Special thanks to @vbuterin, @fradamt for design ideas and to @djrtwo, @timbeiko, Vasiliy Shapovalov, Isidoros Passadis, Kelly Olson for feedback.

TLDR

: We propose a fungible and governance-free liquid staking derivative (LSD) compatible with solo validating. The LSD is secured via hardware-based slashing protection and enjoys higher capital efficiency than Lido's stETH.

Construction

We first describe a slashing-protection program P

running in trusted hardware such as Intel SGX. The program generates signing key pairs (pubkey, privkey)

such that privkey

is kept private within the secure enclave. Signing beacon blocks and attestations is done by the trusted hardware (which maintains a small and prunable database of previously-signed material) to protect against slashing.

We now describe the smart contract C

managing the staking derivative, which we denote sETH.

- minting

: The contract mints 31 sETH for every validator that sets C

as its withdrawal contract and provides a hardware attestation (a signed message verifiable onchain) that its keys were generated by P

. (Notice 32 staked ETH is backing 31 sETH, with 1 extra staked ETH acting as collateral.)

- ejections

: The contract ejects, upon receipt of a proof, validators that have a balance under 31.99 ETH (and have C

as withdrawal contract). A small reward (e.g. 0.1 sETH) incentivises triggering the ejection. (Ejections by withdrawal contracts require in-consensus support which is actively being worked on.)

- redemptions

: The contract operates a first-come-first-served queue for redemptions of sETH for ETH, similar to Lido's plans for redemptions. Redemption requests may trigger ejections as appropriate to withdraw liquid ETH from validators.

Security argument

We argue that every 1 sETH is backed by 1 ETH. There are only two types of validator penalties:

- slashing penalties

: This is prevented by the trusted hardware. Note that the hardware assumption can be hardened to an n

-of-n

assumption using an n

-of-n

secret-shared BLS signing key with the n

BLS key shares split across n

devices from different manufacturers.

- non-slashing penalties

: Validators enter the exit queue soon after their balance goes under 31.99 ETH. Since non-slashing penalties accrue slowly, the withdrawable validator balance (minus 0.1 ETH to cover the ejection incentive) will likely not go under 31 ETH (a value configurable to match protocol risk tolerance).

Advantages over Lido

- solo validation

: The design is friendly to untrusted solo validators, including small stakers validating from home.

- no governance

: The design does not require a governance token to manage a whitelist of operators.

- capital efficiency

: The design has a capital inefficiency of roughly 3% if 31 sETH is minted for every 32 ETH validator. Lido has roughly 10% capital inefficiency from delegation fees—5% operator fees, 5% Lido fees.

- no cartelisation risk

: The design does not require delegation to operators which may cartelise. This reduces exposure to social slashing.

- decentralisation ethos

: The design improves alignment with Ethereum's decentralisation ethos.

The fundamental tradeoff suffered by the design is the reliance on the n

-of-n

hardware assumption. Unfortunately, Intel SGX may currently be the only secure hardware platform with externally-verifiable attestations.

Productive vs non-productive sETH

As described above, sETH is a non-productive LSD redeemable for the principal of participating validators. Such non-productive LSDs are sufficient for use cases such as leveraged staking, exposure to staking rewards without exposure to ETH, as well as early liquidity prior to clearing the exit queue.

If desired, the design can be modified to make sETH a productive asset with exposure to staking rewards, similar to Lido's stETH. This can be done for consensus-layer rewards by having validators cover for any sub-optimal performance using the extra staked ETH collateral. This can also be done for transaction fees and MEV with in-consensus MEV smoothing.