

It seems that if coins are indivisible/immutable, then one can have Plasma Cash as a simple Merkle tree without having any blockchain. The reason for this is that since the coins are immutable, there is no need for global transaction ordering/consensus. For a particular coin you only need its history and other coins are irrelevant. Therefore, a blockchain may be an overkill

Here is a quick sketch of how this could work - comments are welcome

1. Each coin-chain is a linked list of ECDSA signatures one on top of another.
2. If I want to pass my coin-chain to someone else, I simply append the address of the receiver to the SHA-3 hash of the current tip of the list and sign it creating a new tip. The coin-chain then becomes one entry longer.
3. The Plasma operator maintains a Merkle tree of all coin-chains.
4. When I transfer a coin-chain to someone else, I submit the new tip of the coin-chain to the Plasma operator. The Plasma operator then waits to receive say 1000 submissions, keeping them in the pending queue. Once the Plasma operator receives 1000 submissions, it recalculates Merkle root and posts the Merkle root to the Plasma smartcontract, which just becomes a sequence of Merkle roots. Plasma operator then provides me a Merkle proof of inclusion of the updated coin-chain in the Merkle tree.
5. A transaction is confirmed once the Merkle root is updated in the Plasma smart contract.
6. Exiting becomes really easy - to exit I simply sign a transfer of my coin-chain to address 0.
7. Double-spend is impossible because coin-chains in the Merkle tree are ordered by coin-ID, and there is only one coin-chain for a particular coin ID.
8. The current coin-chain owner always has the longest coin-chain, so if someone tries to revert transactions by shortening a coin-chain, the owner can always provide a fraud proof
9. If a coin-chain grows too long, one can checkpoint it (cut old history), checkpoint security can be achieved by maintaining a separate Merkle tree of checkpoints and storing the Merkle root of checkpoints in Plasma smart contract.