Metro: A peer-to-peer cross-chain digital asset exchange

©Metro.software 2018
metrosoftware@zoho.com

Abstract

The pegged sidechain technology allows us to safely move assets from the asset mainchain to the side chain. The application of this concept for several main chains and one common side chain makes it possible to create a blockchain for circulating tokens from different blockchains. This allows us the implementation of a decentralized exchange for assets issued on blockchains that make possible the implementation of pegged sidechains. In particular, such chains are any POW chains with Turing-complete smart contracts. In the original article on which our work relies, this technology is being developed for Bitcoin but at this moment not included into the consensus, but we hope it will be.

Introduction

Bitcoin and other cryptocurrencies that followed solved third party problem for payments and store of value. They allow any two willing parties to transact directly with each other without the need for a trusted third party (intermediary). The solution turned out to be so remarkable that it gave birth to a new economic entity – decentralized corporations. Each cryptocurrency is a measure of value of its decentralized corporation.

And now we have the new third party problem. We do not have a convenient way to move a value from one decentralized corporation to another without the involvement of a third party – centralized cryptocurrency exchanges.

Trustless cross-chain trading known as atomic swap is first step to solve this problem. However it has two disadvantages: first, that it's rather slow; second, that trading can be canceled by either of the parties in the process of execution after the parties came to an agreement.

We need a cross-chain exchange that provides a user experience not inferior to the centralized exchanges.

Two-side pegged chains

Our work is based on the concept of Pegged Sidechains [2] introduced by Blockstream team. Sidechain concept is based on a special smart contract which allows to transfer any main chain asset to side chain and back.

> DEFINITION We call it cross-chain transfer smart contract or just *transfer contract*.

When somebody sends asset tokens to cross-chain transfer smart contract, it locks them, and unlocks the same quantity of pegged asset on the side chain after a while. And the same behavior applies to transfers in the opposite direction.

In terms of original article, implementing a chain as a side chain to several main chains allows us to have pegged assets from different chains on it.

> DEFINITION We call such multi-peg side chain a *ledger chain*, and asset main chain we call an *asset chain*.

On-chain exchange

There are a lot of successful implementations of on-chain exchanges. Unfortunately they give us ability only trade assets issued on the same chain or promissory notes of the issued on other chains asset secured by third parties.

Combining the on-chain exchange with the ledger chain for multiple asset chains, we get a decentralized cross-chain exchange.

Transferring an asset from an asset chain to the ledger chain is like exchange deposit and transferring an asset from the ledger chain to an asset chain is like exchange withdrawal.

Fast blocks give user near real time trading experience. Blockchain developed precisely and exclusively for on-chain trading allows to do it with fewer computational costs than general purpose blockchains with Turing-complete scripting.

Proof-of-Work and Proof-of-Stake hybrid consensus

There are two main types of consensus at the moment.

In Proof-of-Stake (POS) blockchains users’ right to release a new block is proportional to their holding stake and doesn't require any spending of resources. Releasing a block that does not fall into a main chain doesn't lead to any material loss whereas in Proof-of-Work (POW) blockchains users’ right to release new block is proportional to their computing power and involves electricity costs and opportunity costs of engaging the equipment. Releasing a block that does not fall into the main chain leads to a material loss. Therefore the support of the both chains in case of a chain split is economically unprofitable for POW blockchains. Support of multiple chains requires to divide the computing power and when one of the chains is discarded causes a material loss. However maintaining both chains may be profitable for POS. In the case of a chain split, the stake remains unchanged in each chain, and nothing hinders the support of several chains.

So, POS blockchain reorganization does not damage the producers of the blocks. Also, in POS everybody knows who produces the next block. Thus, POS blockchain can afford more frequent blocks.

On the other hand, Proof-of-Work has one advantage over the Proof-of-Stake — there is no need of additional data to check an eligibility of a block release and determine longest chain from outside of the blockchain. To do the same for Proof-of-Stake we need to know a lot of additional data: at least stake holders balances.

Using a hybrid consensus allows us to combine the pros of both approaches: frequent blocks for the on-chain exchange trading and strictly determined state of the system for the transfer contract.

> DEFINITION *Key block* is a block that conforms to POW consensus and *fast block* conforms to POS.

Frequency of fast block occurrence is once every 3 seconds and for key block — every 10 minutes. So we have about 200 fast blocks *cluster* for every key block.

For POW retarget we used modified dark gravity wave algorithm. The only change is using 12 blocks for calculation instead of 24.

Mining and circulation supply

Each key block creates new coin owned by the miner (creator of the block). This gives us an additional way to initially distribute coins into circulation. Miner's block reward starts from 2,000 MTR and decreases by half every 200,000 emission blocks. Each block reward halving period takes approximately 3 years and 10 months. Emission ends in 35 emission periods and miners get total of 800,000,000 MTR. During first emission period miners get 400,000,000 MTR. Also 200,000,000 initially distributed MTR coins will be unlocked during first emission period (1,000 MTR each emission block). Thus only 1,000,000,000 Metro tokens will be issued. Developers will get 100,000,000 initially distributed Metro tokens and another 100,000,000 will be received by NXT community.

Transmitting hubs

There are special nodes called transmitting hubs whose purpose is to increase the speed of the block propagation through the peer-to-peer network. Transmitting hubs are financially interested in blocks rapid delivery through the network. Block producers send their produced blocks to transmitting hubs. Hubs deliver blocks to their subscribers (users who voted for it) and other peers.

Users vote for the best latency transmitting hubs. Ten hubs with the maximum stake of votes receive a reward – forging power increase by 10% until the next voting round.

Voting period starts each 200,000 blocks and lasts for 20,000 blocks. The number of votes that an account owner can give to a transmitting hub is equal to its balance divided by 10,000 MTR. Thus, accounts with a balance below 10,000 MTR do not participate in the voting. One can give the full volume of votes for each of at most 5 hubs. After voting ends, the best transit nodes obtain a reward. A hub gives to its subscribers the priority right to use the service. The ability to prove the vote for a hub without disclosing voting account is implemented using shuffling technology for hub virtual tokens.

A vote cast for a hub is rewarded by points assigned to user, indicating a secondary account to which priority right will be given. By signing the request with the key of this account, the node identifies itself as a subscriber. In case of a DDoS attack this will allow the hub to process requests from its subscribers separately from anonymous requests. In each round of voting, and for each hub a unique secondary account is used. This avoids exposing the connection between the main account and user's IP address. In the first implementation service does not depend on whether the user gave vote for this node or not. The first implementation is done on the basis of voting system only, in the second implementation the ability to prove a vote for a hub is added.

Forging

The forging power (a right to issue fast blocks) is proportional to the forger's stake. The forging power of each participant is determined by the balance that has not moved anywhere between the last 30 *clusters*.

> DEFINITION balance that has not moved anywhere between the last 30 *clusters we call effective balance* .

The implementation is based on the blind shooting algorithm. The difference from the standard implementation is that each key block changes the deterministic sequence of block generators. The forger receives the commission of transactions included in the issued block.

Supplying

The possibility of a cross-chain exchange is based on the ability to establish the truth about the state of one blockchain within the context of another one. *Suppliers* are engaged in the synchronization of blockchains by the supply of provable data. Suppliers ensure the integrity of the multi-blockchain system and therefore receive the most of the collected trading fee as a reward.

Supplying from asset chains

Due to the Proof-of-Work, when we receive the translation of the block from the asset chain, we can easily verify that the necessary work has been performed and so be protected against spurious asset chain data. The supplier inserts the broadcast into the special non-transactional area of the fast block. In case of insertion of incorrect (in terms of POW) data, it should be discarded by the rules of consensus, and it’s supplier loses the block reward. The amount of reward is determined at the time of the supply, but is credited after the required confirmation period dictated by asset chain POW. This is done in order not to reward the barren (obsolete, orphan) block broadcasts.

DEFINITION Supplying from asset chains into Metro is done by *inward suppliers*.

Supplying into asset chains

To avoid barren Metro blocks supplying into asset chains, suppliers need to wait until Metro key block receives 6 Proof-of-Work confirmations. The fact of supplying blocks into the asset chain becomes known in the Metro chain at the time of the reverse supplying and can be validated taking into account the asset chain confirmation requirements.

To supply blocks into the asset chain, it becomes necessary to pay the outside fee and there is a risk that the supplier reward will not be sufficient to offset it. A sign of this is that, prior to the release of the next key block, none of the suppliers did not supply the previous one. Thus, if simultaneous translation of several key blocks occurs, this is an occasion to increase the reward. And the more blocks are simultaneously translated the more reward needs to be increased.

So, when the ratio of the Metro key blocks frequency to the asset chain blocks is equal to r, in case of the i blocks are transferred, the following share is withheld from the inward suppliers in favor of the outward suppliers

$k_i=2^{i-1}/(2^{i-1}+r)$.

This formula provides the same reward in normal case and provides the doubling of the reward for each additional block in the translation.

DEFINITION Supplying from Metro to asset chains is done by *outward suppliers*.

Binding asset chains

Placing data from the asset chain into the key block of the Metro chain, for example, as a special transaction, will allow binding of the asset chains to each other. The Merkle root that includes this transaction id will fall into all the asset chains, and the availability of translation will be provable. This does not require additional overheads other than the standard transaction fee, to stimulate miners to include the transaction in the block. As mentioned in “Supplying from asset chains”, the data are held in a non-transactional area, and can be referenced from key block transaction of a special type. The unit that holds one external block is called Envelope, and we can place Envelope hash into that transaction. Depending on asset chain, Envelope can contain additional commitments not included in the block header of the asset, so Envelope hash can be thought as a Merkle root of the tree containing external block hash plus those commitments.

So for example when we add Ethereum and Ethereum Classic to the Metro exchange, we obtain relay between them out of the box.

Trading

In order to guarantee the usual user experience the trading experience on the Metro subway system will be similar to the one on centralized exchanges as much as possible. First of all, this concerns the ability to set and cancel orders for free.

To protect from spam, we set limits on such actions depending on the size of the stake. The estimated capacity of the Metro blockchain is 7,344,000 transactions per day. And accordingly, the calculation formula for the number of free trading transactions per day N is given by formula:

$N = a * 0.007344 / p$

where a is the number of MTR coins belonging to user and p is the share of coins in circulation from the maximum number of coins (1,000,000,000). For example, in 2 years after the start of the blockchain, only 30% of the coins from the maximum supply will be in circulation. A user with 10,000 MTR will be able to make 244 trade transactions per day for free.

Free transaction rights can also be an asset and can be traded.

The trading fee for a fulfilled order will initially be set at 0.1%, which corresponds to fees on centralized exchanges. In the future, this number will probably be reduced if the stake holders come to such decision.

Currency integration smart contracts

Deposit and withdrawal are implemented in a smart contract which eliminates the possibility of double spending during these processes.

To transfer asset chain coins into ledger chain asset, the asset chain coins are sent to a special address (transfer contract) on the asset chain where they can only be unlocked afterwards by offering proof of possession on the ledger chain.

Pegged assets on the ledger chain represent coins locked on an asset chain. So long as a coin is locked on the asset chain, the same amount of pegged asset can be freely transferred and traded within the ledger chain without further interaction with it’s parent chain.

When users want to transfer coins from the ledger chain back to the asset chain, they send the pegged asset to special address on the ledger chain, produce a sufficient proof that this was done, and use the proof to unlock a number of previously-locked coins with equal denomination on the asset chain.

To ensure the operation of smart contracts, the following actions are performed.

Suppliers pass the headers of key blocks to the smart contract on the asset chain. The data is transmitted to asset chain after a confirmation period has elapsed. For Metro chain we set the confirmation period to 6 key blocks. Confirmation period ensures that the regular reorganizations of the ledger chain have already passed.

In order to avoid the situation when several suppliers incur expenses for the supply of data to the asset chain, the supplier order is deterministic. The right to supply the block is given to the forgers who released the fast blocks early in cluster.

The first one can do it right after the confirmation. The second – one minute after the 6th confirmation. The third – in 2 minutes, etc. So, if the first forger skips his turn, the second one can supply the data etc. A confirmation that the data was transmitted not earlier than the supplier had such right is the transaction timestamp in the asset chain. If the supplier violated the supply rules, it will not be rewarded by Metro consensus.

In case that a block already has 7 confirmations, and it has not been passed to the asset chain, the right of delivery is carried on to the next cluster. In this case the forger is obliged to transfer both blocks and is entitled to a double reward, according to the formula described above.

Data from the asset chain is also delivered after the confirmation period specific for asset chain (for example for Ethereum Classic we plan setting it to 20 blocks).

Thus, in the ledger chain, we will know that the data is delivered to the asset chain after some time (about 5 minutes for ETC).

Compensation of suppliers is determined precisely at this moment. And after the maturation period, which lasts for 10 key blocks, supplier can dispose of their reward.

Smart contract is verifying supplied data to meet POW rules. Namely, the target value and the hash of the data is matched with the target.

We plan to add integration with the Ethereum Classic first. So we'll describe how its transfer contract works.

Deposit

To make deposit, user sends coins to the transfer contract and passes the address in the ledger chain to which the corresponding amount of the asset should be credited.

After the confirmation period (20 asset chain blocks, 5 minutes), the block header in which the state of the transfer contract was changed will be delivered to the ledger chain. There is a *contesting period* (20 key blocks, 200 minutes) after this. This time is given for the alternative data supply in case the data with the deposit were falsified. In order for asset POW to be able to falsify the data attackers need to mine alternative chain. So, attack will cost to them something. Even if they have such a resource, they can prefer to just simply make double spend (51%) attack on asset chain instead of attacking us.

After that, on the ledger chain, depositor needs to make a deposit request, which includes a deposit transaction on the asset chain, with a Merkle tree path confirming that the transaction is included in one of the asset chain blocks delivered to the main chain. Or we can use state root instead of transaction root. It depends on which approach will require less bytes.

The result is the transfer of the deposit to the address specified in the deposit transaction.

Withdrawal

To withdraw coins a withdrawal transaction is created in the ledger chain. The required amount of assets is taken away from the depositor account.

After the confirmation period, the block header with the withdrawal will be delivered to the smart contract on the asset chain (6 key blocks, 60 minutes). There is a contesting period (200 asset chain blocks, 50 minutes) after this. This time is given for the supply of alternative data in case the data containing the withdrawal tx were falsified. Due to POW, to be able to falsify the data, attackers need to mine alternative blocks. So, the attack will cost to them something. Due to hybrid consensus, correct chain is not only protected by computing power but also by a stake. So, for example, if attacker has only 10% of active stake he, needs to have 91% of Metro network hash rate.

After the contesting period, a proof of the withdrawal should be provided to *transfer contract* on the asset chain. It includes transaction on the asset chain and Merkle tree path confirming that the transaction is included in one of the ledger chain blocks which transfer contract knows about.

The result is a transfer to the address specified in the withdrawal transaction.

Chain length and stake protection

Every blockchain consensus has rules on how to determine which chain should be chosen in case of a split. In our case chain with a greater cumulative difficulty is considered correct. Cumulative difficulty is calculated as the sum of the difficulties of clusters. The cluster is the key block and the subsequent fast blocks until the next key block. On average, the cluster consists of a key block and 200 fast blocks. The complexity of the cluster is calculated as the square root of the product of the normalized work target of the key block and the normalized sum of the stake base target of the fast cluster blocks.

$CD = \Sigma\ (wt * \Sigma\ st)^{1/2}$

By attaching the block to the chain its author confirms chosen chain with either the computing power of the block, or with it’s stake.

For the key block production, computing power is required. The validity of the key block production is easily verified. To determine the validity of the fast block production, you need to know the stakes distribution.

The suppliers send the headers of the key blocks to the transfer contract in the asset chain, which contains, among other things, forger Merkle root, which makes forgers’ balances provable to transfer contract and give us the upper estimate of the forger power with which an attack would be executed.

Processing all of the fast blocks outside the ledger chain would cost a lot. So to establish the right Metro chain outside of the ledger chain (in the transfer contract on the asset chains) a simplified mechanism is used. Key blocks contain vote-transactions of active forgers confirming their participation in this chain. Transfer contract receives metro block with the transactions Merkle root, so these votes are provable on the asset chains. Having an upper estimate for the forging power, this allows us to apply the stake protection of the correct chain without having to know about each fast block.

Withdrawal fee

Deposit is done as a regular transaction on an asset chain. All costs for the data supply to the ledger chain are taken over by the ledger chain itself. Therefore, there are no issues with deposit costs.

To make withdrawal, we must supply the data to the asset chain and for many assets this will incur a cost. To compensate these costs to those who bear them, a withdrawal fee is established.

We calculate the average cost of the block supply during the last 100 blocks. This value is multiplied by 0.8 and divided by the number of withdrawals in these blocks. And then rounded up to one significant decimal digit. The amount is taken less than the cost of supply, so that suppliers would have the motive to save on asset network transaction fee. Withdrawal fee can not exceed the cost of delivery of 10 blocks, even if during them there was no withdrawal.

Withdrawal fee goes to either the miner who included it in block or the supplier who place this block into the asset chain. It goes to the miner if the last 3 bits of the transaction id coincide with the last 3 bits of the hash of the mined block (probability of 1/8) otherwise it goes to the supplier.

Thus, when the reward for the block during reward halving process falls below 1/8 of the withdrawal fee, miners will possibly start to mine trying to pick it up for themselves and before it's not profitable and process will be random.

Atomic swap

Atomic swap [2] is a technique for exchanging assets with accounts kept on different chains without the need for trust. Two counter transactions are created each on it’s own chain, and either they are both executed or both remain un-executed. Using it for coins/tokens on an external chain and assets issued to represent them on the ledger chain, we can create an alternative approach to deposit and withdrawal without the need for waiting considerable time for key block confirmations.

With intent to withdraw or to deposit an asset, the user creates a swap request or seeks a counter request. The desired amount of the requests may differ, exactly like with exchange orders. So we have a market for atomic swaps with order matching. When a depositor and withdrawer find each other, the atomic swap takes place between them and each side gets the desired assets.

Atomic swaps allow to apply market price formation to withdrawal fee. In the case of an initially overstated fee, only large amounts would be drawn through the withdrawal mechanism. A small profit for the withdrawal of small amounts through atomic swap will be collected by professional swappers, who would accumulate the asset, periodically make one major withdrawal and pay a withdrawal fee from their profits.

In addition, when the atomic swap market is formed, it will speed up the deposit and withdrawal since users indicate the number of confirmations sufficient for them rather than wait for the number required by the consensus.

Conclusion

Centralized exchanges are points of failure in the cryptoeconomy ecosystem. They may limit the exchange of certain cryptocurrencies under the pressure of the regulator. They can become a source of de-anonymization of cryptocurrency users because they are obliged to follow the "Know your customer" (KYC) and "Anti- money laundering" (AML) regulations. They can be (and have repeatedly been) a source of financial losses to cryptocurrency users due to hacker attacks and dishonesty of the owners.

We believe that the application of the principles outlined in this paper for the implementation of a decentralized exchange will help to begin moving towards eliminating these risks.

References

[1] Enabling Blockchain Innovations with Pegged Sidechains - https://blockstream.com/sidechains.pdf

[2] Alt chains and atomic transfers - https://bitcointalk.org/index.php?topic=193281