Intro

Rollup projects are looking for ways to minimize DA cost, but, most of the time, this effort ends up weakening the security of these systems by turning them into Validiums or Optimiums. On the other hand, now that we have state validating bridges, discussions around Plasma are starting to pop up again.

In this post we want to discuss “Optimistic DA” constructions like the one initially introduced by Metis two years ago or the recently proposed OP Plasma spec which will be used by the Redstone OP stack chain.

Definitions

- Rollup

: project with full onchain DA and the guarantee that users can always exit permissionlessly under less-than-majority trust assumptions (e.g. single honest challenger, cryptographic assumptions).

- Plasma

: project with offchain DA and the guarantee that users can always exit permissionlessly under less-than-majority trust assumptions.

- Validium/Optimium

: project with offchain DA relying on a majority trust assumption on DA attestations for exits.

Setting

The single operator (i.e. the sequencer) is supposed to share the full data publicly and periodically posts data commitments onchain, in the same way as in a regular Validium/Optimium. The only attack we need to worry about is data unavailability: invalid history, double spends, not latest owner attacks are solved by the validating bridge and the usual burn-unlock or lock-mint mechanisms.

Users have the ability to push transactions onchain without any action required by the permissioned sequencer, in the same way that deposited transactions work on OP Bedrock [1]. Moreover, users have also the ability to self propose state roots.

DA challenges

Every sequencer submission is subject to a challenge period. During this time, anyone can challenge a data commitment claiming its unavailability. If the sequencer posts the full data onchain, the challenge is deleted and the chain progresses as usual. If the challenge times out, the data commitment is reverted and the chain reorgs to the previous data commitment. A data commitment is considered finalized if the DA challenge period elapses without challenges or when the full data is published.

Since data unavailability is unattributable onchain, one has to come up with a mechanism that either punishes or rewards DA challengers by default without knowing whether the claim was right or not. Arguably, the most reasonable incentive structure that allows for this construction to have some benefits on DA cost side and prevents the money-pump vulnerability is to place the same cost on the challenger and sequencer when a challenge is created. This is done by requiring challengers to lock a bond that is approximately equal to the money spent by the sequencer to publish the full data that gets burned if the challenge is not successful.

Security considerations

Let’s say that the sequencer is malicious and plans to steal all the funds in the bridge by finalizing an unavailable data commitment that cannot be challenged by a fraud proof system over the state. Challengers can either force the sequencer to make the data available or revert the data commitment to the latest available one. Users can now exit by forcing withdrawal transactions independently via the base chain and self proposing state roots.

Since the mechanism punishes challengers by default, the malicious sequencer can exploit the incentives by never sharing the data. It is sufficient for the sequencer to economically outlast the altruistic DA challengers to finalize an unavailable root and steal all the funds. Therefore, the system is considered secure if the altruistic challengers can economically outlast the centralized sequencer.

The system does not require all users to be online to force transactions like in Plasma Free, but just requires one honest and active DA challenger at any given time.

Comparison with Stage 2 Optimistic Rollups

While the single honest DA challenger assumption might seem similar to the single honest challenger assumption for state fraud proofs, the assumption is actually worse since it requires altruistic DA challengers to have more funds than the sequencer. This is not a problem in Optimistic Rollups since the challenger is guaranteed to profit from an honest challenge, given that state transition faults are attributable.

The problem with this DA challenge scheme emerges when the challengers have no more money to spend on challenges. For Stage 2 Rollups, as described in the Stages Framework, we allow projects to upgrade the contracts if there is at least a 30 days window for users to exit, meaning that we require users to be online at least once every 30 days. In the same way, we can consider the case in which DA challengers have the funds to challenge unavailable data commitments for at least 30 days, delaying the potential confirmation of an invalid state root and providing users with an exit window. Since the amount of funds required is quantifiable, it is possible to get an assurance that the system is secure if users become online at least once every 30 days, or an amount of days proportional to the funds dedicated to it. Properly allocating the funds requires offchain coordination.

[1] The presence of this mechanism is the main difference between the Metis construction and OP Plasma. For the full details, see L2BEAT's risk analysis.