My goal is to come up with a sharding scheme

that has a high collation rate

, without sending every collation to the main chain. This to save on gas

and get better scaling

.

The idea is to let the validators create a chain of collations off-chain

and only send a combination header containing all off-chain collations once every X collations. Note that you still want to publish the header on a regular basis for cross shard communication and finality.

Building the collation chain

The order of the validators is known in advance and a validator is only allowed to build an off-chain collation on top of a collation of his direct predecessor. If lot of validators in row participate we can build a long collation-chain. Every participator in the chain is allowed to send the combination header to the main chain at any time. We want to avoid that a validator sends an older version to the main chain, so all participators have to sign the latest combination header to let them commit not to send any older headers.

Skipping validators

If a validator does not participate or is offline, one participant of the collation-chain sends the combination header to to main chain. If the non-participating validator does not send a collation header within a certain number of blocks, the next in line validator can send its header to the main chain and the non-participating validator is skipped. After that, the validators can start building a new collation-chain off-chain. A validator is allowed to skip previous validators that have not send a header to the chain, but has to wait a certain number of blocks per skipped validator. This waiting period per validator is a few factors longer than the off-chain collation interval, so the off-chain collation-chain builders do not have to worry about being skipped.

Attack by censoring

An attacker could try to revert a collation-chain by censoring the combination header transaction for a long enough period to be able to send a header and skip all participants.

As an extra safety measure, it is possible for a combination header to revert collations headers on the main chain from the validators that skipped the collation-chain builders as long as the collation-chain contains more collations than the number of reverted collation headers.

Because we do not allow building an off-chain collation-chain on top of a collation header that might be reverted and there is a minimum block interval between headers, we give the censored validators more time to get their combination header confirmed and withstand the attack.