# Shinobi Protocol

Ninja and Kunoichi

September 1, 2021

**Abstract**

Shinobi is a protocol for generating Secret Bitcoin (SBTC), an SNIP-20 token backed by bitcoin on the Secret Network. Bitcoin private keys are stored only in the Trusted Execution Environment (TEE) on the Secret Network. The protocol's governance token — the SHINOBI token (SHINOBI) — will be used as a reward for the minters of Secret Bitcoin as well as the registerers of block headers in the Bitcoin and Secret Networks. It will also be required as a fee when bitcoin is withdrawn from the Secret Network. Privacy on the protocol is ensured by keeping transactions on the Bitcoin Network anonymous. This will be implemented by configuring the unit of bitcoin deposited to (or withdrawn from) the network to a commonly used denominator (e.g., 0.1 BTC or 1 BTC), thus obfuscating the trace of bitcoin being sent through the protocol. Secret Bitcoin can be sent anonymously across the Secret Network.

## 1 Introduction

With the recent development of Decentralized Finance (DeFi), it has become common to exchange or swap different digital assets using a smart contract platform. In particular, there is a huge demand for tokens pegged to bitcoin and many protocols have implemented such conversion/swap features.

One such protocol is Wrapped Bitcoin (WBTC), an Ethereum-based token with the largest volume and issuance amount among similar projects. The WBTC protocol is built around a secure custodial structure, which is managed by a company that boasts the best custodial technology in the industry. Given the custodial nature of the protocol, there is no fundamental or structural difference compared to Tether (USDT), a stablecoin issued by Tether Limited. In both projects, there is a trusted third party that manages a pegging mechanism of the asset.

There are several projects trying to implement a peg to bitcoin without depending on a trusted third party, one of them being renBTC of the Ren protocol. The underlying bitcoin is managed through multi-signatures of people staking a certain amount of the REN token, as well as multi-signature admin keys held by the developers. The security concern with this implementation is that the value of the staked REN tokens could become less than the value of bitcoin stored on the Ren protocol, undermining protocol security.

Other projects, such as tBTC and PolkaBTC, attempt to solve this issue through over-collateralization of native tokens (e.g., ETH, KEEP, DOT, etc.). However, this approach leads to several issues — the system is predicated on the trustworthiness of the collateral, the asset can be locked in a contract that generates little to no returns, and the implementation essentially puts a cap on the amount of bitcoin that the protocol can handle.

To address those issues, we propose a solution that leverages the Secret Network, a network of trusted execution environments that verify the blocks and transactions on the Bitcoin network.

A trusted execution environment, or TEE for short, is a secure environment for code execution often located within a CPU. Any computation conducted within the TEE, as well as its result, remains hidden from external CPUs, with the relevant data being isolated from the outside environment. The Shinobi protocol stores Bitcoin private keys in TEEs, enhancing the anonymity and security of the Secret Network. The caveat here is that one needs to trust the chipmaker to manufacture the hardware properly and some relevant issues (e.g., side-channel attack) should also be taken into account.

## 2 Bitcoin Light-client on the Secret Network

In order to mint Secret Bitcoin on the Secret Network, we need to have bitcoin deposited to the protocol, with the deposit address generated with a private key that only exists within a TEE. In addition, we need to have a Secret Contract verify that bitcoin was deposited to this deposit address. For these features to work, a Bitcoin light-client has to be built on the Secret Contract so that Merkle proof can be established. Once the protocol is initialized, the following steps will be executed:

1. First, the header of the most recent Bitcoin block will be registered on the Secret Contract, with a reward in the form of the SHINOBI token provided in the process. When there is a delay in header registration, the reward will be increased to incentivize registration. The protocol makes this adjustment autonomously, with the amount of increase based on the time difference between when the last header was registered and when a new header is registered — the more delay there is between the two, the greater the reward a header registerer will get. The reward is reduced by half for every registration attempt. This means that the node that successfully registers a new block header will get a full reward and the reward for each subsequent node will be cut in half until it becomes zero for the 11th node and thereafter. Anyone can verify that the block header is consistent with the corresponding block on the Bitcoin network, and that the risk of reorganization is negligible, by examining the current Proof of Work (PoW) difficulty on the Bitcoin network.

2. Once the initial block header is registered, anyone can add the next block header by constructing a hash chain in relation to the previous block header and ensuring that the PoW difficulty requirements are met. The subsequent blocks can be registered in the same way.

3. In the event of a reorganization of the Bitcoin blockchain, we need to be able to reconstruct the chain from a block at which the reorganization occurred. The protocol will verify that the new valid chain has more PoW associated with it than the existing chain via the following implementation:

   (a) Blocks with 6 or more confirmations are considered to be final.

   (b) At least 2 blocks will be required for a reorganization.

There simply needs to be enough financial incentive for block headers to be registered properly on a regular basis, and there is practically no need for anonymity of the Secret Network in the registration process. With 6+ confirmations required for a deposit to be reflected on the network, the security level of the deposit mechanism would be equivalent to that of a typical cryptocurrency exchange platform.

## 3 Anonymity on the Bitcoin Network

While it is meaningful to have a trustless token available on the Secret Network, it is even better to have anonymity ensured in every step of the process. In light of this, it will be desirable to prevent deposit transactions sent to a Secret Contract from being recognized as such on the Bitcoin network. We will propose the following implementation to achieve this:

1. The protocol will support deposits through standard Bitcoin transactions. With Taproot not implemented on the Bitcoin network as of the time of writing, some specific transactions, such as those involving Atomic Swap or the Lighting Network, are easily discernible. However, a deposit transaction to the Secret Network is conducted in the same manner as a normal, Pay-to-Witness-Public-Key-Hash (P2WPKH) transaction, with no special attributes that would make it stand out from other transactions.

2. Each deposit is linked to a unique deposit address and each deposit/withdrawal transaction contains one single input to ensure that only the sender of the transaction can see it as being conducted for the deposit/withdrawal purpose. This implementation requires that there be exactly one UTXO for a Bitcoin withdrawal transaction (i.e., no "change" output), and that the deposit and withdrawal amounts be the same, absent the mining fees. This can be achieved by fixing the deposit/withdrawal unit to a commonly used unit (e.g., 0.1 BTC or 1 BTC). In fact, most UTXOs have easily identifiable amounts associated with them, such as 0.1 BTC, 1 BTC, etc., and adopting these numbers as a fixed deposit/withdrawal unit will help enhance transaction fungibility. The protocol will initially support the units of 0.1 BTC and 1 BTC, with other units (0.5 BTC, etc.) potentially added in a future implementation for improved user experience.

## 4 Secret Network Light-client on the Secret Network

Secret Bitcoin can be redeemed for bitcoin by specifying a (destination) Bitcoin address and burning the Secret Bitcoin. This will initiate a send transaction signed by a private key stored in the contract. Here, one can attempt to exploit the system and cause unintended withdrawals of the protocol fund by having the protocol immediately redeem Secret Bitcoin for bitcoin after the former is sent to a burn contract. This will cause the Secret Bitcoin to be sent to the burn contract in a local environment without the transaction being broadcast to the Secret Network, which allows the sender to receive bitcoin while also retaining ownership of Secret Bitcoin on the network. To prevent this from occurring, we will adopt the following implementation:

1. Redemption will not be executed immediately after Secret Bitcoin is sent to a burn contract for a Bitcoin withdrawal — bitcoin will not be sent until this withdrawal request has been verified to be conducted on a valid chain (i.e., the Secret Network).

2. The hash chain of the Secret Network's headers will be registered on each Secret Contract so that the validity of each redemption request can be verified. The SHINOBI token will be provided as a reward for this registration process.

3. Similar to the registration process for Bitcoin block headers mentioned above, the reward will be increased as an incentive mechanism when there is a delay in the registration of a Secret Bitcoin block header.

The registration will only occur for every 50 or more blocks or when the validator of the block header is changed, whichever event happens earlier. This helps reduce the gas fees required for header registration by grouping together the header information of several blocks and broadcasting it to the Secret Network in one transaction. Furthermore, each Bitcoin withdrawal from the network will entail a fee paid in the SHINOBI token.

# 5 SHINOBI Token

The SHINOBI token is created when new Secret Bitcoin is minted or a block header of the (Secret) Bitcoin network is registered on a Secret Contract. The SHINOBI token will be distributed to those who have contributed to the growth of the Shinobi ecosystem by implementing one of these actions. Please note that 20% of the issued amount will be allocated to the protocol developers to ensure continued funding for the project development. In addition, the token is required as a fee when one wants to redeem Secret Bitcoin for bitcoin.