Federated peg sidechain design notes

Entities:

- User
  - ➔ Has source of funds on main chain.
  - ➔ Has a target address they wish to receive funds in on side chain (‘deposit’ transaction).
  - ➔ Alternatively, has funds on the side chain that they wish to redeem for main chain funds (‘withdrawal’ transaction).

- Federation nodes (one or more)
  - ➔ Have custodial multisig address on main chain with locked funds.
  - ➔ Have custodial multisig address on side chain with locked funds.
  - ➔ Have individual private keys that collectively form the federation's multisignature address.
  - ➔ Monitor transactions occurring on the main chain.
  - ➔ Monitor transactions occurring on the side chain.

Processes:

- Each federation node independently detects 'deposit' transactions made on the main chain by a user
  - ➔ Blockstream paper relies on 'pay to contract' construct with homomorphic payment address.
    The intention of this is to make linkability of main chain transactions to side chain transactions more difficult (but it does not obscure amounts).
    For the initial deliverable we can use an OP_RETURN output in the deposit transaction to denote the side chain destination address.
  - ➔ Federation node detects deposit transaction based on destination address being the federation's main chain multisig.
  - ➔ Each federation node signs partial transaction transferring side chain custodial funds to the address encoded in the OP_RETURN.
  - ➔ Partial transactions are circulated between federation members so that a complete signed transaction can be formed.
    (See BIP 174 for transaction serialisation format - this can be used eventually).
    This aspect needs further design - it is inefficient having every federation node broadcast to every other federation node.
    Perhaps have a deterministically designated 'master' for each transfer attempt that receives and collates partial tx?
    If the master is not available or reneges within a predefined period, another node becomes the master.
  - ➔ The exact ‘exchange rate’ of main-to-side transactions is determined solely by the federation.

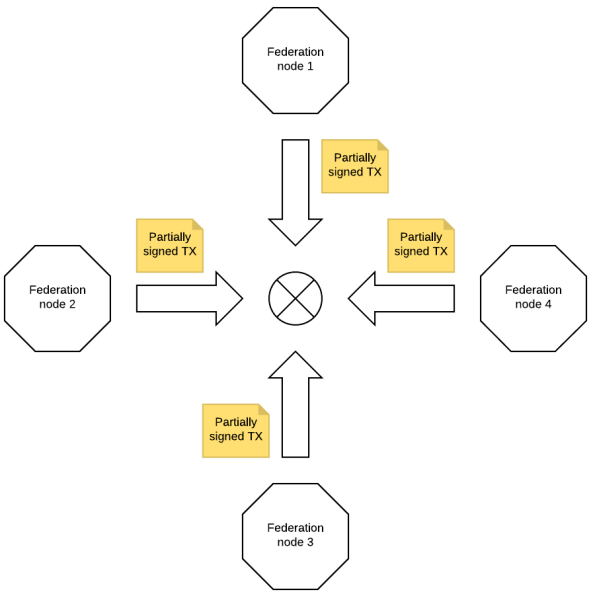

Figure 1 Aggregation of partial transactions by federation members

- Each federation node independently detects 'withdrawal' transactions made on the side chain by a user
  - ➔ This operation is essentially the inverse of the deposit transaction. Note also that the federation may elect to disallow withdrawals entirely at their own discretion. This could be the case where an ICO was used to raise funds on the main chain, and side chain coins are distributed to ICO participants as a reward. The main chain funds would then be used by the federation for their own purposes while the side chain continues to exist as a separate economic entity.

- Federation key storage
  - ➔ Can ultimately be in hardware security module e.g. Ledger solution

- Misc design notes
  - ➔ User knows which federation address to trust based on unique identifier of sidechain stored with appointment proof(s) of initial members. These appointment proofs are signed by other federation members. The first federation member bootstraps the rest.

Open issues (research if Blockstream methodology has solutions):

- Appointment of federation members
  - ➔ Most likely will not have any members in common between different sidechains
  - ➔ Blockchain generation should appoint initial single federation member
  - ➔ This member should then appoint subsequent members
  - ➔ Need to specify quorum requirements e.g. does every subsequent appointment require unanimous approval of existing members?
  - ➔ Appointment protocol (Peer to peer or stored on chain? On chain means users can independently track authorisation but does leak federation size info)
- Removal of federation members
  - ➔ Quorum requirements
  - ➔ Removal vote collation protocol (peer to peer or stored on chain?)
- Large scale abandonment of duties by federation
  - ➔ This has to be prevented by the creator of the sidechain by careful selection of federation members
- Catastrophic loss of key material for main chain federation
  - ➔ Loss of side chain material can be recovered from by recreating the entire chain with new federation keys. There would need to be agreement amongst sidechain users to begin using the new chain instead
  - ➔ Loss of key material on the main chain is not recoverable without a hard fork. This is because there are funds encumbered by a multisignature address that can no longer be signed for. The side chain can continue to operation autonomously, but funds cannot enter or leave it