POPCHAIN Cross-chain Transaction Specification

Version：	V1.1.0	No：	TH-TL-POP-07
Security level：	A+	Department/Project：	R&D department
Product：	POPCHAIN cross-chain transaction design	Subsystem：	

About the book

Overview

- This book is the blockchain project of POPCHAIN Foundation - POPCHAIN hardware terminal-POPBOX product hardware requirements specification.
- POPCHAIN Foundation provides software and hardware design and implementation solutions for the project. The POPCHAIN Foundation has the final right to modify and interpret this document and program.

Contents

I. Requirements Overview

1. Background

Cross-Chain, as the name suggests, is a direct value flow through a technique that allows the value to cross over the barriers between two chains. The current technologies for the Cross-Chain transaction mainly include:

1) Intermediary Agency

   Cross-Chain transactions are via intermediaries, so a trusted third-party intermediary agency is necessary.

2) Cross-Chain Atomic Transactions

   Transactions are initiated spontaneously by asset owners in different chains, either successfully completing a Cross-Chain transaction or returning the unsuccessful asset to the original owner without a trusted third party.

3) Sidechain

   The Sidechain carries out the inter-chain asset transfer with Mainchains by theSPV or miner voting. The Sidechain is equivalent to the attached chain of the Mainchain, and does not produce assets, which means the Sidechain block has no coin reward.

2. Requirements

To facilitate the participation of more people and to increase the community popularity, PCH is distributed to other blockchain wallets.

In addition, POPCHAIN, as a public blockchain, supports Sidechain to apply rich applications in the future. Different applications can use Sidechains with different characteristics.

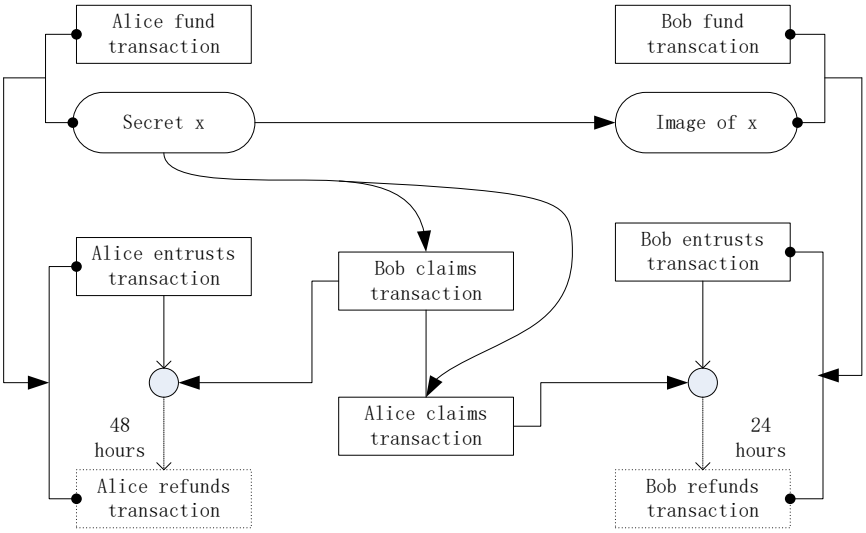
II. Cross-Chain Atomic Transaction Technology Implementation

1. Cross-Chain Atomic Transactions

Cross-Chain atomic transaction means an atomic transaction with only two conditions; successful and unsuccessful transactions.

1) When a transaction is successful, both parties of the Cross-Chain transaction successfully exchange the assets on the chain.

2) When a transaction is unsuccessful, the parties of the Cross-Chain transaction fails to exchange the assets on the chain on time, and the original assets are returned to the individuals.



[Cross-Chain Atomic Transactions]

The diagram above shows a Cross-Chain atomic transaction process; Alice on POPCHAIN and Bob on the Sidechain for a Cross-Chain transaction. Cross-Chain transactions rely on a commissioned transaction generated with a "secret". Unlocking this transaction requires either of the following two conditions:

1) One party initiates the claim transaction with a signature and a secret x.

2) If the other party does not initiate the claimed transaction, a valid refund for the transaction can be initiated after the agreed time, as indicated by the dotted line in the above figure.

   If Alice generates a commissioned transaction and does not send x to Bob within 24 hours, she will have to wait for 24 hours. This is a penalty for her failure to transfer, and Bob's property is not lost.

Once Bob generates the commissioned transaction, Alice takes the initiative. She can send x to Bob, or she can directly unlock Bob's commissioned transaction, but Alice's claimed transaction must contribute x.

So, Bob should pay attention to see if Alice's claimed transaction has occurred on the block. If he finds it, Bob has at least 24 hours to initiate a claim.

2. Cross-Chain transaction script

The following is an implementation of the Cross-Chain transaction script between Alice on POPCHAIN and Bob on a Sidechain.

The x and x images: x is a random number of 256 bits generated by Alice. x through the SHA256 and RIPEMD160 algorithms can generate x like <X_HASH>, the length is 160 bits.

Alice initiates a lock script (scriptPubKey) for agency transaction:

```
IF
    HASH160 <X_HASH> EQUALVERIFY
    <Bob_pch Pubkey> CHECKSIG
ELSE
    <48 hours> CHECKSEQUENCEVERIFY DROP
    <A_pch Pubkey> CHECKSIG
ENDIF
```

Bob initiates a lock script for the agency transaction (scriptPubKey):

```
IF
    HASH160 <X_HASH> EQUALVERIFY
    <Alice_s Pubkey> CHECKSIG
ELSE
    <24 hours> CHECKSEQUENCEVERIFY DROP
    <Bob_s Pubkey> CHECKSIG
ENDIF
```

The witness script for Alice's claim transaction (scriptSig):

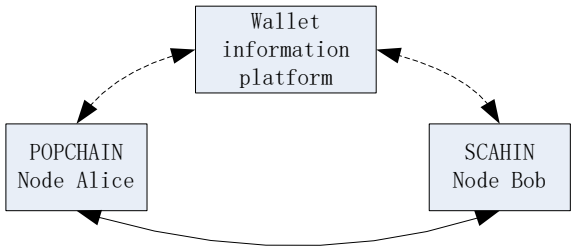
```
    < Alice_s'Sig > x TRUE
```

Bob's witness script for claim strip (scriptSig):

```
    <Bob_pop'Sig > x TRUE
```

3. The Information Platform

Cross-Chain transactions involve three objects, the POPCHAIN wallet node, the Sidechain wallet node, and the information platform. The relationship between them is shown in the following figure.



[The Information Platform]

The messaging platform only provides communication among nodes and does not participate in specific Cross-Chain transactions. Its security performance does not affect Cross-Chain transaction security, so the messaging platform can be implemented by any communicable tool.

When Alice on POPCHAIN has a redemption requirement, she can post a message on the message platform, or view the messages posted by others on the message platform. The establishment and implementation of real Cross-Chain transactions is indicated by the solid arrows in the figure above.

4. Process Instances

Background：

Alice on POPCHAIN has an asset of 10PCH that needs to be converted into an asset of 100S on a Sidechain by 1:10.

Process：

1) Alice posts a message on the POPCHAIN messaging platform:

2) I own 10PCH, the asset of POPCHAIN, and now I want to redeem the 100S asset on the Sidechain;

3) Bob browses the message sent by Alice on the POPCHAIN message platform, and also wants to convert the 100S on his Sidechain to 10PCH on POPCHAIN.

4) Alice and Bob exchange their respective collection addresses;

5) Alice generates a secret x and an agency transaction J and sends the image of x and the agency transaction J to Bob.

6) Bob generates an agency transaction K in his Sidechain wallet and sends K to Alice;

7) Alice tells Bob about the secret x within 24 hours, then Bob can use this secret to unlock the transaction J. Similarly, if Alice wants to unlock the transaction K, the secret x must be disclosed on the Sidechain. At this time, Bob can check the transaction to find the secret x;

8) If Alice repents, Bob's assets on Sidechain are returned after 24 hours; Alice's assets on POPCHAIN are also returned 48 hours later.

III. Sidechain technology

Unlike Cross-Chain atomic transaction, the Sidechain technology emphasizes the authority of the Mainchain. The Sidechain is attached to the Mainchain, but in some functions (such as speed), it has its own distinctive features. Of course, the Sidechain also supports Cross-Chain atomic transaction.

The core of the Sidechain technology is the safe transfer of assets between the Mainchain and sidechain assets, which we call the "Two-way peg".

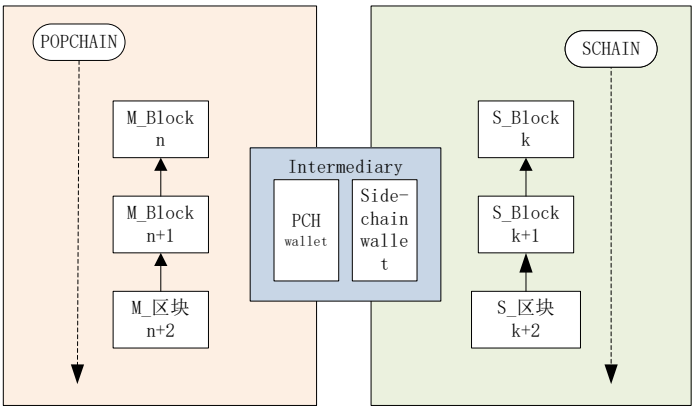
"Two-way peg" explanation:

Two-way: MMainchain funds → Sidechain, Sidechain funds → Mainchain.

Peg: The exchange rate for the "Two-way" transfers is fixed.

1. The Sidechain of the Intermediary Mechanism

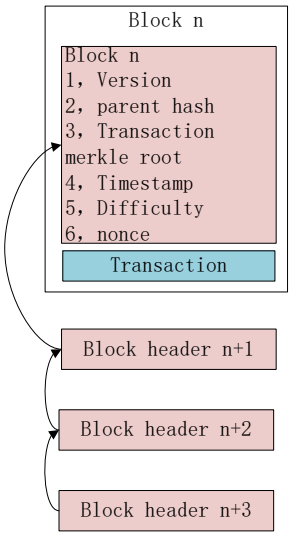
Two-way peg is achieved through intermediaries and objects that require asset transfer. First, assets are transferred to the intermediary on the chain and then are distributed by the intermediary.



[The Sidechain of the Intermediary Mechanism]

2. Sidechain

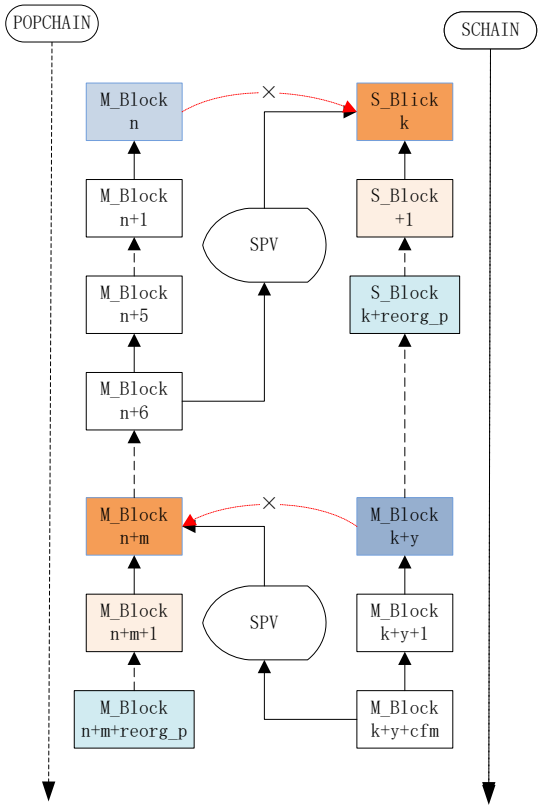
A block consists of block headers and transactions. The structure of the block header is as follows:



[Sidechain]

To verify a transaction, a block header table is provided for the blockchain, the merkle tree of the transaction is combined with the node, and the block is generated for the transaction.

If it is considered difficult to construct a block header, the entire list of block header can be used as a valid proof of authenticity.



[Sidechain]

The picture above shows the operation of Sidechain. The key to Sidechain lies in the understanding of SPV. The Sidechain's understanding of the Mainchain's SPV is easierMainchain, because it is more difficult to forge a list of SPV block headers of a Mainchain. However, it is much more difficult to understand the SPV of the Sidechain. The difficulty of the Sidechain is set to be higher than that of the Mainchain, so the mining speed of the Sidechain is not faster than the Mainchain. If the difficulty is low, it will facilitate the forgery of SPV stealing assets.

3. Drivechain

The design principle of the Sidechain is that POPCHAIN does not observe the existence of a specific Sidechain, and the Drivechain requires POPCHAIN to have a certain understanding of Sidechain. The recovery of the Drivechain is done by the miners voting.

Pegging from POPCHAIN to Sidechain:

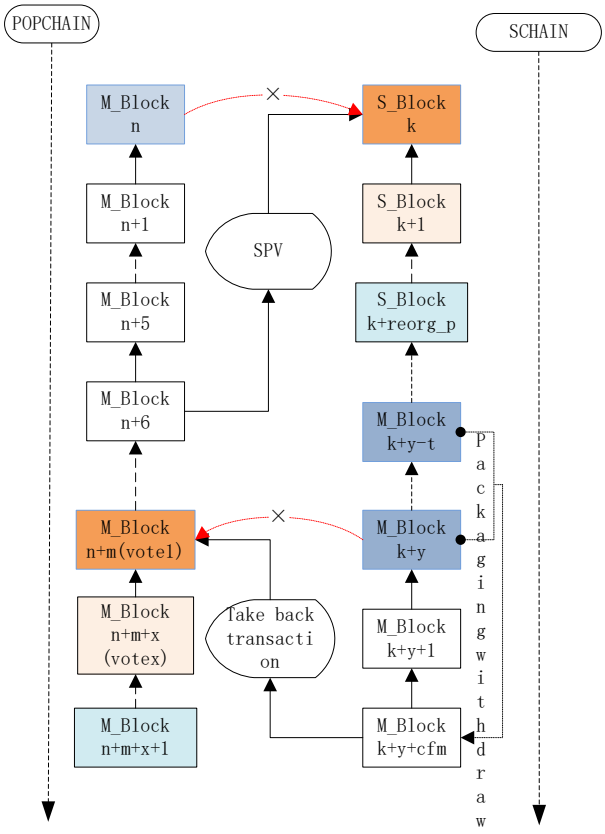
As mentioned earlier, the SPV of the Mainchain is not easy to forge, and Sidechain can easily verify the correctness of the Mainchain by pegging transactions.

Pegging from Sidechain to POPCHAIN:

The miners of Sidechain package a withdrawal transaction over a period of time and post it on the Mainchain to form a special deal on the Mainchain.

The input referenced by withdrawal transaction of Sidechain is the anchor transaction initiated by POPCHAIN to Sidechain. The miners of the Mainchain vote on the withdrawal transaction, and the withdrawal transaction that reaches the number of votes in the voting window will be packaged by the miners into the block. Miners of the Mainchain must have the ability to verify withdrawal transaction and therefore can do joint mining. The joint and the solo miners are both Mainchain and sidechain miners and are the only miners that can verify the withdrawal transaction and make credible votes on the Mainchain.

The operation of the Drivechain is as follows



[Drivechain]