TLDR

: We propose a natural way to merge Casper and sharding votes via crosslinks. The dual-purposing of sharding infrastructure for Casper leads to a particularly harmonious and efficient design. The scheme provides atomicity of validation roles across Casper and sharding, and yields Casper accounting “for free”.

Construction

For concreteness let’s assume 512-of-1024 shard committees and 128-period epochs. A “shard checkpoint” is a collation with no descendant in its epoch.

Once per epoch and per shard the corresponding shard committee can cast at most one “aggregated vote”. An aggregated vote explicitly specifies a shard checkpoint, and implicitly specifies a Casper source and target as follows:

- Casper target

: The target is the beacon block serving as the checkpoint heartbeat.

- Casper source

: The source is the youngest beacon block finalised with respect to the Casper votes tallied up to the target.

Individual Casper votes from validators only count if they are part of a crosslink. That is, the following two conditions must hold:

- Full notarisation

: The checkpoint must reach a quorum of 512 of the 1024 committee members.

- Crosslinking

: The fully notarised checkpoint must be included in the beacon chain.

Discussion

The intuition is that “1 validator 1 vote” is replaced with “1 crosslink 1 vote”. At the cost of some loss of granularity, tallying Casper votes becomes especially cheap because one aggregated BLS signature corresponds to a “megavote” backed by at least 512 * 32 ETH = 16,384 ETH. You can think of this vote aggregation technique as a form of enshrined pooling, with dynamic pool membership thanks to validator shuffling.

The design allows for deep dual-purposing of infrastructure:

- Messages and signatures

: Notarisation messages and signatures are dual-purposed for both crosslinking and Casper voting.

- Gossip channels and aggregation

: Shard gossip channels and aggregation infrastructure are also dual-purposed. (A post on iterative aggregation is upcoming.)

- Coordination

: Shard coordination points are dual-purposed to also coordinate Casper targets and sources.

Finally, the sharding and Casper validation roles are atomically merged, i.e. it is not possible to be one without being the other. This atomicity helps with security (it avoids crosslinking falling behind finality, or vice versa) but also allows us to dual-purpose accounting infrastructure:

- Accounting

: We have a single “crosslink reward” for both shard notarisation and Casper voting. In other words, Casper accounting comes for free from sharding accounting.