Overly Optimistic Rollups - Or Rollups with data availability assertions

This shall be just a quick refresher that one actually don't have to submit all data for a rollup system on-chain to be permission- & trustless.

Idea step through:

1. Instead of defaulting to submit all sidechain related data on the rootchain, we only submit the block hashes.

This can also be used to bundle & aggregate a lot of blocks inside a single rootchain transaction.

To the rootchain: let block = [blockHash1, blockHash2, blockHashN...]

1. All peers use the blockHashN

values to lookup the data on (for example) IPFS.

Peers may wait for a few seconds so that the data can propagate through IPFS.

If any data is not available after a certain threshold, then any peer can submit a data availabilty assertion to the rootchain rollup protocol.

1. The data availabilty assertion can trigger a global timeout, inside that timeframe, the block proposer from step 1 must reveal the data of any given blockHashN

by submitting it on the rootchain.

1. If the block proposer fails to do so, the rollup protocol can mark the block(s) as invalid and slash the block proposer. etc…

Conclusions

If the rollup protocol introduces an additional - or widens the actual - chain progression timeframe to allow for data availability assertions,

then this has the potential to further reduce gas costs.

Though, this probably breaks the Optimistic Rollup by definition   .