Required reading: A minimal sharding protocol that may be worthwhile as a development target now

We can extend the minimal sharding spec to reduce in-shard block times, and particularly make in-shard block times not dependent on a majority being online, as follows. Instead of the chunks_root

in the committee vote being the root hash of a single chunk, it now is a hash of the header of a block in the chain of that particular shard. A proof-of-custody mechanism is added to ensure that:

1. The linked header, and all headers between that header and the header previously linked for that shard, must be available.
2. As a corollary of (1), the linked header must be a descendant of the header previously committed to for that shard (note: this follows from the cross-link fork choice rule described earlier)
3. For every header in that shard between the current and previous header (including the current, not including the previous), the collation body must be available.

The committee that can create a cross-link is chosen based on main-chain randomness based on exponential backoff: suppose that the last main-chain block when a collation for that shard was linked is T. Let R[i] be randomness from block i. For any block S > T, find the most recent block B such that B.number - T

is an exact power of 2 (possibly with some minimum, eg. 128). Use R[B] as the source for a valid committee.

This accomplishes two goals:

- It ensures that a committee does not have infinite time to find each other and collude to make an invalid block, as eventually any committee will get replaced by another one.
- It gives a newly assigned committee ample time to download and verify the linearly growing amount of data that they are assigned to attest to (specifically, the committee need only be able to verify data twice as fast as the chain is growing).

If more than 33% of nodes are offline, then cross-links will not happen, but the chain on each shard will be able to keep growing.

One possible addendum may be to not allow making a cross-link for a shard until the previous cross-link is finalized; this would allow the notarization committees to not have to worry about complicated dependent fork choice rules, as the “root” of the shard chains from which shard fork choice is evaluated from would be clear since the previous cross-link would already have been finalized.