See this post for a description of the attack and proposed fix. We propose an alternative fix below.

Construction

During his assigned period p

the eligible validator gathers the proposals (i.e. signed collation headers) he has received from all proposers. He also prepares a proposal of his own, e.g. the proposal with an empty collation body. Those proposals are Merklelised to form a root r

.

The validator prepares a commitment C

by signing [p, r]

and broadcasts C

to all proposers. The commitment C

bonds the validator to using a proposal authenticated against r

. That is, when the validator pushes a proposal to the VMC, he also includes a Merkle path from the proposal to r

.

If the validator shares a commitment C'

for the same period p

but with a different root r'

then any whistleblower can have the validator slashed (and get a whistleblower's bounty).

Discussion

The commitment and authentication of proposals combined with the slashing condition means that proposers that have received the commitment C

can safely reveal the collation body for their proposal with the validator, without the risk of the validator "stealing" the transactions.

The VMC can be setup so that the eligible validator only receives the collation subsidy if the collation body is made available. With such a setup proposers would know that that the eligible validator has a financial preference for proposals for which he has access to the corresponding collation body. Therefore proposers are incentivised to share their collation body with the validator to increase the probability of having their proposal picked by the validator.

In an environment where collation subsidies represent a significant portion of proposer bids, or where withholding attacks are common, an honest and rational validator will likely push proposals to the VMC for which he has received the corresponding collation body, thereby addressing the withholding attack.