April 7, 2025

Babylon, Bitcoin Staking Mechanism and Japanese Law

So Saito
Founding Partner/ Attorney-at-Law
So & Sato Law Offices

This article describes the structure of "Babylon," a pioneering Bitcoin (BTC) staking project and considered the largest of its kind today, and the related issues under Japanese law.

Until now, staking has mainly taken place on Proof of Stake (PoS) chains such as Ethereum. Staking in PoS is a mechanism to increase the security of the chain by participating in the validation of transactions on the network, etc., in exchange for a reward.

In contrast, because Bitcoin employs Proof of Work (PoW), it has been believed that, in principle, there is no revenue opportunity from staking in the traditional sense of the term. The most common means of monetization using BTC has been through centralized lending services and tokenization solutions such as wBTC (Wrapped BTC).

Babylon is a project that aims to overcome these limitations of BTC utilization and realize trustless staking using BTC, and is currently one of the most popular protocols in this field. This paper examines its technical structure and issues under Japanese law.

In order to fully understand Bitcoin staking, it is helpful to have a foundational understanding of the staking mechanisms used in PoS chains, as well as the concepts of liquid staking (e.g., by LIDO) and restaking (e.g., by EigenLayer).

For more information on these topics, please refer to the following articles authored by our firm:

(References)

(1) Our previous Article on POS chain staking (in English)

・https://innovationlaw.jp/en/staking-restaking-under-japanese-law/

(2) Our previous Articles on POS chain staking (in Japanese)

・Organizing Legal Issues on Staking 2020.3.17

・DeFi and the Law - LIDO and Liquid Staking Mechanisms and Japanese Law 2023.10.17

・EigenLayer and other Restaking Mechanisms and Japanese Law 2024.5.10

I. Overview of Legal Issues

(1) The Babylon mechanism itself does not appear to fall under the custody regulations under the Payment Services Act (PSA).

(2) The structure of Babylon is not considered to constitute a collective investment scheme (fund) under the Financial Instruments and Exchange Act (FIEA).

(3) If a liquid staking provider holds custody of a user's BTC private key, such a provider may fall within the scope of custody regulations under the PSA. Legal classification should be assessed on a case-by-case basis depending on the structure.

(4) Japanese crypto asset exchanges are generally permitted to offer BTC staking services through Babylon under the current legal framework.

(5) One practical issue for Japanese crypto asset exchanges is that the rewards granted through the Babylon protocol may be altcoins that are not classified as "handled crypto assets" for that exchange. In such cases, the exchange is not permitted to custody these altcoins on behalf of users under current Japanese regulations. Accordingly, alternative measures must be considered, such as (i) transferring the altcoins to the user’s unhosted wallet, or (ii) selling or swapping them via a DEX or an overseas partner, and then crediting the user with BTC or Japanese yen.

II. Basic Overview of Babylon

1 What is Babylon's Bitcoin Staking?

Bitcoin uses PoW (Proof of Work), which means that staking is not possible in the same way as with Ethereum.

Babylon introduces a new mechanism that enables BTC staking, with the following key features:

1 BTC is staked not to secure the Bitcoin network itself, but to secure other networks that rely on PoS-like economic security mechanisms, collectively referred to as Bitcoin-Secured Networks (BSNs).

2 Rewards are determined by the secured networks, typically in the form of their native tokens.

3 BTC can be used to secure multiple such networks simultaneously, potentially increasing yield (albeit with higher associated risks).

4 Staking does not require transferring the BTC private key; instead, it is conducted in a trustless and non-custodial manner using one-time signatures (EOTS: Extractable One-Time Signatures).

2 What does it mean to stake BTC to secure other PoS networks?

One of Babylon's most important features is that it uses Bitcoin to enhance the security of "other" PoS networks.

The eligible networks are those that meet certain technical requirements and generally fall under the broad category of PoS-based systems—i.e., networks that have their own validator sets.

Currently, Babylon has announced test integrations and partnerships with various types of networks, including rollups, data availability (DA) chains, and oracle networks.

3 PoS Network Security and Staking

In a Proof-of-Stake network, security is provided by validators who stake assets—either their own or those delegated to them by third parties—to verify transactions and produce blocks.

If validators behave dishonestly, the staked assets may be slashed (i.e., partially confiscated), creating a strong financial incentive to act honestly and support the stability of the network.

In many PoS networks, delegated staking is possible, allowing token holders who do not run validators themselves to delegate their tokens to trusted validators.

In such cases, validators are responsible for the staked assets regardless of whether they are self-staked or delegated.

However, in order to participate in staking—either directly or via delegation—users must first acquire the native token of the target PoS network.

For emerging or smaller-scale networks, this presents several challenges:

- There are relatively few holders of the token (due to acquisition costs and price volatility),
- Token ownership may be highly concentrated,
- As a result, there may be a limited number of validators or insufficient total stake, weakening the network's security guarantees.

Babylon aims to address these challenges by allowing Bitcoin holders to contribute to the security of such networks—collectively referred to as Bitcoin-Secured Networks (BSNs)—without requiring them to acquire the native token or transfer custody of their BTC.

Security participation is instead enabled through a trustless, signature-based mechanism.

4 Enhanced security with BTC

As mentioned above, Babylon introduces a mechanism to enhance the security of PoS-based networks by leveraging BTC, an external asset, to address the inherent security limitations these networks may face.

Specifically, BTC holders contribute economic security by staking their BTC, which is used to support the security of external networks.

Importantly, this BTC collateral is not transferred directly to the PoS networks. Instead, it remains in the user's self-managed script on the Bitcoin network, and staking is performed via the Babylon protocol through a cryptographic signature (digital proof of intent).

This design enables non-custodial and trustless participation, eliminating the need to deposit or lock up BTC with a third party.

By introducing such externally sourced security, PoS networks can leverage BTC's high liquidity and market capitalization to reinforce their security infrastructure—without relying solely on their native tokens.

This mechanism is particularly promising for emerging PoS networks, where token distribution may be highly concentrated and the validator set small, leading to weaker security. Babylon's BTC-based model may serve as a viable complement to address these vulnerabilities.

5 Rewards Are Paid in Tokens on the PoS Network

The rewards for staking BTC through Babylon are not paid in BTC itself, but in the native tokens designated by the PoS network that receives the security service.

From the perspective of the PoS network, this structure allows it to externally source economic security (in the form of BTC) by using its own native tokens as incentives. Through appropriate token issuance and incentive design, the network can attract BTC stakers without requiring external capital.

For BTC stakers, this provides the benefit of earning yield in the form of external PoS network tokens—without needing to transfer or wrap their BTC. This feature may present a new yield opportunity, particularly for long-term BTC holders looking to earn passive returns on their assets.

Risk Associated with Rewards Being Paid in Other PoS Tokens

While Babylon offers BTC holders the opportunity to earn yield, there are several risks associated with the fact that rewards are paid in the native tokens of external PoS networks rather than in BTC.

This structure may also present practical and regulatory challenges, especially for users staking through crypto asset exchanges in Japan. As discussed in Section IV-3 below, it could act as a disincentive for such platforms to offer Babylon staking services.

Risks Associated with Receiving Rewards in Other Tokens

• Price Volatility Risk of Reward Tokens

The reward tokens received from PoS networks generally have lower market capitalization and liquidity compared to BTC, making them more susceptible to price volatility.

Even if the nominal reward amount is high, a sharp decline in the token price could result in a significantly reduced effective yield.

• Liquidity and Redemption Risk

If the reward tokens are issued by a relatively niche or illiquid chain, they may be difficult to redeem on the open market, or suffer from large bid-ask spreads, reducing the actual profitability of staking.

• Continuity and Stability of Reward Design

If the PoS network changes its reward policy or reduces incentives in the future, the economic appeal of Bitcoin staking may diminish.

Moreover, if the chain's operations are unstable, there is a risk that rewards may not be distributed properly or consistently.

6 Trustless Staking Without Private Key Transfer in Babylon

Babylon is designed to allow BTC holders to participate in network security as providers of economic collateral—autonomously and non-custodially, without transferring their private keys to any third party.

This architecture enables truly trustless staking, eliminating the need for traditional asset transfers or reliance on custodians.

(1) What It Means Not to Transfer the Private Key

In conventional staking and DeFi use cases, utilizing crypto assets typically requires one of the following actions:

- Wrapping the original asset (e.g., BTC) into a token that can be used on another chain (e.g., wBTC)
- Locking the asset into a third-party custodian or smart contract as collateral

Both methods effectively require giving up control of the private key, at least temporarily, which introduces risks such as asset leakage or loss due to smart contract vulnerabilities.

Babylon avoids these risks by enabling signature-based staking mechanism. This allows BTC holders to retain full control over their assets while still participating in economic security provision.

(2) Technical Mechanism: Declaration of Staking Intent via One-Time Signature (EOTS)

Babylon utilizes a cryptographic technique known as Extractable One-Time Signatures (EOTS) to allow BTC stakers to both prove their ownership of BTC and explicitly accept responsibility for contributing to the security of a PoS-based system.

The basic flow of this mechanism is as follows:

1. The BTC staker selects a finality provider and generates the transaction data necessary to initiate staking.
2. The transaction includes the following conditional clauses:
   (i) The designated BTC cannot be transferred for a fixed period (e.g., three days);
   (ii) If certain predefined conditions arise during that period, the BTC will be sent to a predetermined address (typically a burn address);
   (iii) However, the BTC staker retains the right to cancel (revoke) the transaction at any time before the fixed period ends, as long as no slashing condition has been triggered.
3. The “predefined conditions” referred to in (ii) generally correspond to slashing events—e.g., if the selected finality provider engages in dishonest behavior (such as submitting double signatures), the BTC will be forcibly sent to the burn address as a

penalty.

4. The BTC staker finalizes the process by signing the transaction using a one-time EOTS (Extractable One-Time Signature), thereby proving BTC ownership and formally declaring their intent to participate in security provision.

This design enables PoS networks to receive a security guarantee backed by BTC, a highly liquid external asset, while the Babylon protocol itself provides a comprehensive framework for detecting malicious behavior and executing slashing penalties.

Method of Signature (Source: Babylon's Litepaper https://docs.babylonlabs.io/papers/btc_staking_litepaper%28EN%29.pdf?utm_source=chatgpt.com)

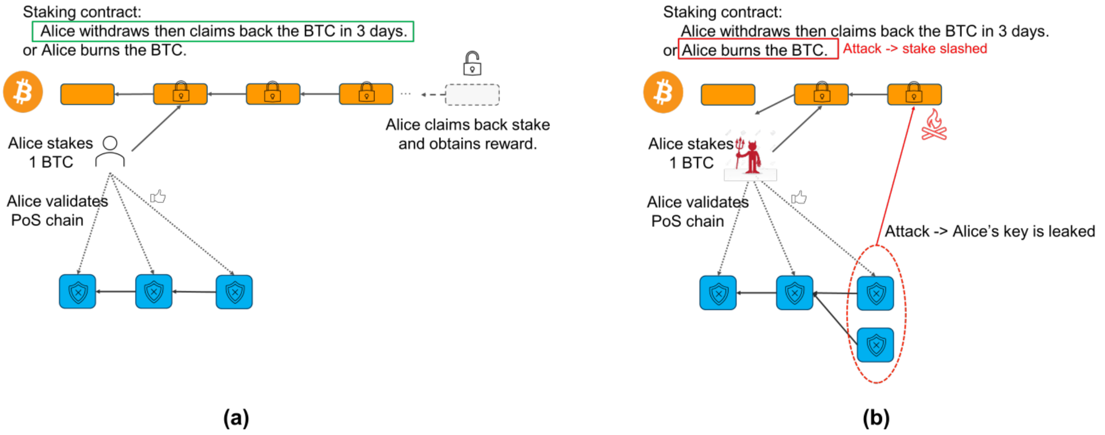


Figure 2: A Bitcoin staker's journey: (a) the happy path: Alice stakes, validates the PoS chain, requests unbonding, and unstakes in 3 days; (b) the unhappy path: Alice stakes, commits a safety offense to the PoS chain, and then her bitcoin got burned.

7 Significance and Limitations of Trustless Design

The BTC staking mechanism enabled by Babylon is characterized by a trustless and non-custodial architecture, in the following respects:

- BTC remains in the user's self-managed script and is never transferred to a third party.
- The intention to provide collateral can be expressed solely through a cryptographic signature (digital proof), without relying on centralized intermediaries or smart contracts.
- Participation in security provision and the receipt of rewards are possible based solely on that signature.

This structure, which minimizes the need for trust in third parties, is closely aligned with Bitcoin’s foundational principles of self-custody and decentralization.

However, it is important to note that the system is not entirely “trustless.”

Certain functions—such as verifying signatures, executing slashing, and distributing rewards—are handled by the Babylon Genesis Chain, described below.

In other words, while BTC itself is never directly deposited or locked up, a degree of “protocol trust” is still required—specifically, trust in the legitimate operation and correct implementation of the Babylon protocol, including the Babylon Genesis Chain.

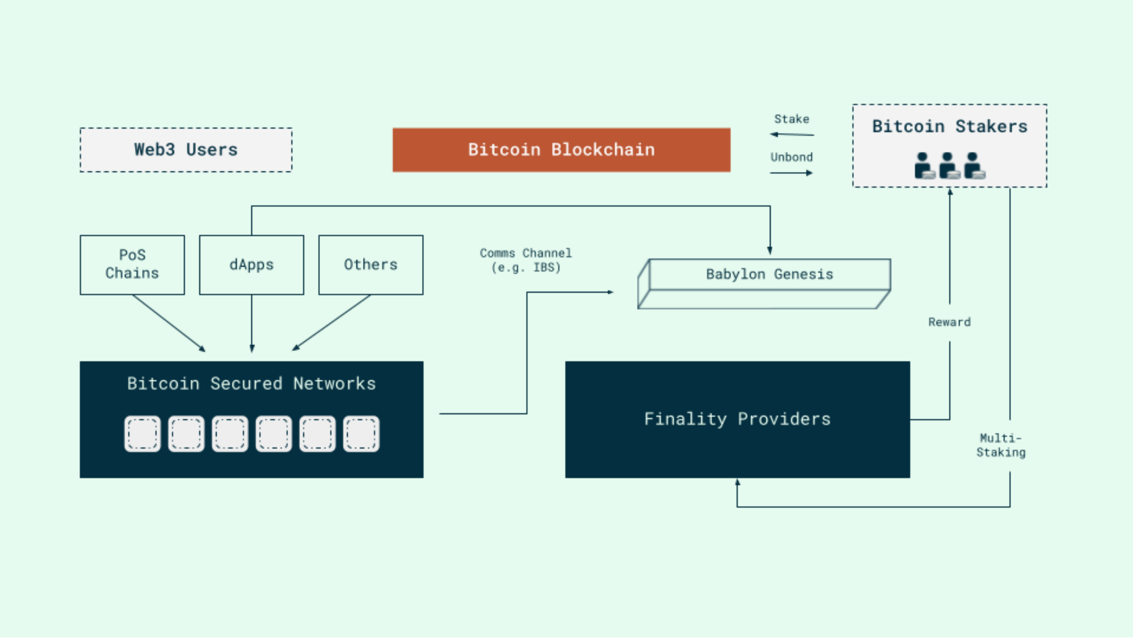
III. Important Entities in the Babylon Ecosystem

The entities involved in the Babylon ecosystem are diverse, but some of the key participants include following:

1 Important Entities about Babylon

Figure: Babylon Overview

(Source: Babylon.docs https://docs.babylonlabs.io/guides/overview/)



(1) Bitcoin-Secured Networks (BSNs)

- **Summary**:

Bitcoin-Secured Networks (BSNs) refer to a category of networks (or chains) that enhance their security by integrating Bitcoin's economic security via Babylon. These networks typically operate on PoS or PoS-like systems and utilize BTC as external collateral to strengthen their security infrastructure.

- **Role**:

PoS networks, particularly in their early stages, often face security challenges due to a small or overly centralized validator set and insufficient economic collateral. By incorporating BTC through Babylon, BSNs can achieve the following:

(i) Enhanced Security with BTC

By leveraging BTC—a highly liquid and trusted external asset—PoS networks can strengthen their resilience against network attacks (currently focused on mitigating double-signing risks).

(ii) Improved Finality Guarantees

BSNs can obtain "external finality" for their blocks through cryptographic signatures submitted by Babylon's finality providers, further strengthening consensus assurance.

(iii) Incentive Design to Attract BTC Stakers

By offering rewards in their native tokens or stablecoins, BSNs can economically incentivize BTC stakers to participate in securing the network, offsetting the cost of enhanced security.

• **Typical Use Cases (Examples)**:

- Emerging app chains built with the Cosmos SDK
- PoS networks with volatile or weak native token economics
- Ethereum Layer 2 chains
- Gaming chains, DePIN networks, AI chains, and other specialized blockchain applications
- In theory, Babylon can provide security to all PoS networks.

(2) Finality Providers

• **Summary**:

Entities that observe and verify block finality on PoS networks secured by Babylon, and submit cryptographic finality signatures accordingly.

• **Role**:

- Generate and submit finality signatures to the Babylon protocol
- Ensure honest behavior, as fraudulent signatures may trigger slashing penalties

• **Note**:

Finality providers differ from traditional validators in other chains. Their core responsibility is to observe the finality of blocks on the target PoS network and report that information to the Babylon chain.

However, they play a somewhat validator-like role in that they create and submit cryptographic signatures, earn rewards for doing so, and are subject to slashing in case of misconduct.

Comparison of Finality Providers and General PoS Validators

Item	Finality Provider (Babylon)	General PoS Chain Validator
Block Generation	❌ Not performed	✅ Performed
Finality Observation	✅ Performed	❌ Typically not involved (finality is emergent)

Signature Type	✅ Signs finality data	✅ Signs blocks and voting messages
Slashing Risk	✅ Yes (for fraudulent finality signatures)	✅ Yes (for double signing, downtime, etc.)
Reward Mechanism	✅ Yes (based on submitted signatures)	✅ Yes (based on block production and delegation)

(3) Bitcoin Stakers

• **Role**:

Hold BTC and contribute to the security of PoS networks by submitting off-chain cryptographic signatures to Babylon.

• **Reward**:

Receive staking rewards from the PoS networks in return for providing BTC as collateral via Babylon.

• **Key Characteristics**:

- BTC stakers do not need to transfer their BTC or private keys to any third party.
- They retain full control over their assets while participating in staking.
- The process is non-custodial and trustless by design.

BTC stakers can also delegate their staking to finality providers.

Even in such cases, no BTC or private key is transferred, and the delegation is completed through a non-custodial mechanism.

(4) Babylon Genesis Chain (one of the BSNs)

- The Babylon Genesis Chain is a Cosmos SDK-based PoS Layer 1 blockchain designed to operate the Babylon protocol.
- Although it is one of the Bitcoin-Secured Networks (BSNs), it plays a central role within the Babylon ecosystem, serving as its foundational coordination layer.

Function	**Description**
Signature Verification	Receives and verifies signatures from BTC stakers and finality providers.
Slashing Enforcement	Executes slashing penalties when fraudulent or malicious signatures are detected.
Finality Recording	Records the finality of blocks from PoS networks on Bitcoin (e.g., via timestamping).
Cross-Chain Relay	Relays verified security information and signatures to other

	BSNs.

- If you participate as a finality provider securing the Babylon Genesis Chain, you will receive the chain's native token, "BABY," as a reward.

(5) Liquid Staking Protocol (not shown in the figure above)

A protocol that facilitates BTC staking via Babylon on behalf of BTC holders, aiming to improve operational efficiency, usability, and liquidity. While the main focus is on liquid staking, a hybrid model that combines restaking (reuse of the same BTC for multiple networks) may also be adopted where appropriate.

Key functions:

(i)Streamlining Operations

Since it is burdensome for BTC holders to individually generate signatures and monitor activity across multiple PoS networks, the protocol handles the following tasks:

- Selection of PoS networks for staking
- Automatic generation and management of EOTS signatures
- Collection and distribution of staking rewards

(ii) Issuance and Utilization of Liquid Staking Tokens (LSTs)

The protocol issues liquid staking tokens (e.g., stBTC) backed by the user's staked BTC position. This allows the user to retain liquidity of their assets even while staking, enabling secondary use in DeFi and other ecosystems.

(iii) Complementary Use of Restaking

By carefully managing risk, the protocol may reuse the same BTC signature across multiple PoS networks (i.e., multi-staking), thereby maximizing yield.

2 Supplement: Relationship Between the Babylon Ecosystem and the Babylon Genesis Chain

The relationship between the Babylon ecosystem and the Babylon Genesis Chain is nuanced and may require clarification.

The Babylon Genesis Chain is a PoS Layer 1 blockchain that plays a central role within the Babylon ecosystem. However, it is not synonymous with the ecosystem itself.

The Babylon protocol refers to a broader framework encompassing multiple Bitcoin-Secured Networks (BSNs) that utilize Bitcoin-based economic security via Babylon.

If a participant joins Babylon as a finality provider and provides finality to the Babylon Genesis Chain, they receive "BABY", the native token, as a reward.

Finality providers currently serve the Babylon Genesis Chain, where they contribute to finality and receive BABY, the native token, as compensation. Although the Babylon protocol is designed to be extendable to other Bitcoin-Secured Networks (BSNs), finality provisioning beyond the Genesis Chain has not yet been implemented. In the future, other BSNs may adopt the Babylon finality mechanism and offer their own tokens as rewards to finality providers.

In addition, the Babylon Genesis Chain has its own set of validators, who stake BABY and participate in block production and consensus. These validators are also rewarded in BABY for their contributions to the network's operation.

1 Overview of BABY Token: Acquisition Methods and Utility

Item	Details
Token Name	BABY (Native token of the Babylon Genesis Chain)
Means of Acquisition 1	Stake BABY and participate as a validator in block production and validation on the Babylon Genesis Chain
Means of Acquisition 2	Provide finality to the Babylon Genesis Chain using BTC as a finality provider
Primary Use Case 1	Staking collateral for validator participation
Primary Use Case 2	Governance (proposal creation and voting rights)
Primary Use Case 3	Network fees (planned in the future)
Additional Notes	Rewards in other BSNs are typically paid in each BSN's own native token, not BABY

2 Comparison: Finality Providers vs. Validators (on the Babylon Genesis Chain)

Item	Finality Provider	Validator (Babylon Genesis Chain)
Staked Asset	BTC (non-custodial)	BABY token (non-custodial)
Primary Role	Provide finality (submit signatures) to BSNs	Block production and validation on Babylon Genesis Chain
Target Chain(s)	Babylon Genesis Chain and other BSNs	Only the Babylon Genesis Chain
Reward Token	BABY or BSN-native token (depending on the chain)	BABY token

Slashing Risk	Signature invalidation and BTC burn (e.g., double signing)	Slashing of staked BABY (e.g., double signing or downtime)
Staking Method	Declaration of intent via BTC signature (held in a self-managed script; delegation also possible)	On-chain BABY token staking (self-custodied; delegation also possible)

IV. Bitcoin Staking and Japanese Law

Based on the above assumptions, this section outlines the key legal issues related to providing or using a Bitcoin staking service such as Babylon.

In particular, the analysis focuses on two core questions:

- Whether the **custody regulations** under the Payment Services Act (資金決済法) apply, and
- Whether the **fund regulations** under the Financial Instruments and Exchange Act (FIEA, 金融商品取引法) are triggered.

1 Babylon and the Custody Regulation of Crypto Assets

In the context of BTC staking via Babylon, a key legal issue is whether the provision of BTC as economic security constitutes the “management” or “custody” of crypto assets under Japanese law.

Under custody regulations based on the Payment Services Act, the primary legal criterion is generally understood to be whether the service provider holds the private key required to transfer the user’s crypto assets.

This interpretation is supported by an official public comment issued in connection with the 2019 amendments to the Act:

“If a business operator does not possess any of the private keys necessary to transfer the cryptographic assets of a user, the business operator is not considered to be in a position to proactively transfer the cryptographic assets of the user, and therefore, basically, is not considered to fall under the category of ‘managing cryptographic assets for others’ as stipulated in Article 2, Paragraph 7, Item 4 of the Payment Services Act.”

In this regard, the private key required to transfer BTC is never shared with or transferred to any entity, including the Babylon Genesis Chain or finality providers.

The technical structure of the system is as follows:

- The BTC staker selects a finality provider and generates the necessary transaction data to initiate staking.
- The transaction includes a conditional instruction, such as:

(i) the BTC will be locked for a specified period; and

(ii) if a slashing event occurs, the BTC will be transferred to a predefined burn address.

- The BTC staker signs this transaction using a one-time EOTS (Extractable One-Time Signature), thereby proving ownership and expressing intent to participate in staking.

This design enables BTC to serve as economic security without transferring control of the private key, ensuring that the BTC remains in the staker's custody unless slashing conditions are triggered.

Accordingly, Babylon and finality providers would generally not be considered to fall under custody regulations under the Payment Services Act.

However, it should be noted that certain Liquid Staking Protocols may offer services that involve taking custody of users' private keys. In such cases, those entities may indeed be subject to custody regulations, and a case-by-case legal assessment would be required.

2 Babylon and the FIEA Regulations

In Babylon, BTC is provided as economic security, and BTC stakers receive compensation while bearing certain risks such as slashing. From this structure, a legal question arises as to whether Babylon might be classified as a "fund" (collective investment scheme) under Japanese law.

(1) Definition of "Fund (Collective Investment Scheme)" under Japanese Law

Article 2, Paragraph 2, Items 5 and 6 of the Financial Instruments and Exchange Act ("FIEA") broadly define a "fund" (collective investment scheme) as follows:

(A) Covered Forms of Rights (any of the following):

1. Partnership agreement
2. Silent partnership agreement
3. Investment limited partnership agreement
4. Limited liability partnership agreement
5. Membership rights in a general incorporated association
6. Other similar rights (excluding those established under foreign laws)

Note: Items 1–5 are illustrative; "other rights" are interpreted broadly, regardless of legal form.

(B) Description of the Scheme (all of the following must be satisfied):

- Investors contribute cash or assets (including crypto assets, per Cabinet Order);
- The contributions are used in a business; and
- Investors have rights to receive dividends or a share in the property derived from that business.

(C) Exclusions:

- The scheme does not apply where all investors are actively and substantially involved in the business (per Cabinet Order requirements); or

- Where investors are entitled to returns only up to the amount they invested (limited liability form).

(D) Foreign Funds:

- Similar rights based on foreign laws may also be regulated under separate provisions.

(2) Applicability of Fund Regulations to the Babylon Protocol

While Babylon might fall within the category of "other similar rights" in (A) above and does not appear to meet the exclusions under (C), it is unlikely to satisfy all of the conditions under (B). Accordingly, it may not constitute a fund under the FIEA, for the following reasons:

- The BTC provided by the staker is positioned as economic collateral, not as a capital contribution or investment to Babylon's operating entity.
- The staking rewards are not dividends from Babylon's business, but rather token-based rewards issued by the PoS networks that benefit from the staker's security provision.
- The BTC staker does not entrust assets to any centralized management entity but simply interacts with the protocol by signing a transaction; the assets remain in self-custody unless slashed.

From these perspectives, Babylon's BTC staking mechanism does not appear to meet the definition of a fund under the FIEA.

(3) Applicability of Fund Regulations to Finality Providers and Liquid Staking Protocols

Babylon allows BTC stakers to delegate their staking authority to finality providers. However, since this process does not involve the transfer of private keys, such delegation is not likely to fall under a fund regulation.

On the other hand, certain Liquid Staking Protocols may offer services that involve taking custody of users' private keys. In such cases, a careful legal analysis is required to determine whether such schemes meet the definition of a fund under the FIEA, particularly in light of the structure of asset control and contribution.

V. Crypto Asset Exchanges and Babylon Staking

This section examines the legal and operational issues that may arise when a Japanese crypto asset exchange operator performs BTC staking via the Babylon protocol using assets deposited by users.

1 Position of Staking within Crypto Asset Exchange Business

Many crypto asset exchanges in Japan provide staking services as part of their business operations.

To our understanding, as long as users do not bear the risk of slashing (i.e., potential loss)12, such services are generally treated as part of the core business of "receiving deposits

[1] In this regard, it is important to consider whether the risk of slashing can be properly managed by the crypto asset exchange operator, and whether such risk may have a material impact on the exchange's business operations.

In general, when a crypto asset exchange offers staking services, it enters into an outsourcing agreement with a validator (or an equivalent entity), which typically includes provisions addressing responsibility for slashing-related losses. However, validators may not always be capable of covering the full extent of any damages arising from slashing incidents, particularly if their financial capacity is limited. Moreover, while some degree of risk mitigation may be possible through insurance or other hedging mechanisms, the scope of such protection is often constrained.

As a result, exchanges are faced with the practical challenge of how to construct an appropriate compensation framework in the event of losses caused by slashing. This gives rise to the broader issue of how slashing risk should be appropriately allocated among users, exchanges, and validators in the context of staking operations.

By contrast, where a user directly designates a validator and engages in staking at their own discretion—outside the scope of an exchange—the slashing risk is generally understood to be borne by the user.

[2] It should be noted that if users are contractually required to bear the slashing risk, the scheme may potentially fall within the scope of a "fund" (collective investment scheme) as defined under the Financial Instruments and Exchange Act (FIEA).

However, we are not conducting a detailed legal analysis on this point at present. Depending on the structure, there may be room to interpret the arrangement as a combination of a deposit and a mandate agreement from the user, under which any losses are borne in accordance with the terms of the mandate—rather than as a collective investment scheme. Further legal clarification would be necessary on a case-by-case basis.

of crypto assets" as defined in Article 2, Paragraph 15, Item 4 of the Payment Services Act.

This legal interpretation should remain applicable even when Babylon is used as the underlying protocol—no special legal treatment or additional licensing is expected to be required.

2 Compatibility with Cold Wallet Regulations

Under Article 60-11, Paragraph 2 of the Payment Services Act and Article 27, Paragraph 3, Item 1 of the Cabinet Office Ordinance on Crypto Asset Exchange Services, crypto asset exchanges in Japan are required to segregate users' crypto assets from their own assets and hold them in cold wallets.

In most PoS staking systems, private keys used for asset transfers do not need to be moved; rather, a separate validator key is used. This practice is generally considered not to conflict with cold wallet requirements.

In Babylon, there is no concept of a validator key. Instead, staking is performed via cryptographic signatures called Extractable One-Time Signatures (EOTS). Importantly, the private key for BTC remains in the possession of the BTC staker—in this case, the exchange operator—and is never transferred or exposed to third parties.

Therefore, since the exchange does not move or manage private keys externally, Babylon staking is not expected to conflict with cold wallet custody obligations.

3 Handling of Altcoin Rewards in Babylon

A unique practical issue with Babylon staking is that while BTC is used as the staked asset, the rewards are typically paid in the native tokens (i.e., altcoins) of the target PoS network, rather than in BTC itself.

For example, when staking ETH, both the staked asset and the reward are ETH, which poses no legal or operational issues for exchanges that have already registered ETH as a "handled crypto asset" with the Financial Services Agency (FSA).

In contrast, when staking BTC via Babylon, the resulting rewards may be in the form of tokens such as BABY or other native tokens of PoS networks that are not registered as handled crypto assets. This presents a compliance challenge under the Payment Services Act.

Several operational approaches can be considered:

(1) Custody of Altcoins by the Exchange and Grant to Users

In this approach, the exchange holds the altcoins it receives as rewards and allocates them to users.

While it may be possible to register certain major tokens (e.g., BABY) as handled crypto assets, and some tokens associated with Babylon partner networks (e.g., ATOM, SUI) are already listed in Japan, it is not realistic to file individual registrations for every potential reward token.

(2) Direct Delivery of Altcoins to Users' Self-Managed Wallets

Here, the exchange does not custody the reward tokens but transfers them directly to each user's self-managed wallet. This bypasses the need to register the tokens as handled crypto assets.

However, this approach presents practical challenges: requiring users to manage wallets for a wide range of altcoins is burdensome from both a UX and operational support perspective. It also introduces potential transaction costs and operational risks.

(3) Sale or Exchange of Altcoins, and Payment of Rewards in BTC or JPY

Under this method, the exchange converts the reward altcoins into BTC or JPY (e.g., via a DEX or an overseas partner), and then distributes those converted assets to users as rewards.

While this may raise concerns that the exchange is engaging in crypto asset exchange services involving unregistered crypto assets, such risks may be mitigated through appropriate contractual arrangements.

Specifically, if the agreement with the user clearly states that:

- The user deposits BTC for staking, and
- The exchange will return rewards in BTC or JPY (not altcoins),

then the exchange's sale or swap of the altcoins can be viewed as part of its internal process for sourcing rewards, rather than as a crypto asset exchange activity involving third parties.

In this structure, the exchange merely acquires and disposes of unregistered tokens on its own account, which is generally not considered a regulated activity under current law.

(4) Conclusion

In light of the above, under the current regulatory framework, it appears that the most realistic and effective approach for crypto asset exchanges is to structure their operations based on scheme (3).

That said, from the perspective of BSNs, there are concerns about potential ongoing selling pressure caused by continuous liquidation of reward tokens. Therefore, the sustainability of the system as a whole should also be carefully considered in future discussions.

Acknowledgments

In preparing this article, I received valuable input from the teams at **Kudasai Inc.** and **Next Finance Tech Inc.**, both of whom are well-versed in Babylon staking. I also benefited from informal yet insightful suggestions from individuals involved with the **Babylon protocol**.

However, any remaining errors or interpretations are entirely my own and do not represent the official views of any specific entity

Disclaimer

The content of this document has not been reviewed by any regulatory authority and represents a general legal analysis based on interpretations currently considered reasonable under applicable Japanese law. The views expressed herein reflect the current thinking of our firm and are subject to change without notice.

This document does not constitute an endorsement of any specific staking mechanism, including Bitcoin staking, the Babylon protocol, liquid staking services, or any related technologies or platforms.

This material is provided solely for informational and blog purposes. It does not constitute legal advice, nor is it intended to be a substitute for legal counsel. For advice tailored to your specific circumstances, please consult with a qualified attorney.