

After the beacon chain will enable withdrawals, both exit and entry queues will clog for multiple months, maybe forever. The reasons for that, besides the genuine desire to stake/unstake:

1. stake compounding
2. key rotation

Both of these don't have to involve changing the validator set, and shouldn't clog the queue. The clog can be greatly reduced by adopting additional features to allow key rotation and skimming off the rewards.

## Compounding stake in the beacon chain

To make the most out of your stake, you must run (your total amount of ETH)/32

validators. If you deposit 32 validators at 32 ETH each and after half a year each of them earns 1 ETH of rewards, to get the most out of your stake you need to get the 32 ETH of rewards off them and start a new validator.

By current spec, the only way to do it is to unstake all of your validators and redeposit 33 of them (that's disregarding fees).

When withdrawals are enabled, there will be hundreds of thousands of validators (conservatively - 300000 of them) with a good number of rewards that would want to compound their stake.

With current settings, that would clog the exit/entry queue for 10 months, and in that time the rest of the validators, including freshly deposited, will get more stake on them, driving the next wave of compounding and so on. Most likely the eventual equilibrium here is a permanent clog of a few weeks on both queues.

Note that these withdrawals/deposits are not "real" in the sense that people doing them do not wish to change the validator set - they just want to skim and restake the rewards.

That can be amended with an EIP to "skim" the rewards - partial withdrawal of validator's balance over 32 ETH. That way compounding is still possible but there's no need to exit/reenter for a validator, and there's no stress on queues.

## Key rotation

Beacon chain had been launched with key handling infra that is much less mature than today. Some people would want to rotate both their withdrawal credentials and validation keys to a different setup. That will be especially important when the time of secret-shared validators established via distributed key generation will come.

By current spec, the only way to rotate any of them is through withdrawal and restaking. It's impossible to give an informed estimation of how many validators that is, but I know it's at least 18000 of Lido's validators.

That too can be rectified with an EIP.

## What do

I think the best way forward would be:

1. Extend [0x3 withdrawal credentials](#) with a [generalized message relay](#) that would allow building a number of features for beacon chain by using existing execution layer fees mechanisms for spam protection. Fees can be amplified on the execution layer with custom smart contract logic. Alternatively, rate limits can be imposed.
2. Make a "skim rewards" message using this mechanism that would make a withdrawal of rewards over 32 ETH from the validator to the withdrawal credentials. If execution environment tx fees seem inadequate for spam prevention, additional application-level fees or rate limits can be imposed.
3. Adopt a withdrawal credential rotation solution, e.g. [\[1\]](#), [\[2\]](#), or [\[3\]](#).

Validator key rotation is also often desired by node operators, but it is a much more nuanced topic. It can represent actual validator churn, not a routine security operation, and some uses of it should be subject to exit/entry queues, so this operation should be handled with care. There's a proposal to implement it via adding a new kind of message in consensus layer and a new kind of credentials [\[4\]](#).

Based on feedback, I'll try to get the ball rolling in that direction. I believe that clogging the queues for months is undesirable (though not critical), and should be avoided if possible.