Draft

Proposed solution for trustless exchange of BTC -> BTSX by Emil Velichkov (http://lnkd.in/nPbhxG).

Immagine we have an investor Richy who holds BTC and BTSX. Richy wants to exchange some of his BTC for BTSX.

Summary

Provided the following proposal is implemented Richy will be able to buy BTSX with BTC using both (BTC and BTSX) blockchains. The proposal describes how a BTSX holder Mike could ask to sell some of his BTSX for BTC. Mike's ask order includes Mike's own BTC address, BTC->BTSX exchange ratio and sufficient amount (in BTSX) that become unspendable. Mike's offer is expressed on BTSX blockchain similar to current bitBTC ask. Richy on the other hand creates a bid order that includes Richy's BTSX receive address, desired BTC->BTSX exchange ratio and optional BTSX collateral. Orders should be matched similarly to bitAssets. When matched Richy is responsible for sending the agreed amount of BTC to Mike's address in specified timeframe. [Optional]Otherwise Richy should lose the collateral.

Prerequisites

1. BTSX Delegates monitor the BTC blockchain for transactions with output to specified address
2. BTSX users should be able to post standing orders for BTSX->BTC exchange and vice versa. Orders should include BTC/BTSX address of owner, BTC->BTSX exchange ratio. [Optional]Sufficient collateral should be provided. All the funds used should become unspendable.

Basic Analysis Of Prerequisites

1. Requirement for BTSX Delegates to monitor the BTC blockchain would indeed impose more work on the delegates. However delegates could make the work required to verify BTSX block by other nodes easier by including some information directly into BTSX blockchain. For example: in order for each BTSX node to easily verify the confirmation of given BTC transaction (and with this the validity of BTSX block) the delegate could include the following information into BTSX blockchain:

    - BTC Block number
    - ~~BTC Block hash (optional)~~
    - BTC Transaction number (or any other means of identifying transaction)
    - BTSX transaction id that requires BTC blockchain monitoring

Given the above information any node could relatively easy verify the existence and confirmation of such transaction by requesting only the specified block number from BTC full node(s). Using the above-mentioned method should have only slightly higher requirements for BTSX nodes due to the need to verify BTC transactions on request.

2. There shouldn't be any technical obstacles in implementing this though it might require hard fork.

Process

1. Mike (or anyone else) should be able to post a standing ask order to exchange BTSX for BTC. It should contain:
   1.1 Mike's own BTC address (should be unique for each order)
   1.2 Desired BTC->BTSX ratio
   1.3 Desired amount of BTSX to exchange.
   1.4 [Optional] Required collateral in case of BTC holder failing to fulfil the deal
   ~~1.5 [Optional] Maximum amount of time (timeout) to wait for BTC holder to fulfil the deal~~
   Transactions not satisfying the above rules are invalid.
2. Richy (or anyone else) should be able to post a standing ask order to exchange BTC for BTSX. It should contain:
   2.1 Richy's own BTSX address (should be unique for each order)
   2.2 Desired BTC->BTSX ratio
   2.3 Desired amount of BTC to exchange
   2.4 [Optional] Amount of collateral.
   2.5 "Deadline Transaction" described by drltc in https://github.com/drltc/bitbond-proposal/blob/master/btc-trade.md#implementing-expiration-times
3. All standing orders described in 1 and 2 should be visible to anyone similar to current bitAsset orders.
4. Orders 2. and 3. are matched the same way currently bitAssets are matched. Note that optional collateral requirement should be taken into account when matching.
5. If a match occurs between Richy and Mike then Richy has to send to Mike's address the specified amount of BTC in the specified timout (1.5) otherwise he should lose the collateral pledged.
6. When Richy's transaction sending BTC to Mike is confirmed -> delegates should include the required information in the blockchain so other nodes can easily verify. And transfer required amount BTSX from Mike to Richy
7. If the "Deadline Transaction" is confirmed all of Mike's locked funds are instantly released and Richy's collateral is lost.
8. If the "Deadline Transaction" is rendered invalid (due to Richy's other transactions spending some of the same inputs) -> This is the same as Richy failing to fulfill the deal => Richy's collateral is lost.

Possible Issues
It is possible some BTC miners to try to take advantage of Richy's collateral refusing to include his transaction in the BTC blockchain. However he should include sufficient fee that will sweeten the transaction. It is possible for a large mining pool to offer large amounts of BTSX trying to harvest collateral. However biders and askers have plenty of freedom in choosing the desired deal parameters (collateral, timeout, ratio) and given the random nature of BTC blocks mined such scenario is unlikely and if it happen it is exactly what both parties agreed beforehand.

Another issue could be Richy not fulfilling his part of the deal. However that is what the collateral and timeout are for. You get what you ask for.

Other Solutions
Richy can always deposit BTC to an exchange such as BTER. However this requires trust in the exchange and limits the potential buyers to those using the same exchange.

Conclusion

Using the proposed method any user that has both BTSX and BTC should be able to buy BTSX paying in BTC. Furthermore this enables global crypto free market and cross-chain trading.

Draft
v0.0.2 - Added the concept of "deadline transaction"
v0.0.1 - Initial