ShuttleFlow Light Paper

Enabling Integrated Governance of Multi-Chain Homogeneous Assets

Abstract

Crypto-assets, issued on public blockchains based on decentralized consensus mechanisms and transferred from one DApp to another, are indispensable tokens of value in the blockchain ecosystem. However, different public blockchain systems are interdependent, and so are the assets native to different chains. The interoperability of multi-chain assets can lead to better cross-chain portfolios of high-quality assets, and accelerate the development of the industry. As high-quality public blockchains keep springing up, the existing solutions to one-to-one cross-chain swaps have already fallen short since the cross-chains of N nodes require N^2 cross-chain bridges, which take up a considerably large workload. This promotes the development of multi-chain asset interoperability technology that relies on transit chains.

The cost and efficiency of asset interoperability should not be the threshold of ecosystem development. To this end, the ShuttleFlow Cross-Chain Asset Protocol emerged to further enable multi-chain interoperability of assets. ShuttleFlow provides DApp developers with solutions to integrate deposits and withdrawals of decentralized multi-chain homogeneous assets at a low cost while building cross-chain bridges and related infrastructure with Conflux Network, a high-performance public and permissionless chain as the transit chain.

Terminology

To better describe ShuttleFlow's integrated governance solution for multi-chain homogeneous assets, the following list is the definitions of terms used throughout the document:

1. Homologous assets: assets issued on one chain (Ethereum, Binance Smart Chain, ETC.), but mapped on to different chains by cross-chain transactions;

2. Homogeneous assets: assets issued on multiple chains, but essentially belonging to the same type of token standard;

3. Issuing chain: the public blockchain where assets are issued;

4. Source chain: the public blockchain where assets are to be mapped off of;

5. Transit chain: a public blockchain for asset exchange, which is referred to as Conflux Network in the White Paper;

6. Destination chain: the public blockchain that the assets are to be mapped onto;

7. Mapped asset: Asset A becomes A' after being transferred from the source chain to the destination chain, and A' is the mapped asset of A

Here is an example of a cross-chain scenario in which homologous assets are simply transferred from the source chain to the destination chain. The terms among the above-mentioned terminology in this scenario can be clarified through the following chart:

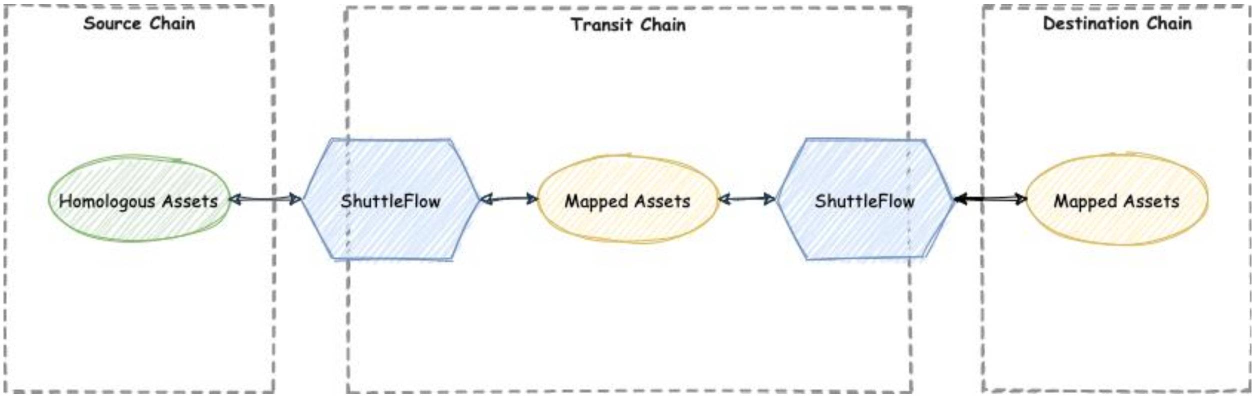

Figure 1

1. Background

The rapid growth of the DeFi ecosystem on Ethereum in 2020 has greatly stimulated the migration of digital assets from various centralized services to decentralized alternatives, and the growing public blockchain space has also triggered a fierce turf war, as several highly anticipated layer-1s launched their mainnet amid a booming DeFi market. Statistics show that by March 2021, the amount of locked value of digital assets on the Ethereum chain has exceeded $38 billion, followed by Binance Smart Chain with $10 billion and Heco chain with $2 billion. With the rise of high-quality public blockchains, cross-chain circulation of homogeneous assets which were issued on multiple chains has drained project developers' energy and hindered liquidity. Therefore, a low-cost integrated governance system for multi-chain homogeneous assets must be immediately available to traders as we progress towards a multi-chain DeFi ecosystem.

2. Related Work

Since BTC has the highest market value among all cryptocurrencies, there have been several services for transferring BTC assets to other public blockchains, such as wBTC, tBTC, and renBTC. Besides, Ethereum, the largest smart-contract public blockchain with the highest market value, has given a rise to ETH and ERC20 asset cross-chain services, such as Near Protocol's “Rainbow Bridge”, “Binance Bridge”, and Ren's “RenVM”. These cross-chain solutions generally focus on one-to-one cross-chain mapping without adequate openness, and thus DApp developers cannot implement cross-chain solutions of new tokens without permission; besides, as high-quality public blockchains increase, we are now facing N-chain interoperability instead of dual-chain interoperability. It is extremely costly to use dual-chain interoperability solutions to handle N-chain interoperability, and the latter requires dual-chain cross-chain bridges supporting the magnitude of N^2. The larger N is, the higher the maintenance costs will grow. Therefore, an N-chain interoperability solution with a transit chain as the hinge can better fit in line with the current industry trends.

The dominance of the Ethereum ecosystem has made it more or less interoperable with various public blockchains, Ethereum has become the de-facto transit chain for cross-chain asset circulation. However, if Ethereum is used as a transit chain to connect all homogeneous assets on Ethereum and other public blockchains, it should meet high-frequency circulation demands caused by token transfers. However, the limited performance of Ethereum's underlying infrastructure often leads to network congestion and a surge of transaction fees.

3. An Introduction to ShuttleFlow

The name “ShuttleFlow”, which consists of “Shuttle” and “Flow”, means allowing assets to shuttle between multiple public chains through cross-chain bridges as freely as Waterflow does. To meet the demand for high performance and low transaction cost from cross-chain hubs, ShuttleFlow has chosen Conflux Network, a high-performance public blockchain, as the base transit chain to offer a decentralized integrated governance service for multi-chain homogeneous assets.

Conflux Network optimizes the performance of the PoW consensus algorithm to over 3000 TPS without compromising on security, which enables on-chain transactions with finality in seconds. Therefore, its performance is sufficient to meet the requirements for a transit chain. Moreover, Conflux Foundation provides gas fee subsidies for all smart contracts on its chain, so users can use contract services on the Conflux Network chain for free without holding any CFX, and this can also cover the transaction costs of the transit chain.

3.1 Cross-chain scenarios

According to different situations, such as whether the same type of assets is issued as homogeneous assets on multiple chains, and whether the issuing and transit chains are the same, we classify the integrated governance of multi-chain homogeneous assets into the following three typical scenarios.

3.1.1 Homologous asset cross-chain mapping when the issuing and transit chains are the same

Cross-chain mapping in this scenario is the most convenient and preferable. If the project owner issues the token on the transit chain natively, it can be directly mapped and transferred to other public blockchains via ShuttleFlow Protocol. If Conflux Network is the transit chain, the procedure is shown as Figure 2:

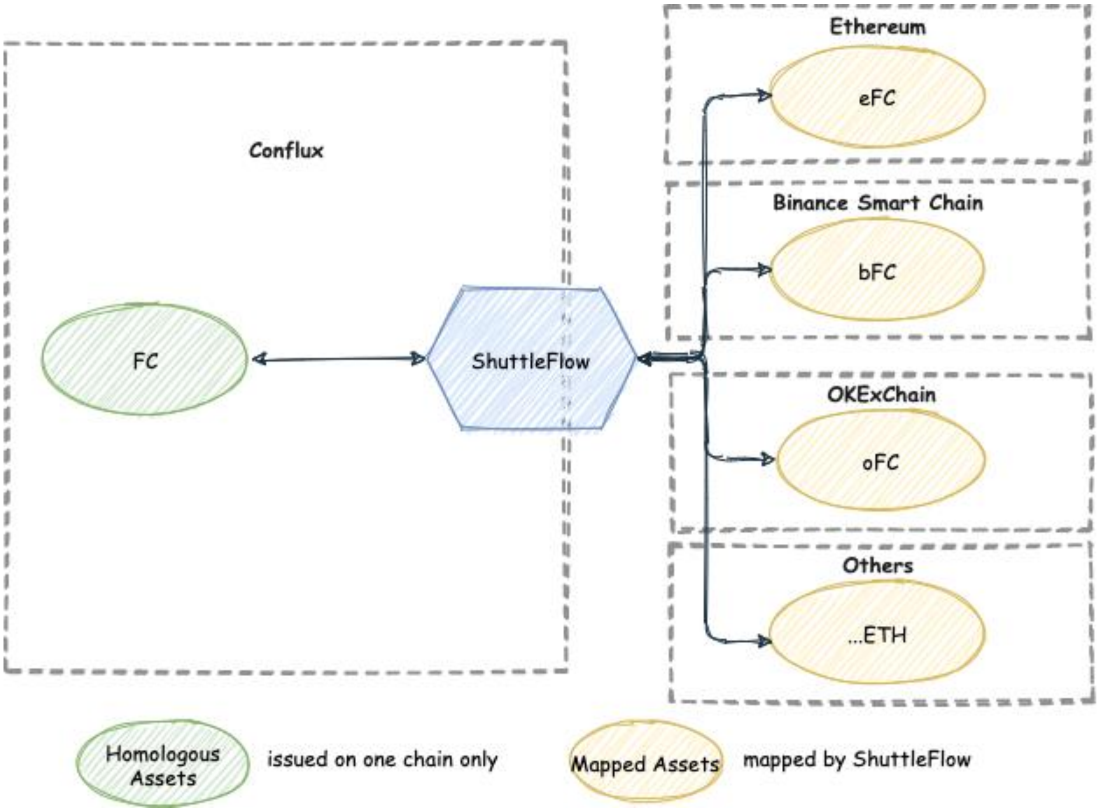

Figure 2

Take FC, a native ERC777 asset on Conflux Network as an example, it can be burned and transferred to Ethereum via ShuttleFlow with a single click under the Alliance's custody, and participate in Ethereum's ecosystem projects seamlessly as a mapped asset "eFC". Conversely, ShuttleFlow can also achieve a one-click cross-chain operation when an eFC is needed to be transferred back to the Conflux Network chain for a fast and free transaction, after which it can participate in the Conflux Network chain projects as a native asset.

Since the tokens are issued on the Conflux Network chain natively, they are homologous assets, and the mapped assets transferred to other public blockchains are pegged 1:1 to the native assets on the Conflux Network chain, so the project owners do not need to worry about the liquidity and the risks of token burn on other chains. Moreover, there is no access threshold for cross-chain application of tokens. Therefore, project owners can directly apply to be the cross-chain service providers of the tokens of their newly launched projects, who can set their own rules for token transfer and gas fees.

3.1.2 Homogeneous asset cross-chain mapping when the issuing and transit chains are different

Cross-chains in this scenario are more complicated since the mapped assets of the homogeneous assets on the transit chain should also be exchanged. Project owners may issue homogeneous assets on the same chain or homogeneous assets concurrently on multiple chains. Under this circumstance, mapped assets on all chains should be mapped on the transit chain (e.g. Conflux Network) to achieve interoperability among homogeneous assets on multiple chains, it is necessary to map the assets on each chain to the transit chain (e.g. Conflux Network). Then StableSwap exchange services like Curve could be used for asset cross-chain swaps. This detailed procedure is shown as Figure 3 :

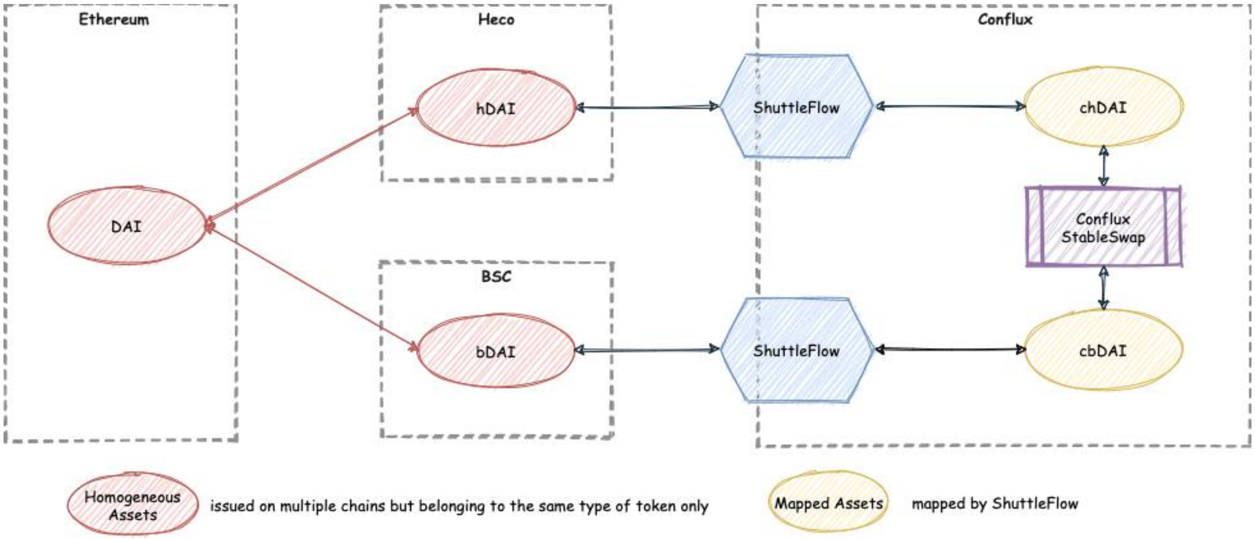

Figure 3

Assume that DAI, issued natively on Ethereum is transferred to the Heco and BSC chains, becoming hDAI and bDAI respectively. If users want to transfer hDAI on Heco to BSC (which means exchanging hDAI for bDAI) ShuttleFlow will first set up the respective mapped assets of Heco’s and BSC’s DAI on the transit chain Conflux Network, which are referred to as chDAI from Heco and cbDAI from BSC after. ShuttleFlow will then inject the liquidity of the chDAI and cbDAI pair into StableSwap services like Curve. Through this method, users can complete the exchange process of hDAI -> (ShuttleFlow) -> chDAI -> (Curve) -> cbDAI -> (ShuttleFlow) -> bDAI with one click, and the entire process can finish without being aware of the intermediate processes in between. Besides, users only need to pay the gas fees of transferring hDAI and bDAI from Ethereum.

3.1.3 Permissionless multi-chain asset interoperability

ShuttleFlow adheres to the principle of zero permission, which means anyone can become a cross-chain service provider for any token on the public blockchains that ShuttleFlow has integrated. Think about the following scenario: a project owner wants to move ABC token to other chains such as Heco and BSC after launching it on Ethereum, but with some public blockchains having access threshold for cross-chain gateways, ABC cannot immediately access other chains. With ShuttleFlow's permissionless transit chain service, ABC’s multi-chain interoperability can be achieved directly as is shown in the Figure 4:

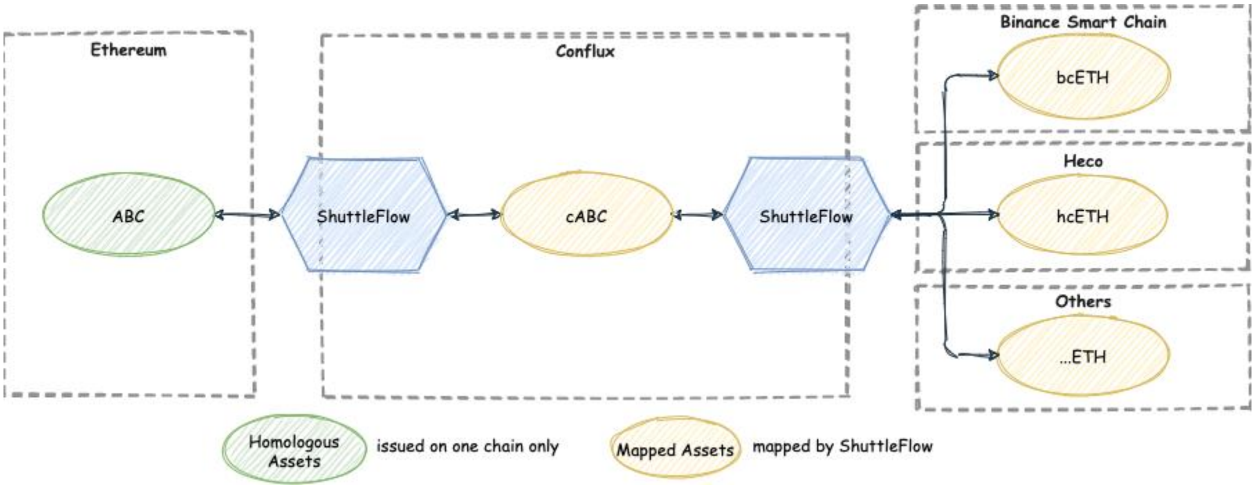

Figure 4

ABC can be first mapped as cABC via ShuttleFlow on the Conflux Network chain, then cABC can be mapped on the BSC chain and become bcABC. ShuttleFlow's feature of the no-access threshold can provide all tokens with decentralized cross-chain service so that the circulation of tokens is no longer a barrier to project development and innovation.

3.2 Cross-chain Asset Mapping

ShuttleFlow implements cross-chain asset mapping by using 2/3 multi-signature technology. In the early stage, ShuttleFlow seeks well-known wallet providers, trusted merchants, and decentralized exchanges to form a Cross-Chain Custodian Alliance（”The Alliance”）. The Alliance uses an invitation system with a rigorous selection mechanism considering the company’s reputation. Each Alliance member will maintain one Alliance Node.

Let us take BTC as an example. Using multi-signature technology, members of the Alliance can mint cBTC on Conflux Network, pegged 1:1 to BTC, providing minting and burning services. The specific process works like this:

First, we need to create a multi-sig account on Bitcoin to lock the BTC collateral required to mint cBTC. We also need to deploy a smart contract on Conflux Network that manages and records the minting and burning of cBTC. The Bitcoin multi-sig account and the cBTC smart contract are jointly managed by the members of the Cross-Chain Custodian Alliance discussed above. The Alliance employs an off-chain admittance mechanism, where the entry of new members is decided by existing members. Each member of the Alliance runs a custodian node. This custodian node is responsible for monitoring and verifying on-chain events on both the Bitcoin chain and Conflux Network, as well as submitting the corresponding transactions after an event has occurred.

3.2.1 Minting

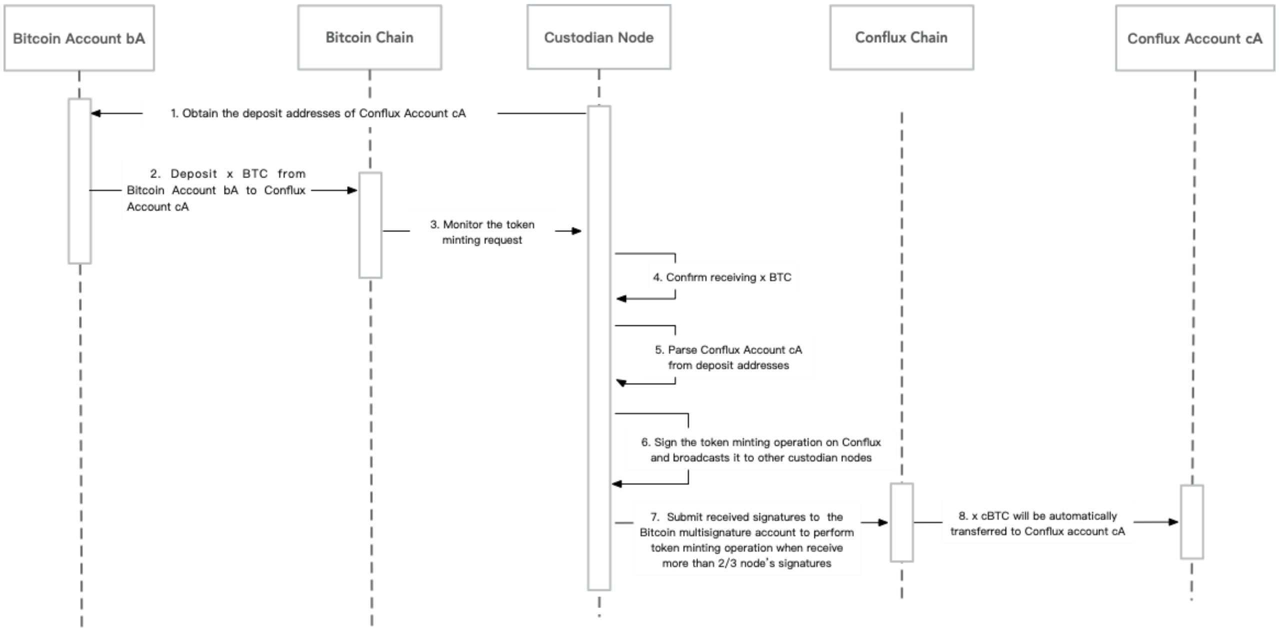
Bitcoin Account bA
Bitcoin Chain
Custodian Node
Conflux Chain
Conflux Account cA
1. Obtain the deposit addresses of Conflux Account cA
2. Deposit x BTC from Bitcoin Account bA to Conflux Account cA
3. Monitor the token minting request
4. Confirm receiving x BTC
5. Parse Conflux Account cA from deposit addresses
6. Sign the token minting operation on Conflux and broadcasts it to other custodian nodes
7. Submit received signatures to the Bitcoin multisignature account to perform token minting operation when receive more than 2/3 node's signatures
8. x cBTC will be automatically transferred to Conflux account cA

Figure 5

1 The Custodian Node provides the deposit address of Conflux Network Account cA of user A.

2 User A transfers x BTCs into the deposit address from his Bitcoin Account bA.

3 The custodian node in the Cross-Chain Alliance detects the token minting request to the multi-signature account on Bitcoin.

4 The Custodian node makes confirmation of receiving x BTCs and waits for the corresponding transaction on Bitcoin to get confirmed and achieve finality and verifies that x BTC has been received.

5 The custodian node parses Conflux Network Account cA from deposit addresses.

6 The custodian node signs a token minting request *"mint x cBTC to Conflux Network account cA"* on Conflux Network and broadcasts it to other custodian nodes.

7 Once a custodian node has received more than 2/3 of all nodes' signatures for this operation, it submits the collected signatures to the cBTC smart contract on Conflux Network to perform the token minting operation. Repeated submissions are ignored.

8 After the smart contract has executed the token minting operation, x cBTCs are automatically transferred to the Conflux Network account cA.

3.2.2 Burning

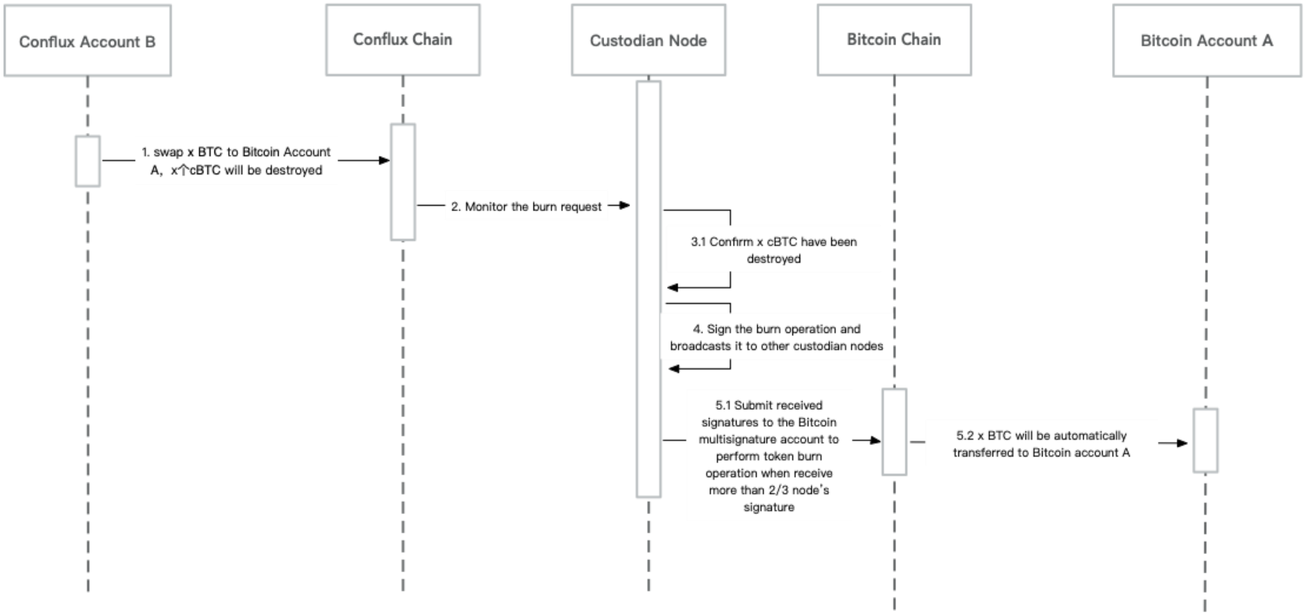
Conflux Account B
Conflux Chain
Custodian Node
Bitcoin Chain
Bitcoin Account A
1. swap x BTC to Bitcoin Account A，x个cBTC will be destroyed
2. Monitor the burn request
3.1 Confirm x cBTC have been destroyed
4. Sign the burn operation and broadcasts it to other custodian nodes
5.1 Submit received signatures to the Bitcoin multisignature account to perform token burn operation when receive more than 2/3 node's signature
5.2 x BTC will be automatically transferred to Bitcoin account A

Figure 6

1 An Alliance member's Conflux Network account cA submits a transaction to the cBTC smart contract to state a burn request *"swap x BTC to Bitcoin account bA"*. cA needs to transfer x cBTC to the smart contract as part of this transaction, and the transferred cBTC (amount x) will be destroyed. The information of the Bitcoin account bA is specified as a request parameter.

2 The custodian nodes of the Cross-Chain Alliance detect the burn request in the cBTC contract on Conflux Network.

3 After a custodian node has detected the request, it waits for the corresponding transaction on Conflux Network to get confirmed and achieve finality and verifies that x cBTC has been destroyed.

4 Once the burn request has been verified, the custodian node signs the burn operation *"transfer x BTC to Bitcoin account bA"* on Bitcoin and broadcasts it to other custodian nodes.

5 Each custodian node collects signatures independently:

5.1 Once a custodian node has received more than 2/3 of all nodes' signatures for this operation, it submits the collected signatures to the multi-signature account on Bitcoin to perform the token burn operation. Repeated submissions are ignored.

5.2 After the smart contract has executed the token burn operation, x BTCs are automatically transferred to the Bitcoin account bA.

3.3 Permissionless Applications for Cross-chain Asset Mapping

The applications for cross-chain asset mapping are permissionless. To support more cross-chain assets between Ethereum and Conflux Network, ShuttleFlow has initiated the Token Captain application mechanism. Anyone can support any cross-chain mapping of tokens on the Ethereum and Conflux Network by becoming a Token Captain, for each token, there will only be one Token Captain, most likely the initial token issuer.

Token Captain will need to provide initial collateral, and a portion of cTokens to deduct the actual realized cost of the user's cross-chain mapping. For example, if mapping ETH to Conflux Network, the Token Captain needs to collateralize some cETH for users. If the user amount is too large, and the collateralized tokens have all been consumed, the Token Captain needs to add collateral to ensure the operation of the mapping service.

The captains can formulate the fee charged from users for each cross-chain mapping. The on-chain processing cost of each cross-chain map is deducted from the cETH collateral by the Token Captain. The cross-chain fee and new address fee will eventually be settled on the wallet address of Token Captain.

3.4 Alliance Governance

3.4.1 Change of Alliance members

When new members wish to join the alliance, all existing members will cooperate to complete a multi-signature transaction and transfer the BTC in the current multi-signature account to a new multi-signature account including the new member. When existing members wish to exit the alliance, all other existing members will cooperate to complete a multi-signature transaction and transfer the BTC that in the current multi-signature account to a new multi-signature account without the departing member.

3.4.2 Private key management of alliance members

The multi-signature mechanism of alliance nodes is used to protect the smart contract. Any changes of contracts or assets need to be authorized by alliance members, when more than 2 / 3 nodes co-signatures reach a consensus, the cross-chain transaction can be confirmed and completed.

To improve transaction experience and efficiency, each member of the alliance has two private keys, which are stored in the hot wallet and the cold wallet respectively, and used for small and large market-cap token acceptance:

- For the acceptance of smaller market-cap tokens, the private key in the hot wallet is used, the alliance node can monitor the request in real-time, verify the data on-chain automatically, and execute the signature automatically. The token acceptance request can get feedback immediately.
- For the acceptance of larger market-cap tokens, the private key in the cold wallet is used, a second manual audit will be needed after the alliance node automatically monitors the verification request. The asset acceptance request needs to wait for the completion of the manual audit.

4. ShuttleFlow Roadmap

In Q1 of 2020, ShuttleFlow v1.0 was officially launched. It has been running smoothly for one year, supporting 49 kinds of assets with a total value of $25 million, from Bitcoin and Ethereum to the Conflux Network chain.

In Q1 of 2021, ShuttleFlow plans to release v2.0 to complete the function of reversely crossing the assets from the Conflux Network chain to the mainstream public chains like Ethereum. At the same time, it will complete the two-way function of cross-chain mapping with exchange public chains: Binance Smart Chain (BSC), Huobi ECO Chain (Heco), and OKExChain.