SOLIDITY FINANCE

OracleSwap

Smart Contract Audit Report

AUDIT SUMMARY

OracleSwap is developing two token contracts, a decentralized exchange, and a yield farming platform.

For this audit, we reviewed the following contracts on the Flare Mainnet:

- OracleToken contract at 0xD7565b16b65376e2Ddb6c71E7971c7185A7Ff3Ff.
- OracleBar contract at 0x5795377c85e0fdF6370fae1B74Fe03b930C4a892.
- MasterOracle contract at 0xF90C08C27B1a637804F3d85C155033696e25bFDB.

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.

- OracleSwapRouter contract at 0x73E93D9657E6f32203f900fe1BD81179a5bf6Ce4.

AUDIT FINDINGS

> *Please ensure trust in the team prior to investing as they have substantial control in the ecosystem.*
> *Date: April 21st, 2022.*
> *Updated: April 22nd, 2022 to address changes made by the team.*
>
> ### Finding #1 - OracleToken - High
>
> ***Description:*** *The* `_transfer()` *function is missing a call to the* `_moveDelegates()` *function.*
> ***Risk/Impact:*** *Any user could delegate votes to a delegatee, then transfer their tokens to another address which is then able to delegate additional votes to the same delegatee by using those newly acquired tokens.*
> ***Recommendation:*** *The project team should add a call to the* `_moveDelegates()` *function within the* `_transfer()` *function so delegated votes from those tokens are also transferred to the new user.*
> ***Update:*** *The team has indicated they won't be utilizing the voting and delegation aspects of the token.*

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.

> ### Finding #2 - MasterOracle - High (Resolved)
>
> ***Description:*** *The* `migrate()` *function can swap all LP tokens from any staking pool for an equivalent amount of tokens from the "Migrator" contract which is set by the owner.*
> ***Risk/Impact:*** *The owner can transfer all LP tokens from all pools to the "Migrator" contract using the* `migrate()` *function at any time.*
> ***Recommendation:*** *The project team should remove the* `migrate()` *function.*
> ***Resolution:*** *The team has burned ownership of the MasterOracle contract without setting the "Migrate" address (see transaction here). By doing so, the* `migrate()` *function cannot be called on any pool and no LP tokens can be exchanged.*

CONTRACTS OVERVIEW

> - *The contracts utilize the SafeMath library to prevent overflow/underflow attacks.*
>
> *OracleToken Contract:*
>
> - *The current total supply of the token is set to 1 billion $ORACLE.*
> - *At the time of writing this report, 99.99% of the total supply is*

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.

>   - *The other three holders own a cumulative 0.0001% of the total supply.*
> - *A mint function is present in the contract and could be previously utilized only by the MasterOracle contract to mint any amount of tokens to specified addresses, increasing the total supply at any time; the MasterOracle contract can no longer utilize the mint function preset as its ownership has been revoked.*
> - *There is no burn function but users may transfer their tokens to the 0x..dead address to reduce the circulating supply at any time.*
> - *Each $ORACLE token represents votes intended to be used in a DAO where one token represents one vote.*
> - *Users may delegate their votes to another address allowing them to vote on behalf of the user.*
> - *Once votes are delegated, the user must explicitly delegate them back to themselves to regain their votes.*
> - *Users also have the option to delegate through the use of a signed message generated off-chain, allowing for a gasless delegation for the user.*
> - *The owner was previously able to transfer ownership at any time.*
> - *The contract complies with the ERC-20 token standard.*

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.

> - *Users can use this contract in order to swap a team-designated token in exchange for $xORACLE tokens; the $ORACLE token is intended to be the team-designated token.*
> - *The total supply of the token is currently 100 $xORACLE.*
> - *At the time of writing this report, 100% of the total supply is held by an unverified address.*
> - *A mint function is present in the contract but can only be utilized when users deposit $ORACLE tokens, which increases the total supply.*
> - *A burn function is present in the contract but can only be used when exchanging $xORACLE tokens back for $ORACLE tokens.*
> - *Users can deposit $ORACLE tokens in exchange for $xORACLE tokens that represent shares; $xORACLE tokens are minted to the user.*
> - *Users can exchange their $xORACLE tokens back to $ORACLE tokens at any time; $xORACLE tokens are burned from the user when exchanging back to $ORACLE tokens which decreases the total supply.*
> - *The exchange rate is calculated based on the total supply of $xORACLE tokens and the total number of $ORACLE tokens within the contract.*
> - *The team must exercise caution when setting the oracle token and must avoid using any fee-on-transfer tokens; if a fee-on-transfer token is used as the oracle token then this contract*

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.

> *MasterOracle Contract:*
>
> - *This contract allows anyone to deposit team-designated staking tokens in order to earn rewards in the form of a reward token; the $ORACLE token is intended to be used as the reward token.*
> - *On deposits and withdrawals, pending rewards are calculated and transferred to the user.*
> - *Users' rewards are dependent on their amount staked, time staked, and the pool's reward per share amount.*
> - *There is a bonus multiplier of 10 applied to all users' time staked accrued before the bonus end block; the start block and bonus end block are set on deployment.*
> - *The reward per share amount is calculated using the contract's reward per block rate and the pool's allocation point percentage.*
> - *Each time rewards are calculated, the required amount of reward tokens are minted to the contract; additionally, the developer address is minted 10% of the calculated reward amount.*
> - *The user can also trigger an emergency withdrawal, which will transfer all the user's deposited tokens to their wallet address, forfeiting any rewards.*
> - *Users can migrate any of the pools' LP tokens to a new LP contract at any time; the "Migrator" contract is used to create an equal amount of new LP tokens which are then used as the*

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.

> - *The "Migrator" contract was not provided in the scope of this audit, so we are unable to provide an assessment of the contract with regards to security.*
> - *Ownership of the contract has been renounced by the team.*
> - *The owner was previously able to transfer ownership at any time.*
> - *The owner was previously able to add new staking pools at any time.*
> - *The owner was previously able to change the "Migrator" address at any time.*
> - *The owner was previously able to change all pools' allocation points at any time.*
> - *The owner was previously able to update the reward per block rate to any value at any time; the reward per block rate has been set to 0.*
> - *The developer address can set a new developer address at any time.*
> - *The team should be careful not to add the same token twice.*
> - *The team must exercise caution when setting the staking token and must avoid using any fee-on-transfer tokens; if a fee-on-transfer token is used as the staking token then this contract should be excluded from the token's fee mechanism.*
>
> *UniswapV2Pair Contract:*

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.

> *and swapping between the assets in the liquidity pool.*
>
> - *Anyone can use the mint function to mint an amount of LP tokens proportional to the amount of tokens in the contract that are not accounted for in the reserves.*
> - *Users can add liquidity by providing an equivalent value of each token and are minted an LP token in return. The LP tokens may be burned to receive the underlying assets at any time.*
> - *If the "Migrator" contract address from the OracleSwapFactory contract is the caller of the initial liquidity add, then the liquidity amount is set by the "Migrator" contract's* `desiredLiquidity()` *function.*
> - *The "Migrator" contract was not provided in the scope of this audit, so we are unable to provide an assessment of the contract with regards to security.*
> - *Anyone can use the swap function to transfer out an amount of the assets from the pool such that the new K value is at least as much as the current K value.*
> - *The swap function supports flash swaps which allows anyone to use a contract to borrow any amount of any asset, as long as the borrowed amount of each asset is returned within the call.*
> - *A 0.3% fee is taken on an exchange between tokens which is sent to the "FeeTo" address set by the OracleSwapFactory contract.*
> - *In the event that the team's platform fee is enabled, 25% of the fee is minted as LP tokens to an address controlled by the team.*

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.

> - *Alternatively, anyone can use the sync function to include any excess tokens in the reserve amounts so that they cannot be removed.*
>
> *OracleSwapFactory Contract:*
>
> - *This contract is used to deploy new UniswapV2Pair contracts specifying two underlying token assets.*
> - *A "FeeTo Setter" address is set upon deployment.*
> - *Anyone can create any pair any any time, as long as the pair has not been created yet.*
> - *Only one UniswapV2Pair contract can exist for any combination of two token assets.*
> - *The "FeeTo Setter" address can set the "FeeTo", "Migrator", and "FeeTo Setter" addresses to any address at any time.*
>
> *OracleSwapRouter Contract:*
>
> - *This contract is used to interact with any UniswapV2Pair liquidity pool contract created by the OracleSwapFactory contract.*
> - *Upon adding liquidity, the user specifies the desiried minimum amount of each token in the pair to add to the liquidity pool; the user is minted UniswapV2Pair LP tokens representing their share of ownership of the liquidity pool.*
> - *Upon removing liquidity, the user specifies the desired minimum amount of each token asset to receive from the liquidity pool:*

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.

> - *Liquidity removals support ERC-712 permits which allow the user to approve the Router to spend the user's LP tokens in a gasless manner.*
> - *Anyone can use this contract to swap one token asset for any other supported asset along a user-specified path of token assets.*
> - *When dealing with tokens that have a fee-on-transfer, the estimated output does not properly subtract the fee. As a result, users of fee-on-transfer tokens must set a slippage percentage prior to executing trades.*

AUDIT RESULTS

Vulnerability Category	Notes	Result
Arbitrary Jump/Storage Write	N/A	PASS
Centralization of Control	N/A	PASS

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.

Vulnerability Category	Notes	Result
Delegate Call to Untrusted Contract	N/A	PASS
Dependence on Predictable Variables	N/A	PASS
Ether/Token Theft	N/A	PASS
Flash Loans	N/A	PASS
Front Running	N/A	PASS
Improper Events	N/A	PASS
Improper Authorization Scheme	N/A	PASS
Integer Over/Underflow	N/A	PASS

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.

Vulnerability Category	Notes	Result
Oracle Issues	N/A	PASS
Outdated Compiler Version	N/A	PASS
Race Conditions	N/A	PASS
Reentrancy	N/A	PASS
Signature Issues	N/A	PASS
Unbounded Loops	N/A	PASS
Unused Code	N/A	PASS
Overall Contract Safety		PASS

OracleToken Contract

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.

INHERITANCE CHART

FUNCTION GRAPH

FUNCTIONS OVERVIEW

OracleBar Contract

INHERITANCE CHART

FUNCTION GRAPH

FUNCTIONS OVERVIEW

MasterOracle Contract

INHERITANCE CHART

FUNCTION GRAPH

FUNCTIONS OVERVIEW

OracleSwapFactory Contract

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.

FUNCTION GRAPH

FUNCTIONS OVERVIEW

OracleSwapRouter Contract

INHERITANCE CHART

FUNCTION GRAPH

FUNCTIONS OVERVIEW

ABOUT SOLIDITY FINANCE

Solidity Finance was founded in 2020 and quickly grew to have one of the most experienced and well-equipped smart contract auditing teams in the industry. Our team has conducted 1000+ solidity smart contract audits covering all major project types and protocols, securing a total of over $50 billion U.S. dollars in on-chain value across 1500 projects!.
Our firm is well-reputed in the community and is trusted as a top smart contract auditing company for the review of solidity code, no matter how complex. Our team of experienced solidity smart contract auditors performs audits for tokens, NFTs, crowdsales, marketplaces, gambling games, financial protocols, and more!

Contact us today to get a free quote for a smart contract audit of your project!

WHAT IS A SOLIDITY AUDIT?

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.

Audit takes this a step further by verifying economic logic to ensure the stability of smart contracts and highlighting privileged functionality to create a report that is easy to understand for developers and community members alike.

HOW DO I INTERPRET THE FINDINGS?

Each of our Findings will be labeled with a Severity level. We always recommend the team resolve High, Medium, and Low severity findings prior to deploying the code to the mainnet. Here is a breakdown on what each Severity level means for the project:

- **High** severity indicates that the issue puts a large number of users' funds at risk and has a high probability of exploitation, or the smart contract contains serious logical issues which can prevent the code from operating as intended.
- **Medium** severity issues are those which place at least some users' funds at risk and has a medium to high probability of exploitation.
- **Low** severity issues have a relatively minor risk association; these issues have a low probability of occurring or may have a minimal impact.
- **Informational** issues pose no immediate risk, but inform the project team of opportunities for gas optimizations and following smart contract security best practices.

GO HOME

© Solidity Finance LLC. | All rights reserved

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.

team which develops the language.

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.