TLDR

: This post suggests a networking optimisation for theproposal commitment scheme. By encrypting and broadcasting collation bodies early we can compress the reveal phase, to the benefit of proposers and validators.

Background

The proposal commitment scheme has four phases:

1. Propose

: Proposers broadcast proposals (collation headers).

1. Commit

: The eligible validator broadcasts a commitment to proposers.

1. Reveal

: The top few paying proposers share their proposed collation body.

1. Select

: The eligible validator broadcasts the selected proposal for inclusion in the VMC.

In the worst case all four phases need to be done within a single period, i.e. 5 main chain block times (~75 seconds). From a networking perspective the commit and select phases are not particularly burdensome. Both phases broadcast a single short message, namely the commitment and the selected proposal respectively.

On the other hand, the propose and reveal phases are expensive. The propose phase needs to last long enough for most proposals to be communicated to the eligible validator. This is to the benefit of the eligible validator and to the proposers as a whole. The reveal phase is expensive because collation bodies are relatively large, and because the eligible validator will attempt to download the top few paying proposals in parallel.

In the construction below we shift the costs of the reveal phase to the propose phase. That way the propose phase can be generously large, and the three other phases be relatively small.

Construction

We modify the propose and reveal phases as follows:

- In the propose phase proposers broadcast, in addition to their collation header, their encrypted collation body. Encryption is done using an ephemeral key. We suggest the eligible validator only downloads the encrypted collation body of the top paying (say, top 10) proposers.
- In the reveal phase, the top paying proposers share their ephemeral key with the eligible validator. Because of their small size ephemeral keys can be downloaded from all top paying proposers in parallel.