Many thanks to Justin for inspiration and Drew, Domothy, Barnabe, and Amir for feedback.

TLDR:

Requiring node operators to pay upfront to run validators can improve permissionless liquid staking protocols.

Context:

Permissionless Liquid Staking Protocols (LSPs) like Rocketpool require node operators (NoOps) to put up capital to run validators whereas permissioned LSPs like Lido do not and instead rely on governance to whitelist professional NoOps. While the former is better for Ethereum's economic security and decentralization, the latter's capital efficiency allows it to out-scale others to the point where it is close to surpassing a major consensus threshold and threatens to eventually become Ethereum's governance.

EIP-7514 helps to slow this problem with minimal changes but an enshrined solution is still being researched e.g.Dankrad's article and Mike's article. In the meantime, improving the competitiveness of permissionless LSPs is a another way to slow Lido's growth. We propose "Smoothing Commitments" as an out-of-protocol solution for the following problems permissionless LSPs face:

- Rug-Pooling as coined by Justin Drake where NoOps steal MEV from stakers.
- NoOps with poor validator performance will produce less LST rewards.
- A tendency towards cartelization via profitability standards.
- Long validator queues and low churn rates stunt the growth of new LSPs.

Construction:

Assume node operators lock C

ETH collateral which can serve as tier 1 capital in enshrined designs or be combined with 32 - C

ETH with today's specs.

The NoOps pay the LSP a non-refundable Smoothing Commitment

(SC) to borrow ETH to run a validator for a minimum duration, e.g., M=1

months. If the NoOp's SC expires before being renewed, their validator is exited from the beacon chain and C

is returned, adjusted for penalties.

In exchange, the NoOp receives 100\%

of the consensus and execution rewards earned by their validator. The SC can be priced via an auction, where a NoOp's bid expresses "I am willing to pay this much to work for M

months."

Example:

If a NoOp expects a 10\%

profit margin and bids 0.90

ETH then they are expecting their validator to earn 1

ETH over the next M

months. The NoOp locks C

ETH collateral and pays LST holders 0.90

ETH of rewards upfront to borrow 32

ETH to launch a validator. Assuming the NoOp does not extend their commitment duration by rebidding, their validator is ejected after M

months and they get back C - P

ETH, where P

is the penalties they've accrued.

Advantages:

- Good NoOp incentives:

NoOps who paid SCs cannot recoup their initial payment unless they perform as well as the average expected validator, incentivizing for excellent long-term performance.

- MEV-autonomy:

NoOps retain 100\%

of their MEV, eliminating the need to police rug-pooling or enforce an MEV strategy.

- Decoupled rewards

: The LST's rewards depend on how many SCs are paid rather than validator performance, i.e., LST holders earn whenever a validator joins or renews their SC.

- Resists Cartelization:

SCs help address a concern where profitability standards automatically cartelize permissionless LSPs. By allowing MEV-autonomy and decoupling validator performance from LST rewards, nodes can choose non-profit-maximizing MEV strategies without being ejected for underperforming.

- Fast growth:

Since SCs can constitute months of rewards upfront, new permissionless LSPs can quickly grow and compete, even during extended validator queues.

- Simple:

SCs are straightforward and do not require changes to consensus to implement.

- Compatible:

SCs can be incorporated into LSPs that leverage DVT /anti-slashers, incorporated into future enshrined solutions, and is compatible with MEV-burn.

- Restaking:

LSPs that engage in restaking can price restaking rewards into their SCs.

Disadvantages:

- New:

Despite their similarity to T-Bills, SCs are new and require education.

- Less Forgiving:

NoOps that need to exit early must forfeit their SC.

- Growth risk:

SC dynamics could cause an LSP to grow too quickly.

Open Questions:

- Which auction format is most desirable?
- Does this introduce new centralization vectors?
- Can this mechanism also improve permissioned LSPs?