This is an idea based on some reflections that I have had about potential ways to move parts of Kleros to L2.

In the taxonomy of L2 scaling solutions, we have tables like:

I suggest that one might be able to add another column to the table for “(Crypto-economic) Oracle”.

Basically this would work similar to Optimistic Rollup or Plasma in that when side-chain information is needed on-chain, some aggregator that has made a deposit reports it on-chain and can be challenged in some challenge period. However, in the event that an aggregation of off-chain information is flagged as being malicious, instead of having presenting an on-chain fraud proof, one queries a crypto-economic oracle.

This obviously comes with tradeoffs, particularly one would need to have confidence in the oracle. If we used this for Kleros, this would mean resolving disagreements over the state of a side-chain in (an on-chain version of) the Kleros court. So as other aspects of Kleros already require a certain confidence in the Kleros court as a security assumption, this might not be too burdensome an additional assumption for us; however, if some other application that didn’t have an internal oracle was to use this kind of scaling, that obviously adds security assumptions. (In passing, our governance mechanism already works similarly to this, where there is a step where people can submit which governance updates have been approved by the community, and if there is a disagreement this raises a dispute in the Kleros court.)

On the other hand, this approach means that you never

have to bring the state of the side-chain on-chain. That could remove implementation issues compared to Optimistic Rollup/Plasma, and you completely avoid scenarios where you need so much information from the side-chain at the same time in case of dispute that you tax the capacity of the main chain.

The question of whether to put data on-chain or not is interesting here. On some level, if you have human beings (like the jurors in the Kleros court) that are being incentivized to rule on whether a given state transition is valid or not, you might also be able to ask them to make subjective judgments about whether data is “available”. If the data is not put on-chain, it is somewhat less canonical to talk about what “availability” means, and the participants might or might not be able to reliably come to a consensus on such questions. I could imagine that it might depend on the application. However, you could still put all of the required data on-chain in the call-data and have a sort of “Oracle Rollup” to avoid such issues. For application specific solutions, you could also conceivably do intermediate things where more data identified as more important goes on-chain and less important data does not to weigh cost against resistance to some kinds of attacks.

In these notes, I go into this in somewhat more detail for one version of what this might look like in the application specific situation of putting (some of) the Kleros courts on L2.

I would be curious to hear people’s thoughts on this vein of approach, and whether anyone notices any subtle points or issues that draw from what the community has learned from its experience with various L2 ideas that would be relevant here.

Also, in passing, I just noticed that a related idea was briefly hit on in this discussion:Against proof of stake for [zk/op]rollup leader election