TLDR

: We expand on proposer/notary separation as introduced in[this post](). We suggest a simple proposer selection mechanism and compare the scheme with that of the [retired phase 1 spec]().

Construction

The SMC in the main shard is endowed with a “proposer registry” per shard which keeps track of proposer deposits. At every period of a given shard, a proposer is pseudo-randomly sampled as the “eligible proposer” with probability proportional to the deposit size relative to the total deposit pool in the proposer registry for the shard.

Shards use main chain blockhashes delayed by 20 minutes (relative to some shards-and-main-chain synchronisation mechanism unspecified here) as the RNG, with a corresponding 20-minute lookahead. Similarly, shards sample from the main chain proposer registry delayed by 20 minutes. Should the main chain reorg by more than 20 minutes, shards must also reorg (both the data layer and the execution layer) and recalculate eligible proposers.

We allow notary deposits to be reused across proposer registries, incentivising notaries to be proposers on at least one shard.

Discussion

In the retired phase 1 spec collators had a dual purpose. When calling addHeader

a collator would simultaneously cast an availability vote for collations in the windback, as well as make a proposal selection. In other words, collators played a role in both the data layer and the execution layer. This conflation of roles led to the proposal commitment mechanism and trapping game to address proposal withholding.

The idea with proposer-notary separation is to provide a cleaner separation between the data and execution layers. Notaries participate exclusively at the data layer without selecting a proposal and associated proposer. Instead the eligible proposer is selected autonomously by the main chain, and given monopoly rights to suggest a proposal for the corresponding period.

Beyond the removal of the proposal commitment game and the cleaner separation of concerns, this scheme comes with a number of advantages:

1. Reduced offchain overhead

: The eligible proposer directly broadcasts his proposal (0.5 round trips), as opposed to many proposers simultaneously broadcasting proposal headers and bodies to the eligible collator, with a total of 2 round trips to make a proposal selection. The reduced offchain latency overhead allows for more time to construct proposals.

1. No balance maintenance

: In the retired phase 1 proposers had a balance per shard from which would bids where deducted from. This meant that balances had to regularly be “topped up” by proposers, causing onchain overhead and introducing cashflow complexities for proposers.

1. Incentive alignment

: In the retired phase 1 collators would get rewarded the bulk of the transaction fees despite proposer-executors doing the work of executing and selecting transactions (see also [this post]()). With proposer/notary separation, notaries rightfully only get paid collation subsidies for their availability efforts, and proposers get paid transaction fees.

1. No forced cashflows

: In the retired phase 1 there were forced cashflow cycles from main chain ETH to shard vETH and back. Indeed, bids were paid for in ETH by proposers who then received vETH which then needed to be exchanged back for ETH for balance maintenance. Even orphaned proposals were paid for in ETH with a refund in vETH.

1. Stronger ETH enshrining

: In the retired phase 1 spec ETH was the default currency to pay bids, but nothing prevented proposers from privately paying bids in any number of other assets (e.g. ERC20s). With the new scheme the only

option for getting selected as eligible proposer is to stake ETH.

1. Decoupled proposer lookahead

: In the retired phase 1 spec the collator was effectively the “tier 1” proposer, and the proposers were “tier 2” proposers. The collator lookahead (required for windback) meant that the tier 1 proposer also suffered from lookahead. With the new scheme the tier 1 proposer lookahead is independent from the notary lookahead, and can be completely removed with a RNG-and-anchoring scheme such as [this one]().

1. No proposer censorship

: Because the proposer is autonomously selected by the main chain, there is no opportunity for the main chain to be partial to a subjective proposer selection algorithm. This removes the possibility of proposer censorship by collators.

1. No collator bribing

: Again, because the proposer is autonomously selected by the main chain, this is a significant mitigation against proposers bribing collators to not build on the head.

1. Capital reuse and guaranteed proposer pool

: Allowing notaries to reuse deposits across proposer registries enables capital reuse and yields a baseline pool of proposers. For example, with 10,000 notaries and 1,000 shards we get an average of at least 10 proposers per shard from notaries alone.

1. Natural merging of proposers and executors

: While proposers and executors both execute transactions, it made sense to separate proposers and executors in the retired phase 1 to not require proposers to make a deposit. With the new scheme both proposers and executors need to stake, so merging roles is natural. This allows for capital reuse and allows us to require proposals to also come with a state root claim as a further optimisation.

1. Tier 2 proposal markets

: The new scheme does not enshrine infrastructure for the tier 1 proposers to interact with tier 2 proposers, but nothing precludes sub-proposal markets to reuse the proposal commitment game at the application layer. The local gas idea allows for trustless sub-proposal markets to emerge.