Hi folks,

We have developed a mechanism based on BLS signature aggregation to enable Plasma-style smart-contracts, that overcome the data availability problem and avoid exit games. At a high-level, we achieve this by requiring participants' signatures on a Merkle root before it is committed to the root chain. We design a protocol to allow for the L2 chain to securely move forward even when some participants are temporarily offline or withhold their signatures maliciously. This mechanism results in orders of magnitude lesser curve exponentiations and signature verifications for the operator and the smart-contract; on the other hand, gas costs are estimated to scale with the number of missing participants in each round (and O(1) in number of transactions). In ZK Rollup, for ex, gas costs (roughly) increase instead with the number of transactions.

Our preprint is available here: https://arxiv.org/abs/2003.06197 . The context and model we motivate in this work (that the side-chain is applied to) is a generic 2-sided marketplace.

Please let us know if you have any questions/comments or just interested in talking about it more.

Best regards,

Madhu & team