This is the idea to execute multiple transactions atomically in Plasma Cash.

related discuttion: Plasma Cash defragmentation, take 3

Proposal

- confirmation signature(It need for exit and challenge).
- confirmation signature is Sign(root, H(tx1), H(tx2)).
- Tx1 has H(Tx2) as pair

and Tx2 has H(Tx1) as pair

- Users have to prove inclusion of all pair transactions, so they send all pair transactions and proofs for exit and challenge.

An example

- atomic swap
- Tx1: Alice sends coinA to Bob
- Tx2 Bob send coinB to Alice

Attacks

- If Bob is a malicious operator and he withholds Tx1 and Tx2.
- In case of that Bob exit coinB with invalid history and later he exits coinA.
- Alice have to challenge(invalid history) to coinA’s exit.
- Bob respond to challenge with Tx1, Tx2, proofs, and confSig after 6days 23hour.
- Alice cannot challenge(invalid history) to coinB’s exit because coinB’s exit period could end up
- Alice have to challenge(invalid history) to coinA’s exit.
- Bob respond to challenge with Tx1, Tx2, proofs, and confSig after 6days 23hour.
- Alice cannot challenge(invalid history) to coinB’s exit because coinB’s exit period could end up
- In case of that Bob exit coinB with invalid history.
- Alice has to exit coinA soon.
- Bob challenge(spent) with Tx1, Tx2, proofs and confSig after 6days 23hour.
- Alice cannot challenge(invalid history) to coinB’s exit because coinB’s exit period could end up
- Alice has to exit coinA soon.
- Bob challenge(spent) with Tx1, Tx2, proofs and confSig after 6days 23hour.
- Alice cannot challenge(invalid history) to coinB’s exit because coinB’s exit period could end up

Modification for these attacks

- “beforeChallenge - startExit” must be longer than “respondChallenge - beforeChallenge” and spentChallenge period.
- For example, all exit period is 2week, “beforeChallenge” available period must be 8days, “respondChallenge” and “spentChallenge” available period is 6days.

References

- Plasma Cash defragmentation, take 3