Between STARKed data availability roots and Kate commitments (plus some not-yet-published techniques for computing N reveals of a deg-N polynomial in O(N * log(N)) time), we have the possibility of fraud-proof-free data availability checking schemes.

Fraud-proof-free data availability checking schemes have the advantage that they preserve many more of the properties of traditional non-sharded blockchains: if a block is accepted by a client at time T, it will continue to be accepted at any time after T, there's no possibility that a fraud proof will invalidate it after the fact. This opens the door to the following possibility: what if we have a sharded blockchain without

committees, where the only

mechanism for verifying data is data availability checks?

Here is one possible design:

- There exists a base chain, similar to an ethereum-like non-scalable blockchain. Anyone can post transactions to it, etc.
- Users have the ability to pay a fee to send a special type of transaction, which contains a data commitment (think: STARKed data availability root, or a Kate commitment) to some data D.
- When including a data-commitment-carrying transaction, block proposers/miners first do a data availability check (ie. sample eg. 30 random coordinates) to verify that the data is available. They would need to do this through an anonymizing network to avoid an attacker satisfying only their checks and not anyone else's.
- When verifying a block for any purpose (as a client or a block proposer/miner), for any data-commitment-carrying transaction you would do a data availability check. You would only accept a block for which every availability check passed.

These are the entire rules of the system; particularly, there are no committees, proofs of custody, etc. We lean on data availability sampling fully and absolutely for security.

Why do this?

- It's extremely simple, in fact it's arguably as simple as a sharded system can be. It provides consensus on a chain and on the fact that the data in that chain is available, which can be used as a base layer to build systems like rollup on top of.
- It's secure; there's always some risk that a small number of block producers and users get tricked by some unavailable data by random chance, but with overwhelming probability the rest of the network will not be tricked, and so will reject any blocks containing commitments to that unavailable data.
- It does not have 2/3 online assumptions that committee-based systems do

Why possibly not do this? A few reasons:

- We might strongly desire to scale computation and not just data, doing computation at layer 1 rather than layer 2, so as to avoid layer 2 relying on synchrony assumptions
- Committees have important side benefits, so we may need committees anyway. Particularly, (i) a Casper FFG chain already need thousands of validators per slot to send messages to reach finality, so we may as well dual-use those signatures, and (ii) there's stability benefits to having a randomly selected ~128 validators that are guaranteed to have actually downloaded and stored the data.

That said, this certainly is possible as a construction.