I’m sure this a noob question but … why is it important that “anyone” can verify the blockchain, be it PoW or PoS? Can’t we raise block limits if we relax this assumption? Doing so will solve the scalability problem without sharding / rollups / etc, though you can always add those on for even more gains.

Reasoning:

1. Consensus is N/2 of N, verifying is 1 of N.

If even 10% of miners claim that the longest mined chain has a double spend (or faulty rewards etc) sitting in it, that’s enough cause for concern. Social layer of consensus will have to kick in. Note that you need 51% of miners to collude for this situation to occur in the first place.

1. Verifying is a cost.

It doesn’t matter if it’s $100 or $100k, the fact is it’s a cost that no one is incentivised to undertake. You could bake in an incentive at the consensus level - but then how do you identify “unique” verifiers? That’s just the sybil problem which is solved by measuring hashpower or stake - so you might as well let the verifier set be the same as the mining / staking set.

The current assumption for PoS security is:

Take the set of people who can buy atleast 32 ETH ($32k right now), and some technical skill, and are willing to make a long-term low Sharpe bet on Ethereum. This set should not contain a colluding majority.

What if we add the assumption

that the set only contains people who can “burn” $20k annually in server costs and still profit? This increases the minimum investment needed to be profitable in practice, and therefore narrows the set of people who can stake.

Isn’t it still a reasonable assumption that this set does not contain a colluding majority? Note that people are being weighted by their stake anyways, so most of the people with a significant contribution to stake are already rich and belong to the second set.

More formally, wealth distribution

in the world is significantly skewed. The top 2% of people own over 50% of global wealth. Assuming there exists a liquid market for ETH and ethereum becomes a global settlement layer, this wealth distribution is only going to transfer over to ethereum. Some early birds will make gains but there isn’t a guarantee that global wealth distributions will become significantly fairer if ETH gains adoption and its price shoots up.

So we are anyway reliant on the wealthiest 2% of users not containing a colluding majority (again assuming ethereum becomes a global settlement layer). Why is a figure as low as 32 ETH necessary to be the minimum viable stake?