

Saw this today by Dr Orlovsky: <https://github.com/dr-orlovsky/typhon-spec>

Basically, this paper describes sidechains on Bitcoin using any consensus scheme. In particular, this work may enable plasma sidechains with any consensus/fraudproofs etc residing on the Ethereum chain.

This idea is highly preliminary, but resolves many important requirements for trustless cross-chain trading.

Step 1: Side chain on BTC,

As described in link above. Holds BTC sidechain tokens (BTC-SC) analogous to those on ethereum (ETH-SC). Both have equal value. Some sidechain parameters need to be chosen carefully, in order to accomodate varying finality, block confirmation and congestion characteristics.

Step 2: Transfers between BTC-SC and ETH-SC tokens

State/fraud proofs/contracts mediating consensus can continue to operate on Eth chain. This implies nodes operate on both main chains.

Step 3: Add other btc/eth like coins:

The actual consensus and co-ordination chain can remain ethereum. There is probably a low upper limit on the coins that can be added since anything other than a solid coin will weaken the chain considerably. BTC and ETH should be sufficient. The other attractive features of other coins namely, speed and privacy can simply be added to the plasma chain.

Advantages:

1. A simpler alternative to: Cosmos, Polkadot and other cross-chain efforts.
2. Simpler way to add confidential/privacy features to legacy chains.
3. High speed alternative to atomic swaps as a way to perform trustless cross-chain trading, i.e. no escrows, channels or any other on-chain setup needed.
4. Only on-chain footprint is deposit/withdrawal from sidechain – similar cost to deposit/withdrawal from exchange.