TLDR

: We present a signature aggregation scheme intended as a possible alternative to BLS signatures in the context of committee voting, with applications such as committee-based notorisation and fork-free sharding.

Construction

Let V

be a committee of voters v_1, ..., v_n

. For a given message m

every voter can cast one vote by signing m

. For concreteness we set |V| = 423

(as inspired by Dfinity) and require a threshold of t

votes (e.g. t = |V|/2

) to form a quorum.

Given at least t

votes, some collateralised claimer (e.g. an eligible proposer, blockmaker or collator) can aggregate the votes by creating a bitstring B={b_i}

of size 423 bits, where b_i=1

represents a claim that v_i

signed m

, and b_i=0

otherwise. The claimer signs [m, B]

to form a signature s

. The cryptoeconomic aggregated signature is [m, B, s]

.

During some challenge period anyone can challenge the claimer to provide the signature of m

from v_i

if the bit b_i

is set to 1. Failure to provide the signature in time slashes half the claimer's collateral, and rewards the other half to the challenger.

Discussion

The overhead of the aggregation scheme is 423 bits (53 bytes). Every voter (e.g. a notary, collator, validator) knows whenever the claimer is reporting a false vote from himself, so it is risk-free for the voter to challenge the claimer.

Compared to BLS signatures, the aggregation scheme does not require a setup phase among the voters. The scheme is also quantum secure if s

and the votes (signatures of m

) are quantum secure.