BitHive

BitHive BTC Staking

LITEPAPER

BitHive

Synopsis

Bitcoin has grown into a mainstream asset with a $1.2 trillion market cap, with leading institutions like BlackRock holding and trading BTC via ETFs. However, much of the BTC is sitting idle. There is a pressing need to better utilize this massive amount of capital, especially in the context of helping secure Proof-of-Stake (PoS) networks and Actively Validated Service (AVS). BitHive aims to revolutionize Bitcoin by providing a secure, scalable platform tailored for native BTC staking to serve a variety of use cases. We propose a modular architecture for all types of PoS based networks that benefit from the security guarantee provided by staked BTC, without bridging or relying on third-party custodians. Furthermore, BitHive acts as a cornerstone for all restaking primitives to be built upon, empowering a diverse set of AVS.

1. Background

Proof-of-Stake is a class of blockchain consensus mechanism to prove that validators have put “stake” (something of value, usually the base coins of the networks) into the network that can be destroyed (aka slashed) if they act dishonestly. It has become the main consensus algorithm for many blockchain protocols, including Ethereum, due to its scalability, better energy-efficiency, and reduced centralization risk. In essence, PoS chains are secured by capital (stake) instead of work, unlike PoW chains.

Despite these advantages, PoS chains are incredibly difficult to bootstrap. It usually means that a PoS network needs to provide a significant amount of token incentives to secure the chain, which results in a high inflation rate. The inflation tends to create selling pressure of the token, hindering the growth of the network. What’s worse is that the volatility of an early stage token could further exacerbate the problem, leading to even higher inflation, sometimes over 100% as witnessed in a lot of chains launched in the past few years.

AVS faces similar bootstrapping challenges. An AVS is any blockchain-based system that uses restaking mechanisms to support unique validation methods, such as oracles, bridges, data availability layers, sidechains, and more. Many dApps are dependent on these services, and each service used to rely on its own security, leading to compounded vulnerabilities.

BTC as an asset is naturally better suited to help secure PoS chains and AVS. It represents about half of the total market cap of all crypto assets, has a very low utilization rate, and is less volatile. BTC itself is also not used to secure the Bitcoin chain due to its PoW nature, making it an ideal collateral for securing PoS networks and AVS.

2. BitHive's Bitcoin Staking Protocol

BitHive was thus created to address the growing demand for a secure and scalable platform for native Bitcoin staking and restaking. We present a modular architecture for all types of PoS blockchains that can benefit from the security guarantee provided by staked $BTC. The protocol does not rely on bridging or third-party custodians. The staked $BTC from BitHive can also be restaked to serve various AVS use cases.

BitHive utilizes native Bitcoin scripts on the Bitcoin chain, ensuring the highest degree of security. BitHive facilitates the Bitcoin staking operations using NEAR's Chain Signatures, and decentralized off-chain relayers, which we will expand in the below sections. It is worth noting that users only need a BTC wallet to operate; they do not need NEAR accounts or $NEAR tokens. When considering only deposits and withdrawals, **the system does not require trust in the NEAR's Chain Signatures or the relayers.**

For restaking, BitHive integrates Allstake's Meshed Restaking. Meshed Restaking is a concept pioneered by Allstake; it enables users to natively restake a wide range of assets (LSTs, LRTs, LP tokens, stablecoins, etc.) on multiple chains including NEAR, Ethereum, Solana, Ton, and more. Most notably,

Meshed Restaking allows the PoS chains/AVS to use a combination of these assets, including their own base/governance tokens for shared security. For instance, a new AVS XYZ can accept both $BTC and its token $XYZ for shared security. This not only expands the use cases of staked $BTC, but also enables the PoS Chains/AVS to simultaneously seek the most robust security while capturing value for its tokens.

3. BitHive's Technology Ingredients

3.1 Premises

- Users only need a BTC wallet to operate
- It is not required for the users to have NEAR accounts or tokens;

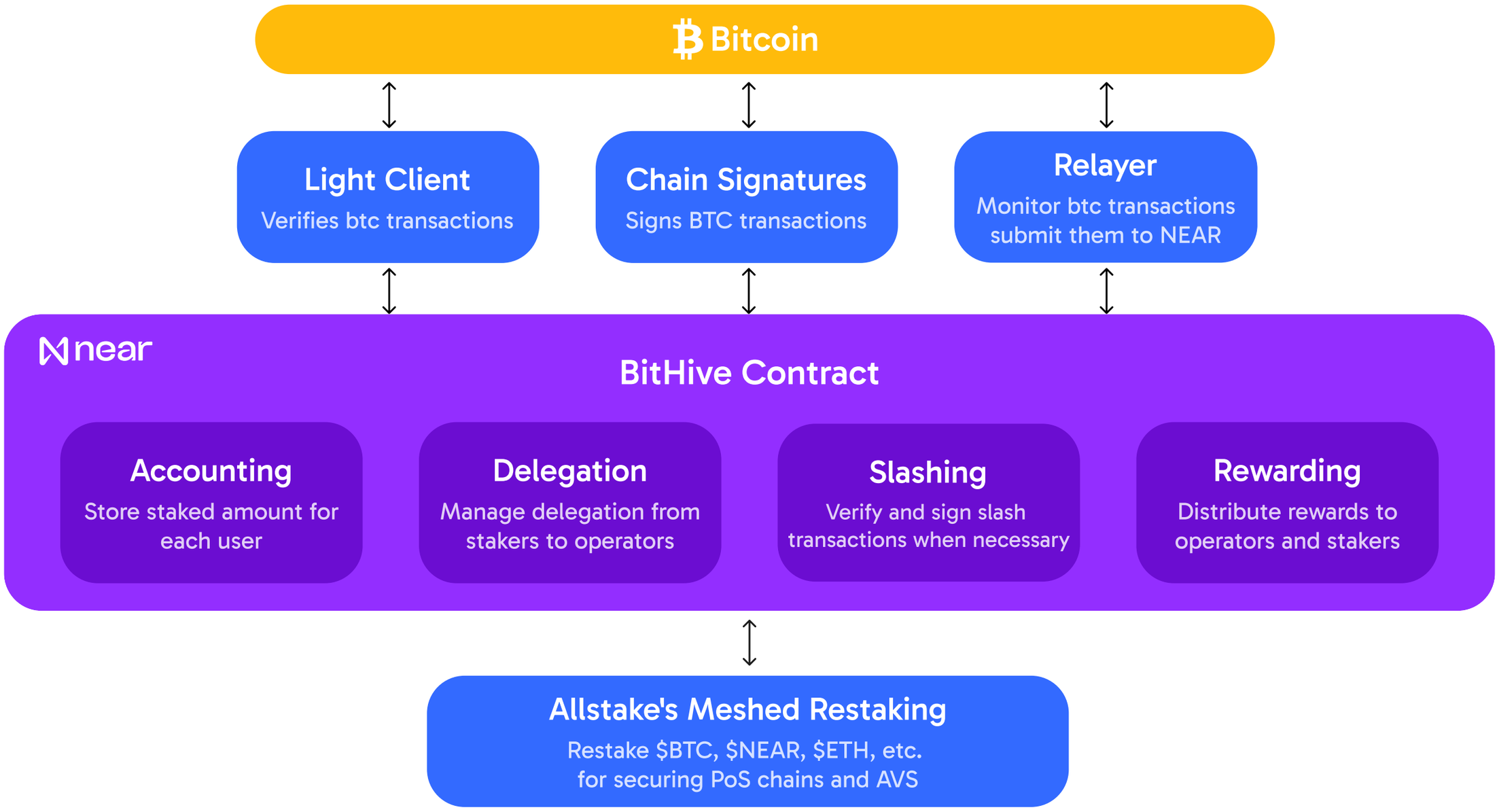
3.2 Components

- **BitHive Contract:** Built on NEAR Protocol, the BitHive Contract manages user interactions, including staking, unstaking, and withdrawal requests. It verifies signatures and records user data.
- **Relayers:** Off-chain entities that facilitate communication between users and the BitHive contract, ensuring decentralization and permissionless operation.
- **BTC Light Client:** Validates transactions on the Bitcoin network, providing necessary transaction authentication.

3.3 Dependencies

- **BTC to NEAR:** Requires a BTC light client on NEAR for transaction verification.
- **NEAR to BTC:** Uses Chain Sgnatures to initiate BTC transactions.

4. BitHive's Protocol Architecture



Light Clients: enable the BitHive contracts to verify the legitimacy of Bitcoin transactions. This mechanism allows for a trust-minimized environment by processing transaction proofs without needing the full Bitcoin blockchain, ensuring security while streamlining verification.

Chain Signatures: allow the BitHive Contract to sign various staking related Bitcoin transactions. The management of BTC is performed securely and verifiably in a decentralized manner. For more information on Chain Signatures, please visit https://docs.near.org/concepts/abstraction/chain-signatures.

Relayers: facilitate bi-directional message relay between NEAR and the Bitcoin chain, allowing for seamless communication across the chains. In addition to handling cross-chain messaging, the Relayer processes user requests, invoking the relevant methods in the BitHive contract for asset management and other related functions.

BitHive Contract

1. **Accounting:** keeps a precise record of staked Bitcoin, including the amount of the BTC being staked and its status (e.g. waiting period before being able to be withdrawn). It provides a unified data interface for external parties and AVS to access up-to-date staking data.

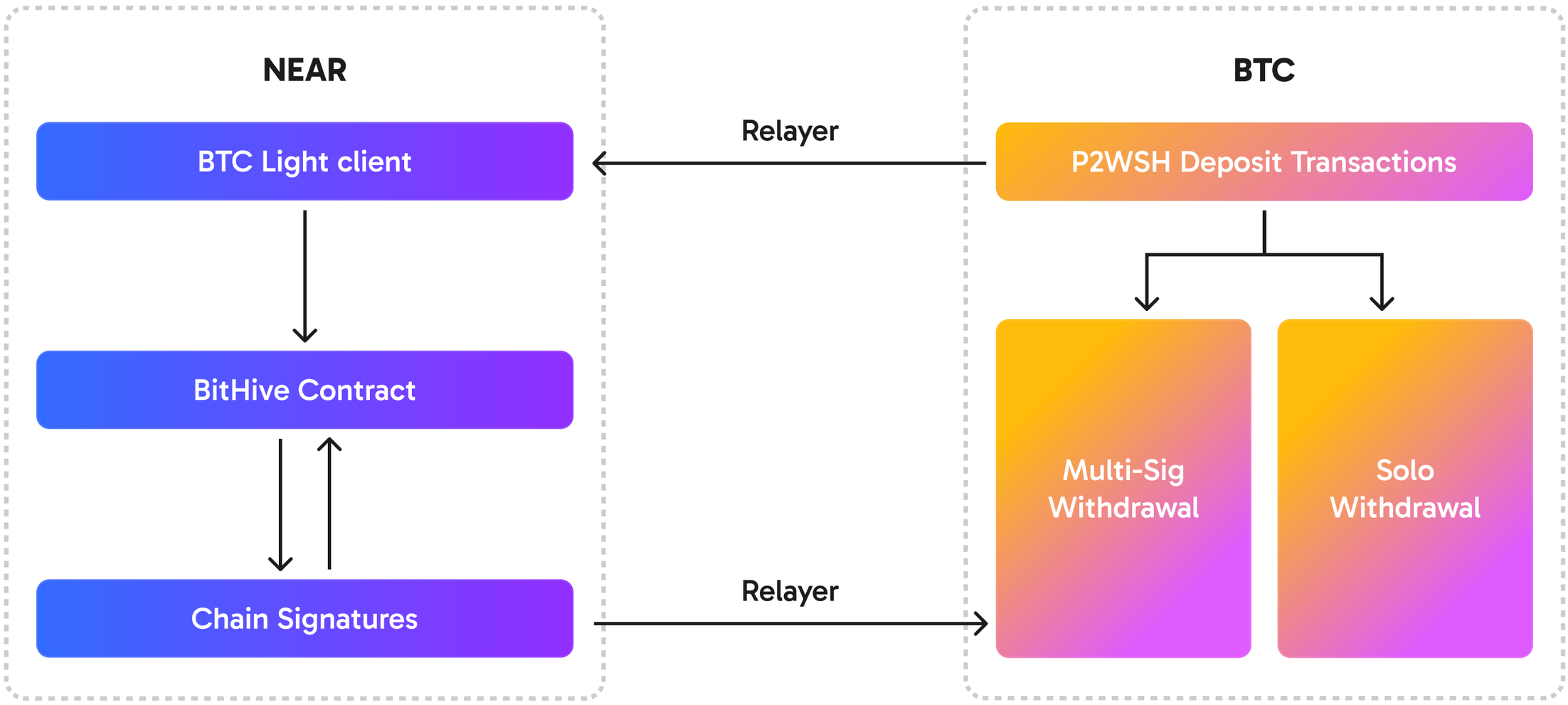
2. **Delegation:** manages the delegation of the BTC staked to operators. It tracks BTC staked to each operator, ensuring delegation processes are transparent and efficient.

3. **Slashing:** if an operator misbehaves, the BitHive Contract enforces slashing penalties, after confirming the misconduct with AVS. The slashing results in the forfeiture of the BTC staked to the misbehaved operator, thereby reinforcing the security of the network.

4. **Rewards:** AVS typically incentivize operators with tokens or points based on their performance. The Rewards module is responsible for distributing the appropriate amount of tokens to restakers and operators in alignment with AVS certifications.

Allstake's Meshed Restaking：

Allstake is a Meshed Restaking protocol on top of BitHive; it enables users to natively restake a wide range of assets (LSTs, LRTs, LP tokens, stablecoins, etc.) on multiple chains including NEAR, Ethereum, Solana, Ton, etc., and allows the PoS chains/AVS to use a combination of assets for shared security. For instance, a new AVS XYZ can accept $BTC, $NEAR, and its token $XYZ for shared security. This not only expands the use cases of staked $BTC, but also enables the PoS Chains/AVS to simultaneously seek the most robust security while capturing value for its tokens.



4.1 Deposit Process

- **Deposit:** To make a deposit, the user transfers the desired amount of BTC to a P2WSH address, where the UTXO of the script can only be spent if one of the following conditions is met:
    - Signed by both the BitHive contract's MPC signature and the user's BTC private key
    - After a lock-up period (e.g., 3 months), signed solely by the user's BTC private key

This approach ensures that even if the BitHive contract has a bug or the chain signatures' MPC network is compromised, the user's funds cannot be withdrawn without his/her own signature. Even in the small likelihood of the chain signature system going down, the user can eventually withdraw his deposit after the lock-up period.

- **Off-Chain Relayers:** identify the deposit transaction and submit it to the BitHive Contract. The BitHive Contract then verifies the transaction's validity using the BTC light client and records the user's deposit information.

These relayers are permissionless and replaceable; anyone can submit deposit information to the BitHive Contract. However, the relayers are responsible for covering the transaction fees and storage costs on NEAR.

4.2 Withdrawal

The users can withdraw their deposits before the lock-up period ends by following a straightforward process.

1. **Queue Withdrawal:**
    a. The user first signs a withdrawal message with their BTC private key.
    b. The signed withdrawal request is then submitted to the BitHive Contract via a relayer. The contracts verify the signature's validity, records the request and places it in the withdrawal queue. The user must wait a certain period (e.g., 2 days) before the BTC can actually be withdrawn to their wallet.
    c. This step does not require interaction with the BTC network.

2. **Complete Withdrawal:**
    a. After the waiting period, the user needs to ask the relayer to send a "complete withdrawal" request to the BitHive Contract on his/her behalf.
    b. Once the management contract confirms that the withdrawal waiting period has completed, it calls the Chain Signatures contract to sign a withdrawal script.
    c. After receiving the withdrawal script and its signature, the user also needs to sign the withdrawal transaction with his/her private key and use these two signatures to withdraw BTC to his/her own wallet.

- **Transaction Fees:** due to the nature of BTC, the withdrawal transaction naturally contains the fees required to perform the transaction (by the difference between outputs and inputs). Therefore, neither the worker nor the BitHive contract needs to pay the BTC gas fee; it will be covered by the user's deposit.

- **Partial Withdrawals:** Partial withdrawals are supported. The remaining funds can be redeposited by constructing a new transaction and repeating the deposit process, transferring to a new P2WSH, thus continuing the deposit.
- **Off-Chain Relayers:** throughout the process, the relayer acts as a replaceable intermediary; anyone can directly send the relevant messages to the BitHive Contract (but will need to pay NEAR's gas fees), making the system independent of specific relayers.

4.2 Slashing

Slashing is one of the defining elements of a PoS chain. Malicious attack and other dishonest behaviors would cause issues to the network and thus need to be punished; the stake would be slashed, and the violating validators would lose the funds. Slashing provides the security guarantee for a PoS chain; as long as at least ⅔ of the delegated stake are performing effectively and honestly, the PoS chain is live.

BitHive's design handles slashing follows the process below. After a user makes a deposit and delegates his/her funds to an operator, a transaction that makes his/her BTC slashable is created accordingly. If the operator causes slashable issues such as malicious data manipulation or extended inactivity as defined by the PoS chain or AVS, the BitHive Contract initiates a slashing transaction on that operator. This will result in the forfeiture of the user's slashable assets delegated to the operator. The slashing transaction is constructed by native Bitcoin scripts in a way that the user cannot reject, as long as this slashing transaction is authenticated by the BitHive Contract and signed by Chain Signatures.

On the other hand, if the operator maintains reliable performance without incidents during the delegation period, users are able to withdraw their full deposit without needing a 3rd party. However, it is important to note that when users choose to undelegate, they have to wait for a specified period (e.g., two days) to fully exit, allowing BitHive to verify that the users' assets are not subject to slashing.

5. Trust Dependencies

When considering only deposits and withdrawals, **the entire system does not require trust in the BitHive Contract or Chain Signatures.** Even if these systems have bugs or become unavailable, they will **NOT impact the security of the users' deposits** (though they may temporarily affect them). This has been explained in the deposit section.

There is no trust dependency on any off-chain relayers. Anyone can operate a relayer, and there could be multiple relayers supporting the protocol. All information submitted by the relayers can be verified on-chain, preventing the protocol from being affected by fraudulent messages. If all relayers become unavailable, users can choose to submit NEAR and BTC transactions themselves; the system availability should not be affected.

6. Comparison with Babylon

As the only two native Bitcoin Staking Protocols, the comparison of BitHive with Babylon often comes up. Both platforms stake BTC natively in a non custodial way, and both address the need for shared security. The main differences are the following:

Control Layer. Babylon launches with its own DPoS chain as the independent control layer managing staking and security, whereas BitHive utilizes NEAR as the control layer. NEAR has achieved 100% uptime since October 2020 with 220+ validators. We purposefully choose this design because we believe that NEAR, as a top 20 project by market cap, will be significantly more decentralized and secure than launching our own chain for an extended period of time (possibly forever). It is the more logical move for us in this upcoming modular crypto age.

Interchain State Relayer. Babylon Chain is based on the Cosmos SDK and utilizes IBC as the interchain state relayer, so it plans to focus mainly on providing shared security for Cosmos based App chains. On the other hand, BitHive uses Chain Signatures and light clients; it can be applied to PoS networks across a wide range of consensus mechanisms.

Use Cases. As mentioned above, the main use cases that Babylon is able to natively serve are Cosmos based Appchains, whereas BitHive can help secure PoS chains based on various consensus algorithms. What is more, BitHive (as part of Allstake) can also provide security for various Actively Validated Services, such as oracles, bridges, data availability layers, and sidechains, all of which are empowering many applications across the crypto industry. Thanks to its modular design, BitHive is more flexible and can natively serve more use cases.

7. Future Work

This litepaper provides a high level overview of BitHive's Bitcoin staking protocol, addressing the market of $1.2 billion worth of unencumbered Bitcoin. BitHive empowers users to stake BTC natively in a secure, non-custodial way. It has a modular design, using NEAR Protocol as the control layer and Chain Signatures for cross-chain interoperability. Together with Allstake, BitHive can provide shared security through multi-asset meshed restaking for not only PoS chains, but also various types of AVSs.

In the future, we plan to publish more documents for operators and AVSs. Specifically, one of the main use cases we are exploring is to become the first in the industry to bring Bitcoin staking into securing MPC networks, such as NEAR's Chain Signatures MPC network. The symbiotic relationship between BitHive, Allstake and Chain Signatures has natural synergy; the protocols combined have the potential to become one of the most robust and heavily used AVS, providing tangible yield based on real usage and volume.