Currently, withdrawal credentials in Lido are a 6/11 threshold signature where individual key shards are held by notable members of the Ethereum community. All ether deposited to beacon chain up to this point (slightly more than 600k) is using these credentials and is under the risk of collusion between 6 out of these 11 signatories.

Next Thursday Lido will vote to upgrade withdrawal credentials to an upgradeable smart contract. All the further deposits after the successful vote will use a smart contract address as withdrawal credentials, meaning that for new ETH in system threshold signature collusion is no longer a risk.

Between the 20th and 27th of July, we will run a threshold signature drill to make sure the respective key shards remain accessible. When Ethereum introduces withdrawal credentials rotation capabilities, or withdrawals - whichever comes first - the threshold signature will be rotated to the smart contract withdrawal address as well.

Current state

The first set of withdrawal credentials - 6/11 threshold signature were generated during a ceremony that took place between December 13th and 16th, 2020, performed by a group of the industry's trusted builders.

Chorus One, Staking Facilities, Certus One, Argent, Banteg (yearn.finance), Alex Svanevik (Nansen), Anton Bukov (1inch), Michael Egorov (Curve/Nucypher), Rune Christensen (MakerDAO), Will Harborne (DeversiFi) and Mustafa Al-Bassam (Celestia) came together over a four-day event to generate threshold signatures for Lido's withdrawal keys in a secure environment on air-gapped machines.

All ether deposited from Lido to beacon chain to this day (more than 600k) is using these credentials. If 6 out 11 of these builders collude, they will eventually be able to steal the funds or hold Lido hostage. If 6 out of them lose their shards of a key, the ether will be stuck forever (akin to what happened to Stakehound's Ether).

Thankfully, the DKG ceremony was designed in a way where the only thing that has to be backed up is a seed phrase, and every OG in the space has a good experience with storing seed phrases. Every participant had verbally confirmed they've got their secret share backed up.

Even then, this is obviously not a sustainable situation. Lido's ready to start changing it.

Withdrawal credential rotation

Lido DAO is going to change withdrawal credentials (WC)

so that they point to an upgradeable smart contract instead of a BLS key. This will allow for more decentralization as withdrawal logic will be controlled by LDO holders via DAO voting instead of withdrawals being initiated by holders of BLS key parts. The smart contract in question is a simple no-function upgradeable smart contract that uses OpenZeppelin code for upgradeability and is recently audited.

The change is going to take place on the week of 12.07–19.07.2021

.

On Monday, Jul 12

new WC are generated and published. Node operators will validate them and make sure they are able to generate a new chunk of deposit data using the new WC.

On Wednesday, Jul 14

an onchain vote for WC change is started.

On Thursday, Jul 15

the vote for WC change is executed. All validator keys that are not used by that moment are pruned from the protocol. Node operators submit new deposit data till 3:00 PM UTC.

Then an on-chain vote is started for raising validator key limits for those node operators that have submitted new deposit data on this day.

On Friday, Jul 16

4:00 PM UTC: the vote for raising validator key limits is executed and buffered Ether is deposited using the new deposit data.

After that, all new deposits will happen with the smart contract as withdrawal credentials, but it won't change the situation for 600-something thousands of ether already deposited.

Threshold withdrawal credentials drill

Between the 20th and 27th of July, we will run a threshold signature drill to make sure the respective key shards remain accessible. 8 out of our 11 key shard holders are available this week, and this is enough to check we still have the ability to sign withdrawal or key rotation messages when the time comes.

This drill was scheduled for June, but we had to postpone due to the fact we underestimated the difficulty of making modifications to the threshold signature software that would allow running the drill. Instructions for the drill will be published during the next week. We will have to run a second drill when the rest of the key shard holders will make themselves available to make sure nobody lost their shard (probably sometime in August).

Further steps

When withdrawals are available or a withdrawal credential rotation mechanism is introduced (e.g. like in thisproposal or a number of alternative ones), Lido will be able to rotate the threshold withdrawal credentials to smart contract withdrawal credentials, getting rid of this particular risk altogether.