BLOCKCHAIN-SIDECHAIN TRANSACTIONS
WITH "TWIN ACCOUNTS"

by Oleg Tomin, Sergei Smalkov and Viktor Glukhikh

This article outlines one of the ways to transfer assets between a blockchain and its sidechain using a pair of twin accounts, one in each blockchain.

Sidechain described in this article is inherently a child copy (fork) of Ethereum. Similar architecture implies smart contracts and mutual address space. Both blockchains utilise the same type of smart contracts, therefore one can create identical tokens and use identical twin addresses to move tokens across Ethereum and sidechain. We could call this process "token teleportation". This way the intermediary role is assigned to an identical pair of smart contracts, one in each blockchain.

1. Introduction

We currently witness the formation of various blockchain platforms leading to the growth in the number of although valuable but incompatible technologies and cryptocurrencies. At this early stage, we do not have a single universally recognized interblockchain standard. Therefore there is no widely adopted way of exchanging data and assets (aka currencies and tokens) between separate blockchains. It would seem a simple task the industry has been craving for. Indeed, there are many prospective cross-chain platforms and services that address the issue. For example, there are currency conversions, exchanges for traders, equivalent to real pegged currencies. Unfortunately, most, if not all of them are centralized in one way or another.

As the current practice shows, any distributed ledger service built on principles of even minor centralisation undermines the whole idea of decentralization, and thus, security and anonymity. A number of projects proposed their solution: Oraclize - Decentralised network of oracles, Cosmos project, Polkadot and other. Most of them solve the crosschain exchange problems with their own blockchain and currency, which increases complexity in the world of blockchains further multiplying interblockchain barriers.

Ethereum smart contracts are an extremely powerful tool. Ethereum itself has the means of crosschain communication in the form of oracles - single intermediary nodes.

The only piece of the puzzle missing is the decentralised nature of the oracles. With the development of Ethereum, as a universal platform for smart contacts, we can see another neat and simple way to solve the problem of crosschain interaction.

We could turn our attention to the concept of Plasma (Ethereum add-on). The idea of Plasma lies in the hierarchy of blockchains.

Thus anyone could make his own token by forking the same universal Ethereum platform - one Ethererum sidechain for each new token. With some adjustments, one could make sidechain to fit his tokens needs while not compromising Ethereums universality. Thus, the following innovations are possible:

- different consensus algorithms,

- different algorithm of mining fees,
- built in p2p, tor, VPN.

The main idea is to utilise identical tokens, one on a blockchain and another on a sidechain, backed by the mechanism for their direct exchange one to the other.

One possible scenario could be based on identical sibling pair of smart contracts loaded to Ethereum and sidechain. These two smart contracts could move tokens between each other and between the blockchain and sidechain.

To move tokens from the blockchain to the sidechain smart contracts freeze a certain number of tokens on Ethereum and unfreeze the same amount on the sidechain.

This process could be called teleporting in resemblance to the work of a teleport. If you send tokens from the blockchain to the teleport, they will disappear on the one side and reappear on the sidechain. The reverse teleportation works in the reverse order.

The possible modification to the sidechain mentioned previously could help reduce transaction time and fee.

2. Blockchain-sidechain interface token teleportation algorithm

Let's build an Ethereum sidechain with identical smart contracts and a single address space.

These sibling smart contracts called Teleport will work as the interface between the blockchain and the sidechain.

We will teleport tokens between identical twin accounts on the blockchain and the sidechain and back. We will call this “twin accounts” technology.

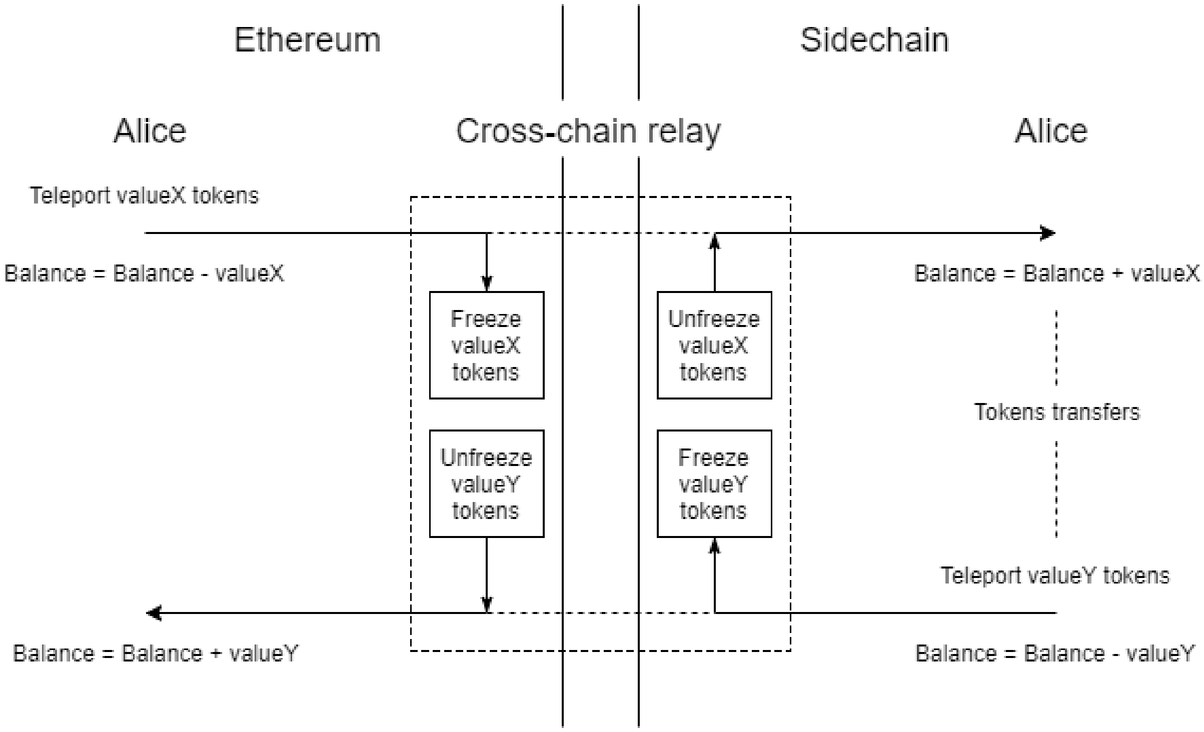

Fig.1. Blockchain-sidechain token teleportation algorithm

As can be seen from the above diagram, at any given time our user has a certain number of tokens. Some of them are on Ethereum, while the rest are on the sidechain. Tokens are identical and can be collected at any given time on one of the twin accounts. The total balance of the tokens for a given pair of accounts is always equal to the sum of the balances of the pair.

The process is synchronous. Transactions in the blockchain and sidechain go in turn, one after another. The synchronous nature of the process could help avoid the "double spend" attacks.

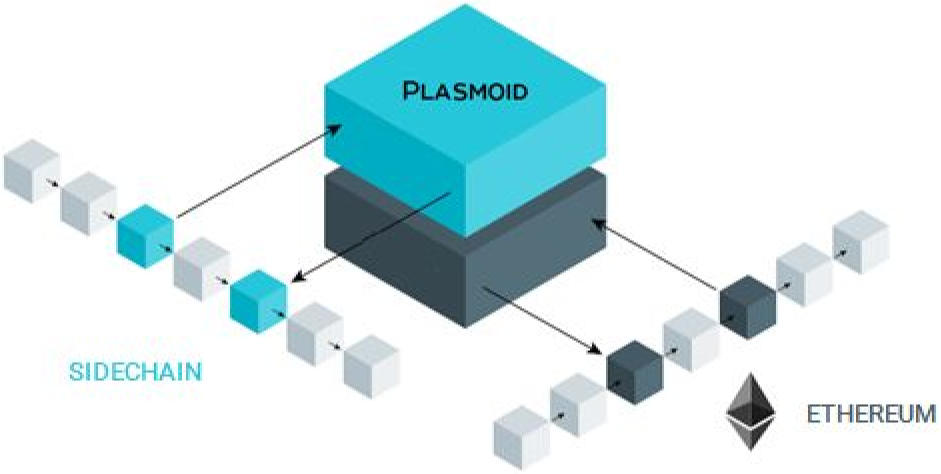

Fig.2. Crosschain oracle Plasmoid

The whole process of tokens teleportation is managed by a special node Plasmoid (crosschain oracle). To initiate teleportation client DApp calls for Teleport smart contract, which in its turn assigns one of the registered and active Plasmoids as an oracle for this specific exchange. Plasmoid is a server with a set of logic that translates signed transactions, requests and replies between Plasmoid, blockchain and sidechain. Plasmoids receive fees for their work and compete with each other for the right to be an intermediary oracle.

In the smart contract, there should be special storage for Plasmoids unique profiles. Plasmoid must be registered in the smart contract to have the right to be the intermediary. The registration of Plasmoid implies a certain amount of tokens hold as a pledge. The amount of frozen tokens determines the number of exchanges Plasmoid can process.

3. Security

Token teleportation algorithm also addresses security issues in a number of ways. Teleport smart contract should maintain the log of teleportations. So that, in the case of incidents, it would be possible to trace the progress of teleporting and restore the correct course of operations. The mandatory amount of pledged tokens or coins work as security insurance. Plasmoids would also have to hold a certain amount of tokens to be elegible as exchange intermediary oracle.

4. Conclusion

As can bee seen, this algorithm with twin accounts and smart contracts, is one elegant and simple yet powerful way of interblockchain communication. The whole concept can become a good starting point for development in the field of direct crosschain exchange, so called atomic swap. Furthermore, it may also be another step towards universal interblockchain programming language and the concept of internet of blockchains.