Intro

info Terms "validator", "key", "validator key", and "deposit data" have the same meaning within the document.

∑ TL;DR

Community Staking Module (CSM) is a permissionless staking module aimed at attracting community stakers to participate in Lido on Ethereum protocol as Node Operators. The only requirement to join CSM as a Node Operator is to be able to run validators (according to the Lido on Ethereum policies) and supply abond . The stake is allocated to the validator keys in the order in which the keys are provided, given the keys are valid. Thebond is not directly associated with the actual validator's stake but instead treated as a security collateral. Thebond is a characteristic of a Node Operator; hence, it is collateral for all Node Operator's validators. This allows for thebond reduction. The more validators the Node Operator has, the less thebond for one validator. Node Operators get their rewards from thebond rebase and from the Node Operator's portion of the staking rewards. Node Operator's portion of the staking rewards is socialized (averaged) if the validators perform above the threshold. Accumulated CL penalties resulting in a balance reduction below the deposit balance and stolen EL rewards are confiscated from the Node Operator'sbond . Node Operators should perform validator exits upon protocol request or can exit voluntarily.

Glossary

- Thestaking router
- (SR) is a smart contract within the Lido on Ethereum protocol that facilitates stake allocation and rewards distribution across different modules;
- Astaking module
- (SM) is a smart contract or a set of smart contracts connected to the staking router, which:* maintains the underlying operator and validator sets,
-
    - is responsible for on/off-boarding operators,
-
    - maintains validator deposits, withdrawals, and exits,
-
    - maintains fee structure and distribution for the module and participants, etc,
-
    - conforms to the IStakingModule interface;
- Bond
-
    - a security collateral that Node Operators must submit before uploading validator keys into CSM. This collateral covers possible losses caused by inappropriate actions on the Node Operator's side. Once the validator exits from the Beacon chain and all losses that occurred are covered, the collateral can be claimed or reused to upload new validator keys.
- TheLido DAO
- is a Decentralized Autonomous Organization that decides on the critical parameters of controlled liquid staking protocols through the voting power of governance token (LDO).
- ANode Operator
- (NO) is a person or entity that runs validators;
- Lido
- is a core contract of the Lido on Ethereum protocol that stores the protocol state, accepts user submissions, and includes the stETH token;
- stETH
- is an ERC-20 token minted byLido
- smart contract and representing a share of thetotalPooledEther
- ;
- Deposit data
- refers to a structure consisting of the validator’s public key and deposit signature submitted toDepositContract
- . This term can also be referred to askeys
- in the text. Validator private keys are created, stored, and managed by Node Operators exclusively;
- DepositContract
- is the official Ethereum deposit contract for validator deposits;
- DepositSecurityModule
- orDSM
- is a set of smart contract and off-chain parts mitigating thedeposit front-run vulnerability
- ;
- A validator is considered to be“unbonded”
- when the current Node Operatorbond
- is not sufficient to cover this validator;
- A validator is considered to be"stuck "

- if it has not been exited timely following an exit signal from the protocol;
- TheCurated module
- is the first Lido staking module previously referred to asNode Operators Registry
- ;
- Easy Track
- is a suite of smart contracts and an alternative veto-based voting model that streamlines routine DAO operations;
- Accounting Oracle
- is a contract which collects information submitted by the off-chain oracles about state of the Lido-participating validators and their balances, the amount of funds accumulated on the protocol vaults (i.e., withdrawal and execution layer rewards vaults), the number of exited and stuck validators, the number of withdrawal requests the protocol can process and distributes node-operator rewards and performsstETH
- token rebase;
- VEBO
- or Validators Exit Bus Oracle is a contract that implements an on-chain "source of truth" message bus between the protocol's off-chain oracle and off-chain observers, with the main goal of delivering validator exit requests to the Lido-participating Node Operators.

General info

CSM is a staking module offering permissionless entry with abond . This module aims to become a clear pathway for independentcommunity stakers (solo stakers or home stakers) to enter the Lido on Ethereum protocol (LoE) node operator set. Thebond requirement is an essential security and alignment tool that makes permissionless entry possible without compromising the security or reliability of the underlying staking protocol (LoE).

Module specifics

All staking modules should conform to the sameIStakingModule interface. That inevitably results in modules having a lot of common or similar components and logic. CSM is no exception here. For example, key storage components are based on the existingCurated module . However, several aspects are different and worth a separate mention.

Exited and Withdrawn

TheCurated module uses the "exited" statuses of the validator (bothSlashed and Exited andUnslashed and Exited) as the last meaningful status in accounting since, after this status, the validator is no longer responsible for any duties on the Beacon chain (except for the rare cases of the delayed sync committee participation). CSM, in turn, needs to know about each validator's exact withdrawal balance to decide onbond penalization. Hence, the module uses the "exited" counter reported by the accounting oracle only to return a correct number of "active" keys to the staking router and implements permissionless reporting methods to report the validator's withdrawal balance once the validator iswithdrawn .

Stake distribution queue

A Node Operator must supply abond to upload a new validator key to CSM. It is reasonable to allocate a stake in an order similar to thebond submission order. For this purpose, a FIFO (first in, first out)stake allocation queue is utilized. Once the Staking Router requests keys to make a deposit, the nextX keys from the queue are returned, preserving thebond submit order.

Alternative measures for "stuck" keys

The presence of "stuck" ("Delinquent" in theoriginal terms) keys for the Node Operator indicates theLido exit policy violation. In this case, a module should apply measures for the policy-violating Node Operator. CSM uses measures that are different from those of the curated module. The measures are described in the correspondingsection .

info Note: CSM does not apply any measures to "Delayed" validators mentioned in theLido exit policy .

Node Operator structure

The Node Operator data structure in CSM is similar to that of theCurated module , with several minor differences:

- Thename
- property is omitted as redundant for the permissionless module;
- TherewardAddress
- is used as a recipient of rewards and excessbond
- claims;
- A new property,managerAddress
- , is introduced. The Node Operator should perform method calls from this address;
- A new property,totalWithdrawnKeys
- , is introduced to count the total count of the withdrawn keys per Node Operator;

- A new property,depositableValidatorsCount
- , is introduced to count the current deposit data eligible for deposits;
- A new property,enqueuedCount
- , is introduced to keep track of the depositable keys that are in the queue. Also useful to determine depositable keys that are not in the queue at the moment;

Further reading

- Join CSM
- Rewards
- Penalties
- Validator exits

Guides

- Subscribing to events Edit this page Previous Lido IPFS applications Next Intro