

Currently, validators are able to enter and leave the validator set relatively quickly: each time a validator set transition happens, 1/64 of the validator set can switch in or out, and so in the normal case, every validator can switch out within a day. There is a much slower queue for withdrawing

, to prevent validators from all withdrawing as soon as they perform a large-scale attack before they can be penalized. I argue that this current status quo is suboptimal, and we should set the withdrawal delay to a minimal constant (eg. 1 day) and instead use a much more conservative bound on entry/exit rate to serve the same function.

I claim this is a good idea for a few reasons:

- CBC Casper compatibility

: part of CBC philosophy is that the chain does not need to converge on one specific mechanism to determine canonical “finality”; applications can choose what thresholds they use. The current validator set change mechanism (1/64 every time the chain finalizes) requires the chain to have a canonical finality oracle.

- Light client friendliness

: having a much slower bound on validator set change makes it easier for light clients to skip ahead a relatively long distance at a time.

- Ability to resume finalization via a surge of friendly deposits

: if there are not enough validators that are online, a fixed rate limit on entry/exit, that does not

require the chain to finalize to proceed, would allow altruistic ETH holders to swoop in and join the validator set to cause it to resume finalization.

- Resistance to discouragement attacks

: a discouragement attack ([link to mini-paper here](#)) involves an attacker (with $\geq 33\%$ stake) causing a medium amount of disruption to consensus, with the purpose of making it unprofitable for others to validate. This drives others to leave, making further attacks cheaper and more profitable. Making it simply not possible for validators to leave quickly (intuition: you joined the army, the fort is under attack, you have to stay around to defend it, being on-call for that sort of thing is the job description!) is the best known strategy to increase the cost of discouragement attacks.

The alternative is simple to implement:

- Reduce the maximum number of validators that can enter or exit from 1/64 of the total to a much lower fraction, or even a square root or a constant (think: 1-3 months to rotate the entire validator set)
- Repurpose the withdrawal queue into a entry/exit queue. Repurpose `exit_slot`

as the slot when either (i) a deposit was processed or (ii) an exit was triggered. Post-exit withdrawal is now a fixed length of time (possibly extendable with proofs of custody)