stETH superuser functions

Superuser privileges and accounts

StETH token is the upgradable contract behindAppProxyUpgradeable proxy athttps://etherscan.io/address/0xae7ab96520de3a18e5e111b5eaab095312d7fe84 . Lido DAO can change the implementation with the successful DAO vote.

StETH can be stopped by the DAO vote. No operations changing stETH balances can be performed on the stopped contract:

1. transfer
2. call reverts;
3. No mints or burns can be performed. Note that StETH contract can mint stETH only in two cases: user deposits (tokens are minted to the depositor's address) or fee distribution (where tokens are minted in accordance to fee calculations to the addresses set in the contract — namely the DAO treasury, the insurance fund and the Node Operator's reward addresses);
4. Users can't submit their ETH to the Lido;
5. Oracle can't push updates on the Consensus Layer staking state;
6. No ETH buffered in Lido can be sent to the Ethereum deposit contract;
7. Staking withdrawals can't be performed.

Superuser roles

TODO: OutdatedBURN_ROLE

StETH contract specifies PAUSE_ROLE (address can pause the protocol) and BURN_ROLE (address can burn stETH tokens):

- ThePAUSE_ROLE
- assigned only to the DAO Voting contracthttps://etherscan.io/address/0x2e59a20f205bb85a89c53f1936454680651e618e
- TheBURN_ROLE
- assigned to theBurner
- contract with additional ACL parameters effectively allowing to burn stETH tokens only from the contract own balance. Tokens could be requested to burn only by direct request from the DAO Voting.

Note that there are other roles for DAO management, but they don't affect the token actions. These roles are MANAGE_FEE (set staking fee amount), MANAGE_WITHDRAWAL_KEY (set withdrawal credentials of the protocol), MANAGE_PROTOCOL_CONTRACTS_ROLE (set oracle contract address, set DAO treasury address to send fee to, set DAO insurance address to send fee to). The roles and addresses can be checked in the Aragon UIhttps://mainnet.lido.fi/#/lido-dao/permissions/app/0xae7ab96520de3a18e5e111b5eaab095312d7fe84

Oracle rebasing reports

StETH is a rebasable token. It receives reports from the Oracle contract (handleOracleReport method) with the state of the protocol's Consensus Layer validators balances, and updates all the balances of stETH holders distributing the protocol's total staking rewards and penalties. The protocol employs distributed Oracle reporting: there are five Oracle daemons running by the Lido Node operators, and the Oracle smart contract formats beacon report on the consensus of three of five daemon reports. On top of the consensus mechanics, there are sanity checks for reports with sudden drops in total Consensus Layer balance or rewards with higher-than-possible APY. Current Oracle contract ishttps://etherscan.io/address/0x442af784A788A5bd6F42A01Ebe9F287a871243fb . Note that: 1) DAO can set another address for the Oracle contact via vote; 2) Oracle implementation can change via vote.

Superuser privileges decentralization

The superuser privileges are managed by the Lido DAO's governance system. To enact any change the DAO has to have a successful vote.

Oracles are: 1) limited in impact 2) distributed - there are five of them, all top-tier professional node operators.

Superuser actions thresholds

The "superuser actions" with the StETH token are performed via DAO votes. The votes are managed by the Aragon voting. Voting power is proportional to the addresses' LDO token balance (https://etherscan.io/token/0x5a98fcbea516cf06857215779fd812ca3bef1b32). For the voting to pass successfully, it should:

1) get at least 5% of the total LDOs to be cast "for" the vote; 2) get at least 50% of votes cast "for" the vote. The voting duration is 72 hours.

There are five Oracle daemons running by the Lido Node operators, with 3 of 5 needed to agree on the data they provide. On top of the consensus mechanics, there are sanity checks for reports with sudden drops in total Consensus Layer balance or rewards with higher-than-possible APY.

Superuser keys management

Token management roles belong to smart contracts, and any changes in roles must pass through the successful DAO vote.

Oracle operators are: Stakefish, Certus One, Chorus One, Staking Facilities, P2P Validator.

Superuser keys generation procedure

There was no special keygen ceremony, as the permissions are managed by smart contracts. The votes can be cast by the EOAs and smart contracts with the voting power proportional to the addresses' LDO balance. Edit this page Previous AIP Next stETH on AAVE caveats