[Proposal] Re-Based

The currently proposed sequencing/proving design is complex, slow, and has centralizingly-high operating costs[1]. Based rollups offer a simple, fast, and composable alternative.

This proposal extends based rollup [2] to address specific concerns around latency, censorship and liveness.

To recap, a based rollup is L1 sequenced, where anyone may submit the next L2 block on L1. Fees are denominated in ETH, with L1 searchers/builders proving and submitting profitable blocks. A block-fee

is levied to fund the protocol.

Proof-bond Preconfirmations

Instead of submitting proven blocks (which may take minutes to produce), sequencers submit unproven L2 blocks alongside a bond. If a proof does not appear within MAX_PROOF_TIME, the bond is burnt, and the chain re-orgs. This allows faster economic preconfirmation of transactions, up to L1 preconf speed. The bond collateral should increase proportionally to the parallel proof-rate and miss-rate.

Anti-censorship Magic

[Proposal] Sequencer Selection: Fernet

IIRC, we had ruled out based sequencing since it doesn’t promote much diversity for L2 sequencers.

[Proposal] Sequencer Selection: Fernet

In general I like the randomness guarantees Fernet provides, with clear incentives for people to run Aztec specific infrastructure, and believe it leads to healthier long term decentralization

To improve the censorship-resistance and credible neutrality of L1-sequencing, an L2 Inclusion List Committee is introduced. The ILC attests to valid transactions that deserve to be included in the next block (it “sees” the mempool).

This is similar to what has been proposed for Ethereum, where the beacon chain is only responsible for inclusion lists.

Details

The ILC uses rotating participation PoS consensus to produce inclusion-lists. See“No free lunch” [3] for ideas on specific inclusion-list designs. The ILC is paid a share of block-fee

.

To support decentralized participation, the number of transactions (and size) is limited. The total volume of transactions may be only a small fraction of what ends up in blocks.

To ensure liveness, ILC inclusion is optional. If block builders do not include/abide-by the inclusion-list, they must pay a censorship-fee

(e.g. 15%). This fee begins to decay after PREV_BLOCK_TIME.

To prevent the ILC from having an advantage in block proposing, attesters enforce timeliness.

Liveness

[Proposal] Sequencer Selection: Fernet

Seems like incentives would lead to just a handful of builder-proposers pushing the blocks to L1 via a MEV sidecar. And if these go down it could affect L2 liveness.

While liveness is unlikely to be a problem (the market is efficient), there may occasionally be short delays (while the network is small).

A volunteer prover network ensures a maximum delay of BUFFER (e.g. 1 L1 slot) once a profitable block can be built.

Details

Volunteers monitor the blockchain, and produce blocks if a delay is detected. Specifically, if a profitable block can be built and BUFFER time has passed, a volunteer coordinator submits a block and nodes begin a race to produce proof-work.

Trusted centralized coordinators are probably sufficient for the few times I expect the volunteer network to actually be used. Shares for work are paid out as normal.