Can someone please explain why we usually target 2/3 threshold when voting on FFG checkpoints and/or crosslinks? Could we instead ask for a more strict majority (e.g. 99%)?

If I'm not mistaken, these is a common practice for validating computations in grid/volunteer computing platforms like BOINC. Validation of blockchain state transitions is essentially the same thing - validation of a bunch of computations.

The point here is that we will need much smaller samples to achieve the same statistical security (I didn't do exact calculations, but this is very obvious if you know how binomial probability is calculated). Practically, BOINC computations gets re-computed/validated 3-20x on average, while in Eth 2.0 we need hundreds of validators.

So, while retaining the same level of security, we can achieve:

1. Lower fees/inflation (less validators are performing the same work)
2. Higher availability of validators (less validators are busy validating a single shard -> more are available to accept new tasks).

Did we simply inherit 2/3 from BFT research, and now we unnecessarily stick to it?

Can we change our thinking paradigm to something similar to TrueBit's computational courts - if we have e.g. 100 validators sample and 99% threshold, we need ONLY TWO honest validators NOT TO SIGN and we know something is wrong?

Thanks.

P.S. Of course, we would use cryptoeconomics to incentivize honest and disincentivize bad actors (this is an obvious improvement over BOINC-like model).