UPDATE: see correction here A model for stage 4 "tightly coupled" sharding plus full Casper; in short, some kind of limited forkful sharding (eg. with a short revert limit) may be unavoidable, though we can have finality come more quickly if desired by reducing the period length to 1 block.

The following describes how “tightly coupled” sharding might work, in a way that simultaneously provides full Casper, along with fast semi-confirmations.

We assume:

- Either data availability proofs, or that nodes simply directly check availability of collations a few blocks back
- A cryptoeconomically secure mechanism for randomly sampling validators
- A chain-based PoS scheme

Consider a chain-based PoS scheme where every block has a proposer, which is randomly sampled from the validator set, and SLOT_COUNT

(eg. 12) collation slots. For each slot, a validator index is sampled, and a shard ID is randomly chosen; this random sampling happens LOOKAHEAD

(eg. 5) blocks in the past (ie. the validator indices and shard IDs for block N

are chosen during block N - LOOKAHEAD

.

Each collation slot can be either empty, or taken up by a collation header, created by the specified validator. A collation header simultaneously serves three

functions:

1. Representing a collation in the specified shard.
2. “Soft-confirming” the parent block.
3. Carrying a Casper FFG vote for the most recent checkpoint.

(1) is the same as collations in the current sharding proposal, except it is tightly coupled

; that is, a block cannot be valid unless all collations it contains are available, and the same is true for all ancestors of that block. Additionally, the sharding is now internally fork-free

: the collation must be built on top of the previous collation for the same shard mentioned in the chain.

Regarding (2), we have two properties. First, each collation that confirms the parent block adds 1 point to the score of the parent block; hence, these collations are the dominant factor that determines which chain is the longest. Second, a single validator creating two collations with the same index at the same height is a slashable offense; hence, if you see a collation with N > SLOT_COUNT/2

slots full, then you know that any competing chain will either require 2N - SLOT_COUNT

slashed validators, or it would have to revert an entire LOOKAHEAD

blocks to get different validators; either condition is hard, so this gives a kind of “soft finality” that can be reached within a single block. This can essentially be Ethereum’s answer to the market desire for blockchains that offer confirmations within a few seconds.

And (3) is self-explanatory. Note that the numbers match up quite conveniently; for example, if there are 100 shards, and we have an implied “period length” of 5, then this implies SLOT_COUNT = 20

; with 20 votes per block, which with 2000 validators gives an equivalent “epoch length” of 100 blocks.