CONTESTS LEADERBOARDS

Connect

Tokemak

Generating sustainable liquidity for the tokenized world. Eliminating inefficiencies and helping LPs to deploy liquidity where it can be the most work is exactly why we are building Tokemak v2!

Context Q&A

On what chains are the smart contracts going to be deployed?

Mainnet

Which ERC20 tokens do you expect will interact with the smart contracts?

- TOKE: 0x2e9d63788249371f1DFC918a52f8d799f4a38C94
- WETH: 0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2
- CRV: 0xD533a949740bb3306d119CC777fa900bA034cd52
- CVX: 0x4e3FBD56CD56c3e72c1403e103b45DB9da6B6668
- LDO: 0x5A98FcBEA516CF06857215779Fd812CA3beF1B32
- BAL: 0xba100000625a3754423978a60c0317c58a424e3D
- AURA: 0xC0c293ce456fFE0fDEfDA2f9f8dB2BD2A6602032

Liquid Staking Tokens

- stETH: 0xae7ab96520DE3A18E5e111B5EaAb095312D7fE84
- wstETH: 0x7f39C581F595B53c5cb19bD0b3f8dA6C935E2Ca0
- rETH: 0xae78736Cd615f374D3085123A210448E74Fc6393
- cbETH: 0xBe9895146f7AF43049ca1c1AE358B0541Ea49704
- frxETH: 0x5E8422345238F34275888049021821368D8BC9f
- sfrxETH: 0xac3E018457B222d93114458476f3E3470B68e3BF
- swETH: 0f951B330fa7b289233dc249e82926f7fb2CF26b78

Curve Pools

- Curve stETH/ETH: 0x06325440D014e39736583c165C2963BA99faf14E
- Curve stETH/ETH ng: 0x21E27a5E5513D6e65C4f830167390997bA8A83Da
- Curve stETH concentrated: 0x828b154032950C8d7f2bB6B183723b3b898056
- Curve stETH/wstETH: 0x4d9f50c103011bC6e9F77210b8999659f760F83B
- Curve rETH/ETH: 0x9c3B46C8bf1a890F9c46c6dF617C26c5F1bC19C
- Curve rETH/wstETH: 0x447DabE8f95c6fE1fFc5e7b05b5bAF7675C3B8
- Curve rETH/frxETH: 0x0Ab5c73799A2B6c1f75265E5b7E5540B3d0DeBF1
- Curve cbETH/ETH: 0x5FA0359b2243A4d9539B9c72cA8bc354c39fC8
- Curve cbETH/frxETH: 0x548E063CB6F3Bw231457b4154e2345286274257
- Curve frxETH/ETH: 0x4132f1935C781E5cufa4f42041F3678647365C7A
- Curve swETH/ETH: 0xe42BAC0c2D7A13Vb5b165FBBd7b4b8778fb30A

Balancer Pools

- Balancer wstETH/WETH: 0x32296969Ef14B8D6c2969C550D4a0449130230
- Balancer wstETH/sfrxETH/ETH: 0x5aFe7a99f86860377DE9b8B8861691b5D0caf6
- Balancer wstETH/rETH: 0x9c6b47ff73e0F5B51B5F75333b43F5f5C3758F2
- Balancer rETH/WETH: 0x1E19CF2D73a72Ef1332C882f20534B6519Bw0276

Maverick Pools

- Maverick ETH/swETH boosted: 0xf97f7FB742C5309b8B5cfb7B4b42c77713aec92c

Note: for LP positions that are staked at Convex/Aura there is an associated Convex/Aura ERC20 token that wraps the Curve LP token and is staked. If Tokemak stakes at Convex/Aura, we do not directly hold the ERC20, but rather wrap and stake in a single function.

Which ERC721 tokens do you expect will interact with the smart contracts?

None

Which ERC777 tokens do you expect will interact with the smart contracts?

None

Are there any FEE-ON-TRANSFER tokens interacting with the smart contracts?

None

Are there any REBASING tokens interacting with the smart contracts?

Yes, stETH (Lido Staked Ether)

Are the admins of the protocols your contracts integrate with (if any) TRUSTED or RESTRICTED?

RESTRICTED

Is the admin/owner of the protocol/contracts TRUSTED or RESTRICTED?

TRUSTED

Are there any additional protocol roles? If yes, please explain in detail:

Yes, Tokemak-V2 has a centralized controller with specified roles. The roles are listed here: https://github.com/Tokemak/v2-contracts/blob/63445b6ce33859116342c86ac6f1696427b721693b/src/libs/Roles.sol

Is the code/contract expected to comply with any EIPs? Are there specific assumptions around adhering to those EIPs that Watsons should be aware of?

src/vault/LMPVault.sol should be 4626 compatible

Please list any known issues/acceptable risks that should not result in a valid finding.

- Off-chain mechanisms listed in subsequent section are expected to be online and execute within their expected frequency
- The LMPStrategy.verifyRebalance() referenced in the LMPVault, and in the LMPDebt lib used by the vault, is expected to only return true when the rebalance is favorable for the vaultAssets.

Please provide links to previous audits (if any).

NA

Are there any off-chain mechanisms or off-chain procedures for the protocol (keeper bots, input validation expectations, etc)?

Yes, there are several off-chain mechanisms

1. LMPVault
   1. updateDebtReporting - initiated externally, but unprivileged operation
   2. rebalance/flashRebalance - initiated externally and is restricted to an allowlist, but LMPStrategy's fully validate the proposed actions.
2. Stats - all stats contracts must have snapshots initiated by a keeper network at on-chain enforced intervals. With the exception of `BaseStatsCalculator.snapshot()` these can be done in an unprivileged manner. `BaseStatsCalculator.snapshot()` requires that snapshots are taken at randomized intervals, so is done by a privileged operator. More details can be found in Stats High Level Docs and Calculator Docs. (TODO update links to hash)
3. src/beacon/PreBeaconChainBacking - will be written to by a protected off-chain component
4. src/liquidation/LiquidationRow - claimVaultRewards() and liquidateVaultsForTokens() will be initiated by protected off-chain components.

In case of external protocol integrations, are the risks of external contracts pausing or executing an emergency withdrawal acceptable? If not, Watsons will submit issues related to these situations that can harm your protocol's functionality.

Pausing or emergency withdrawals are not acceptable for Tokemak.

Do you expect to use any of the following tokens with non-standard behaviour with the smart contracts?

Upgradeable: stETH (wstETH by proxy) and cbETH

Add links to relevant protocol resources

README's in the repo should provide further context.

Commit and exclude contracts:
https://tokemak.notion.site/Audit-2023de2131f452a0e3a1fa616ae7ef?pvs=4

Status: **RUNNING**

TOTAL REWARDS
216,200 USDC

Contest Pool	144,000 USDC
Lead Senior Watson	58,000 USDC
Judging Pool	7,100 USDC
Lead Judge	7,100 USDC

LEAD SENIOR WATSON
xiaoming90

LEAD JUDGE
Trumpero

STARTED
Jul 17, 2023 00:00 PDT

ENDS
Aug 29, 2023 00:00 PDT

Connect your wallet to join this contest

Scope

Tokemak/v2-core-audit-2023-07-14

```
src/
├── SystemComponent.sol
├── SystemRegistry.sol
├── access/
│   └── OwnableStep.sol
├── beacon/
│   └── PreBeaconChainBacking.sol
├── destinations/
│   ├── DestinationRegistry.sol
│   ├── adapters/
│   │   ├── BalancerBeethovenAdapter.sol
│   │   ├── CurveV2FactoryCryptoAdapter.sol
│   │   ├── MaverickAdapter.sol
│   │   ├── rewards/
│   │   │   ├── AuraRewardsAdapter.sol
│   │   │   ├── ConvexRewardsAdapter.sol
│   │   │   ├── MaverickRewardsAdapter.sol
│   │   │   └── RewardAdapter.sol
│   │   ├── staking/
│   │   │   ├── AuraAdapter.sol
│   │   │   ├── ConvexAdapter.sol
│   │   │   └── MaverickStakingAdapter.sol
│   ├── libs/
│   │   ├── BalancerUtilities.sol
│   │   ├── ConvexRewards.sol
│   │   ├── LibAdapter.sol
│   │   └── Ribs.sol
├── liquidation/
│   ├── AsyncSwapperRegistry.sol
│   ├── BaseAsyncSwipper.sol
│   ├── LiquidationRow.sol
├── oracles/
│   ├── RootPriceOracle.sol
│   ├── providers/
│   │   ├── BalancerLPComposableStableEthOracle.sol
│   │   ├── BalancerLPMetaStableEthOracle.sol
│   │   ├── ChainlinkOracle.sol
│   │   ├── CurveV1StableEthOracle.sol
│   │   ├── CurveV2CryptoEthOracle.sol
│   │   ├── CustomSetOracle.sol
│   │   ├── EthPeggedOracle.sol
│   │   ├── MavEthOracle.sol
│   │   ├── SfrxEthEthOracle.sol
│   │   ├── SwETHEthOracle.sol
│   │   ├── TokeOracle.sol
│   │   ├── UniswapV3EthOracle.sol
│   │   ├── WstETHEthOracle.sol
│   │   ├── base/
│   │   │   ├── BaseOracleDenominations.sol
├── rewarders/
│   ├── AbstractRewarder.sol
│   ├── ExtraRewarder.sol
│   ├── MainRewarder.sol
├── security/
│   ├── AccessController.sol
│   ├── Pausable.sol
│   ├── SecurityBase.sol
│   ├── SystemSecurity.sol
├── solver/
│   ├── CommonBuilder.sol
│   ├── Vm.sol
│   ├── helpers/
│   │   ├── ArraysConverter.sol
│   │   ├── BlockchainInfo.sol
│   │   ├── Bytes32.sol
│   │   ├── Integer.sol
│   │   ├── Tuples.sol
│   ├── test/
│   │   ├── SolverCaller.sol
├── staking/
│   ├── OPToke.sol
├── stats/
│   ├── Stats.sol
│   ├── StatsCalculatorFactory.sol
│   ├── StatsCalculatorRegistry.sol
│   ├── calculators/
│   │   ├── CbethLSTCalculator.sol
│   │   ├── CurveV1PoolEthStakingStatsCalculator.sol
│   │   ├── CurveV1PoolNoRebasingStatsCalculator.sol
│   │   ├── IncentivePricingStats.sol
│   │   ├── ProxyLSTCalculator.sol
│   │   ├── RethLSTCalculator.sol
│   │   ├── SfrxethLSTCalculator.sol
│   │   ├── SwethLSTCalculator.sol
│   │   ├── base/
│   │   │   ├── BalancerStablePoolCalculatorBase.sol
│   │   │   ├── BaseStatsCalculator.sol
│   │   │   ├── CurvePoolNoRebasingCalculatorBase.sol
│   │   │   ├── CurvePoolRebasingCalculatorBase.sol
│   │   │   ├── LSTCalculatorBase.sol
├── strategy/
│   ├── CurveUtils.sol
├── swapper/
│   ├── SwapRouter.sol
│   ├── adapters/
│   │   ├── BalancerV2Swap.sol
│   │   ├── BaseAdapter.sol
│   │   ├── CurveV1StableSwap.sol
│   │   ├── CurveV2Swap.sol
│   │   ├── UniV3Swap.sol
├── utils/
│   ├── Arrays.sol
│   ├── CurveResolverMainnet.sol
│   ├── Errors.sol
│   ├── MulticallI.sol
│   ├── NonReentrant.sol
│   ├── PortfolioMath.sol
│   ├── SpotPriceI.sol
│   ├── uniV3/
│   │   ├── BytesLib.sol
│   │   ├── Path.sol
├── vault/
│   ├── BalancerAuraDestinationVault.sol
│   ├── CurveConvexDestinationVault.sol
│   ├── DestinationVault.sol
│   ├── DestinationVaultFactory.sol
│   ├── DestinationVaultRegistry.sol
│   ├── LMPVault.sol
│   ├── LMPVaultFactory.sol
│   ├── LMPVaultRegistry.sol
│   ├── LMPVaultRouter.sol
│   ├── LMPVaultRouterBase.sol
│   ├── MaverickDestinationVault.sol
│   ├── VaultTypes.sol
│   ├── libs/
│   │   ├── LMPDebt.sol
│   │   ├── LMPDestinations.sol
```

©2023 SHERLOCK. ALL RIGHTS RESERVED