FLOKI - Smart Contract Audit Report

AUDIT SUMMARY

FLOKI is building a new ERC20 token with DAO functionality allowing for decentralized governance within the protocol.

For this audit, we reviewed the StaticTaxHandler, TreasuryHandlerAlpha, ZeroTaxHandler, and ZeroTreasuryHandler at commit e94179f25c2e6f28e349763b83beef65ad3187fa on the team's public GitHub and the FLOKI contract at 0xcf0c122c6b73ff809c693db761e7baebe62b6a2e on the Ethereum blockchain.

We previously reviewed the team's token contract on BSC here and on ETH here.

Please ensure trust in the team prior to investing as they have some control in the ecosystem.

[dbd3489e6186c9c3e7233a1eaa550bd9dfcb1cb1](#) to commit [97acb1113cb6facfb43c94bc0c591df2a289d04c](#).

Updated: January 18th, 2022 with the new FLOKI deployment address.

Updated: January 22nd, 2022 to support changes from commit [97acb1113cb6facfb43c94bc0c591df2a289d04c](#) on the team's private GitHub to commit [e94179f25c2e6f28e349763b83beef65ad3187fa](#) on the team's public GitHub.

CONTRACTS OVERVIEW

FLOKI Contract:

- *The total supply of the token is initially set to 10 trillion.*

- *No mint or burn functions exist, though the circulating supply can be decreased by sending tokens to the 0x..dead address.*

- *At the time of this report, 14.43% of the total supply is stored in the [0x..dead address.](#)*

- *12.58% of the total supply is held in an [OKLGAtomicSwapInstance](#) functioning as the FLOKI bridge.*

- *There is a tax fee taken on buys and sells from specified "exchange pools" and sent to a Treasury address controlled by the team when neither the sender nor the recipient are whitelisted from fees.*

- *Addresses on the whitelist are exempt from fees. If either the sender or receiver are exempt, no fees are taken.*

- *Each FLOKI token additionally 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 back to themselves to regain their votes.*
- *Users also have the option to delegate through the use of a signed message, allowing for a gasless delegation for the user.*
- *The owner may update the tax and treasury addresses used during fee calculation at any time*

TreasuryPool Contract:

- *This contract is used to send collected fees to the team as well as perform automatic liquidity adds.*
- *During any sell, the balance of this contract is checked to see if there is any FLOKI collected from fees.*
- *If there is FLOKI in the contract, the contract will perform an automatic liquidity add.*
- *First, a check is done whether the contract's token balance is larger than a specified percentage in the "primary exchange". If it is larger, the percentage will be set to the specified percentage.*
- *A liquidity-add is funded by selling the specified "liquidity percentage" of tokens collected as fees, pairing the received ETH with the token, and adding it as liquidity to the ETH pair.*
- *Any remaining ETH is sent to a Treasury address controlled by the team.*
- *The owner may update the liquidity percentage and max allowed percentage for swap and liquify functionality at any time.*
- *The owner may update the Treasury address at any time.*
- *The owner may withdraw any ERC20 token in the contract at any time. We recommend the team exclude the designated token from this*

StaticTaxHandler Contract:

- *This contract is used to manage the FLOKI tax rate as well as exempted addresses.*
- *The owner may update the tax rate at any time, but the value may only be decreased.*
- *The owner may add and remove addresses from the whitelist at any time.*
- *The owner may add and remove addresses as designated exchange pools at any time.*
- *The owner may set the primary exchange pool at any time.*

General Notes Across All Contracts:

- *If the team wishes to implement the FLOKI token with no fees, they may use the ZeroTreasureHandler and ZeroTaxHandler contracts in place of the TreasuryHandlerAlpha and StaticTaxHandler contracts. These contracts will always return 0 when calculating any tax value.*
- *As the contracts are implemented in Solidity 0.8.X, they are protected from overflows.*
- *Proper structuring of logic to prevent reentrancy attacks.*

RESOLVED ISSUES

TreasuryHandlerAlpha.sol - Finding #1 - Medium

Description: *The team may use the withdraw() function to withdraw any*

and liquify functionality intended to maintain adequate liquidity. The team will also gain voting power as well.

Recommendation: The team should prevent the withdrawal of the designated token using the following line:

```
require(tokenAddress != address(token));
```

Resolution: The team has implemented the recommendation described above.

TreasuryHandlerAlpha.sol - Finding #2 - Informational

Description: The maximum percentage of tokens to be swapped during a swap and liquify is uncapped.

Risk/Impact: If too large of a value is set, a swap and liquify may result in large shifts in the token's value within a trading pool.

Recommendation: The team should exercise caution to not set too high of a limit.

Resolution: The team has implemented the recommendation described above, with a limit of 15% price impact value in the swap and liquify functionality.

EXTERNAL THREAT RESULTS

Vulnerability Category	Notes	Result
Arbitrary	N/A	PASS

Vulnerability Category	Notes	Result
Arbitrary Jump	N/A	PASS
Centralization of Control	The team has transferred control to a MultiSig wallet.	PASS
Delegate Call to Untrusted Contract	N/A	PASS
Dependence on Predictable Variables	N/A	PASS
Deprecated Opcodes	N/A	PASS
Ether Thief	N/A	PASS
Exceptions	N/A	PASS
External Calls	N/A	PASS
Integer Over/Underflow	N/A	PASS

Vulnerability Category	Notes	Result
Multiple Sends	N/A	PASS
Suicide	N/A	PASS
State Change External Calls	N/A	PASS
Unchecked Retval	N/A	PASS
User Supplied Assertion	N/A	PASS
Critical Solidity Compiler	N/A	PASS
Overall Contract Safety		PASS

FLOKI Contract

TreasuryHandlerAlpha Contract

StaticTaxHandler Contract

ZeroTaxHandler Contract

ZeroTreasuryHandler Contract

GO HOME

INHERITENCE CHART

FUNCTIONS OVERVIEW