We can take the minimal sharding protocol that we started withhere and greatly reduce its block time by speeding it up with off-chain pre-confirmations. This gives us the benefits of both off-chain “fast confirmation” (and many other benefits of schemes like this) while at the same time keeping the shard chains clearly rooted in the main chain which continues to be the single locus of global consensus and ultimate finality.

The mechanism works as follows. At the start of a new period, we randomly select N = P/B proposers, where P is the period length and B is the block time, and M notaries. If the start of the period is T, then we define the interval [T + B * k, T + B * (k+1)]

for 0 <= k < N

as sub-period k. At the start of sub-period k, proposer k is expected to submit a collation. During sub-period k, all notaries are expected to submit votes where they vote on the availability of all existing proposals in that period (ie. from sub-periods 0 to k-1). Slashing conditions mandate that each vote cannot disagree with any previous vote in that period, and votes made in period k can be included into proposal k+1, giving a reward to both the voters and the including proposer (all inside the shards).

At the end of the period, the notaries are expected to make on-chain votes on all of the proposals, and another slashing condition ensures that these final votes cannot disagree with the previous off-chain votes.

Version 1: the proposals do need to be on-main-chain, and sub-periods are actual periods of (eg. 5) blocks.

Version 2: the proposals can be off-chain, allowing sub-periods to be shorter than block times if desired. The final votes need to contain a Merkle tree root of the list of all proposals in that period, and notaries are also responsible (via a challenge-response protocol) to provide any of the proposals that they voted for on demand.

In both proposals, both intermediate and final notary votes are subject to the usual skin-in-the-game conditions (if you vote that something is available, you have to provide any piece of it that someone challenges for on demand, and the same for proofs of custody if we so desire).

Notice that if desired, we can set the global period length to 100 blocks. This would overlap with the Casper FFG finality cycle, essentially ensuring that by the time a period finishes, the previous period will likely have already been finalized. Essentially, this would create a regime where the main chain and each shard would proceed independently between finality rounds, but then all synchronize, with every shard rooting and internally confirming in the main chain right before the next Casper FFG checkpoint arrives.