Hey all,

First up, apologies if I’m missing something overly obvious about Plasma. I haven’t been following this line of research too closely, but based on spending a few days trying to design a plasma scheme that I myself cannot break (game theoretically from all participants’ perspective), I have yet to find a workable solution.

My personal grudge is against the mass exit mechanism. But a bit of a background info before I get into that. Plasma seems to be an elegant way to do arbitrary calculations off chain and just commit the root hash into mainnet. Specifically, I like the construction because in theory the plasma operator could be challenged if they construct an invalid state, and if they just drop dead, users can always exit the chain themselves.

But a much more interesting attack scenario from my perspective is if the plasma operator starts to withhold data, but nontheless keep pushing state updates onto mainnet. First up, without the witness data, the operator cannot be challenged that they produced an invalid state (the operator could grieve users with valid but hidden state). As such, by withholding data, the operator can forge arbitrary state roots, and we know noone will challenge it, so imho one valuable aspect of the plasma construction is lost.

At this point, your only option is the mass exit, where each participant tries to get out of the chain before the whole thing implodes. This is what i don’t think will realistically work. The first and most obvious issue is that all the participants need to bail out, otherwise the operator can run off with arbitrary funds (e.g. I can create a root hash with “says” I have N ether (or some UTXO) and submit a merkle proof stating so). I don’t think this is a realistic scenario in itself: there are people within Ethereum who still have not touched their presale wallets in 3 years. I don’t think it’s reasonable to think that all participants of a plasma chain will be able to exit within a time windows that’s small enough to remain actually usable. If not all participants manage to exit, the operator can just forge withdrawals at different amounts and cash out the amount that’s still covered by the inactive accounts.

A second issue imho is that if a plasma chain becomes popular enough (lets assume 10K tps), the operator can pile up a ton of transactions from various participants. Then when it starts withholding state and users start mass exiting, it can keep dripping these queued up transactions back into mainnet. The effect will be that the operator could block a withdrawal request at the last moment for any user who has pending transactions. Eventually the operator’s own fake/double-spent withdrawals could exit while it’s users are kept being griefed.

Am I perhaps missing something too obvious?

Thanks,

Peter