Coin direct exchange protocol

by Oleg Tomin, Sergey Smalkov, Victor Glukhikh

Coin direct exchange protocol (CDX protocol) is an open source protocol for direct exchange of tokens and cryptocurrencies across blockchains.

The protocol is based on Ethereum blockchain and its sidechain Youdex. It works as an interblockchain interface. The algorithms themselves are stored in preloaded on Ethereum and Youdex smart contracts and on oracle nodes. The code of both is licensed under MIT license (opensource) and available to the public on https://github.com/YouDex. At the network level security is taken care of by the p2p protocol alongside with the Ethereum and Youdex consensus algorithms, while at the application level it is handled by the algorithms in smart contracts and client DApps.

CDX protocol was heavily influenced by the following ideas: Twin accounts technology [1], Plasma platform proposed by V. Buterin and D. Poon [2], BTC-relay smart contract [3], Oraclize [4], Interledger protocol [5], 0x protocol [6], DYDX protocol [7] and others.

1. Introduction

Secure tokens and coins direct exchange requires a minimum number of transactions carried out without intermediaries. Ideally, the process should be limited to two transactions, one in each exchange direction. Only this transaction-light method gives maximum speed and minimum overhead.

However, this usually comes at the cost of safety. Due to the inconsistent number of transactions throughput on different blockchains, there is a constant threat of "double waste" and fraud.

The use of multi-signature transactions does not solve the problem in its entirety, overcomplicates and slows down the exchange speed, not to mention the increased costs. As for the centralized services, that although seem to solve the speed issue, unfortunately, it undermine the whole paradigm of security and safety through decentralization.

CDX protocol offers the solution to the problem, securing only single transactions in a form of a pledge (escrow).

At the core of the crosschain services is a pair of identical twin smart contracts - YODA (ERC20 token) and Teleport smart contract. One on Ethereum blockchain and the other on Etherium sidechain Youdex (Ethereum fork). The crosschain transactions are fueled by YODA tokens present in both blockchains, acting as a linking device between the two ledgers.

2. Blockchain-sidechain linking

The key concept behind blockchain linking is a pair of identical "twin accounts". YODA tokens are transferred (teleported) from Ethereum blockchain to its sidechain Youdex and vice versa.

As can be seen from the diagram below (fig. 1), at any given time the user should hold a certain number of YODA tokens. Some of them are on Ethereum, and some are on Youdex. Tokens are identical on both blockchains. Depending on where the tokens are to be used inside Youdex or on Ethereum, they can be transferred at any given time to either of the twin accounts. This is the "twin accounts" concept. More details on the Twin Accounts are in the section [1].

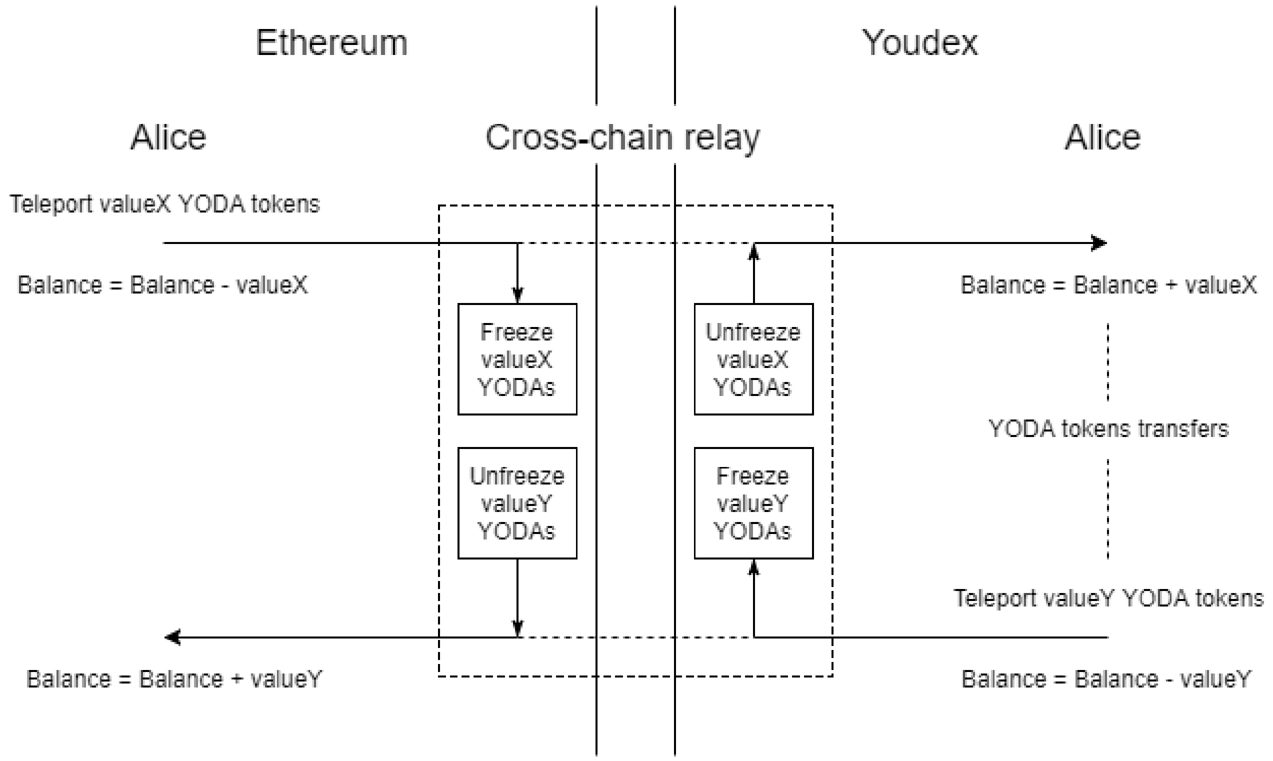
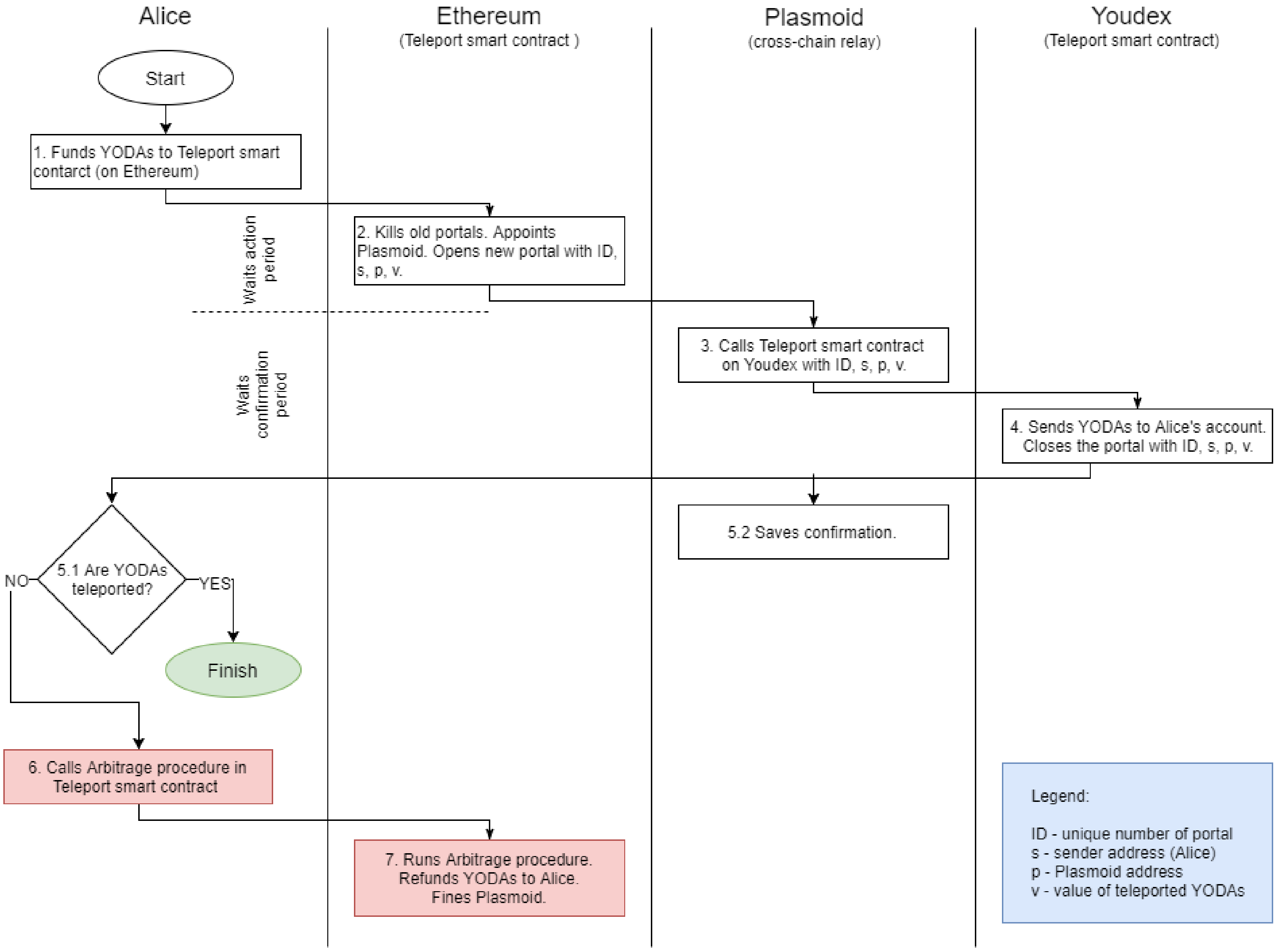

Ethereum
Youdex
Alice
Cross-chain relay
Alice
Teleport valueX YODA tokens
Balance = Balance - valueX
Freeze valueX YODAs
Unfreeze valueX YODAs
Balance = Balance + valueX
YODA tokens transfers
Unfreeze valueY YODAs
Freeze valueY YODAs
Teleport valueY YODA tokens
Balance = Balance + valueY
Balance = Balance - valueY

Fig. 1. Blockchain-sidechain link

A special DApp (cross-chain oracle called Plasmoid) controls the transfer between blockchain and sidechain. It is a node with the set of logic with state control and error handling, that translates signed transactions, requests and responses among nodes on blockchain and sidechain. Plasmoid generates a necessary number of transactions between escrow accounts and user accounts and uses Teleport script to teleport tokens.

3. Teleporting YODA tokens

To transfer YODA tokens from blockchain to Youdex, DApp node initiates transfer by running the predefined script. First, YODA tokens on Ethereum are transferred from Ethereum-side account to the escrow account of Teleport smart contract. Then, on the sidechain the same amount of YODAs are transferred from the escrow account to the Youdex-side user account. To transfer tokens back from sidechain to Ethereum the same steps are taken but in reverse order.



Alice
Ethereum
(Teleport smart contract)
Plasmoid
(cross-chain relay)
Youdex
(Teleport smart contract)
Start
1. Funds YODAs to Teleport smart contarct (on Ethereum)
Waits action period
2. Kills old portals. Appoints Plasmoid. Opens new portal with ID, s, p, v.
Waits confirmation period
3. Calls Teleport smart contract on Youdex with ID, s, p, v.
4. Sends YODAs to Alice's account. Closes the portal with ID, s, p, v.
5.2 Saves confirmation.
5.1 Are YODAs teleported?
NO
YES
Finish
6. Calls Arbitrage procedure in Teleport smart contract
7. Runs Arbitrage procedure. Refunds YODAs to Alice. Fines Plasmoid.
Legend:
ID - unique number of portal
s - sender address (Alice)
p - Plasmoid address
v - value of teleported YODAs

Fig. 2. The algorithm of YODA tokens teleportation

The protocol is synchronous, transactions in the blockchain and sidechain are initiated in turn, one by one, to prevent "double spend" attack. In the event of transaction errors, there is a rollback functionality.

Plasmoid is not the owner of the escrow account. Each Plasmoid has a record in Teleport smart contract. The smart contract and service logic source codes are licensed under MIT license (opensource). In order to bring competitiveness and incentives in the line of decentralization, Plasmoids are paid fees for the cross-chain transactions they process.

Plasmoids will have an open API and SDKs for the integration with third-party services and applications.

The method of interblockchain linking described above brings following advantages:

- almost total decentralization;
- single address space identical in both blockchains;
- use of one pair of keys for both blockchains stored on a given client device;
- identical smart contracts;
- lightweight logic;
- insured transaction security;
- DApps that are connected simultaneously/alternately to blockchain and/or sidechain;
- limitless expandability due to the integration with third-party services.

Below is the detailed outline of direct and cross-chain exchanges of cryptocurrencies, YODAs, ETH, ERC20 tokens on Ethereum supported by the CDX protocol.

4. ERC20 tokens secure exchange algorithm

The availability of teleported YODA tokens allows one to organize a secure, inexpensive and fast exchange of ERC20 tokens. Each party and transaction is secured by a smart contract pledge. The two main ingredients of the exchange are DEx smart contract and DExT script (decentralized exchange of tokens).

To minimize transaction fees and accelerate the exchange pledges are made on Youdex sidechain. Exchange parties must have a sufficient number of YODA tokens already stored on their Youdex accounts. Otherwise, the missing amount of YODAs must be teleported from the main blockchain.

The process of exchange goes as follows. Alice's DApp (order maker) broadcasts onto the p2p network his proposed bid for the exchange of v1 of Token1 to v2 of Token2 with a unique id. Bob's DApp (order taker) responds to the bid and initiates the exchange. Plasmoid crosschain oracle calculates the size of the pledge in YODA tokens based on the current cross-rates of tokens and YODA.

It is assumed that tokens exchange cross-rate is automatically agreed beforehand. Service oracles propose the cross-rate based on the data gathered from the outside markets(The cross-rate negotiation protocol is currently under development).

Plasmoid implements DExT script and Depo function of DEx smart contract according to the following algorithm.

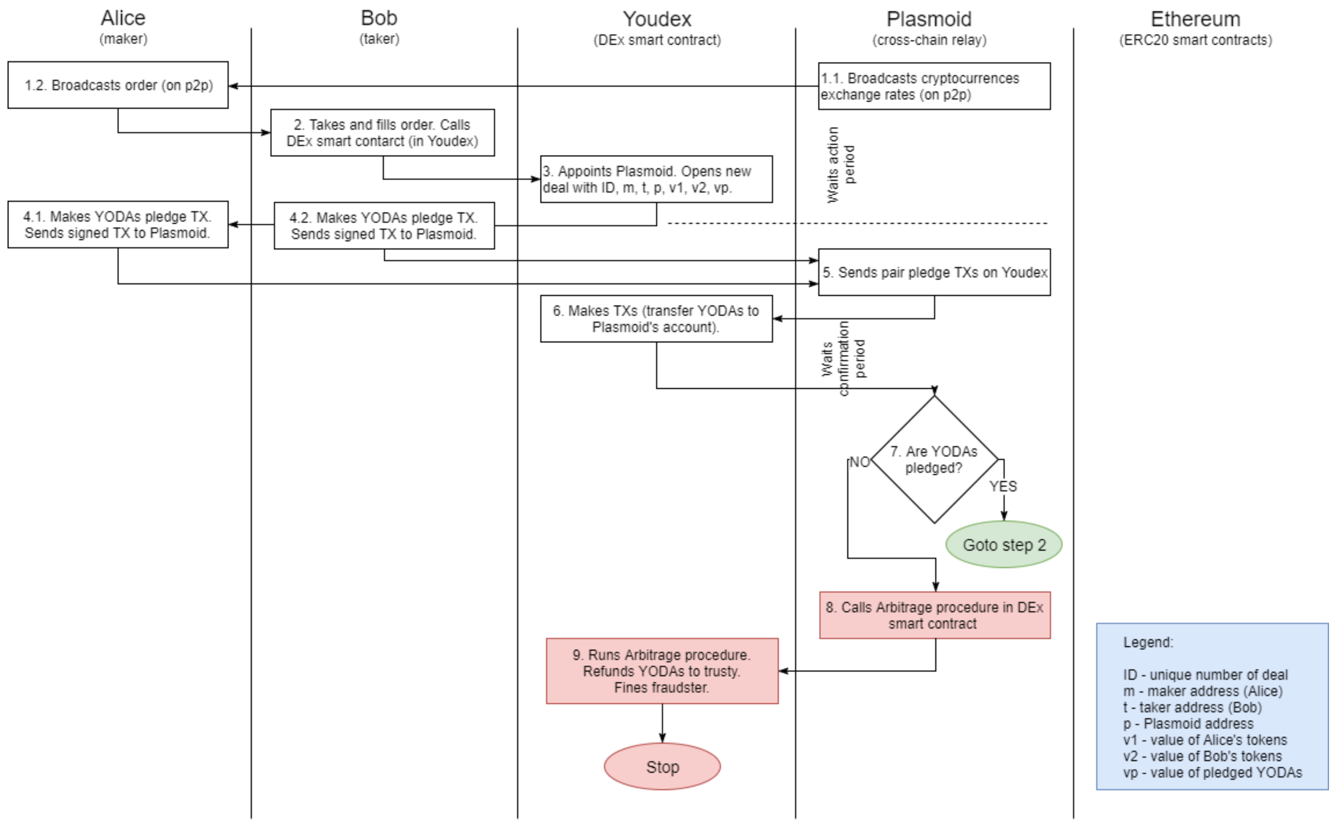

Alice
(maker)
Bob
(taker)
Youdex
(DEx smart contract)
Plasmoid
(cross-chain relay)
Ethereum
(ERC20 smart contracts)
1.1. Broadcasts cryptocurrences exchange rates (on p2p)
1.2. Broadcasts order (on p2p)
2. Takes and fills order. Calls DEx smart contarct (in Youdex)
3. Appoints Plasmoid. Opens new deal with ID, m, t, p, v1, v2, vp.
Waits action period
4.1. Makes YODAs pledge TX. Sends signed TX to Plasmoid.
4.2. Makes YODAs pledge TX. Sends signed TX to Plasmoid.
5. Sends pair pledge TXs on Youdex
6. Makes TXs (transfer YODAs to Plasmoid's account).
Waits confirmation period
7. Are YODAs pledged?
NO
YES
Goto step 2
8. Calls Arbitrage procedure in DEx smart contract
9. Runs Arbitrage procedure. Refunds YODAs to trusty. Fines fraudster.
Stop
Legend:
ID - unique number of deal
m - maker address (Alice)
t - taker address (Bob)
p - Plasmoid address
v1 - value of Alice's tokens
v2 - value of Bob's tokens
vp - value of pledged YODAs

Fig. 3.1. Secure exchange of ERC20 tokens on Ethereum, step 1

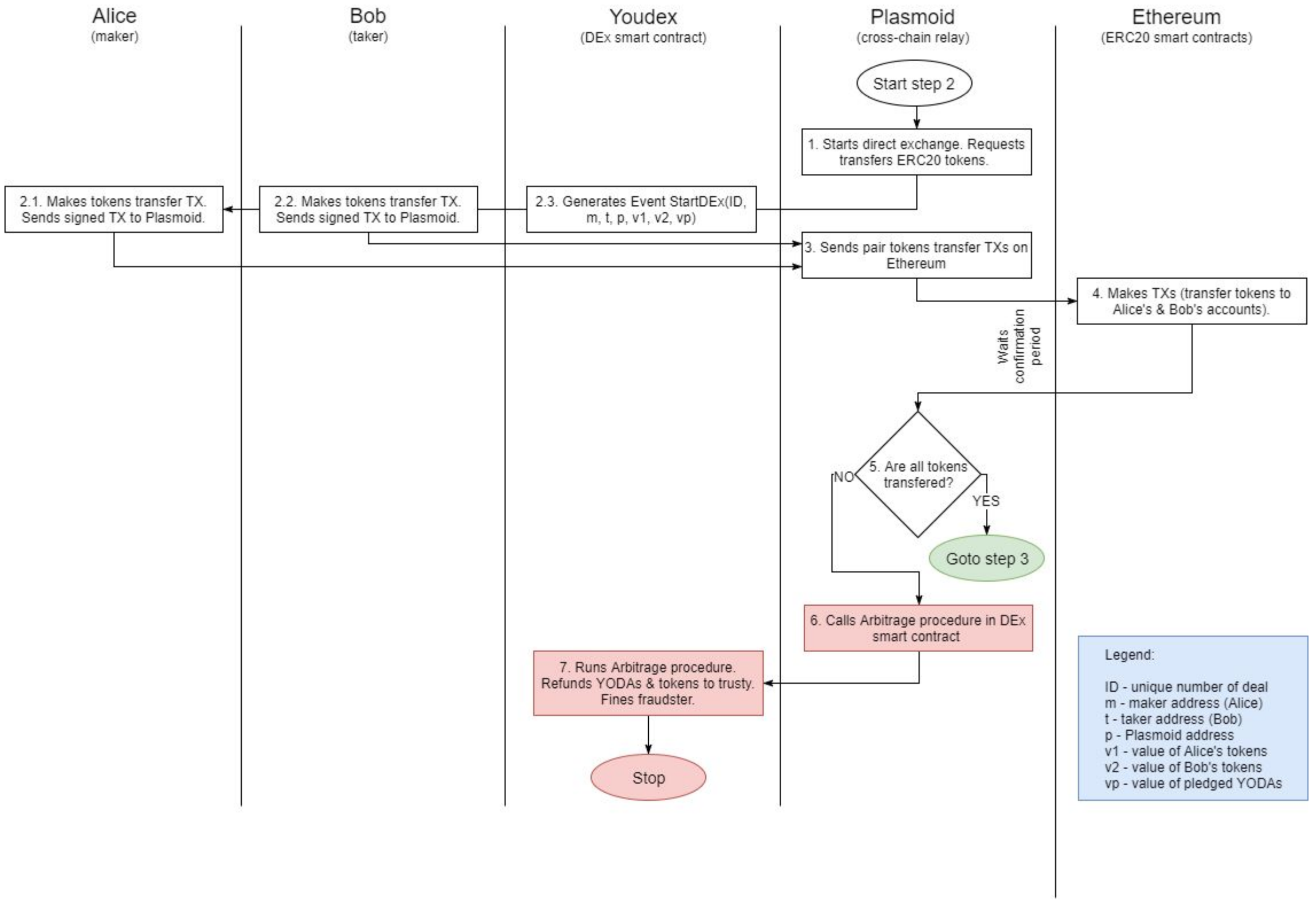

Alice
(maker)
Bob
(taker)
Youdex
(DEx smart contract)
Plasmoid
(cross-chain relay)
Ethereum
(ERC20 smart contracts)
Start step 2
1. Starts direct exchange. Requests transfers ERC20 tokens.
2.1. Makes tokens transfer TX. Sends signed TX to Plasmoid.
2.2. Makes tokens transfer TX. Sends signed TX to Plasmoid.
2.3. Generates Event StartDEx(ID, m, t, p, v1, v2, vp)
3. Sends pair tokens transfer TXs on Ethereum
4. Makes TXs (transfer tokens to Alice's & Bob's accounts).
Waits confirmation period
5. Are all tokens transfered?
NO
YES
Goto step 3
6. Calls Arbitrage procedure in DEx smart contract
7. Runs Arbitrage procedure. Refunds YODAs & tokens to trusty. Fines fraudster.
Stop
Legend:
ID - unique number of deal
m - maker address (Alice)
t - taker address (Bob)
p - Plasmoid address
v1 - value of Alice's tokens
v2 - value of Bob's tokens
vp - value of pledged YODAs

Fig. 3.2. Secure exchange of ERC20 tokens on Ethereum, step 2

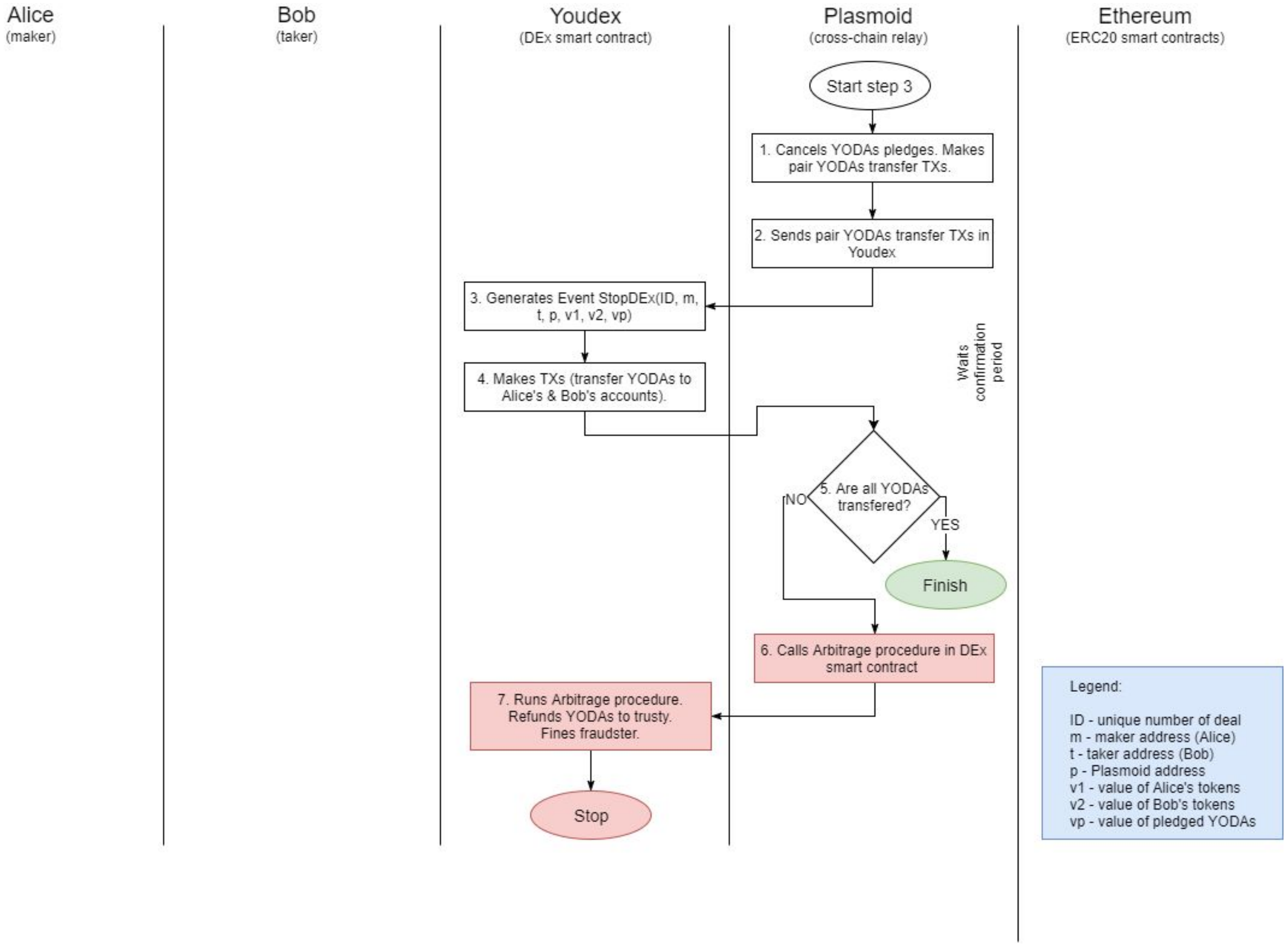

Alice
(maker)
Bob
(taker)
Youdex
(DEx smart contract)
Plasmoid
(cross-chain relay)
Ethereum
(ERC20 smart contracts)
Start step 3
1. Cancels YODAs pledges. Makes pair YODAs transfer TXs.
2. Sends pair YODAs transfer TXs in Youdex
3. Generates Event StopDEx(ID, m, t, p, v1, v2, vp)
4. Makes TXs (transfer YODAs to Alice's & Bob's accounts).
Waits confirmation period
5. Are all YODAs transfered?
NO
YES
Finish
6. Calls Arbitrage procedure in DEx smart contract
7. Runs Arbitrage procedure. Refunds YODAs to trusty. Fines fraudster.
Stop
Legend:
ID - unique number of deal
m - maker address (Alice)
t - taker address (Bob)
p - Plasmoid address
v1 - value of Alice's tokens
v2 - value of Bob's tokens
vp - value of pledged YODAs

Fig. 3.3. Secure exchange of ERC20 tokens on Ethereum, step 3

The protocol is synchronous. First, the pledge is formed though transactions on the sidechain. Then, the exchange takes place via transactions on the main blockchain. Afterwards, the pledged deposit is withdrawn via transactions on the sidechain. Simultaneous transactions on the blockchain and sidechain are forbidden.

Thus, at the core of the CDX protocol are:

- blockchain Ethereum;
- sidechain Youdex;
- smart contracts: YODA (ERC20 token), Teleport, DEx smart contract;
- Plasmoid crosschain oracle.

The basic CDX protocol implementation also provides a secure direct exchange of ERC20 to ETH on Ethereum. Plasmoid uses another script - DexT-ETH, which differs from the DexT script, mentioned previously. The rest of the functionality and logic is similar to the previous algorithm with pledges. The only difference is that instead of a single call to the smart contract transfer function, a signed ETH transfer transaction is broadcasted to Ethereum.

5. Cryptocurrencies Secure Exchange Algorithm

The difference between coins and tokens can be found here

In case of cryptocurrencies crosschain direct exchange, CDX basic implementation for ERC20 tokens should be supplemented by cryptocurrency connectors. Connectors are the extension modules for Plasmoids. Their purpose is to ensure the cryptocurrency's native blockchain support.

The cryptocurrencies exchange itself is managed by Plasmoid (crosschain oracle) and DExC script (decentralized exchange of cryptocurrency coins - modified version of DExT). This coins exchange algorithm is similar to the algorithm of secure ERC20 tokens exchange, mentioned in part 4. The first and third steps are identical to those described earlier (step 1 and step 3 - formation and cancellation of pledges). The difference is in the second step (step 2 - the execution of transactions in the blockchains). Fig. 2 illustrates DExC algorithm in case of BTC-ETH exchange .

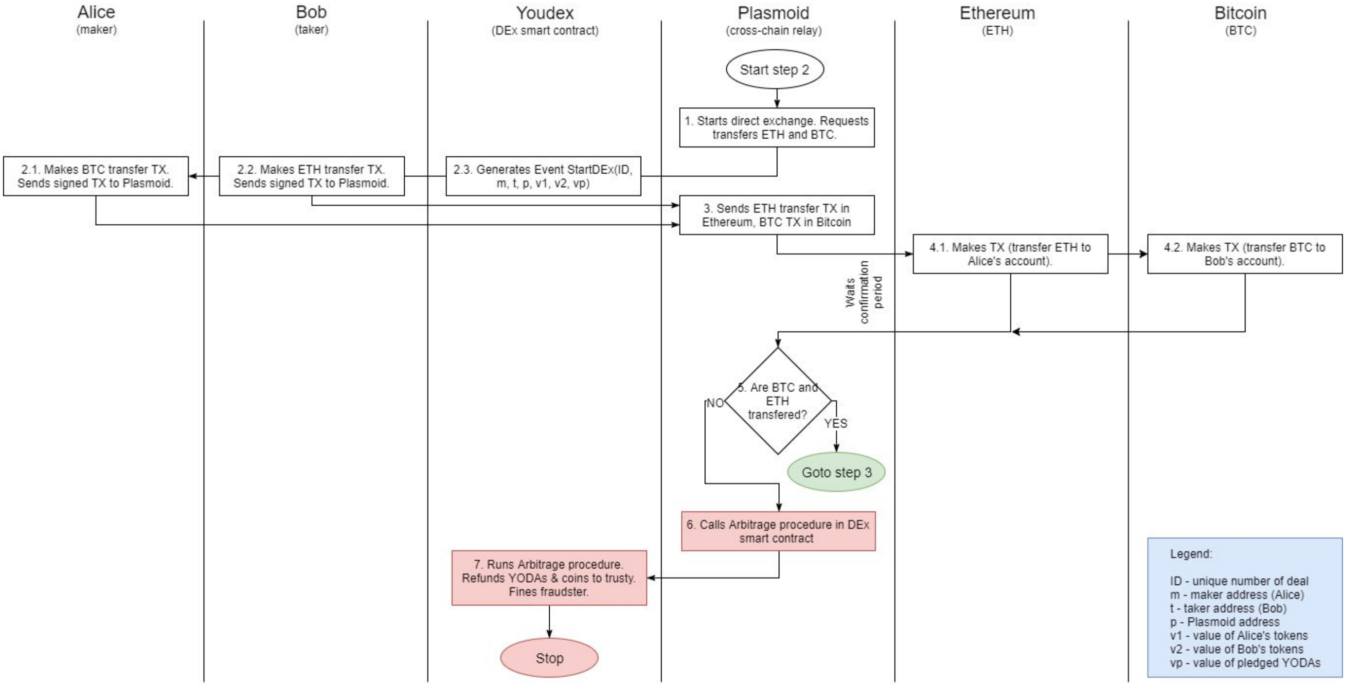

Alice
(maker)
Bob
(taker)
Youdex
(DEx smart contract)
Plasmoid
(cross-chain relay)
Ethereum
(ETH)
Bitcoin
(BTC)
Start step 2
1. Starts direct exchange. Requests transfers ETH and BTC.
2.1. Makes BTC transfer TX. Sends signed TX to Plasmoid.
2.2. Makes ETH transfer TX. Sends signed TX to Plasmoid.
2.3. Generates Event StartDEx(ID, m, t, p, v1, v2, vp)
3. Sends ETH transfer TX in Ethereum, BTC TX in Bitcoin
4.1. Makes TX (transfer ETH to Alice's account).
4.2. Makes TX (transfer BTC to Bob's account).
Waits confirmation period
5. Are BTC and ETH transfered?
NO
YES
Goto step 3
6. Calls Arbitrage procedure in DEx smart contract
7. Runs Arbitrage procedure. Refunds YODAs & coins to trusty. Fines fraudster.
Stop
Legend:
ID - unique number of deal
m - maker address (Alice)
t - taker address (Bob)
p - Plasmoid address
v1 - value of Alice's tokens
v2 - value of Bob's tokens
vp - value of pledged YODAs

Fig. 4. Secure exchange of BTC/ETH, step2

6. Security concerns

CDX protocol requires two transactions, one in each exchange direction, secured by the pledge. This should minimise transaction time and fee while ensuring security at the same time.

In rare occurrences, the exchange of coins and tokens may be interrupted (accidentally or intentionally) in such a way that one of the parties will suffer damage. DEx smart contract maintains an exchange log. The protocol is designed with arbitration functionality that voluntarily adjusts balance sheets of the parties. Balances will be automatically adjusted in YODA coins equivalent at the expense of pledges in the case the consent is not achieved.

In the case of probable incidents, it is always possible to trace back the teleporting process. This will help restore the correct course of operations should there be any deviation from the norm.

Another part of secure cross-chain communication is Plasmoid cross-chain oracle controlled by smart contracts. Plasmoid is authorized to operate only with a sufficient number of YODA tokens hold on the account.

At the network level security is dealt with by the Youdex consensus algorithm.

7. References

[1] https://github.com/YouDex/cdx/blob/master/TWIN_ACCOUNTS.pdf

[2] http://plasma.io/

[3] http://btcrelay.org/

[4] http://www.oraclize.it/

[5] https://interledger.org/

[6] https://0xproject.com/

[7] https://dydx.exchange

Tags:

atomic swap, blockchain, dex, decentralised exchange, smart contract, Ethereum, Bitcoin, crosschain, sidechain, youdex, yoda coin, cryptocurrency, crypto, ico, token, investment, trading, dapp, forex, crowdfunding, token sale, token, bitfinex, poloniex, kraken, kucoin,
binance, fiat, fiat gateway, forex, USDT, OpenUSD, Bitshares, Rudex, etherdelta, Litecoin, Ripple, IOTA, ZEC, Zcash, bitcoin cash, monero, Ethereum Classic, Telegram Open Network, OmisGO, XRP, XMR, OMG, ETC, NEO, BTC, LTC, TON, TRON, to the moon, dump and pump, tradingview, order, deposit, withdraw, liquidity, secure, mining, miner, hedge fund, bitcointalk, twin accounts

Authors

Oleg Tomin, MSc Physics, MBA

Programmer, smart contract developer, innovator. Founder and creator of CityChain - corporate and government voting blockchain for municipal initiatives. The designer of Coin Direct Exchange Protocol. Lecturer on the blockchain.

Sergei Smalkov, MSc Mathematics, MSc CS & Information Security

Expert on information security, compliance, networks, product development, agile and customer development practitioner. Managed and designed distributed facility management system for the largest bank in Russia. Project manager, developer of prototypes.

Viktor Glukhikh, MSc Computer Science, MBA

Serial entrepreneur and CEO in the fields of systems software development and IoT for financial and aviation industries. The designer of mathematical crypto investment models, portfolio and risk management strategies.

Project Youdex.io - Decentralised Crypto Investment Platform

Truly decentralised exchange with volume, multi-currency wallet, portfolio management, trading bots, hedge fund and more.