

Abstract:

If we end up increasing the maximum effective balance, the larger validators could have a reduced attestation power relative to the same amount of stake in multiple smaller validators. Offering increased attester incentives (i.e. extra rewards) for these larger validators would encourage uptake of the option in return for the reduced relative power over the network.

Background:

Large staking-as-a-service providers control a large portion of Ethereum validators. In particular Lido has either passed or is about to pass 33% of all staked ether. As many in the community have [explained already](#), this represents a threat to the perceived credible neutrality of the network and as such threatens future adoption and the fulfillment of Ethereum's potential. Efforts to elicit voluntary caps on their growth have been futile, with their DAO [voting almost unanimously not to self limit](#)

There are now frequent discussions amongst the EthFinance Community (e.g. [A](#), [B](#), [C](#) just in the last few days) and presumably elsewhere regarding this issue, and people are starting to [raise the question](#) of when social slashing should be considered as a way to protect the ecosystem, despite how drastic this option seems.

Proposal:

I believe that the Ethereum ecosystem's real superpower, it's potential to slay Moloch, comes from the ability to design and adapt incentive structures, and so that is the tool I think we should use here. We set up a system to make use of their profit maximalist position by forcing a choice between increased rewards vs increased control.

This idea builds from [@mikeneuder](#)'s proposal to [increase the max effective balance of validators](#) and relies upon that being implemented. Then we give extra attestation rewards to validators with larger balances, but at the same time reduce their attestation weight relative to the same number of ether in smaller balances.

So for example... Alice has 4x validators with 32 ether, earning issuance at around 3.5% (ignore transaction tips and MEV) so say 4.48 ether per year and with attestation power of $4 * 32 = 128$ ether.

Bob has 1 validator with 128 ether, earning issuance at $3.5\% * 1.04 = 4.66$ ether (for example) but with an attestation power of only $\sqrt{4} * 32 = 64$ ether (for example).

In this way, if all Lido (and centralized exchanges) care about is getting as much profit as possible they are incentivized to go for big validators with to take advantage of the Rich-get-richer™ mechanism. In doing so they reduce the influence they have over the network and put relatively more power into the hands of smaller validators.

Obviously the parameters for increased rewards and reduced power could be adjusted to whatever seems appropriate, but as a back-of-the-envelope approximation though, using a Max Effective Balance of 1024 and only the big 4 centralized staking pools (Lido, Coinbase, Binance and Kraken) taking up the option, this could reduce Lido's control over Ethereum to about 11.5%.

However:

I've been slow thinking this idea for a while, and it has a lot of obvious disadvantages:

- Massively fundamental change to how the Beacon Chain works, which I don't even know is possible (if anyone can help me understand this I would really appreciate it);
- Reduced overall attestation weight would reduce Ethereum's security in terms of vulnerability to 33%/51%/66% attacks (though I don't think this would be to particularly risky levels);
- Increased overall rewards would slightly impact Ethereum's economic policy of minimum viable issuance;
- Perception of rewarding the bigger validators more would probably be terrible in the wider crypto community (this might be the most serious issue);
- In the (very) long term would this just delay the problem, postponing discovery and implementation of a better solution.

Conclusion:

The idea has many flaws, and it may be that it would have a larger negative impact than the problem it attempts to solve, but as yet I haven't encountered a solution proposed to Lido's growing dominance that seems more reasonable. While this doesn't seem quite right yet, it seems to me to be the right 'shape' of solution, using incentive gradients rather than brutal forks would presumably be less messy if nothing else! I am very open to learning and criticism, so please do point me towards any resources that might help me with this topic, whether that's links to help understand how possible (or not) this idea may be in practice, or to better solutions that other people are working on.

Disclaimer:

My educational background is in astrophysics rather than computer science/cryptography/ or anything more relevant - therefore please assume that my maths uses liberal [approximations](#) and should be taken as indicative only.

