Draft: version 0.1, last update 04.03.2016
thread on forum: https://bitsharestalk.org/index.php/topic,21763.0.html



“Blockchain as a Wallet” approach as a way to convert Bitshares into a sidechain of Bitcoin

Krzysztof Szumny - noisy, noisy.pl@gmail.com

Abstract

The goal of connecting Bitshares and Bitcoin networks using sidechain is to provide a possibility of trading real Bitcoins on decentralize exchange in a trustless manner. User should be able to keep his private keys to Bitcoins during all that time and at the same time Bitshares network should allow trading that bitcoins in a Bitshares network thanks to bitcoin multisig feature.

1. Motivation

There are already proposed designs of sidechaing Bitshares and Bitcoin networks. Most of them proposed that Bitshares blockchain will have special Bitcoin account, which will be guarded by all witnesses of the Bitshares network and will be like a vault. Bitcoins on that account could be then used as a 100% collateral, which will allow creating a speciall kind of asset, like bitBTC. This aproach creates a single account potentially with large ammount of Bitcoins on it. This is an incentive for adversaries. This may couse that wittnesses which suposed to guards the netowrk may want to collude to take an advantage of being in control. Of course Bitcoins can be stored on multiple accounts instead of one, but this introduce a new problems of managing those accounts and transfering Bitcoins among them to give a possiblity to withdraw large amount of Bitcoins. Besides, how to judge which number of vault accounts is appropritate? The solution for all mentioned problems can be provided by using a seperate Bitcoin accounts build on multisig addresses for each user and giving half of the control of that accounts to Bitshares network.

2. "Blockchain as a Wallet"

With a BaaW aproach, user wanting to transfer Bitcoins to Bitshares sidechain, use special Bitshares client for that, which is responsible for generating new Bitcoin 2 of 2 multisig address. Bitshares client

in order to do that use a public key provided by user. Users private key from that point will be used to authorized all transactions from this account. Second pair of keys is generated by random wittness, and distribiuted among all wittnesses of the network. From that point any witness is able to authorize transaction initialized and already signed by user during block creation. Generated address which is under control of user and Bitshares thanks to 2 of 2 multisig, will be called here “BitcoinBitshares addres” or BBaddress.

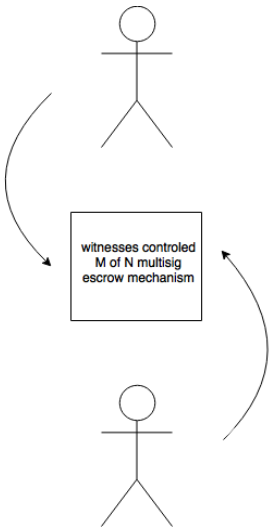
To have a fully functional sidechain with decentralize exchange, new token in Bitshares network need to be introduced - “Mirrored Bitcoin” or MBitcoins. MBitcoins are issued by the Bitshares network when transfer to BBaddress is detected. To have a possibility of doing that, wittnesses have to run full nodes of Bitcoin network. When users transfer funds from BBaddress back to Bitcoin network, proper amount of MBitcoins is burned.

The need for existance of MBitcoins stands from long confirmation time in Bitcoin network. Without additionall token, user would be forced to wait on average 10 minutes to get a confirmation of order execution on decentralize exchange. To have a possibility of fast order execution on the exchange, all operations are performed on MBitcoins.

3. The exchange of assets

In order to execute the exchange order quickly, the operation is performed on MBitcoins. To keep consistency between amount of MBitcoins and Bitcoins assigned to a user, synchronization needs to be made. When MBitcoins transactions is initialized, at the same time the same amout of Bitcoins is transfered. Because in Bitshares network confirmation time is quick, exchange relay on state of MBitcoins tokens. From user point of view, order execution can be marked as finished even before mathing transaction in Bitcoin network will get first confirmation.

Of course, there is a possibility that in Bitcoin network transaction will be rejected, for example becuse of double-spend atack performed by dishonest witness. That means, that Bitshares network need to have a way of reverting ~~transaction~~ initiatialized but not fully finished order, to perform a chargeback. Bitshares network to have a way of doing that and not lose money, actually need to lock those funds. Bitcoins are locked only during performing an exchange by an escrow mechanism.



Escrows do not release funds until it gets confirmation from Bitcoin network, that transaction in fact took place. In the mean time user which bought Bitcoins already see MBitcoins on account, but with “unconfirmed” status.

Escrow mechanism should be implemented with M of N multisig address controlled by witnesses. Releasing funds from escrow should require consensus of all witnesses.

4. Withdrawl

User should not be able withdraw any Bitcoins from BBaddress until MBitcoins and Bitcoins will not be confirmed.

5. Double spending by a wittness

Dishonest witness can deposit funds on BBaddress by prodiving own public key. Because he is a witness, he has also an access to second pair of keys used to create 2 of 2 multisig BBaddress. Having two pairs of keys, witness can try at the same time use matching MBitcoins to buy some assets on exchange and withdraw real Bitcoins with other Bitcoin wallet which has support for multisig. However because all transaction on the exchange are performed with support of escrow mechanism, dishonest witness will not be able to recive bought assets, because escrow mechanism will never recive a confirmation from Bitoin network. In that case MBitcoins which do not have collateral any more, are burned thanks to consensus of the network.

6. Reverting executed order

If during waiting for confirmation by escrow mechanism violation of equal state of MBitcoin and Bitcoin

account will be detected, order on exchange need to be reverted. User should be then informed that Bitshares network detected abuse attempt which was prevent from happening and asked whether his order should be placed on order book one more time or canceled.

7. Multi-currency Wallet

Based on BaaW, decentralized multi-currency wallet can be implemented. The only requirment for integraiting new coin would be a support for multisignature feature.

8. Known drawbacks

Each transaction on the exchange will require covering a Bitcoin Transaction Fee

9. Disclaimer

Term like MBitcoin do not have to be shown to user anywhere. It is just a term needed to distinguish actual Bitcoin from assumption made by Bitshares network.