STATE
MIND

V2 deployment validation

05-05-2023 - 10-05-2023

Table of contents

1. Project Brief

Title	Description
Client	Lido
Project name	V2 deployment validation
Timeline	05-05-2023 - 10-05-2023
Initial commit	e45c4d6fb8120fd29426b8d969c19d8a798ca974, 7e9704d9f40cd17652480a15f2ca9519d6b532d2, a19c6b7e2d661de12e2ba585c251c8d70a1da230
Final commit	e45c4d6fb8120fd29426b8d969c19d8a798ca974, 7e9704d9f40cd17652480a15f2ca9519d6b532d2, a19c6b7e2d661de12e2ba585c251c8d70a1da230

Short Overview

Lido has requested Statemind to validate the deployment of their V2 contracts.

The purpose of the validation is to ensure that the deployed contracts' sources match the audited commit and that the contracts are configured correctly according to the reference docs.

The deployment consists of three main parts:

- Lido's main contracts: lidofinance/lido-dao.
- GateSeals contracts: lidofinance/gate-seals.
- ShapellaUpgradeTemplate contract: lidofinance/scripts.

Reference commits and audit reports

Repository	Commit	Audit Report
lido-dao	e45c4d6fb8120fd29426b8d969c19d8a798ca974	2023-04-28
gate-seals	7e9704d9f40cd17652480a15f2ca9519d6b532d2	2023-04-20
ShapellaUpgradeTemplate	a19c6b7e2d661de12e2ba585c251c8d70a1da230	2023-05-10

Project Scope

The audit covered the following files:

- SignatureUtils.sol
- ECDSA.sol
- MinFirstAllocationStrategy.sol
- LegacyOracle.sol
- Lido.sol
- Versioned.sol
- SigningKeys.sol
- Packed64x4.sol
- OssifiableProxy.sol
- OracleDaemonConfig.sol
- WithdrawalQueueBase.sol
- ValidatorsExitBusOracle.sol
- HashConsensus.sol
- WithdrawalQueue.sol
- AccessControlEnumerable.sol
- Versioned.sol
- UnstructuredRefStorage.sol
- Math.sol
- LidoExecutionLayerRewardsVault.sol
- WithdrawalQueueERC721.sol
- StakingRouter.sol
- GateSealFactory.vy
- ShapellaUpgradeTemplate.sol
- Math256.sol
- MemUtils.sol
- NodeOperatorsRegistry.sol
- StETH.sol
- Pausable.sol
- StETHPermit.sol
- StakeLimitUtils.sol
- WstETH.sol
- WithdrawalVault.sol
- Burner.sol
- AccountingOracle.sol
- BaseOracle.sol
- OracleReportSanityChecker.sol
- PausableUntil.sol
- AccessControl.sol
- DepositSecurityModule.sol
- UnstructuredStorage.sol
- PositiveTokenRebaseLimiter.sol
- EIP712StETH.sol
- BeaconChainDepositor.sol
- LidoLocator.sol
- GateSeal.vy

2. Conclusion

All deployments have been successfully validated, meaning that:

- All audited commits match the deployed contracts fully.
- All default configurations are correct.
- The contracts are ready for upgrade.

Validated commits and audit reports

Repository	Final validated commit	Audit Report
lido-dao	e45c4d6fb8120fd29426b8d969c19d8a798ca974	2023-04-28
gate-seals	7e9704d9f40cd17652480a15f2ca9519d6b532d2	2023-04-20
ShapellaUpgradeTemplate	a19c6b7e2d661de12e2ba585c251c8d70a1da230	2023-05-10

Deployment

File name	Contract deployed on mainnet
DummyEmptyContract.sol	0x6F6541C2203196fEeDd14CD2C09550dA1CbEDa31
OssifiableProxy.sol (LidoLocator)	0xC1d0b3DE6792Bf6b4b37EccdcC24e45978Cfd2Eb
OssifiableProxy.sol (AccountingOracle)	0x852deD011285fe67063a08005c71a85690503Cee
OssifiableProxy.sol (ValidatorsExitBus)	0x0De4Ea0184c2ad0BacA7183356Aea5B8d5Bf5c6e
OssifiableProxy.sol (StakingRouter)	0xFdDf38947aFB03C621C71b06C9C70bce73f12999
OssifiableProxy.sol (WithdrawalQueue)	0x889edC2eDab5f40e902b864aD4d7AdE8E412F9B1
DepositSecurityModule.sol	0xC77F8768774E1c9244BEed705C4354f2113CFc09
OracleReportSanityChecker.sol	0x9305c1Dbfe22c12c66339184C0025d7006f0f1cC
OracleDaemonConfig.sol	0xbf05A929c3D7885a6aeAd833a992dA6E5ac23b09
EIP712StETH.sol	0x8F73e4C2A6D852bb4ab2A45E6a9CF5715b3228B7

File name	Contract deployed on mainnet
Burner.sol	0xD15a672319Cf0352560eE76d9e89eAB0889046D3
HashConsensus.sol (AccountingOracle)	0xD624B08C83bAECF0807Dd2c6880C3154a5F0B288
HashConsensus.sol (ValidatorExitBus)	0x7FaDB6358950c5fAA66Cb5EB8eE5147De3df355a
LidoLocator.sol	0x1D920cc5bACf7eE506a271a5259f2417CaDeCE1d
AccountingOracle.sol	0xF3c5E0A67f32CF1dc07a8817590efa102079a1aF
ValidatorsExitBus.sol	0xA89Ea51FddE660f67d1850e03C9c9862d33Bc42c
StakingRouter.sol	0xD8784e748f59Ba711fB5643191Ec3fAdD50Fb6df
WithdrawalQueueERC721.sol	0xE42C659Dc09109566720EA8b2De186c2Be7D94D9
WithdrawalVault.sol	0xCC52f17756C04bBa7E377716d7062fC36D7f69Fd
LegacyOracle.sol	0xa29b819654cE6224A222bb5f586920105E2D7E0E
NodeOperatorsRegistry.sol	0x8538930c385C0438A357d2c25CB3eAD95Ab6D8ed
Lido.sol	0x17144556fd3424EDC8Fc8A4C940B2D04936d17eb
GateSealFactory.vy	0x6c82877cac5a7a739f16ca0a89c0a328b8764a24
GateSeal.vy (blueprint)	0xEe06EA501f7d9DC6F4200385A8D910182D155d3e
GateSeal.vy (instance)	0x1aD5cb2955940F998081c1eF5f5F00875431aA90
ShapellaUpgradeTemplate.sol	0xa818fF9EC93122Bf9401ab4340C42De638CD600a

STATE
MIND