Shinobi Protocol V2

Ninja and Kunoichi

June 1, 2022

1 Introduction

Shinobi is a protocol for generating Secret Assets backed by multi-chain crypto assets. Secret Assets are private tokens issued on the Secret Network and are pegged one-to-one to the deposited crypto assets (we call them the Base Asset) such as Bitcoin.

Shinobi is one of the so-called Bridge protocols in the sense that assets on other chains can be transferred to the Secret Network as wrapped tokens. In the crypto world today, these "Bridge" protocols play an important role in facilitating the interactions between various chains. Examples include transferring Bitcoin to chains that are capable of using DeFi with Smart Contract (such as Ethereum) and transferring assets on Ethereum to other chains with lower fees. However, many of these Bridge protocols currently rely on a specific entity to manage the deposited Base Asset, introducing a major security risk. When using these Bridges, users must fully trust the specific entity that manages the asset.

In addition, the tokens generated through these Bridges are not confidential, and anyone can use Blockchain Explorer to see when and where these tokens are being used. It is also possible to know who transferred how much to another chain through the Bridge. In some chains, there is a technique called "mixing", in which token transfers are "mixed" with other users' transfers of the same type, thereby removing the connection between the source and destination of the tokens. While this method certainly guarantees the privacy of transfer, traces of mixing remain on the blockchain as mixing transactions generally have completely different characteristics from other transactions. Therefore, it can be said that mixing does not guarantee complete confidentiality.

Shinobi is a protocol that uses the Secret Network to resolve the trust and confidentiality problem described above. Secret Network is a public blockchain that utilizes the hardware secrecy of the nodes that comprise the chain to keep information hidden from the outside world. Therefore, contracts on the Secret Network can implement features that are impossible for other public blockchains such as Ethereum. They include the generation of secret

random numbers and the management of data permissions. Shinobi makes use of these advantages of the Secret Network in various ways. One of them is the Gateway Contract, which is capable of generating and managing secret keys of the deposited Base Asset without disclosing them to anyone. In Shinobi, the Gateway Contract manages the private keys and the addresses of the Base Assets, while the Light Client Contract verifies the transactions, thus realizing the management of the Base Assets without being dependent on a specific entity. The address generated by the Gateway Contract and used by the user for the deposit of the Base Assets are generic addresses, and since the deposit is a generic transaction, there is no trace of usage on the Base Asset blockchain.

Secret Assets issued on the Secret Network through these contracts are issued in the form of a standard token format of the Secret Network called SNIP-20, and this token form can be used to keep information about the transfer and balance confidential.

In the following section, an overview of the protocol is given, followed by a description of each component. It also explains the token model for Shinobi Tokens that plays an important role in Shinobi.

2 Protocol Overview

2.1 Deposit

Users who wish to convert a Base Asset (e.g. BTC) to a Secret Asset (e.g. Secret BTC) will deposit the Base Asset to the Gateway Contract deployed on the Secret Network and receive the same amount of Secret Assets minted by the Gateway.

The following process describes how this is done. First, the user makes a deposit request to the Gateway, which creates a key pair using the cryptographic algorithm of the Base Asset. The Gateway then derives the Base Asset's receiving address and returns it to the user. Since this key pair is created for each deposit request, the user will receive a different receiving address each time. The key pair is encrypted by the Contract VM of the Secret Network and is stored in a state, so it cannot be accessed by any user, contract other than the Gateway, or the Secret Network's node runners. The user transfers the Base Asset to the receiving address. At this time, the Base Chain only shows an ordinary transfer transaction between addresses, and others cannot tell from the transaction that the transfer is to Shinobi Gateway. After the transaction is confirmed by the Base Chain, the user submits the proof of transaction to the Gateway, which delegates the verification of the proof to the Base Chain Light Client Contract that is synced with the Base Chain blockchain. Once the Contract has verified the proof, the Gateway mints the Secret Asset of the same amount as the transferred

Base Asset and transfers it to the Secret Network address specified by the user.

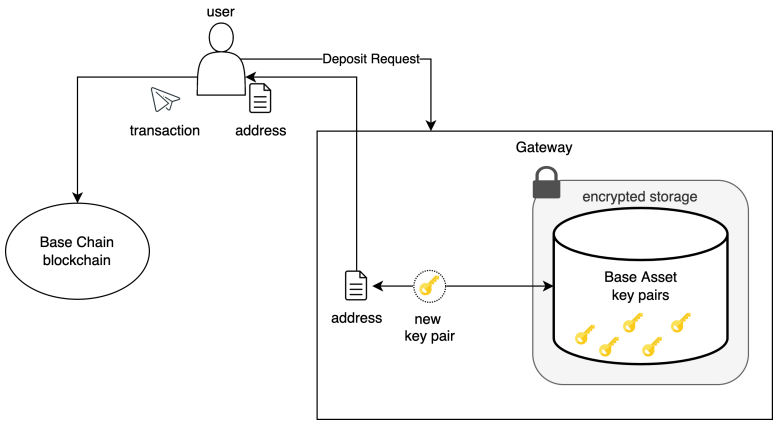

Figure 1: Deposit request

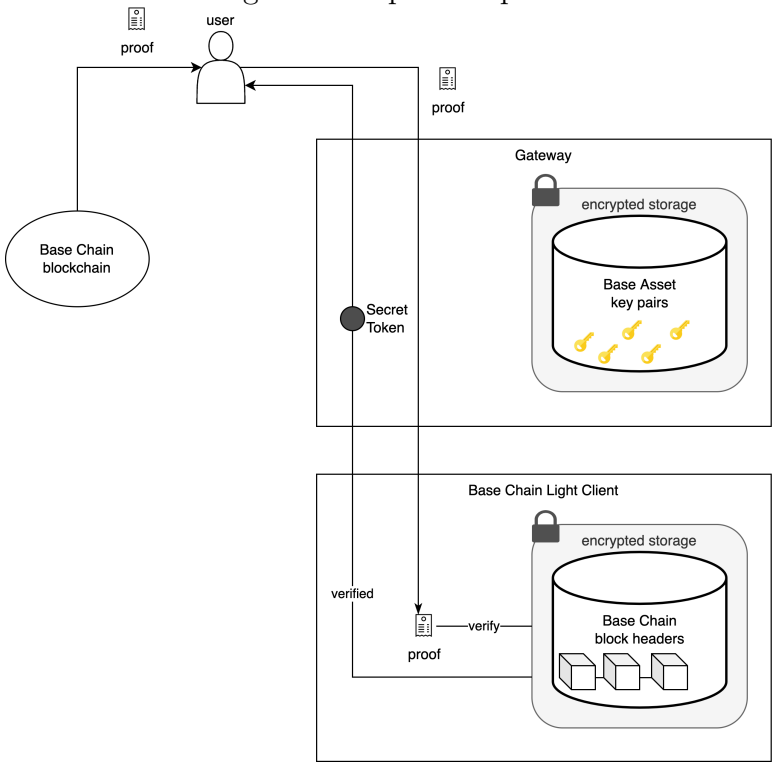

Figure 2: Deposit verification

2.2 Withdrawal

Users who wish to convert a Secret Asset (e.g. Secret BTC) to a Base Asset (e.g. BTC) will transfer the Secret Asset to the Gateway Contract that is deployed on the Secret Network, and receive the Base Asset of the deposited amount subtracted by a predetermined fee.

The following process explains how this is done. First, the user makes a withdrawal

request to the Gateway by transferring the Secret Asset to the Gateway. The Gateway subtracts some fee from the transferred Secret Asset and makes allocations to the Protocol's eligible users. The rest will be burnt as the user's withdrawal amount. Eligible users refer to the holders of the ve Shinobi Token (see the section on ve Shinobi Token for more information). After the transaction of the withdrawal request is confirmed by the Secret Network, the user submits the proof of transaction to the Gateway. This is because the Gateway Contract must verify that the deposit of the Secret Asset is confirmed by the consensus algorithm of the Secret Network. The Gateway delegates the verification of the proof to the Secret Network Light Client Contract that is synced with the Secret Network blockchain. Once the Light Client Contract has verified the proof, the Gateway selects a key pair of the Base Chain from the state that has the same amount of the Base Asset as the burned Secret Asset. The Gateway then signs the transaction that transfers the Base Asset to the address specified by the user and returns it to the user. Finally, the user broadcasts the returned transaction to the Base Chain.

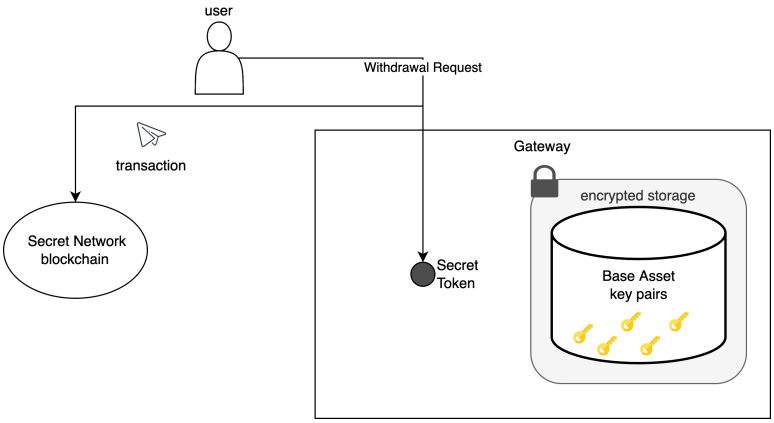

Figure 3: Withdrawal request

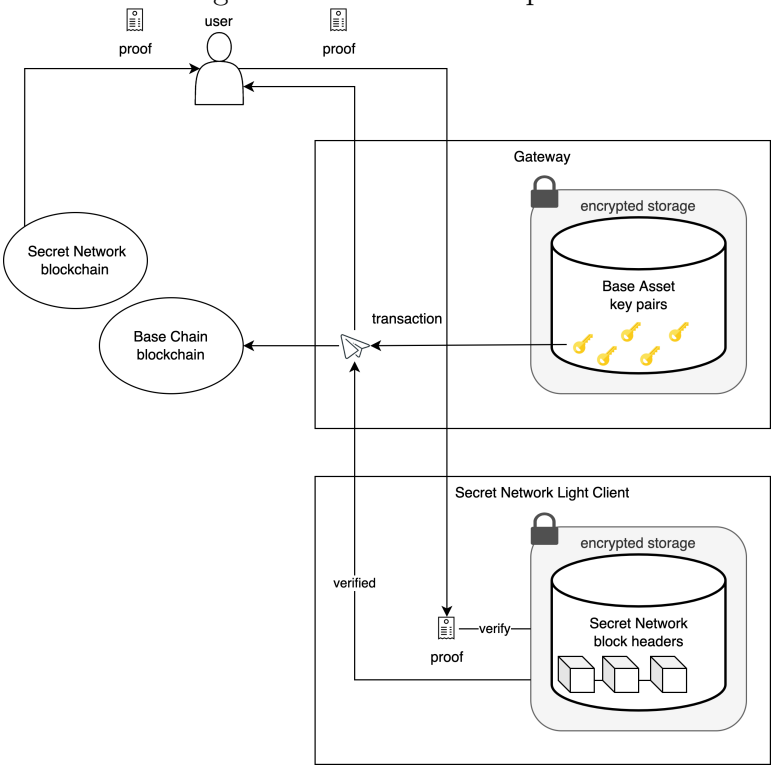

Figure 4: Withdrawal verification

3 Light Clients and Shuriken Network

The Light Client Contract built on Shinobi records the block headers and uses that record to verify the proof of transaction of the Base Assets and Secret Assets submitted by the user. Base Chain Light Client, which records the Base Chain's block headers, is used to verify the transaction of the Base Assets, and the Secret Network Light Client is used to verify the transaction of the Secret Assets. A distributed network called the Shuriken Network

provides block headers to these Light Clients, which verify the validity of the block headers and record them if they are valid. The Shuriken Network is composed of nodes referred to as Shuriken Nodes. Node runners receive Shinobi Tokens as a reward.

4 Multi Asset Compatibility

The Protocol can technically implement any Base Assets that meet the following two conditions;

- The Base Asset can be transferred with cryptographic algorithms that can be implemented in contracts, such as secp256k1 and ed25519.
- The Light Client of the Base chain can be implemented on the contract.

At first, we will implement Bitcoin as the most basic and important Base Asset, but later we will implement for more assets on PoW-based and PoS-based chains.

5 Shinobi Token

Shinobi introduces the Shinobi Token to facilitate consensus building in the decentralized governance within the protocol thus maximizing the value of the protocol. This section describes the distribution of the Shinobi Token and its use, especially the ve Shinobi Model.

5.1 Acquisition of the Shinobi Token and Shinobi DAO

Shinobi Token can be gained by holding the Secret Assets produced from a Base Asset such as Bitcoin. They can also be given to contributors determined by the Treasury Contract managed by the Shinobi DAO. Shinobi DAO is a DAO that is governed by the 1 token = 1 vote method on the ve Shinobi Token generated based on the Shinobi Token. Shinobi DAO can determine various important parameters regarding the Shinobi Token. They include the boost rate for the amount of Shinobi Token acquired when holding the ve Shinobi Token, the amount of Shinobi Token acquired for each type of Secret Asset, and Withdraw Fee for each type of Secret Asset. In addition, when other services that use the Secret Assets are launched, the Shinobi DAO will be in charge of determining their parameters as well.

5.2 ve Shinobi Token

Shinobi aims to develop secret bridges for assets on various chains in the long run and expand its ecosystem, providing privacy to all users in the crypto world. Therefore, it is necessary to establish a system that encourages long-term commitment from the token holders. To accomplish this, the Shinobi team has decided to adopt a token model derived from the ve-token (vote-escrowed) model used by others such as Curve.

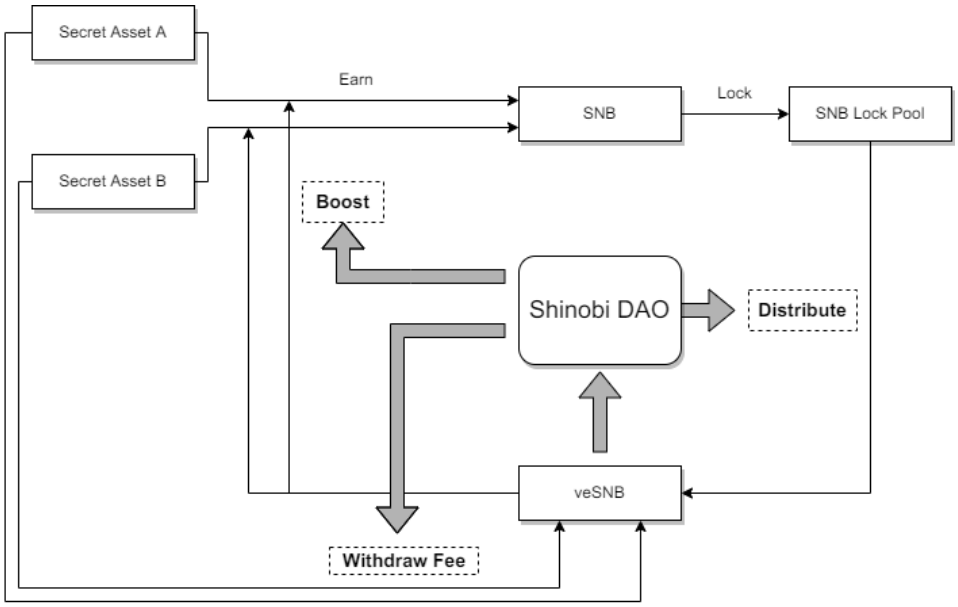

Figure 5: ve-token model of Shinobi

The following is a description of the ve model as applied to Shinobi.

Shinobi Token holders can receive ve Shinobi Tokens by locking their tokens against the lock pool for a certain period of time. The user can choose the lock period from a list of options ranging from short to long term. As a general rule, tokens cannot be withdrawn during the lock period. If withdrawn, a penalty will be imposed according to the remaining lock period.

Holders of the ve Shinobi Token will be given the number of votes that correspond to the number of tokens that they own. Not only that, they can also receive various benefits from Shinobi. When a user withdraws their Secret Asset, ve Shinobi Token holders can receive a portion of the withdrawal fee in the form of a Secret Asset. In addition, those who hold both a Secret Asset and ve Shinobi Tokens can boost the amount of Shinobi tokens they earn by holding the Secret Asset. Furthermore, ve Shinobi token holders who meet certain conditions can receive a discount on the withdrawal Fee when they withdraw their Secret Asset. To what extent they can receive these benefits is determined by the amount of ve

Shinobi Tokens they own and the length of the lock period.

While the ve Shinobi Token themselves cannot be transferred, one can temporarily delegate the voting right in Shinobi DAO. By doing so, the ve Shinobi Token holder can sell or give rights to those who need them, realizing the smooth formation of consensus.

Shinobi aims for its long-term growth by granting significant benefits to Shinobi Token holders with this ve token model and serves to provide a privacy solution through the Secret Network to worldwide crypto users.