Writing up a discussion I had with Jeff Coleman, cc@karl

While a plasma chain needs quite a lot of features for us to be able to implement state channels on the plasma chain, we can implement state channels on ethereum chain funded by a plasma withdrawal if the plasma chain supports multisignature accounts. Here is a concrete proposal sketch.

We use the (no-confirmation, no splitting) version of plasma cash, but with the modification that UTXOs can be encumbered by multisignature (for such a coin, the appropriate threshold of signatures is required to spend the coin or to exit it). A UTXO T is said to fund a state channel A when T is encumbered by multisig with public keys p1, … pN, and each public key owner has a copy of the exit transaction that withdraws T to the ethereum address A, where A is the address of a state channel on ethereum controlled by p1, … pN. Hence, an uncooperative exit (say by pi) looks like this:

- pi exits T
- the challenge period goes by
- the plasma contract sends t.denomination worth of ether to A
- pi starts the state channel uncooperative closeout logic at A

As an example application, if we let A be a payment channel, we already get something like “on-chain splitting” of plasma cash tokens. Recall that plasma cash tokens cannot be split; with this scheme, if p1 has a UTXO worth 2 ether and wishes to send 1 ether to p2, he can use it to fund a payment channel where p1 owns 1 ether and p2 owns 2 ether. After that, p1 and p2 can send small micropayments to themselves within the state channel (notice: the funding UTXO is still on the plasma chain). Of course, we don’t want an on-ethereum-chain transaction to create A just so that p1 can send some money to p2 and receive change; to fix this, we can let A be a counterfactual address, and the simplest way to support this would be to build-in support for withdrawing to counterfactual addresses into the plasma contract (i.e.: to handle a withdrawal to counterfactual address C, the plasma contract waits out the challenge period, then looks up C in the registry to obtain A, then sends the funds to A).

A second example application: A could be a channelized chess game, so a plasma cash UTXO ends up being owned by whoever wins a certain chess game.

Third example: @karl’s “trading with high throughput”, i.e. instant-finality atomic swaps. A simple way to do this might be to have separate plasma chains for each token; to trade with someone, create a payment channel (maybe at a counterfactual address) with atomic swap functionality on ethereum, then fund it from both chains. A tricky question is how you close the state channel once you’re done trading. Assuming you own, say, 5 MKR in a state channel, funded by a 4.5 MKR UTXO and a 0.5 MKR UTXO, you could borrow a 5 MKR UTXO from a change provider, fund your channel with it (assigning ownership of it to you), and then give the 4.5 MKR UTXO to the change provider on plasma (atomically removing it from the state channel).

Notice that you still inherit the “defined participant set” requirement of state channels, and you need to wait out the plasma confirmation time (~300s) to fund your state channels (and then in a dispute you need to wait out the plasma dispute time, 14 days, to “actually fund” your state channel). Hence, a more useful way to think of these setups is as “state channels on ethereum, but using high-throughput plasma for rebalancing”, and for high-speed trading, it might be necessary to use a hub to route your trades through (this hub being someone with lots of plasma tokens locked up in long-lived state channels with different people).

A few things I skipped over: I described the “end-state” in which T funds a state channel, but to arrive at that state safely we need to sign the withdrawal transaction and the appropriate ethereum transactions to create A before creating T. Also, with this scheme @MaxC’s “transactions commit to a block number” modification to plasma cash cannot be used. Furthermore, you now have more griefing vectors: at the very least, the plasma operator can grief everyone, and in addition to that, random people who are your counterparty in a channel (eg they split ownership of a coin with you) can grief you by forcing you to go through the 14-day exit process, which is pretty painful. Lastly, I wish I could post this to both the “plasma” and “state channel” topics, but this forum software seems to insist that topics partition posts.