Please read this informative post from @skozin (especially part d!) before reading the rest of this document.

We propose a new system for mitigating the frontrunning deposit issues that does not require stETH holders to trust the Lido Oracle.

The problem

Here's a quick summary of the problem itself.

When stETH minters deposit their ETH into Lido, they are immidiately minted a corresponding amount of stETH. When the deposited ETH is eventually deposited into the consensus layer deposit contract, in order to ensure the withdrawal credentials of the consensus layer deposit are, in fact, pointed to the Lido contracts, stETH holders rely on a trusted Lido Oracle to verify that a previous deposit with the pending deposit's public key doesn't exist (see this here). This is done through reaching a signature quorum of the Lido Oracle guardians certifying the current merkle root in the consensus layer deposit contract.

Once the Oracle has certified exclusion from the merkle root, the deposit is initiated and the ETH previously deposited into Lido is staked. The issue here arises if the Lido Oracle maliciously certifies a deposit to a validator who has already deposited. Then, some non-Lido entity has control over the 32 ETH deposit's withdrawal credentials, meaning that stETH is no longer backed 1:1 by ETH on the beacon chain.

It is important to note a couple facts before proceeding:

1. This system requires stETH holders to trust the Lido Oracle to keep the backing of stETH and not steal all pending ETH deposits into Lido.

2. The oracle is currently and 4 out of 6 multisig approved by the Lido DAO (as of June 18th, 2022).

3. There is an ability to pause deposits if a guardian provides a signature to do so, however this still requires stETH holders to trust 1 of the 6 guardians to pause deposits when needed.

Although the Lido DAO approval is a good security measure, it isn't equivalent to stETH holders having to trust the DAO itself.

The trustless solution

Description

The new system we propose is an extension of the current system that does not require stETH holders to trust that the Lido Oracle will not steal all pending deposits and "unback" stETH. In addition, the stETH holders just need to assume that 1 cryptoeconomically incentivised watcher (which they can run!) is watching the system rather than assuming that 1 of the 6 guardians is watching.

At the core of the new, proposed system is a idea of a rainy day fund

(RDF). In the new system, the Lido contracts do not allow more than the balance of the RDF to be deposited into the consensus layer deposit contract per day. Ether is still sent to the deposit contract optimistically after a quorum of guardians is reached, but, now, anyone can submit a fraud proof on chain proving that there was a previous deposit corresponding to a certain public key that the Lido Oracle certified within a day of the malicious deposit. Note that this fraud proof is simply a valid merkle proof of the previous deposit against the deposit root certified by the Lido Oracle.

If a valid fraud proof is submitted, the Lido deposit flow is stalled and requires DAO intervention. The DAO must ban the signing guardians and malicious stakers as neccesary. The submitter of the fraud proof should also be rewarded a small amount more than the fee paid for the fraud proof transaction to cryptoeconomically incentivise them to do so. In addition, the fraud proof contracts should withdraw 32 ETH from the RDF for every fraudulent deposit and either:

1. Allow stETH holders to redeem the ETH at the correct, yield adjusted ratio

2. Wait until the system is up and running again and deposit the ETH into the deposit contract

Another option is to completely get rid of the RDF and purely dilute LDO enough to swap for ETH and then proceed with one of the options. This system would require LDO holders to take on risk by trusting the oracle and thus to possibly be compensated for doing so.

Fraud proof windows and RDF backing

To be precise, the reason a 1 day fraud proof window is required is to be resistant to Ethereum censorship attacks. If fraud proofs are censored, malicious deposits will not be accounted for in the Lido contracts, leading to the "unbacking" of stETH. This is precisely the reason that the RDF needs to hold 1 day's worth of deposits. Since fraud proofs can arrive 1 day late, the Lido Oracle could have been certifiying invalid deposits for a day. Thus, the RDF needs to be able to provide enough funds to compensate for the sum of the value of all malicious deposits the Lido Oracle could have certified during the day, which is just the maximum amount allowed to be deposited from Lido per day.

We, personally, believe the fraud proof window can theoretically be reduced down to 1 hour or 30 minutes as followed by Nomad. This would only require the RDF to hold the maximum amount allowed to be deposited by Lido in 1 hour or 30 minutes, which increases capital efficiency. Of course, this reduction is at the cost of tolerance to the base layers censorship resistance properties.

Final thoughts

The new system has some implementation complexity as the fraud proof system needs to be built. Although the fraud proofs themselves are not very complex, the integration with the rest of the system may be more so. On the other hand, we believe such a system would be important for reducing trust assumptions for stETH holders.

-bbuddha, toowoundup