TLDR

: We propose a data availability scheme for collation bodies. The scheme requires collation proposers to prepare availability proofs for their proposals and requires validators to add those to the collation headers in the VMC. Assuming an honest-majority of validators the scheme guarantees both availability and liveliness of collation proposals, and allows for fork-free sharding. The proof is succinct and simple to produce.

Construction

Let B

be a collation body for which a proposer wants to produce an availability proof. Let V

be the (ordered) list of validators of size |V|=n

. For simplicity we assume that validators have fixed-size deposits. The proposer does the following:

1. Shares B

with validators and gathers \lceil n/2\rceil

BLS signatures for B

.

1. The \lceil n/2\rceil

BLS signatures are aggregated into a single BLS signature.

1. The proof is the BLS signature plus n

bits describing which signatures have been aggregated.

BLS signatures are 20 bytes. So if we have 2048 validators the availability proof is a total of 276 bytes. The VMC rewards every validator that contributed to the BLS signature with a small “signing reward”.

Analysis

- Liveliness

: By the honest-majority assumption it is always possible to find \lceil n/2\rceil

validators that are willing to sign B

.

- Availability

: By the honest-majority assumption any sampling of \lceil n/2\rceil

validators contains at least one honest validator that will broadcast B

to the world (e.g. seed B

to IPFS).