the process which ensures finality making it immutable for potential attacks. By receiving voting powers from BTC stakers, finality providers earn commissions from staking rewards denominated in Babylon tokens.

Bitcoin Stakers: The majority of the testnet participants, stakers, stake their Signet Bitcoin to secure the testnet. They can register Phase-1 Signet Bitcoin stakes or create new stakes using Signet BTC for testnet Phase-2. During the first 72 hours, only Phase-1, Cap-1 stakes can register before opening to all stakes.

Liquid Restaking Protocols: The platforms that are designed to facilitate the delegation and recollection process of staked assets in the Babylon testnet environment.

Wallets and dApp Developers: The main function of developers is enabling smooth integration with permissionless smart contract deployment and with the staking web app.

Transaction Flow and Staking Mechanism with Staked BTC:

1. Staking Process: The process of Bitcoin holders locking their Signet BTC into Babylon's trustless self-custodial staking contract which ensures security and integrity in turn.
2. Delegation: The phase when stakers delegate voting power to chosen validators and finality providers, contributing to block production and security without transferring asset custody, meaning that they do not have the direct access to the staker's assets.

3. Transaction Flow: First, transactions initiated by participants are validated by the selected validators, then for enhanced security, critical blocks are anchored to the blockchain by the chosen finality providers.
4. Reward Distribution: For continuous participation and support of the network, stakers earn rewards based on their performance delegated validators and finality providers.

Analysis of Testnet Data

Showing significant growth and integration capabilities, the Babylon testnet has demonstrated its potential and reinforcing role in enhancing PoS network security by leveraging Bitcoin chain. Babylon's ability to mitigate risks from long-range attacks by anchoring PoS blocks to the Bitcoin chain, ensures data immutability. Another benefit of testnet is the illustration of how Bitcoin holders actively participate in PoS networks, which therefore provides economic security.

Performance Metrics:

Network Growth: The testnet experienced rapid expansion, specifically bbn-test-5 chain, raised from 38675 on January 14 to 110363 by January 23 (meaning approximately 7,778 blocks are added per day), demonstrating widespread adoption.

Transaction Throughput: Specific TPS metrics are unavailable, however, we can conclude that the network's scaling ability with increased participation highlights a robust infrastructure.

Reliability and Security: Since Babylon relies on Bitcoin chain, tamper-proof records are guaranteed. However, in testnet phase the slashing mechanism is disabled.

User Experience and Participation:

Setting up the Babylon testnet required cloning the official repository and following a structured installation guide. The process involved installing dependencies such as Golang, configuring network settings, integrating a CLI wallet, and applying as a validator. Syncing the node and obtaining testnet funds were streamlined through community-provided resources. As shown in **Figure 1**, real-time blockchain node logs illustrate the syncing process. The validator application process included generating a BLS key, submitting a validator transaction, and verifying the active set status, which can be seen in **Figure 2**. Throughout the process, GitHub served as a central hub for obtaining updates, troubleshooting, and accessing necessary configurations, making it a critical resource for successful participation in the testnet.

New users can join the Babylon testnet by setting up a testnet node or applying as a validator through the provided GitHub repository. The more detailed information can be obtained from the official Babylon GitHub repository.

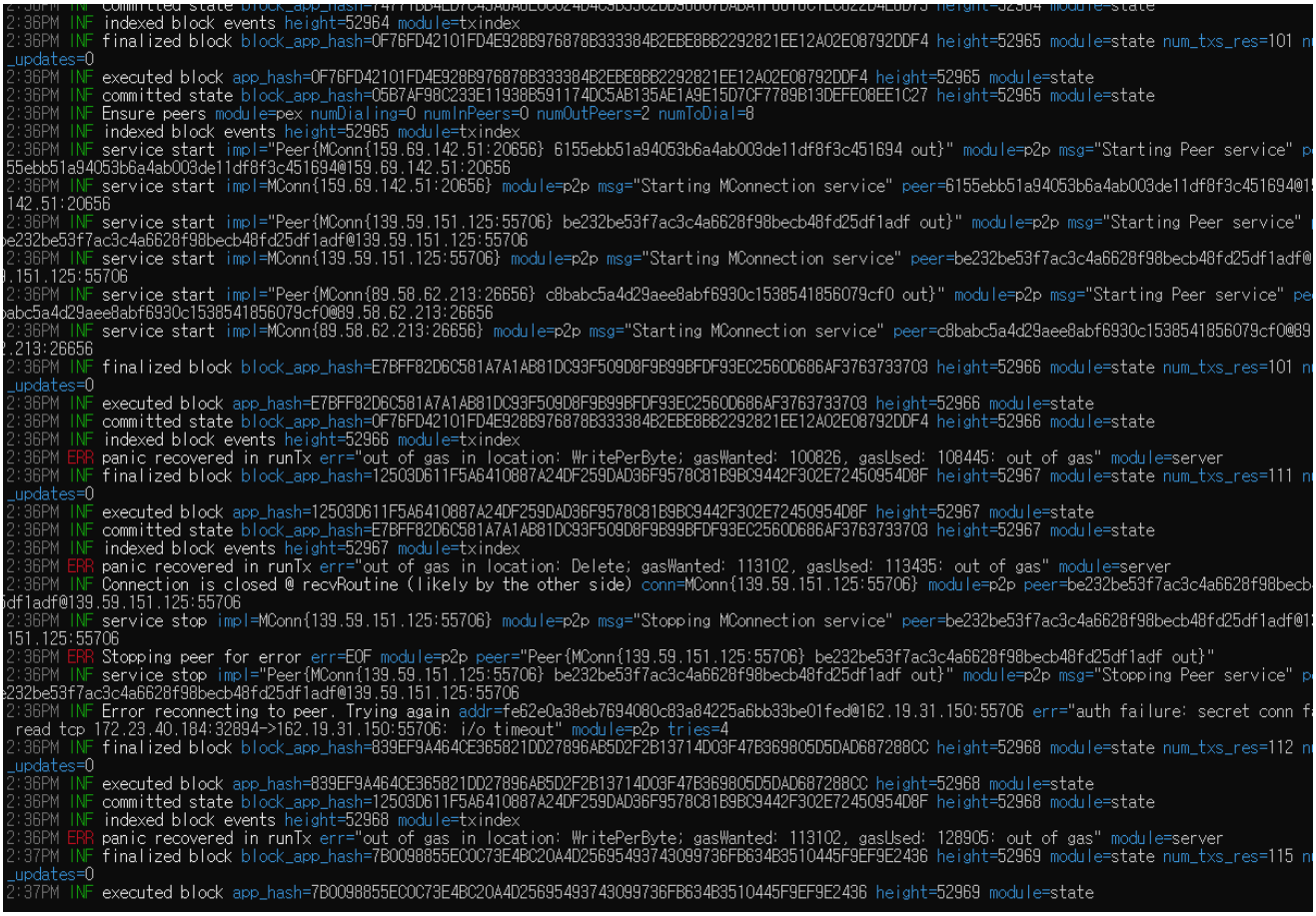

Figure 1. Blockchain Node Logs

This screenshot displays the logs from a blockchain node, showing the execution of blocks, peer connections, and service activities. It includes details about indexed events, finalized blocks, and peer-to-peer service status updates.

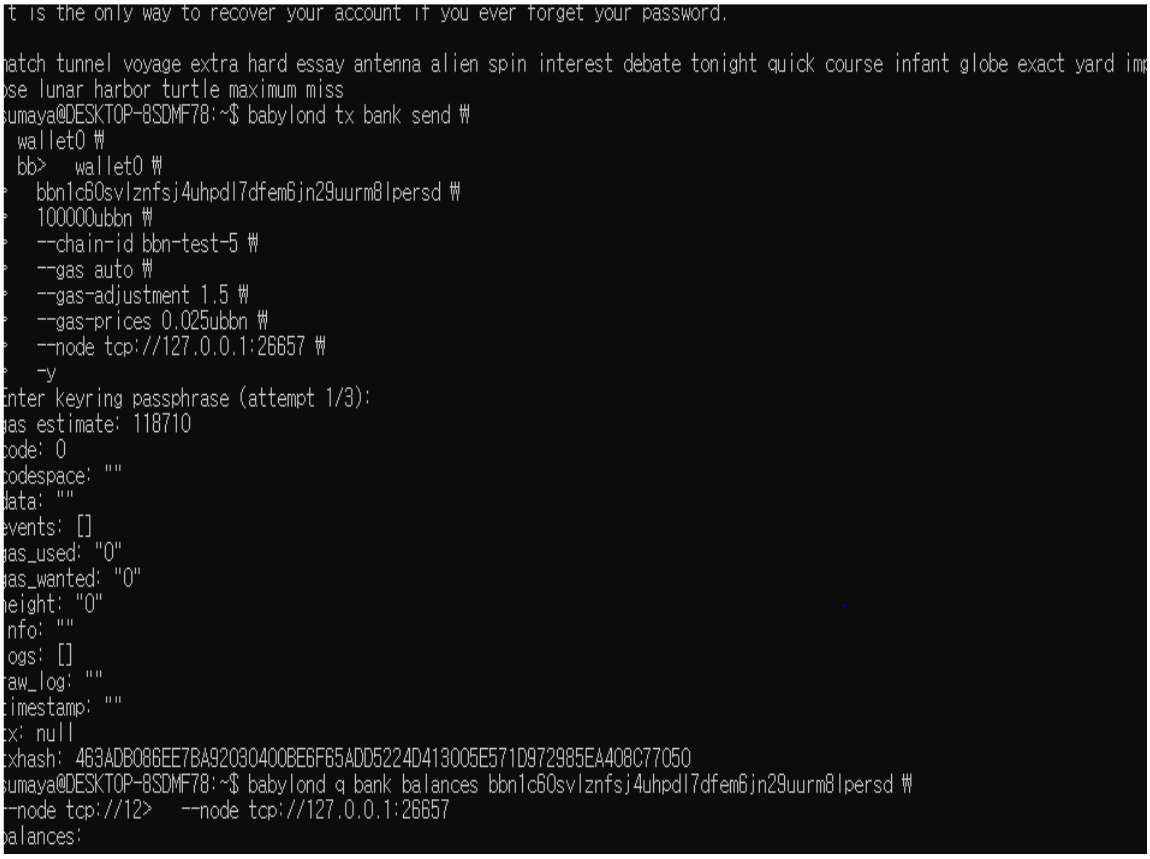

Figure 2. Transaction Execution in CLI

Description: This image captures the process of executing a transaction using the CLI. The command *babylond tx bank* send is used to transfer tokens, and the terminal prompts for the keyring passphrase before finalizing the transaction.

Babylon's testnet operations provide valuable insights into its potential to merge Bitcoin's security with PoS functionalities. Observed growth, integration potential, and performance metrics highlight the protocol's viability for widespread adoption and strengthening decentralized ecosystems through innovative staking mechanisms.

4. Finality Provider Mechanism

Role of Finality Providers

Finality providers are crucial participants in the Babylon BTC staking protocol mainly for securing PoS chains by leveraging Bitcoin staking as collateral. More specifically, they provide finality votes on top of Babylon's consensus mechanism, CometBFT, and get rewarded from commissions from BTC staking delegations. This process advances security and immutability, since adding extra layer of security makes it harder for the attackers to reorganize blocks or cause long-range attacks. According to the latest testnet data from Babylon's staking dashboard, currently there are over 100 active finality providers, which demonstrates the increasing participation.

Finality Provider Architecture and Components

Finality providers in Babylon network rely on a three-component system which provides them with efficient finality voting and staking mechanisms:

1. Babylon Node: This step is crucial for better security, so running a personal node is recommended. The fully synced Babylon node provides a chain data and transaction submission capabilities and details.
2. Extractable One-Time Signature (EOTS) Manager: This component is recommended to run on a separate system for enhanced security. The main role is to handling EOTS key operations, generating one-time signatures and ensuring public randomness.
3. Finality Provider Daemon: This daemon is responsible for monitoring Babylon blocks, committing public randomness, and submitting finality signatures. It also tracks provider status transitions (Active, Inactive, Jailed, Slashed) and ensures secure coordination with the EOTS Manager for key operations. Additionally, it handles staking rewards and their distribution, ensuring providers are properly compensated for their contributions.

The above listed components are essential for maintaining a secure and stable chain, which takes under control that each finality vote satisfies the protocol standards.

Ensuring Finality Using Staked BTC

Finality providers are required to lock up their Bitcoin on the Babylon staking protocol as collateral, solely for the purpose of slashing if they contributed to some malicious activity. As of today, the total amount of BTC on the testnet is over 500 BTC staked.

One of the core mechanisms of the Babylon, the checkpointing mechanism, is the periodic submission of cryptographic proofs of PoS block finalization to the Bitcoin blockchain by the finality providers. This creates an immutable record of any activity done within each network preventing fork reversals and ensures consensus integrity. The security level of the Bitcoin of a finality provider directly proportional to the amount of Bitcoin staked.

The EOTS ensure that if the provider is caught in double signing of conflicting blocks, their private key is exposed, which results in immediate slashing and loss of the voting power for.

Finality mechanism is highly decentralized, not a single entity can claim full control over the voting power. This in turn ensures that finality is fairly based on protocol rules, preventing censorship and manipulation.

Economic Incentives and Risks

Rewards for Finality Providers

Finality providers are financially incentivized through staking rewards, transaction fees, and delegated staking commissions. They earn Babylon tokens (tBABY) based on the number of blocks they finalize, ensuring continuous participation and network stability. Additionally, they receive a portion of transaction fees from PoS networks, along with commissions from Bitcoin holders who delegate their stakes, providing an additional revenue stream.

Potential Slashing Risks & Network Stability

The protocol uses two distinct keys:

- EOTS Key: Mainly used for EOTS signature generation and stored in the EOTS manager.
- Babylon Key: Used for general activities such as: signing transactions and claiming awards, and it's stored in the finality provider Daemon's keyring.

Slashing conditions: Once double signing is detected or submission of conflicting block is proven, their Bitcoin stake is forcibly slashed using EOTS mechanism.

Status Transitions: Providers have different states: Registered, Active, Inactive, Jailed, and Slashed solely based on their behavior. However, once a provider is slashed, they cannot regain the power of voting.

Unbounding Protection: The unbounding period is essential for preventing last-minute-malicious activities. As a result, finality providers should undergo the unbounding period before withdrawing their stake. This prevents the cases of creating a fraudulent block and immediately exiting the network to escape the penalties.

Economic Disincentives for Malicious Behavior: The design of the protocol states that the cost of attempting an attack should significantly outweigh any future short-term benefits. As per Babylon's finality provider documentation, the current slashing rate is set at 33% of the staked BTC, ensuring that dishonest behavior is strongly discouraged.

In conclusion, the role of finality providers in Babylon's PoS security model is pivotal. Their operations contribute to enhancement of trust and decentralization mainly because of

automatic slashing mechanisms, economic incentives and crypto security. Babylon offers a stable staking ecosystem that bridges Bitcoin’s security with the needs of PoS chains by balancing the rewards with automated penalties.

5. Innovation and Competitive Analysis

Proof-of-Stake chains were first introduced in 2012, by Peercoin. Major shift from PoW to PoS chains was mainly due to energy consumption, scalability and decentralization. However, these chains are still known for lack of security compared to immutable PoW chains. Babylon which was founded in 2022 by Stanford Professor David Tse and Dr. Fisher Yu, introduces a novel approach to securing Proof-of-Stake networks by leveraging Bitcoin as a decentralized security layer.

By anchoring PoS security to Bitcoin, Babylon eliminates dependence on traditional PoS validators alone, mitigating risks of centralized control and long-range attacks. This model strengthens economic security by enforcing Bitcoin-based slashing conditions, ensuring that malicious actors face substantial penalties. Unlike traditional PoS security models that rely solely on native staking assets, Babylon enhances network resilience through Bitcoin staking. This mechanism significantly increases the economic cost of attacks, making PoS systems more secure and resistant to long-range attacks. For example, in the event of a coordinated attack on a PoS network, Babylon's Bitcoin staking model ensures that economic penalties are enforced through slashing, making it prohibitively expensive for attackers.

Key Advantages Over Traditional PoS Security Models

Checkpointing: Babylon achieves redundancy by checkpointing the last block of each epoch to Bitcoin, which reduces reliance on validator-set trust assumptions. This process enables PoS transaction data to be timestamped in Bitcoin, which in turn creates an immutable and independently verifiable record. If some malicious activity is detected, or some events that cause the split of the network, the PoS network can rely on these checkpoints to rebuild consensus and maintain stability. This fundamental solution improves the robustness of the network particularly enabling better data security. For instance, an event that caused validator set to go offline causing the PoS chain sensitive to attacks, Bitcoin-anchored finality ensures the integrity of PoS transactions remain intact.

Bitcoin Staking: PoS chains by nature depend on their native tokens for security and stability. However, traditionally, PoS chains are more vulnerable to manipulation. Babylon proposes an approach for an external economic weight to prevent any manipulation that can be made to these chains by Bitcoin staking. Stacking bitcoins mitigates risks related to network centralization and governance attacks. This approach allows a more secure alternative to PoS native token secured chains by reducing single-token governance risks.

Understanding Cap-1, Cap-2, and Cap-3

Babylon's Bitcoin staking protocol is structured in phases called Caps, which define the limits, duration, and conditions for staking. These Caps are essential milestones that ensure the security, scalability, and broad participation of Bitcoin staking.

Cap-1 (August 22, 2024)

- **BTC Staked**: 1,000 BTC
- **BTC Stakers**: 12,720
- **Overview**: Cap-1 introduced Bitcoin staking in a fully self-custodial manner. Bitcoin holders could lock their BTC on the Bitcoin network and delegate PoS voting power to Finality Providers (FPs). This phase laid the groundwork for trustless staking and initial adoption.

Cap-2 (October 8, 2024)

- **BTC Staked**: 22,891 BTC
- **BTC Stakers**: 12,590
- **Overview**: Cap-2 expanded the staking capacity significantly, allowing for more Bitcoin to be staked while improving security mechanisms. More stakers and institutions participated, solidifying Babylon's credibility as a trustless staking solution.

Cap-3 (December 10-17, 2024)

- **BTC Staked**: 33,399 BTC
- **BTC Stakers**: 109,980
- **Overview**: Cap-3 further expanded staking capabilities with an increased transaction limit of **5,000 BTC per stake**. It introduced improved scalability measures to prevent transaction fee spikes and enhanced user accessibility through integrations with multiple wallets and platforms.

Phase-1 Total Staking

- **BTC Staked**: 57,290.61 BTC
- **BTC Stakers**: 135,290

The success of these Caps demonstrated increasing confidence in Babylon's protocol, paving the way for further developments in Bitcoin staking.

Trustless Staking and Its Significance

Trustless staking allows individuals to secure decentralized networks without relying on intermediaries. Unlike traditional financial systems that require third parties, Babylon's Bitcoin

staking protocol leverages cryptography and Bitcoin's scripting language to turn Bitcoin into a fully self-custodial staking asset.

This was demonstrated in December 2024 when an anonymous staker chose to stake directly with Babylon rather than using an LST protocol. This commitment signals a **$1 billion vote of confidence** in Babylon's trustless staking model, reinforcing its security and reliability. The individual executed a test transaction of 1 BTC before proceeding, highlighting their belief in Babylon's decentralized framework.

Market Competitiveness

Babylon is positioned as a transformative force in Web3 security, addressing persistent challenges in blockchain finality and data availability. Key competitive advantages include:

- **Bitcoin Staking Integration:** Unlike traditional PoS models, Babylon combines PoS finality with Bitcoin's established security, reducing vulnerabilities.
- **Decentralization:** Babylon eliminates single-token dominance risks by externalizing security to Bitcoin.
- **Enhanced Protection:** By anchoring PoS transactions to Bitcoin, Babylon reduces the likelihood of governance attacks and economic manipulation.

Advancing the Web3 Ecosystem

Cross-Chain Security Enhancement

- Babylon's Bitcoin-based staking model extends security benefits beyond a single PoS chain.
- This mechanism could safeguard multiple ecosystems, reinforcing trustless, decentralized security.

Trustless Finality Anchoring

- Timestamping PoS blocks on Bitcoin enhances the integrity of decentralized networks.
- Reduces reliance on centralized authorities and increases censorship resistance.

Technical Innovations

Babylon Chain distinguishes itself through the following technical advancements:

- **Robust Security Integration:** By utilizing Bitcoin's security measures, Babylon ensures greater transactional protection.
- **Innovative Economic Incentives:** Enables Bitcoin holders to stake idle BTC, incentivizing broader participation in PoS ecosystems.

- **Scalability and Interoperability:** Supports cross-chain security applications, reinforcing Babylon's role as a foundational Web3 component.

Babylon Chain represents a significant leap forward in blockchain security by integrating Bitcoin staking into PoS frameworks. Unlike traditional PoS models, which rely solely on staked assets for security, Babylon enhances economic resilience, decentralization, and network robustness. By anchoring PoS finality to Bitcoin, Babylon creates a more secure and attack-resistant blockchain ecosystem, making it a critical infrastructure component for the future of Web3.

The December 2024 $1 billion Bitcoin stake further cements Babylon's position as a trusted and scalable solution for decentralized security. This milestone proves that Bitcoiners recognize trustless staking as a legitimate use case, shifting it from an abstract concept to a tangible, high-value implementation.

6. TVL (Total Value Locked) Analysis

Total Value Locked (TVL) is a critical metric in assessing the economic security and adoption of decentralized protocols. In the context of Babylon, TVL represents the total amount of Bitcoin staked within the ecosystem, reinforcing security across Proof-of-Stake (PoS) chains. This section explores Babylon's latest TVL metrics, its contribution to PoS security, and the factors influencing TVL growth.

Babylon's TVL Metrics

As of December 2024, Babylon's Bitcoin staking protocol has achieved significant milestones in TVL:

- **Total BTC Staked:** 57,290.61 BTC
- **Estimated USD Value (at BTC price of $106,526):** $6.1 billion
- **Number of Stakers:** 135,290

Contribution to PoS Chain Security

Babylon's high TVL directly enhances the security of integrated PoS networks by leveraging Bitcoin's economic weight as a trustless collateral base. The ability to stake BTC in a decentralized manner strengthens PoS consensus mechanisms by introducing a robust security layer, reducing risks associated with validator centralization and long-range attacks.

With each phase of Bitcoin staking (Cap-1, Cap-2, and Cap-3), Babylon has demonstrated increasing adoption, with a larger number of BTC stakers committing to the network. The higher the TVL, the more secure the PoS chains utilizing Babylon's infrastructure, ensuring long-term network stability.

Factors Influencing TVL

Several dynamic factors contribute to Babylon's TVL fluctuations:

1. Bitcoin Price Fluctuations

Since TVL is calculated in USD, fluctuations in Bitcoin's price significantly impact the reported value. A higher BTC price increases TVL, while a decline lowers the total valuation. As Babylon continues to expand, BTC market trends will remain a key factor in TVL assessments.

2. Increased Adoption of PoS Chains

The growing integration of PoS networks with Babylon's staking protocol influences TVL expansion. As more chains adopt Babylon's trustless security model, demand for BTC staking rises, leading to higher TVL figures. Key partnerships with leading PoS ecosystems are expected to drive continued adoption.

3. Decentralized Application (DApp) Activity

DApp growth plays a crucial role in increasing staking participation. With more applications utilizing Babylon's staking infrastructure, demand for BTC staking rises, pushing TVL higher. Staking incentives, yield opportunities, and DeFi integrations further contribute to this trend.

4. Institutional and Retail Participation

Babylon's appeal to both institutional investors and retail users influences TVL stability. Large-scale Bitcoin holders, custodians, and liquidity providers participating in BTC staking ensure steady capital inflows, reinforcing Babylon's position as a critical security provider in the PoS space.

Babylon's **Total Value Locked (TVL) of $6.1 billion** highlights its growing influence in the decentralized security landscape. As Bitcoin staking adoption increases, Babylon's TVL is expected to rise, strengthening the economic security of PoS chains. By addressing market dynamics, fostering partnerships, and encouraging staking participation, Babylon continues to solidify its role as a leader in decentralized blockchain security.

7. Conclusion and Recommendations

Key Takeaways

In this report, I have examined the role of Babylon in bridging Bitcoin's security with the scalability of PoS networks, evaluating the claim of enhancing interoperability. Although Babylon is still in the early stages of development, with a TVL of $6.1 billion representing approximately 0.3% of Bitcoin total market value, Babylon demonstrated its initial progress. By ensuring data availability and robust finality, it contributes to the foundational infrastructure of Web3. However, its long-term effectiveness in supporting decentralized applications and financial networks will depend on further adoption and ecosystem development.

Future Applications

Given its strengths in security and finality, Babylon’s integration with emerging projects like **WorldLand** and **My AI Network** presents significant opportunities:

- **WorldLand Integration**: WorldLand is an advanced blockchain ecosystem that supports verifiable AI computing, decentralized cloud services, and Web3 applications. Integrating Babylon’s finality mechanism can enhance security and ensure efficient data availability for AI-driven transactions. This collaboration could help in securing AI-generated data and decentralized AI processing.
- **My AI Network Synergy**: My AI Network operates within WorldLand, allowing users to own and monetize AI agents. Babylon’s Bitcoin-backed security model can provide an additional layer of trust for AI-driven economies, ensuring the integrity of AI agent transactions and protecting against fraud.

Recommendations

1. **Technical Exploration**: Conduct a feasibility study on integrating Babylon’s finality providers with WorldLand’s verifiable AI computing infrastructure.
2. **Staked BTC Optimization**: Further analyze the dynamics of **staked BTC** and **finality providers** to refine the economic incentives for securing AI-driven smart contracts.
3. **Strategic Partnerships**: Establish collaborations with decentralized AI ecosystems, ensuring that Babylon’s security model is integrated with emerging AI and Web3 infrastructures.
4. **Scalability Enhancements**: Explore the use of Babylon’s data availability solutions to optimize WorldLand’s AI marketplace, ensuring cost-efficient and secure AI transactions.

By leveraging Babylon’s strengths, projects like WorldLand and My AI Network can achieve **greater decentralization, improved security, and enhanced scalability**, fostering the next wave of AI-driven decentralized economies.

Bitcoin staking in Babylon's System

Function: *CreateBTCDelegation* (Bitcoin Staking Process):

- ✓ This function processes a Bitcoin staking transaction submitted by a user, verifies all necessary conditions, and registers the delegation in Babylon's state.

```
func (ms msgServer) CreateBTCDelegation(goCtx context.Context,
req *types.MsgCreateBTCDelegation)
(*types.MsgCreateBTCDelegationResponse, error)
```

- ✓ goCtx: the context from the user
- ✓ req: contains staker's public key, Proof of Possession, Staking transaction, finality providers, unbounding information.

1. Getting the Babylon's Context:

```
ctx := sdk.UnwrapSDKContext(goCtx)
```

- ✓ This extracts the Cosmos SDK context, which allows us to read/write blockchain state.

2. Parse the Staking Message:

```
parsedMsg, err := types.ParseCreateDelegationMessage(req)
                    if err != nil {
    return nil, status.Errorf(codes.InvalidArgument, "%v",
```

- ✓ Convert the raw request (req) into structured format (parsedMsg). If something is invalid, returns an error.

3. Verify the PoP:

```
if err := parsedMsg.ParsedPop.Verify(parsedMsg.StakerAddress,
  parsedMsg.StakerPK.BIP340PubKey, ms.btcNet); err != nil {
                        return nil,
    types.ErrInvalidProofOfPossession.Wrap(err.Error())}
```

- ✓ Necessary for the staker to control the bitcoin public key, when failed rejects the transaction.

4. Check for Duplicate Staking Transactions:

```
stakingTxHash := parsedMsg.StakingTx.Transaction.TxHash()

delegation := ms.getBTCDelegation(ctx, stakingTxHash)

if delegation != nil {

return nil, types.ErrReusedStakingTx.Wrapf("duplicated tx
hash: %s", stakingTxHash.String())}
```

- ✓ The code above prevents the same BTC staking transaction from being used. If duplicate, then reject the request.

5. Validate the Finality Providers:

```
restakedToConsumers, err := ms.validateRestakedFPs(ctx,
parsedMsg.FinalityProviderKeys.PublicKeysBbnFormat)

if err != nil {

return nil, err}
```

- ✓ Check if they exist in Babylon, not slashed and at least one is registered finality provider.

6. Fetch Time & Parameters:

```
timeInfo, params, paramsVersion, err :=
ms.getTimeInfoAndParams(ctx, parsedMsg)

if err != nil {return nil, err}
```

- ✓ The code above gets the current blockchain height and Babylon's staking parameters. Determines when the stake starts and ends.

7. Validate Staking Transaction:

```
paramsValidationResult, err :=
types.ValidateParsedMessageAgainstTheParams(parsedMsg, params,
ms.btcNet)

if err != nil {return nil, err}
```

- ✓ The code above checks if the staking transaction follows the staking rules of Babylon.

8. Check if Staking Transaction is Allowed:

```
            if ms.isAllowListEnabled(ctx, params) {
    if !ms.IsStakingTransactionAllowed(ctx, &stakingTxHash) {
        return nil, types.ErrInvalidStakingTx.Wrapf("staking
          tx hash: %s, is not in the allow list",
                stakingTxHash.String())}}
```

- ✓ Puts the staking transaction on the allowlist if meets the requirements and applicable.

9. Additional Gas Costs:

```
            if !parsedMsg.IsIncludedOnBTC() {

ctx.GasMeter().ConsumeGas(params.DelegationCreationBaseGasFee,
```

- ✓ If the staking transaction is not included in the Bitcoin yet, Babylon charges extra gas fees.

10. Construct & Store the BTC Delegation:

```
            newBTCDel := &types.BTCDelegation{
       StakerAddr:       parsedMsg.StakerAddress.String(),
        BtcPk:            parsedMsg.StakerPK.BIP340PubKey,
              Pop:              parsedMsg.ParsedPop,
                        FpBtcPkList:
    parsedMsg.FinalityProviderKeys.PublicKeysBbnFormat,
        StakingTime:      uint32(parsedMsg.StakingTime),
            StartHeight:      timeInfo.StartHeight,
             EndHeight:        timeInfo.EndHeight,
       TotalSat:         uint64(parsedMsg.StakingValue),
     StakingTx:        parsedMsg.StakingTx.TransactionBytes,
```

- ✓ The code above creates a new BTCDelegation object, which stores:
    1. The staker's address & BTC key
    2. The PoP verification
    3. The list of finality providers
    4. The staking transaction details
    5. Slashing protections

11. Save the Delegation:

```
if err := ms.AddBTCDelegation(ctx, newBTCDel); err != nil {

    panic(fmt.Errorf("failed to add BTC delegation that has
              passed verification: %w", err))}
```

- ✓ Stores the delegation inside the Babylon blockchain state.

Restaking in Babylon's System

1. Check if the Delegation is Being "Restaked":

```
restakedToConsumers, err := ms.validateRestakedFPs(ctx,
  parsedMsg.FinalityProviderKeys.PublicKeysBbnFormat)

            if err != nil {return nil, err}
```

- ✓ The function validateRestakedFPs chack if the BTC stake is being redelegated to different finality providers. This allows to stake the BTC with new providers without unbounding first.
- ✓ This process is beneficial when instead of withdrawing and restaking later, Babylon directly moves the stake to another provider.

2. Indexing the Restaked Delegation:

```
                if restakedToConsumers {

  if err := ms.indexBTCConsumerDelegation(ctx, newBTCDel);
                    err != nil {

        panic(fmt.Errorf("failed to add BTC delegation
restaked to consumers' finality providers despite it has
          passed verification: %w", err))}}
```

- ✓ If the delegation is restaked, it is indexed separately. The function indexBTCConsumerDelegation ensures that restaked BTC is correctly recorded.
- ✓ The importance of this is that it allows BTC to be restaked across different consumer chains or providers.

Slashing in Babylon's System

Function: *SelectiveSlashingEvidence* (Slashing Malicious Finality Providers)

```
func (ms msgServer) SelectiveSlashingEvidence(goCtx
context.Context, req *types.MsgSelectiveSlashingEvidence)
(*types.MsgSelectiveSlashingEvidenceResponse, error)
```

- ✓ The function above penalizes the finality providers who perform selective slashing. It verifies if a finality provider has acted maliciously and then slashes them.

1. Get the staking record:

```
btcDel, bsParams, err := ms.getBTCDelWithParams(ctx,
                req.StakingTxHash)

            if err != nil {return nil, err}
```

- ✓ Responsible for retrieving the BTC delegation record using the staking transaction hash, necessary for confirming the stake before performing slashing.

2. Check if the Stake is Still Active:

```
        btcTip := ms.btclcKeeper.GetTipInfo(ctx)

if btcDel.GetStatus(btcTip.Height, bsParams.CovenantQuorum) !=
types.BTCDelegationStatus_ACTIVE && !btcDel.IsUnbondedEarly()
                            {

    return nil, types.ErrBTCDelegationNotFound.Wrap("a BTC
 delegation that is not active or unbonding early cannot be
```

- ✓ The code above is to check if the stake is still active and was unbounded early. To perform a slashing the delegation must be active.

3. Decide the Finality Provider's BTC Secret Key:

```
fpSK, fpPK := btcec.PrivKeyFromBytes(req.RecoveredFpBtcSk)

       fpBTCPK := bbn.NewBIP340PubKeyFromBTCPK(fpPK)
```

- ✓ Extracts the Bitcoin secret key (SK) of the finality provider that allegedly engaged in selective slashing. It is important for verifying the finality provider who signed an invalid transaction.

4. Ensure the BTC Stake Was Linked to the Finality Provider:

```
fpIdx := btcDel.GetFpIdx(fpBTCPK)

if fpIdx == -1 {

return nil, types.ErrFpNotFound.Wrapf("BTC delegation is
not staked to the finality provider")}
```

- ✓ Checks if the BTC delegation was actually staked to the finality provider in question. If the stake was never linked to the finality provider, then slashing does not occur.

5. Check if the Finality Provider Has Already Been slashed:

```
fp, err := ms.GetFinalityProvider(ctx, fpBTCPK.MustMarshal())

if err != nil {

panic(types.ErrFpNotFound.Wrapf("failing to find the
finality provider with BTC delegations"))}

if fp.IsSlashed() {

return nil, types.ErrFpAlreadySlashed}
```

- ✓ Important for ensuring the finality provider has not already been slashed. A provider should not be slashed multiple times for the same activity.

6. Slash the Finality Provider:

```
if err := ms.SlashFinalityProvider(ctx,
fpBTCPK.MustMarshal()); err != nil {

panic(err) // failed to slash the finality provider, must
be programming error}
```

- ✓ The code above marks the finality provider as slashed in the Babylon's system. They lose their stake and cannot participate in the finality anymore. This protects honest stakers and punishes malicious behavior.

7. Emit an event About the Slashing:

```
        evidence := &types.SelectiveSlashingEvidence{
              StakingTxHash:    req.StakingTxHash,
                   FpBtcPk:          fpBTCPK,
              RecoveredFpBtcSk: fpSK.Serialize(),}
  event := &types.EventSelectiveSlashing{Evidence: evidence}
                          if err :=
sdk.UnwrapSDKContext(ctx).EventManager().EmitTypedEvent(event)
                       ; err != nil {
     panic(fmt.Errorf("failed to emit EventSelectiveSlashing
                     event: %w", err))}
```

- ✓ The code above notifies the network that a provider has been slashed, and leaves the evidence recorded on the chain.

8. Mark the Transaction as Refundable:

```
            ms.iKeeper.IndexRefundableMsg(ctx, req)
```

- ✓ This code is necessary to encourage users to report slashing, since it marks the slashing transaction as refundable and the sender will not use extra transaction fees.

9. Return Success Response:

```
   return &types.MsgSelectiveSlashingEvidenceResponse{}, nil
```

- ✓ It is necessary for confirming that the slashing was successful, and the slashed finality provider is now removed from Babylon's network.

References:

1. Babylon Labs. *Babylon's Key Achievements and What to Expect in 2025.* Available at: https://babylonlabs.io/blog/2024-in-review-babylons-key-achievements-and-what-to-expect-in-2025
2. Babylon Labs. *Official Documentation.* Available at: https://babylon.xyz/
3. Babylon Labs. *Bitcoin Staking Litepaper.* Available at: https://babylon.xyz/resources/litepaper
4. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System,* 2008. Available at: https://bitcoin.org/bitcoin.pdf
5. Research on PoS vulnerabilities. Available at: https://arxiv.org/abs/1904.12230
6. Babylon Labs. *SatLayer Integrates with Babylon.* Available at: https://babylonlabs.io/blog/satlayer-integrates-with-babylon
7. Babylon Labs. *Forkless Rollups with Bitcoin Staking.* Available at: https://babylonlabs.io/blog/forkless-rollups-with-bitcoin-staking
8. Babylon Labs. *Testnet 4 Pre-Launch Announcement.* Available at: https://babylonlabs.io/blog/babylon-testnet-4-pre-launch-announcement
9. Babylon Labs. *The Quest for Utility: BTC Staking Ecosystem Update.* Available at: https://babylonlabs.io/blog/the-quest-for-utility-btc-staking-ecosystem-update
10. Babylon Labs. *Technical Preliminaries of Bitcoin Staking.* Available at: https://babylonlabs.io/blog/technical-preliminaries-of-bitcoin-staking
11. Babylon Labs. *What is Bitcoin Staking?* Available at: https://babylonlabs.io/blog/what-is-bitcoin-staking
12. Babylon Labs. *Babylon's Bitcoin Staking Contract.* Available at: https://babylonlabs.io/blog/babylon-s-bitcoin-staking-contract
13. Babylon Labs. *BTC Staking Testnet.* Available at: https://btcstaking.testnet.babylonlabs.io/
14. Babylon Labs. *Babylon Phase 2 Testnet Launch.* Available at: https://babylonlabs.io/blog/babylon-phase-2-testnet-launch

15. Babylon Labs. *How a 10,000 BTC Stake Redefines Bitcoin Staking.* Available at: https://babylonlabs.io/blog/how-a-10-000-btc-stake-redefines-bitcoin-staking

16. Babylon Labs. *What Does Babylon Phase 1 Launch Mean?* Available at: https://babylonlabs.io/blog/what-does-babylon-phase-1-launch-mean

17. Babylon Labs. *Get Ready for Cap 3: Your Guide to Participating in Babylon Bitcoin Staking.* Available at: https://babylonlabs.io/blog/get-ready-for-cap-3-your-guide-to-participating-in-babylon-bitcoin-staking

18. Babylon Labs. *Babylon Bitcoin Staking Mainnet Launch Phase 1 Cap 3.* Available at: https://babylonlabs.io/blog/babylon-bitcoin-staking-mainnet-launch-phase-1-cap-3

19. Babylon Labs. *Babylon Ecosystem Update 2: Unlocking Bitcoin's Full Potential.* Available at: https://babylonlabs.io/blog/babylon-ecosystem-update-2-unlocking-bitcoins-full-potential

20. Babylon Labs. *Babylon Bitcoin Staking Mainnet Launch Phase 1.* Available at: https://babylonlabs.io/blog/babylon-bitcoin-staking-mainnet-launch-phase-1

21. Babylon Labs. *Checkpointing Consumer Zones to Babylon via IBC.* Available at: https://babylonlabs.io/blog/checkpointing-consumer-zones-to-babylon-via-ibc

22. Babylon Labs. *Checkpointing Babylon to BTC.* Available at: https://babylonlabs.io/blog/checkpointing-babylon-to-btc

23. Babylon Labs. *Interchain Timestamping for Mesh Security.* Available at: https://babylonlabs.io/blog/interchain-timestamping-for-mesh-security

24. Babylon Labs. *Babylon Bitcoin Security for Cosmos and Beyond.* Available at: https://babylonlabs.io/blog/babylon-bitcoin-security-for-cosmos-and-beyond

25. Babylon Labs. A New Chapter for Bitcoin: Recap of Bitcoin Renaissance 2024. Available at: https://babylonlabs.io/blog/a-new-chapter-for-bitcoin-recap-of-bitcoin-renaissance-2024

26. Babylon Labs. Babylon Labs GitHub Repository. Available at: https://github.com/babylonlabs-io

27. Tas, E. N., Tse, D., Gai, F., Kannan, S., Maddah-Ali, M. A., & Yu, F. *Bitcoin-Enhanced Proof-of-Stake Security: Possibilities and Impossibilities.* IEEE Symposium on Security and Privacy (SP), 2023. Available at: DOI 10.1109/SP46215.2023.00099