Additional risks due to stETH

Counterparty risk

Any additional smart contract exposes us to counter party risk, more specifically:

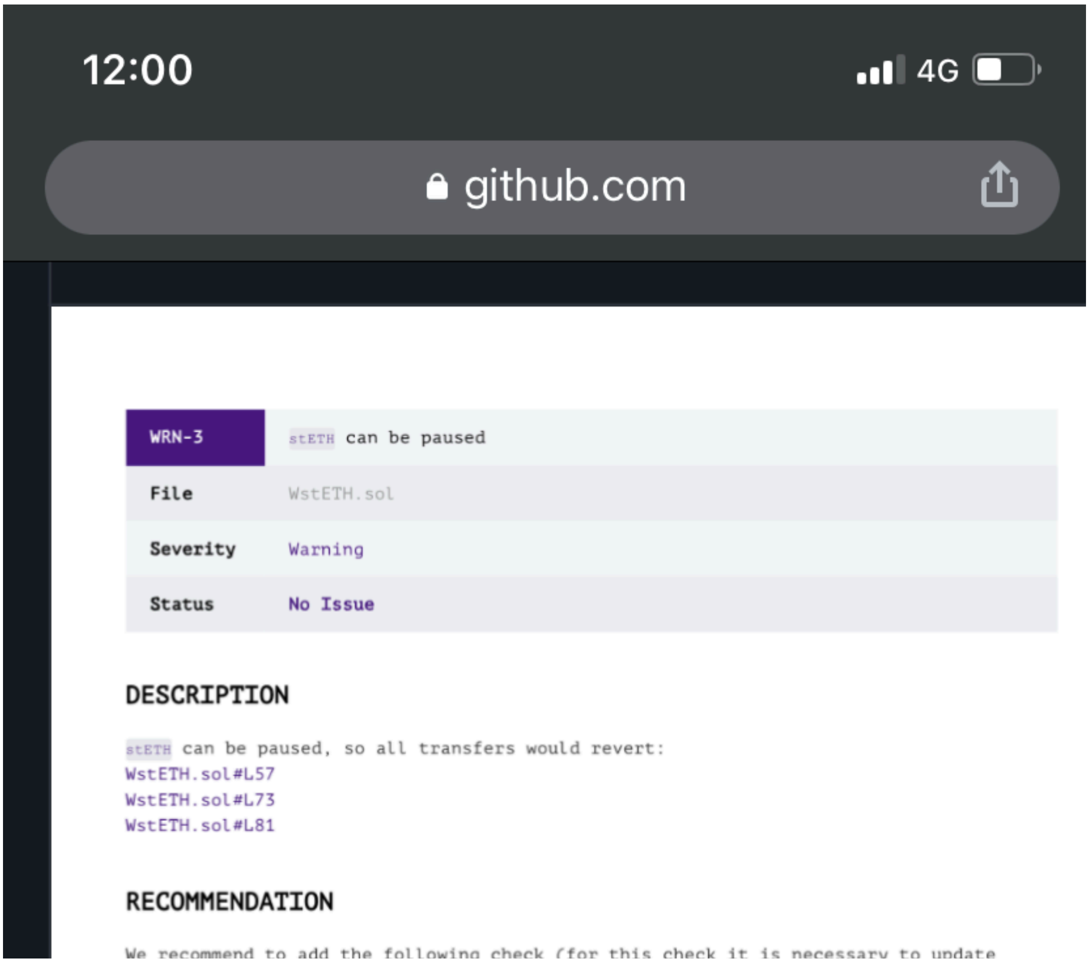
- can any update be performed?
- Who can perform the updates?
- Are there additional risks involved with the system, the configuration and the potential updates to it?

Primer: https://help.lido.fi/en/articles/5230603-what-are-the-risks-of-staking-with-lido#:~:text=Users%20risk%20an%20exchange%20price,entirely%20to%20the%20extent%20possible.

Audits:

https://github.com/lidofinance/audits

Pause = bricked



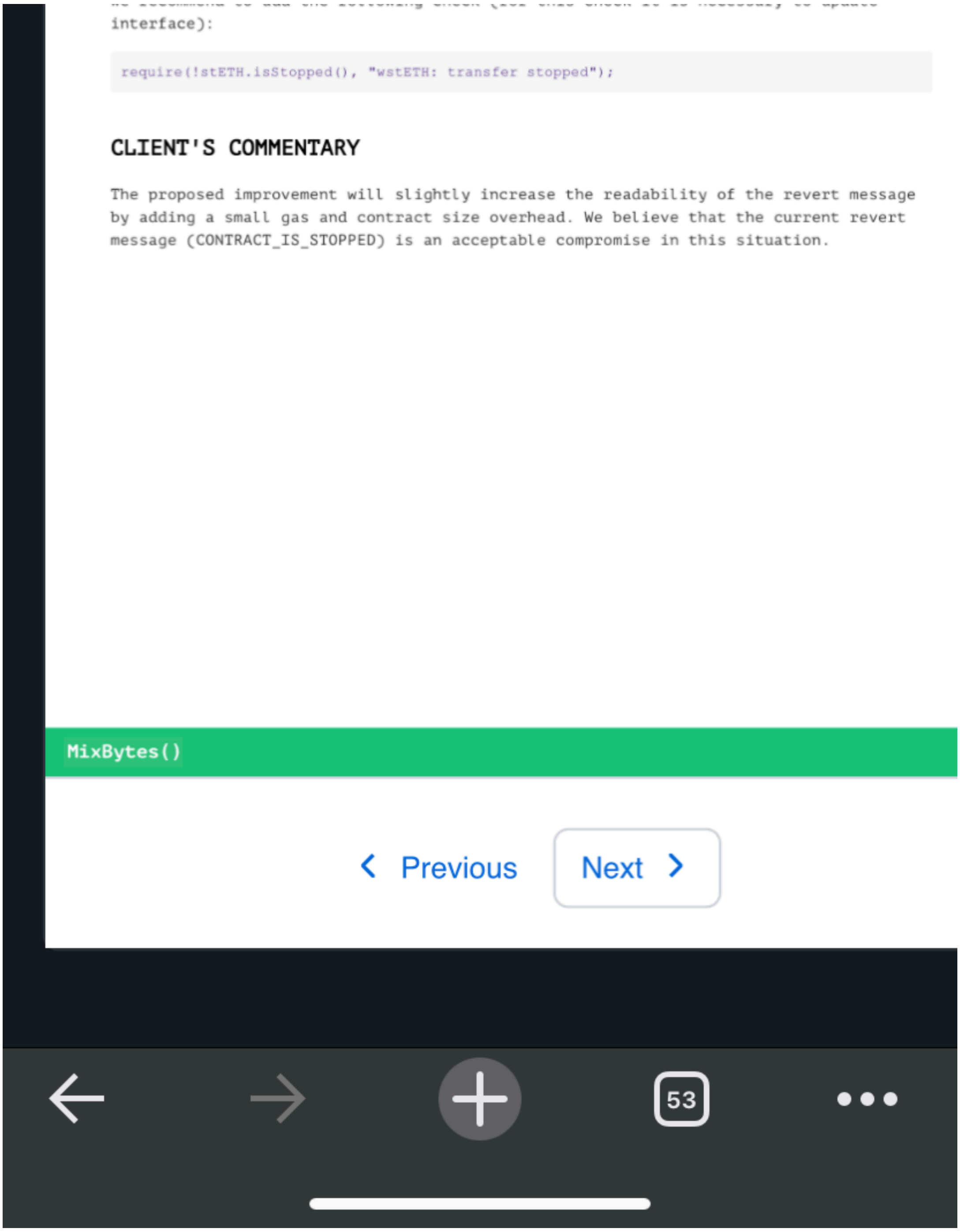
WRN-3	stETH can be paused
File	WstETH.sol
Severity	Warning
Status	No Issue

DESCRIPTION

stETH can be paused, so all transfers would revert:
WstETH.sol#L57
WstETH.sol#L73
WstETH.sol#L81

RECOMMENDATION

We recommend to add the following check (for this check it is necessary to update



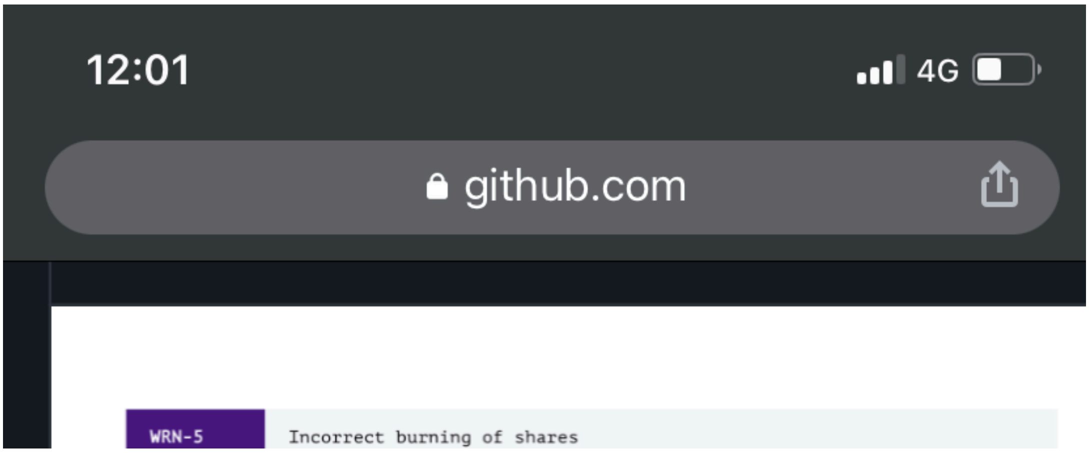
We recommend to add the following check (for this check it is necessary to update interface):

```
require(!stETH.isStopped(), "wstETH: transfer stopped");
```

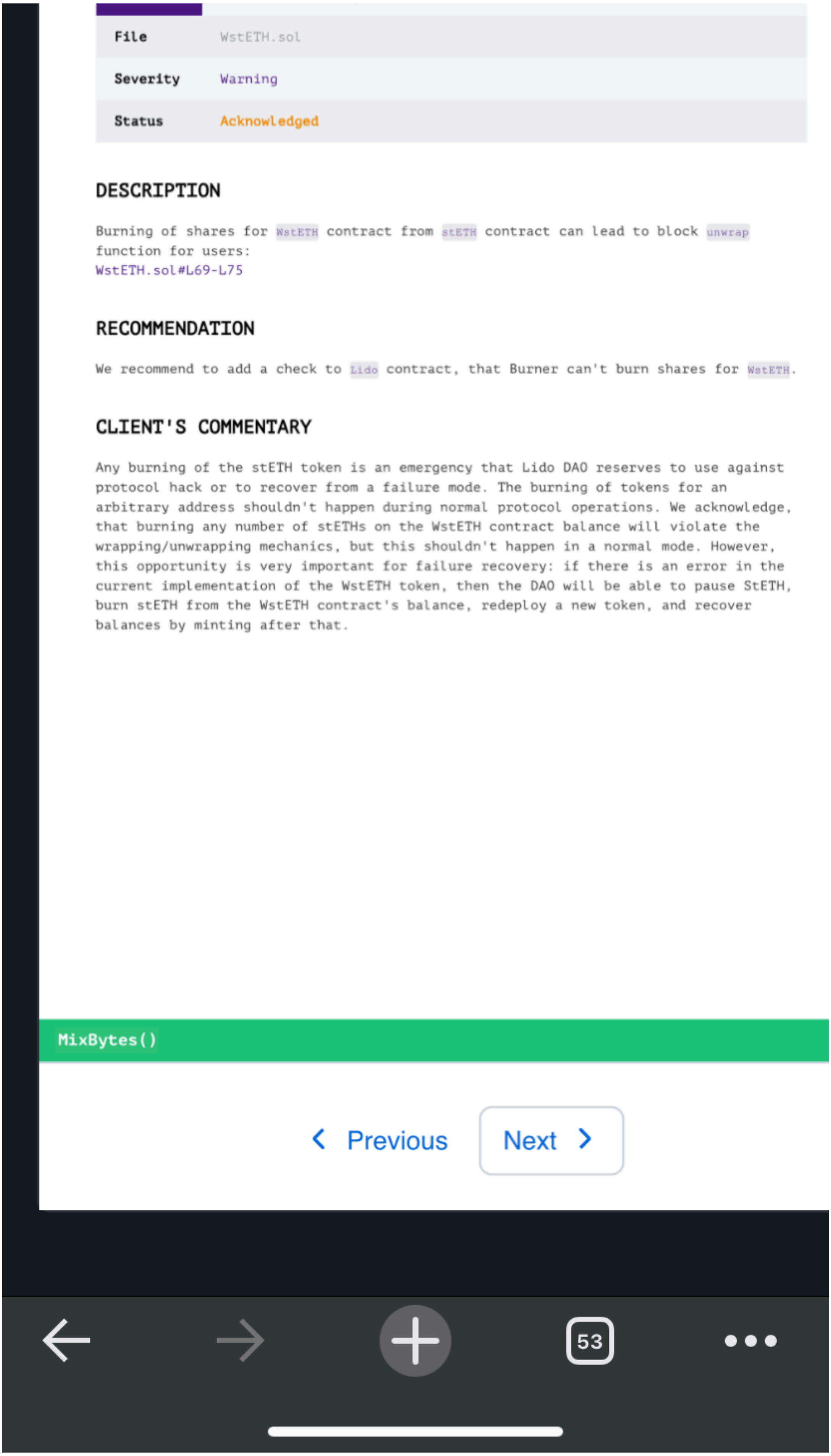
CLIENT'S COMMENTARY

The proposed improvement will slightly increase the readability of the revert message by adding a small gas and contract size overhead. We believe that the current revert message (CONTRACT_IS_STOPPED) is an acceptable compromise in this situation.

Burning = risk of depeg



WRN-5 Incorrect burning of shares



File	WstETH.sol
Severity	Warning
Status	Acknowledged

DESCRIPTION

Burning of shares for `WstETH` contract from `stETH` contract can lead to block `unwrap` function for users:
WstETH.sol#L69-L75

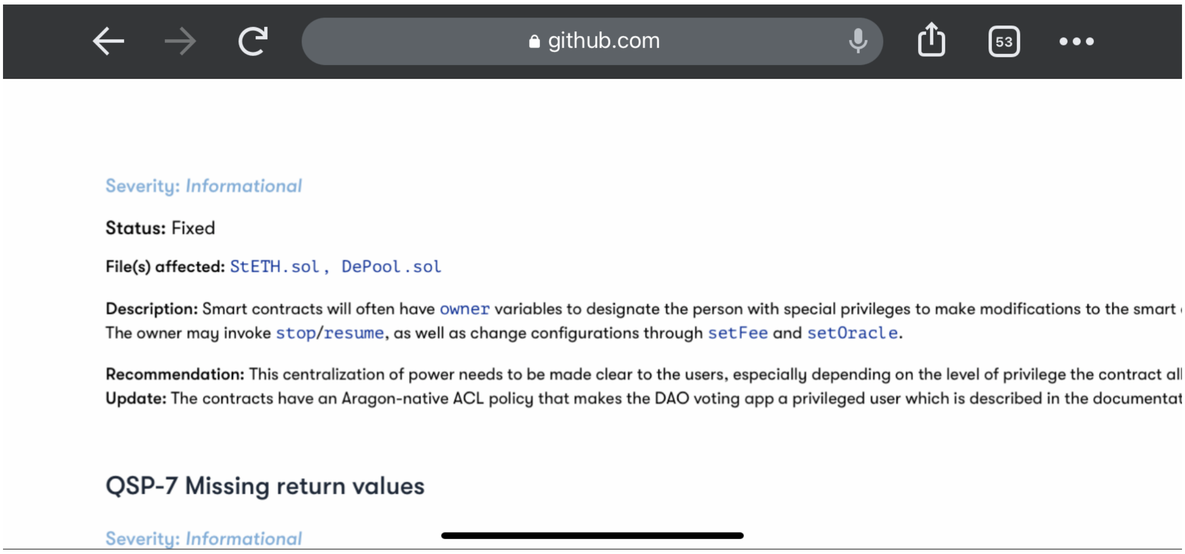
RECOMMENDATION

We recommend to add a check to `Lido` contract, that Burner can't burn shares for `WstETH`.

CLIENT'S COMMENTARY

Any burning of the stETH token is an emergency that Lido DAO reserves to use against protocol hack or to recover from a failure mode. The burning of tokens for an arbitrary address shouldn't happen during normal protocol operations. We acknowledge, that burning any number of stETHs on the WstETH contract balance will violate the wrapping/unwrapping mechanics, but this shouldn't happen in a normal mode. However, this opportunity is very important for failure recovery: if there is an error in the current implementation of the WstETH token, then the DAO will be able to pause StETH, burn stETH from the WstETH contract's balance, redeploy a new token, and recover balances by minting after that.

Further admin privileges at the stETH contract



Severity: *Informational*

Status: Fixed

File(s) affected: `StETH.sol`, `DePool.sol`

Description: Smart contracts will often have `owner` variables to designate the person with special privileges to make modifications to the smart
The owner may invoke `stop`/`resume`, as well as change configurations through `setFee` and `setOracle`.

Recommendation: This centralization of power needs to be made clear to the users, especially depending on the level of privilege the contract all
Update: The contracts have an Aragon-native ACL policy that makes the DAO voting app a privileged user which is described in the documentat

QSP-7 Missing return values

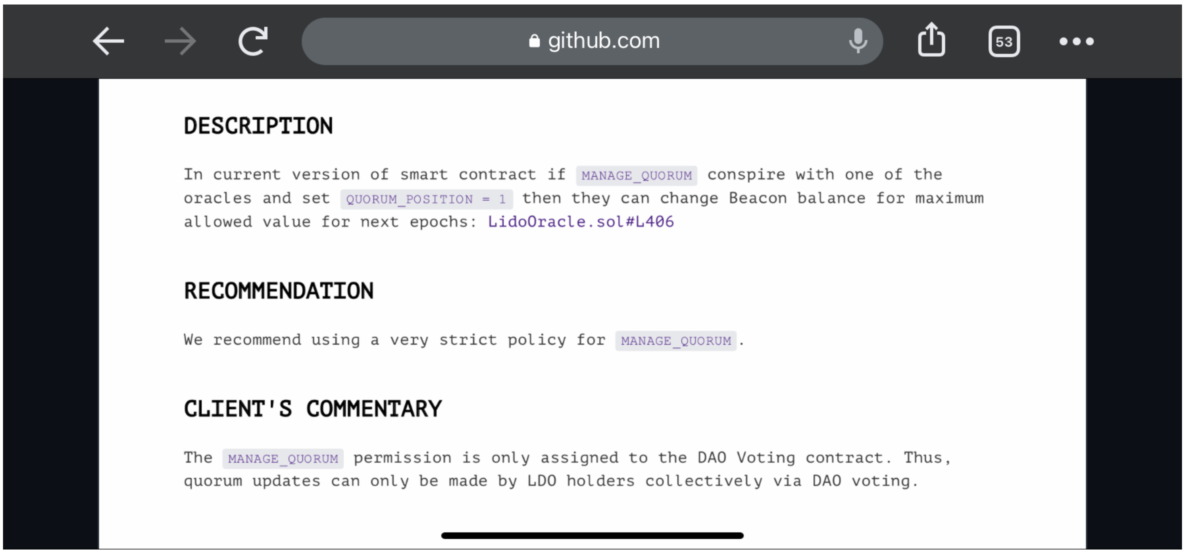
Severity: *Informational*

TODO: Verify this audit was fixed as they claimed they would have

lidofinance/**audits**

audits/QSP Lido Report 12-2020.pdf at main · lidofinance/audits
github.com

Additional governance risk



DESCRIPTION

In current version of smart contract if `MANAGE_QUORUM` conspire with one of the oracles and set `QUORUM_POSITION = 1` then they can change Beacon balance for maximum allowed value for next epochs: LidoOracle.sol#L406

RECOMMENDATION

We recommend using a very strict policy for `MANAGE_QUORUM`.

CLIENT'S COMMENTARY

The `MANAGE_QUORUM` permission is only assigned to the DAO Voting contract. Thus, quorum updates can only be made by LDO holders collectively via DAO voting.

Decentralization profile

An additional counter party can create further questions as for what concerns a fully autonomous system

The counter party may cause the system to break or have privileges access to grief attacks.

The mechanics pertaining to they degree of privilege and how it can be exploited require nuance and depend on the specifics of the implementation

Liquidation profile

The main risk when it comes to liquidating a derivative that is not WETH has to do with the additional risks that a liquidator is taking

Specifically:

- Accessibility risk
- discounts, premiums or queues

More specifically we'd need to figure out if any limitation in terms of a cap on mintable or refer ama le tokens is available.

This naturally reflects in a discount that is indicative of the risks and lack of availability

The withdrawal queue

Withdrawals in Shangai are limited to 40k per day in total, napkin math would put the maximum value at 20k (50%) of eth liquidity available per day

This could cap the size of willing liquidator, although we have yet to see the specific behavior in which withdrawals would be built.

Ultimately any additional fee creates attrition and any delay (enforcing even one block before redeeming stETH into ETH) can be an additional risk that will reduce the willingness of liquidators to take the risk

Oracle risk

The usage of a stETH token implies a peg which may or may not be close to 1 based on additional risks as well as economic incentives

Pricing in these adds additional complexity to the oracle, and opens up to specific new risks, for example view Reentrancy which derives from using curve based oracles

For the sake of PM it would be best to assume that a change in collateral will require an additional round of coding, testing and reviewing of the Oracle Code.

Additional PM considerations

Oracles as mentioned above

New risk factors after liquidity cognizant backtest

The main risk is that the additional complexities end up creating a system that is effectively at the same level of capital efficiency after taking fees and reduced ICR in mind

Liquidity simulation initial thoughts

Brute force crv prices to demonstrate price
Impact based on CDP size

We'd expect curve to hold well but also to demonstrate a bound in terms of actually liquify stETH to ETH that is available to an ETH denominated MM