

Has anyone thought of how to design general smart contracts for plasma?

I have tried for a while and found it really challenging. We have found a way to remove 2-phase confirmation of txs in plasma-mvp, which provides simpler finality of a tx. But we haven't figured out how to implement secure general smart contracts under block withholding attacks.

I think smart contracts on plasma are important and will be useful for:

1. multi-level plasma chain
2. lightning network / state channel on plasma

If the general smart contract for plasma turns out to be impossible in the end, dedicated smart contract can still support the functionalities above.

I'm wondering if there is any progress in the community.