**​​​​Introduction**

Core Chain is currently secured by the Satoshi Plus consensus mechanism, which integrates features from Delegated Proof of Work (DPoW), Delegated Proof of Stake (DPoS), and Non-Custodial BTC Staking. This unique combination allows the Core Chain to leverage hash power delegation, CORE staking, and BTC staking to validate the network, ensuring robust security and decentralization.

Our project, b14g, aims to further enhance these aspects by addressing potential vulnerabilities through the implementation of Observer Nodes and Merge Staking. This proposal seeks to strengthen the security of CoreDAO's BTC staking and enhance the utility of both BTC and CORE tokens within the CoreDAO ecosystem.

**Identifying Improvement Areas in Core Chain**

Our deep dive into the Core Chain's current architecture revealed specific areas where we can contribute:

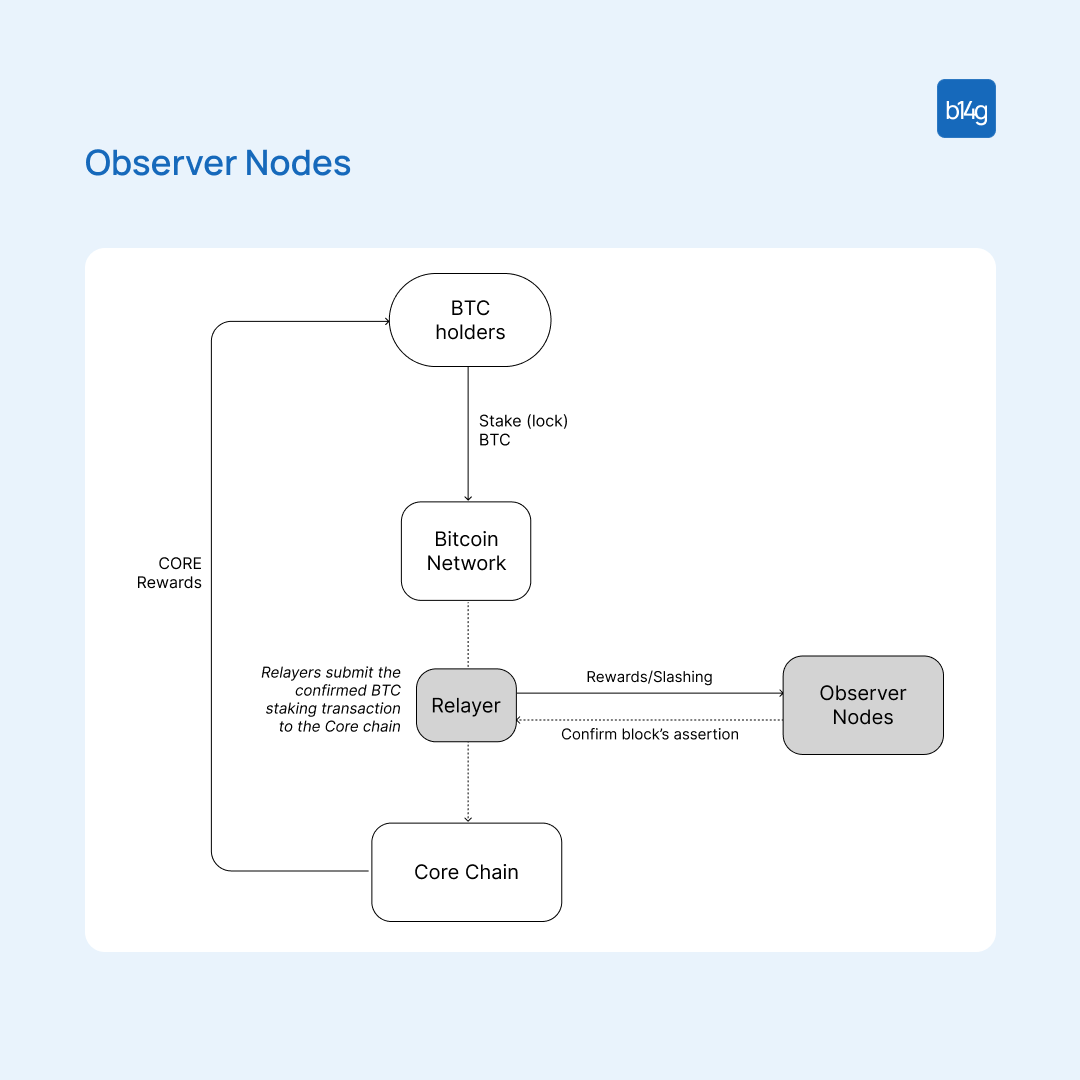
1. Addressing the Relayer Attack Risk in BTC Staking
2. Addressing commitment issue in BTC Staking
3. Expanding CoreDAO BTCFi into b14g

**Addressing the Relayer Attack Risk in CoreDAO BTC Staking**

The current BTC staking on Core Chain relies on a single relayer node managed by CoreDAO to sync data between the Bitcoin network and the Core network. This centralized approach introduces significant security risks, as the relayer becomes a "honey pot" that attracts potential attacks.

**To mitigate this risk, b14g introduces Observer Nodes.**

Here’s a simple illustration of how Observer Nodes work within CoreDAO BTC Staking:



* Observer nodes are responsible for monitoring Bitcoin blocks stored on the Core Chain by Relayers.
* The system is designed to be decentralized, allowing anyone to participate in securing the observation process by staking their assets to Observer Nodes.
* Observers and their delegators (those who stake their assets to the Observer Nodes) are incentivized with rewards for honest and accurate monitoring. Conversely, any dishonest behavior or mismanagement can lead to slashing.

*We will describe in detail how Observer Nodes work and how we address the challenges of integrating Observer Nodes into the current CoreDAO system in the "Observer Nodes Design" section later in this article.*

**Addressing commitment issue in BTC Staking**

Currently, Core Chain allows users to stake Bitcoin on the Bitcoin Network and use the proof of the confirmed BTC staking transaction to participate in validating the Core Chain. However, we've identified a significant drawback: it can't effectively punish malicious stakers.

In Proof-of-Stake (PoS) systems, a stake serves as a commitment by users to secure the network. If they break this commitment by engaging in malicious activities, they risk losing their staked assets through a mechanism known as slashing.

However, in Core Chain's BTC staking, bad actors only lose potential CORE rewards without facing further penalties. Their staked BTC remains unaffected, allowing the staker to continue earning profits on other BTC staking protocols. This situation seems unfair and undermines the security of the Core Chain.

**The Need for a Slashing Mechanism**

To address this issue, a slashing mechanism is necessary for BTC staking on CoreDAO. However, implementing such a mechanism presents challenges:

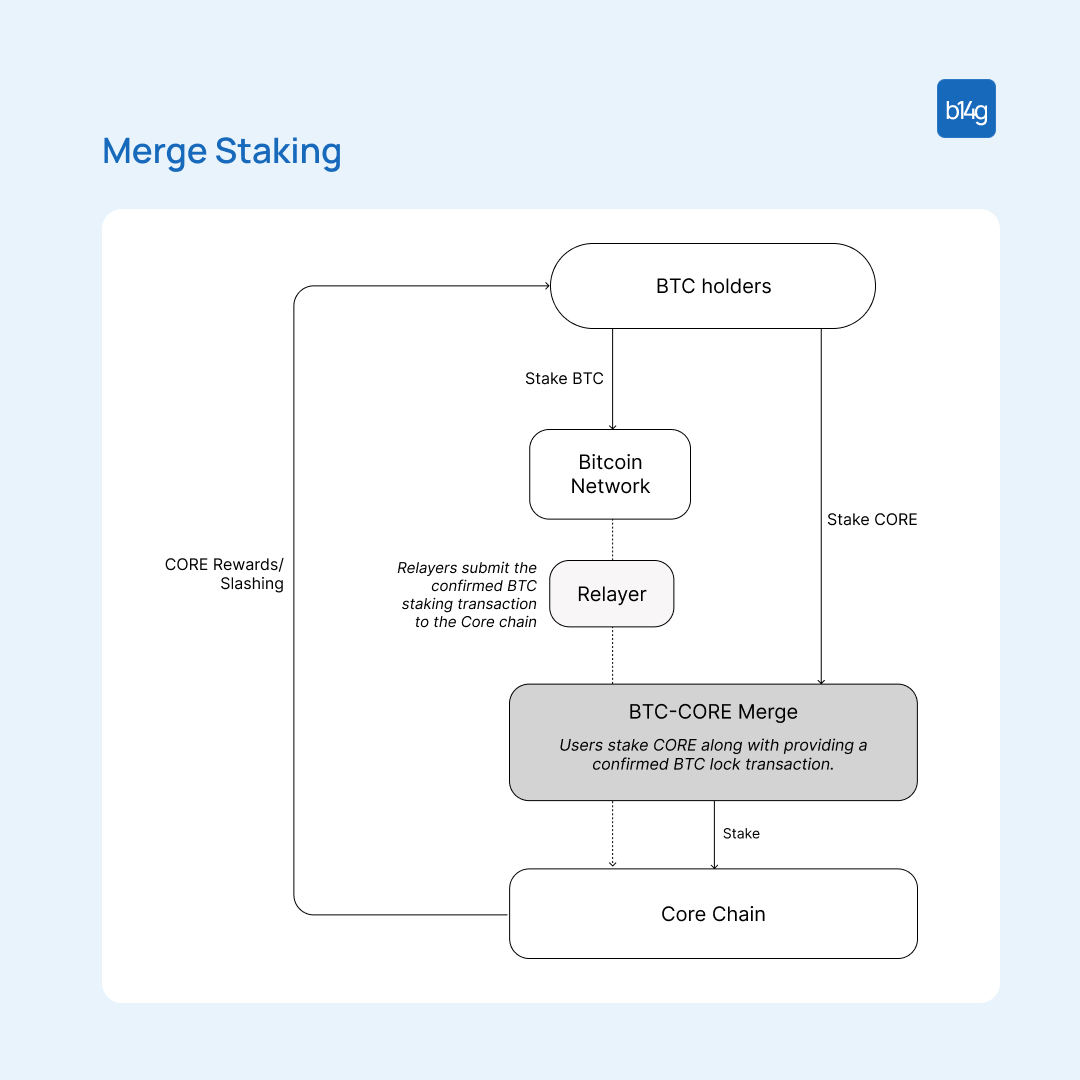
**First,** burning BTC as a penalty is impractical due to its high value. No one would burn gold, right?

**Second,** allowing slashing of BTC introduces security risks. An event on the PoS chain, such as an attack, could trigger the slashing of BTC locked on the Bitcoin network, creating more points of security vulnerabilities.

**The Dilemma: How to enforce penalties without compromising the value and security of BTC?**

To address this issue, b14g employs **Merge Staking.**

Here’s a simple illustration of how Merge Staking works within CoreDAO BTC Staking:



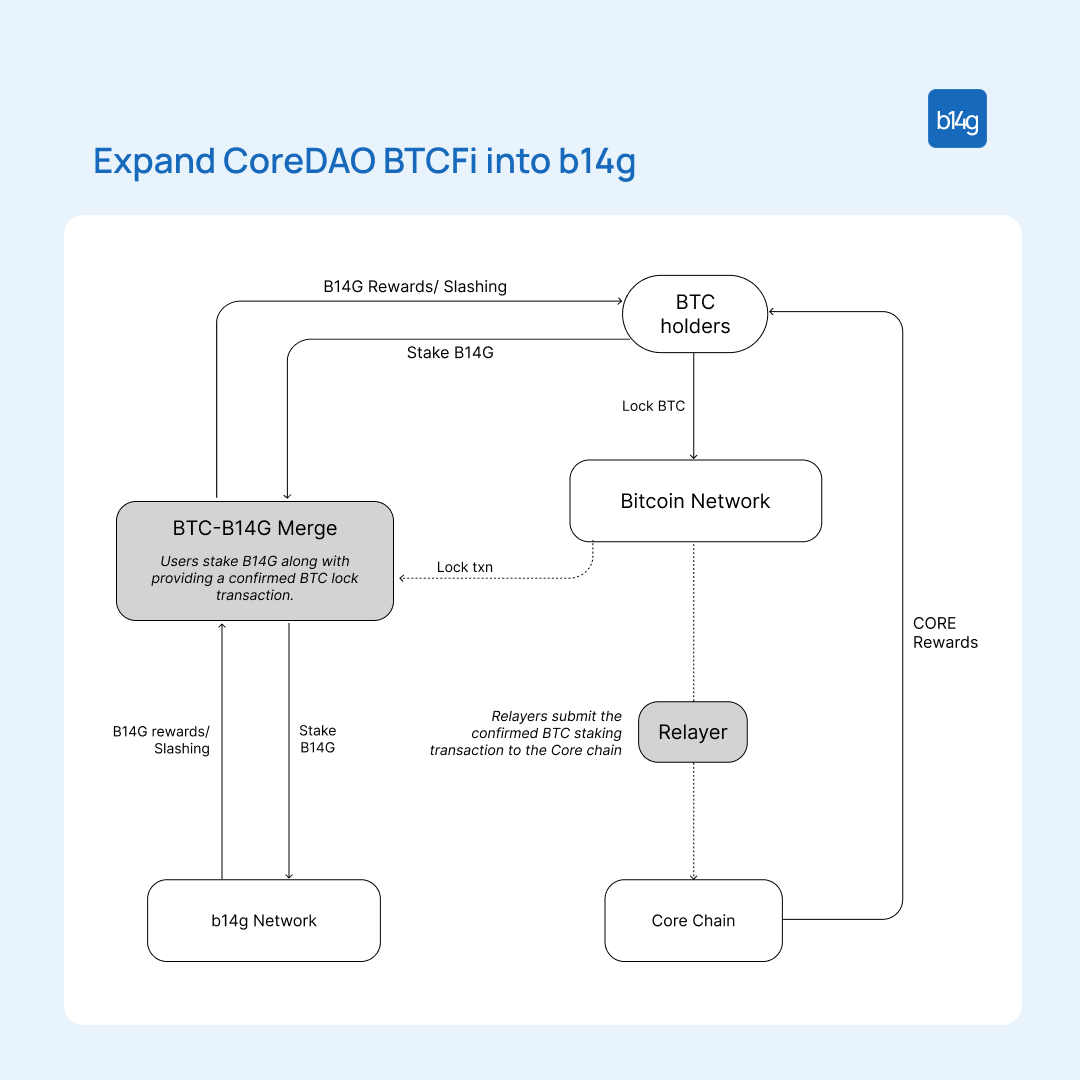
Users can merge CORE with BTC for staking. In case of misbehavior, slashing penalties are applied to the staked CORE tokens, not the BTC.

This approach ensures that the network can penalize bad actors without risking the high-value BTC, thus maintaining both security and fairness in the staking process.

This method also increases the demand for CORE, as it becomes essential for maximizing BTC staking returns. This drives CORE adoption and strengthens its position within the CoreDAO ecosystem.

*We will explore the detailed workings of the Merge Staking and its crucial role in the CoreDAO ecosystem and the broader BTCFi ecosystem in the "Merge Staking Design" section later in this article.*

**Expanding CoreDAO BTCFi into b14g**



For BTC holders who have locked their BTC on CoreDAO, there is another way to earn more rewards. By merging staked BTC with B14G tokens on the b14g platform, users can delegate their stake to validators to secure the b14g network, and earn B14G rewards.

**Observer Nodes Design**

The concept of Observer Nodes is straightforward, but its design involves several complexities. Specifically, we need to address how to bootstrap the Observer Nodes and integrate it with CoreDAO's existing economics.

**1. How to bootstrap the Observer Nodes?**

In simple terms, we need to figure out how to attract people to stake their assets in Observer Nodes to secure the network.

This isn't an easy task.

To begin with, we're considering using CORE, the native token of CoreDAO, for staking. There are several challenges we need to address:

**Firstly,** it can be difficult to find participants who are willing to invest their CORE tokens in Observer Nodes.

**Secondly,** the value of the CORE token is critical for maintaining the system's security. A significant drop in its value could weaken both the Observation Nodes and CoreDAO's security, resulting in a decrease in the Total Value Locked (TVL). This drop in TVL could, in turn, further reduce the token's price, creating a potential “downward spiral".

**Finally,** stakers may need to give up other potential rewards. If users already hold CORE, they might prefer to stake it directly to secure the CORE chain instead of using it for Observer Nodes.

**Addressing the Bootstrap Challenge**

To tackle these issues, we've designed Observer Nodes with a few key strategies:

**Leverage Existing Participants:** The easiest way to find stakers is to engage those already involved in the CoreDAO ecosystem. These participants have a vested interest in CoreDAO’s success, either through Non-Custodial BTC staking, CORE staking, or simply holding CORE tokens.

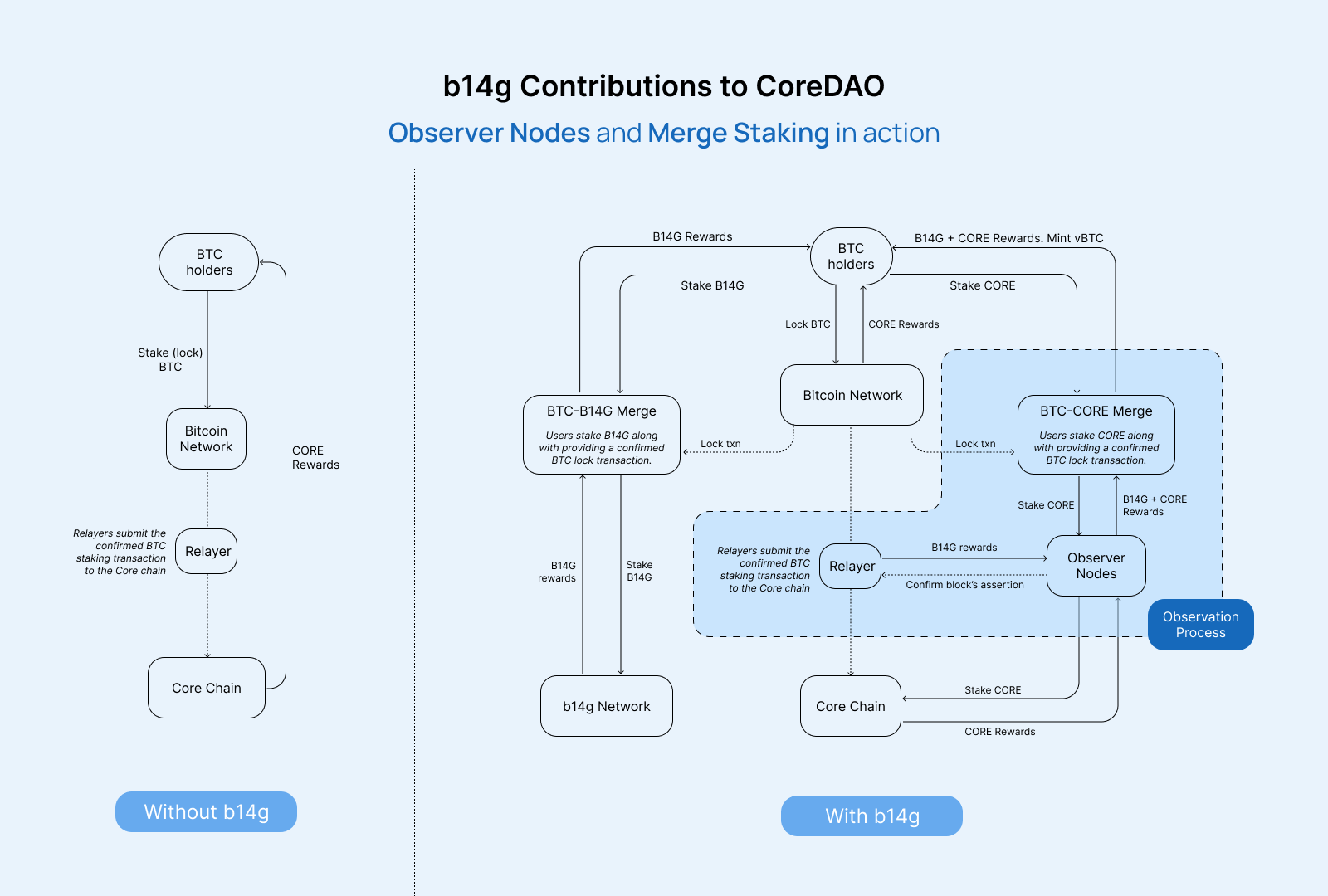
**Restaking Options:** Stakers have the option to restake their assets, contributing to the security of both CoreDAO and other infrastructures while earning staking rewards.

**Merge Staking:** We’ve implemented a Merge Staking that allows stakers to offer economic security using both CORE and other high-liquidity tokens. If one token, such as BTC, has lower volatility and deeper liquidity compared to CORE, it helps considerably increase the total stake value and reduce the risk of “downward spiral". Even if CORE’s price drops, the security provided by staked BTC offers a baseline level of economic stability.

**2. How to integrate Observer Nodes with current CoreDAO's economic framework?**

Answer: We use **Merge Staking.**

Here’s a detailed illustration of how Observer Nodes and Merge Staking work within CoreDAO BTC Staking:



* **Choosing Staking Assets:** We will merge CORE and BTC (particularly BTC locked through CoreDAO’s BTC staking) as staking assets. This leverages existing CORE holders and BTC stakers as participants to secure the Observer nodes.
* **Reducing Opportunity Cost for Stakers:** We’ve designed a system where a portion of the merged CORE is automatically delegated to CORE validators. This delegation offers additional CORE rewards to the stakers, alongside the rewards from Observer Nodes, while also enhancing Core Chain’s security.Moreover, when BTC is merged with CORE, it automatically mints vBTC, an ERC-20 liquid restaking token. vBTC can be used in various DeFi applications, boosting the earning potential for both BTC holders who have locked their BTC through CoreDAO and CORE holders.
* **Implementing Slashing for Credible Commitments:** Slashing penalties will apply to CORE, not BTC, to ensure honesty without risking BTC’s security. This keeps BTC protected from PoS-related attacks and potential security issues.

*By following these strategies, we aim to seamlessly integrate Observer Nodes into CoreDAO’s economic framework, enhance CORE token utility, and provide robust security for Core Chain.*

**Merge Staking Design**

The Merge Staking is a cornerstone of b14g's strategy in completing the Observer Node design, improving CoreDAO BTC staking, and expanding the BTCFi ecosystem.

**What?**

The Merge Staking is a process where users merge BTC with another token to secure other PoS networks and earn rewards for their honest contribution. Conversely, in case of misbehavior, slashing is applied to the counterpart token in the merge, not BTC.

**Why?**

Bitcoin, often referred to as "digital gold," possesses two essential attributes: "digital" and "gold." As a store of value, BTC has proven its worth with a market cap exceeding $1.5 trillion. As a digital asset, BTC should be easily connected with other tokens and integrated into other protocols—an aspect is somewhat limited by Bitcoin's lack of smart contract features.

We design Merge Staking to enhance Bitcoin's "digital" capabilities. This mechanism enables BTC to easily work with any tokens, any protocols, thereby **leveraging BTC to provide economic security to other protocols without compromising BTC’s role as a store of value.**

This approach preserves Bitcoin's role as a store of value in two key ways: first, by ensuring BTC remains non-custodially locked on the Bitcoin network, protecting its security and immutability; and second, by applying slashing penalties to the counterpart token in the merge rather than to BTC itself—reflecting the idea that no one would want to "destroy their gold."

By allowing BTC to merge with other tokens for staking, b14g aims to enhance the security of associated protocols. Specifically, BTC, with its lower volatility and deeper liquidity compared to many protocols' native tokens, can significantly increase the total value staked and reduce the risk of a "downward spiral." Even if the price of a native token falls, the security provided by staked BTC offers a baseline level of economic stability for the protocol.

**Beyond BTC, B14G, and CORE.**

Merge Staking is not limited to BTC, B14G, and CORE. It can be adapted to merge BTC with various tokens, facilitating easy integration between BTC and other protocols. This flexibility helps expand the BTCFi ecosystem, paving the way for more robust and versatile blockchain networks.

**Technical Details**

The technical architecture of observer nodes and Merge Staking is based on the following principles:

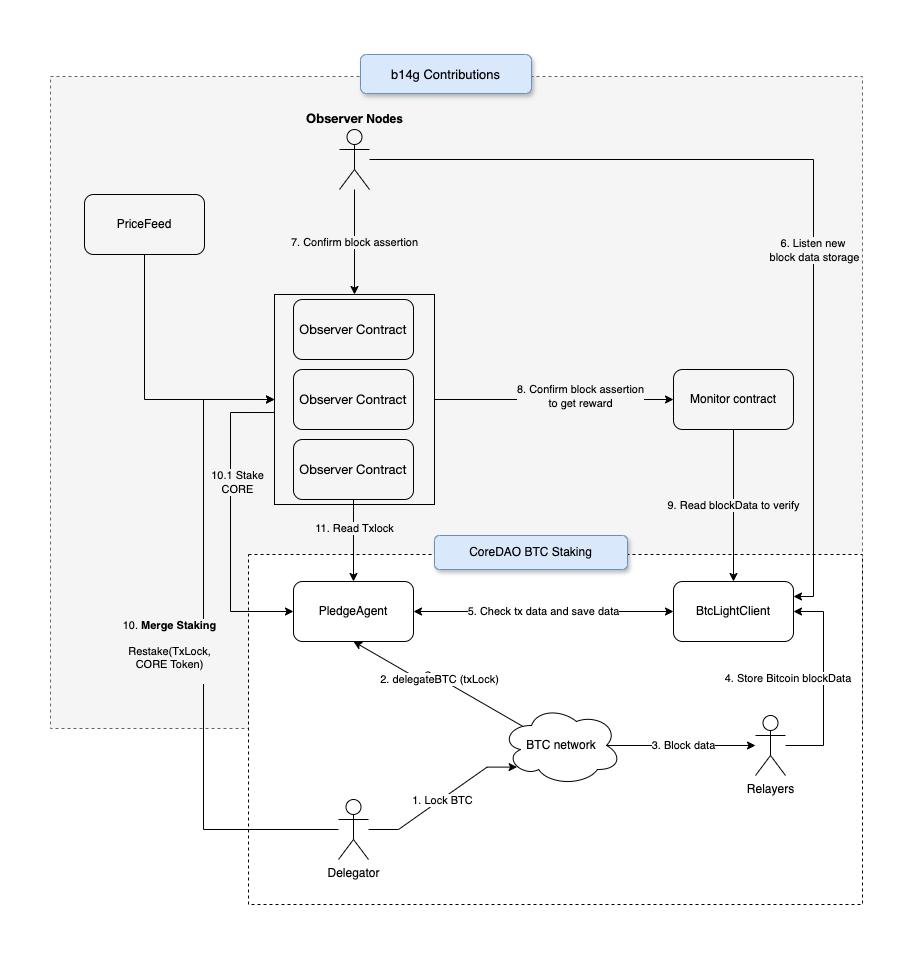
* It is simple. Minimize changes to the existing Core Chain to ensure compatibility and ease of integration.
* It is decentralized. Maintain a decentralized structure to ensure correct storage and verification of Bitcoin block data while safeguarding Core Chain security.
* It is user-friendly. Streamline processes for locking, merging, staking, minting assets to enhance user experience.

**1. Main Components**

* **Delegator**: A BTC holder who wants to stake their BTC on CoreDAO.
* **Relayers**: Entities that relay information between Bitcoin network and Core Chain.
* **Observer**: Responsible for monitoring Bitcoin blocks stored on the Core Chain, confirming the accuracy of each block stored in the BTCLightClient contract. Observers are rewarded for accurate confirmations and penalized for inaccuracies.
* **Observer Node:** Monitors, verifies, and confirms Bitcoin block data stored on the BTCLightClient contract.
* **Merge Staking:** After BTC staking, users merge BTC (BTC lock txn) with CORE tokens to stake or delegate their stake to Observer nodes. A portion of the staked CORE is locked in an observer contract as reserve in case of a slashing penalty. These locked CORE tokens are also automatically delegated to CORE validators for CORE Staking.
* **Merge Ratio:** The ratio for merging CORE tokens with BTC is determined using a price feed. This ensures that the value of CORE relative to BTC is maintained at 30%.
* **Reward Distribution:** Rewards are distributed proportionally based on the amount of CORE delegated. Penalties impact both the observers and their delegators' staked CORE.

**2. Implementation**

The following figure illustrates how b14g contributes to the CoreDAO BTC staking mechanism:



**CoreDAO's Current Process**

**(1)** The delegator locks BTC on the Bitcoin network by creating a BTC lock transaction.

**(2)** The delegator then delegates the locked BTC to the PledgeAgent Layer 2 contract on CoreDAO by calling the delegateBtc function. This function specifies the staking details, including the TxLock and the validator to whom the delegator wishes to assign their stake.

**(3) and (4)** CoreDAO uses a relayer node to monitor new Bitcoin blocks and store them on the BTCLightClient contract. Currently, this relayer node is managed centrally by CoreDAO, which introduces significant security risks as the relayer node represents a potential single point of failure.

**(5)** The PledgeAgent contract verifies the BTC lock transaction from step 2 by cross-checking the data stored in the BTCLightClient. Following this verification, the PledgeAgent updates the staking score for the associated validator.

**b14g's Contribution**

**Observer Nodes**

**(6)** Observer nodes listen to blocks stored on the BTCLightClient contract. These nodes verify the accuracy of the data on BTCLightClient by cross-checking it with the actual block data on the Bitcoin network.

**(7) and (8)** The observer nodes call the submitAssertion function on the Observer contract to forward their confirmation on block assertions to the Monitor contract.

**(9)** The Monitor contract cross-checks the data from the observer nodes' assertions with the data stored on the BTCLightClient. If the data matches, the observer nodes receive B14G rewards for their previous assertions when the next BTC block is added on BTCLightClient contract. If the data does not match, the observer nodes face slashing on their staked CORE.

**Merge Staking**

**(10)** After the BTC lock transactions are verified on the PledgeAgent contract, delegators can proceed with the Merge Staking. This involves merging locked BTC and CORE for restaking onto the Observer contract or delegating their stake to Observer nodes. The process uses the Restake(txBTCLock) payable function to stake CORE tokens along with BTC lock txn details and delegate the stake to the Observer contract.

In this setup, CORE tokens are subject to slashing if the delegated Observer nodes misbehave. Additionally, a portion of the staked CORE is automatically delegated to CORE validators using the delegateCoin() payable function of the PledgeAgent contract. This delegation helps to earn additional CORE rewards and enhances the security of the Core Chain.

**(11)** The Observer contract reads the lock transaction details stored on the PledgeAgent contract (from step 5) to confirm that the BTC has been staked before proceeding with restaking (step 10).

**Final Thought**

**Contributions to CoreDAO**

With the introduction of Observer Nodes and the Merge Staking, b14g reduces risks associated with single-point relayer failures and provides a more robust penalty system to CoreDAO BTC staking. This not only boosts security but also increases the utility and demand for CORE tokens, benefiting the entire network.

**Contributions to BTCFi**

In the broader BTCFi ecosystem, the Merge Staking by b14g provides a scalable way to integrate BTC into DeFi. By merging BTC with other tokens like CORE for staking, it allows BTC holders to easily participate in DeFi without compromising the security of their assets. For protocols, it now becomes easy to leverage the economic security power of BTC.

**Future of BTCFi**

Looking ahead, we foresee a bold future for BTCFi. We believe Bitcoin will soon assert its dominance not just in market cap value but also in economic security power, becoming the 'king of crypto' in every sense.