Here are some usability and security problems that in my humble opinion do not make Plasma Cash fit for real life. Theoretical constructions is one thing, real life product that satisfies product-market fit is totally another thing.

1. The entire idea of mass exits is infeasible. For a Plasma chain of 100 million users, it would take 10(!) years for all of users to exit having the current state of the main net. The gas fees would go enormously high during this period of time.

2. Non-inclusion proofs grow linearly with time. If the proof size is 1K and block time is one second, a coin which is 10 year old needs 300GB of a proof. Paying with 10 coins and receiving 10 coins of change back then amounts to transferring 6TB(!) of proof per transaction. Try this with your internet provider. A single payment would take days in this situation.

3. Users are required to download process and verify gigabytes of Merkle roots per transaction.

4. Payments are extremely hard to make because the receiving party needs to have the exact change, and there is no way to split the coins.

5. There is no one economically interested to prevent self-spent-coin challenges. In particular, one can make one billion utxos by just paying the same $1000 coin to yourself.

Then out of these UTXOs one can randomly try exiting 1000 of them to make $1M.

Since there is no counterparty, one can only rely on third party “validators” to catch the thief. But these “validators” can be bribed by the thief, and it is enormously hard to become a “validator”, since you need to have the history of the chain FROM THE BEGINNING OF TIME. In fact, a Plasma chain plus 10 “validators” is not much different to a side chain.

1. The economic model for the “validators” is not feasible. One cant pay policemen a share of thiefs money, otherwise police departments in cities like Palo Alto, would become bankrupt. If a particular Plasma chain has no fraud attempts for a while, the “validators” will lose their source of income, and will have to simply purge the multi-terabyte data stores they need to protect the chain.