In the context of proposer-validator separation@vbuterin exposed a proposer withholding attack. In an attempt to solve proposer withholding, a proposal commitment mechanism was suggested to prevent validators from stealing collation bodies, thereby encouraging proposers to safely share their collation bodies.

By itself the commitment scheme is not sufficient because validators are incentivised to maintain “credit scores” for proposers, i.e. evaluate the likeliness of proposers not withholding their collation bodies. In this post we augment the commitment scheme with a challenge scheme to address the credit score issue.

Construction

We require every proposal to contain the root r

of a “fine-grain” Merklelisation of the corresponding collation body. (Let B

be the collation body. We partition B

into 32 byte chunks B[0], ..., B[n-1]

and build r

by Merklelising the chunks B[i]

.)

We now give proposers the right to challenge validators of their own proposals. That is, a proposer can issue a transaction to the VMC challenging the validator to disclose some chunk B[i]

for one of his validated proposals. The challenge passes if the validator responds (within one epoch, say) with a Merkle path from B[i]

to r

. The challenge fails otherwise.

If the challenge fails the validator is slashed, and half the validator’s deposit is given to the proposer.

Discussion

The above challenge scheme is a way to enforce validators to only include proposals to the VMC for which the corresponding collation body is available to them, thereby nullifying credit scoring. Indeed, whenever a validator includes a proposal to the VMC without downloading the collation body from the proposer this is an opportunity for the proposer to set a trap by partially withholding the collation body. Even a single 32 byte chunk withheld by the proposer is enough to slash the validator and earn the proposer a large financial return.