



Audit Report

Fractional Rocket Token

February 2022

Source Github
commit 186bee2a13455ec944fb73b8922ea971a05aa52b
Audited by © coinscope

Table of Contents

| | |
|---|-----------|
| Table of Contents | 1 |
| Contract Review | 3 |
| Audit Updates | 3 |
| Contract Analysis | 4 |
| ELFM - Exceed Limit Fees Manipulation | 5 |
| Description | 5 |
| Recommendation | 5 |
| BC - Blacklisted Contracts | 6 |
| Description | 6 |
| Recommendation | 6 |
| Contract Diagnostics | 7 |
| CO - Code Optimization | 8 |
| Description | 8 |
| Recommendation | 8 |
| L01 - Public Function could be Declared External | 9 |
| Description | 9 |
| Recommendation | 9 |
| L02 - State Variables could be Declared Constant | 10 |
| Description | 10 |
| Recommendation | 10 |
| L09 - Dead Code Elimination | 11 |
| Description | 11 |
| Recommendation | 11 |
| Contract Functions | 12 |
| Contract Flow | 15 |
| Summary | 16 |



Disclaimer

17

About Coinscope

18

Contract Review

| | |
|---------------|---|
| Github | https://github.com/Fr0ck/audit |
| Commit | 186bee2a13455ec944fb73b8922ea971a05aa52b |

Audit Updates

| | |
|----------------------|----------------------|
| Initial Audit | 16h of February 2022 |
| Corrected | |

Contract Analysis

● Critical
 ● Medium
 ● Minor
 ● Pass

| Severity | Code | Description |
|---|------|---|
| ● | ST | Contract Owner is not able to stop or pause transactions |
| ● | OCTD | Contract Owner is not able to transfer tokens from specific address |
| ● | OTUT | Owner Transfer User's Tokens |
| ● | ELFM | Contract Owner is not able to increase fees more than a reasonable percent (25%) |
| ● | ULTW | Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent |
| ● | MT | Contract Owner is not able to mint new tokens |
| ● | BT | Contract Owner is not able to burn tokens from specific wallet |
| ● | BC | Contract Owner is not able to blacklist wallets from selling |

ELFM - Exceed Limit Fees Manipulation

| | |
|--------------------|------------------|
| Criticality | critical |
| Location | contract.sol#L39 |

Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by calling the `setPercentage` function with a high percentage value.

```
function setPercentage(uint16 reflectionPrctg, uint16 treasuryPrctg, uint16 marketingPrctg) external onlyRole(DEFAULT_ADMIN_ROLE) {  
    reflectionPercentage = reflectionPrctg;  
    treasuryPercentage = treasuryPrctg;  
    marketingPercentage = marketingPrctg;  
    emit PercentageUpdated(reflectionPrctg, treasuryPrctg, marketingPercentage);  
}
```

Recommendation

The contract could embody a check for the maximum acceptable value.

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

BC - Blacklisted Contracts

| | |
|-------------|-------------------|
| Criticality | medium |
| Location | contract.sol#L130 |

Description

The contract owner has the authority to stop contracts from transactions. The owner may take advantage of it by calling the `setBlacklist` function.

```
require(!isBlacklisted[from] && !isBlacklisted[to], "Blacklisted: user  
blacklisted");
```

Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

Contract Diagnostics

● Critical ● Medium ● Minor

| Severity | Code | Description |
|----------|------|--|
| ● | CO | Code Optimization |
| ● | L01 | Public Function could be Declared External |
| ● | L02 | State Variables could be Declared Constant |
| ● | L09 | Dead Code Elimination |

CO - Code Optimization

| | |
|--------------------|------------------|
| Criticality | minor |
| Location | contract.sol#L77 |

Description

There are a lot of checks that are taking place on every transaction but do not depend on the transaction's properties.

```
require(reflection != address(0) && treasury != address(0) && marketing !=  
address(0), "Tax : Address not set correctly");  
require(reflectionPercentage + treasuryPercentage + marketingPercentage != 0,  
"Tax : Percentage not set correctly");  
  
// Calculate amount  
uint256 reflectionAmount = uint256(reflectionPercentage) * amount / 100_00;  
uint256 treasuryAmount = uint256(treasuryPercentage) * amount / 100_00;  
uint256 marketingAmount = uint256(marketingPercentage) * amount / 100_00;
```

Recommendation

The fee addresses sanity check, the percentage zero equality check and the uint256 type cast could be moved to the setters functions.

L01 - Public Function could be Declared External

Criticality

minor

Location

Token/TokenBasic.sol#L37,74,163

Description

Public functions that are never called by the contract should be declared external to save gas.

```
snapshot  
setBlacklist  
initialize
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality

minor

Location

Token/FrockTokenV1.sol#L17

Description

Constant state variables should be declared constant to save gas.

`burnPercentage`

Recommendation

Add the constant attribute to state variables that never change.

L09 - Dead Code Elimination

Criticality

minor

Location

Token/TokenBasic.sol#L116

Description

Functions that are not used in the contract, and make the code's size bigger.

```
_mint
```

Recommendation

Remove unused functions.

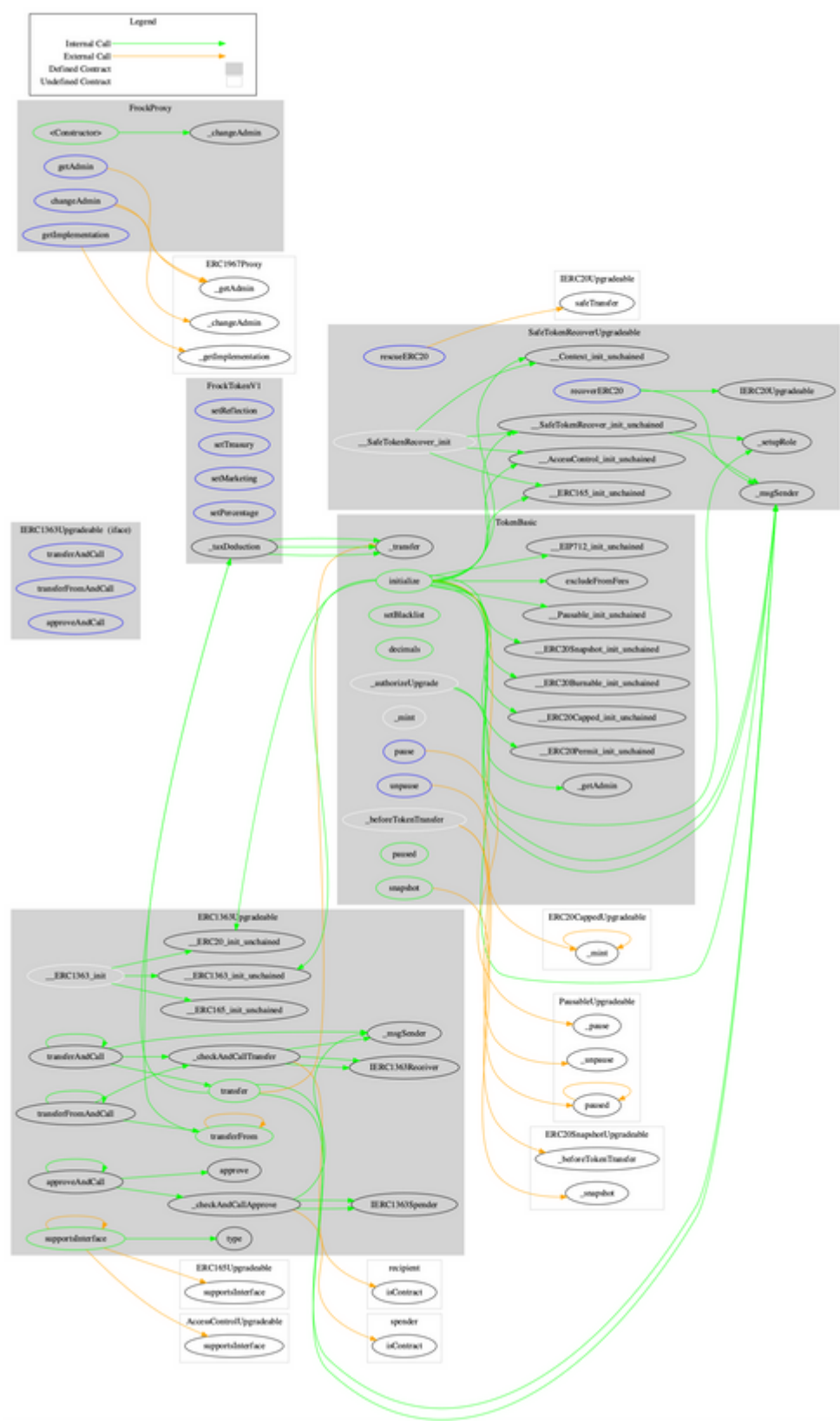
Contract Functions

| Contract | Type | Bases | | |
|------------------------------------|-----------------------------------|---|------------|-------------|
| | Function Name | Visibility | Mutability | Modifiers |
| | | | | |
| SafeTokenRecoverUpgradeable | Implementation | Initializable, AccessControlUpgradeable | | |
| | __SafeTokenRecover_init | Internal | ✓ | initializer |
| | __SafeTokenRecover_init_unchained | Internal | ✓ | initializer |
| | recoverERC20 | External | ✓ | onlyRole |
| | rescueERC20 | External | ✓ | onlyRole |
| | | | | |
| ERC1363Upgradeable | Implementation | Initializable, ERC20Upgradeable, IERC1363Upgradeable, ERC165Upgradeable | | |
| | __ERC1363_init | Internal | ✓ | initializer |
| | __ERC1363_init_unchained | Internal | ✓ | initializer |
| | supportsInterface | Public | | - |
| | transferAndCall | Public | ✓ | - |
| | transferAndCall | Public | ✓ | - |
| | transferFromAndCall | Public | ✓ | - |
| | transferFromAndCall | Public | ✓ | - |
| | approveAndCall | Public | ✓ | - |
| | approveAndCall | Public | ✓ | - |
| | _checkAndCallTransfer | Internal | ✓ | |
| | _checkAndCallApprove | Internal | ✓ | |
| | | | | |
| IERC1363Upgradeable | Interface | IERC20Upgradeable, IERC165Upgradeable | | |
| | transferAndCall | External | ✓ | - |

| | | | | |
|---------------------|---------------------|---|---------|--------------|
| | transferAndCall | External | ✓ | - |
| | transferFromAndCall | External | ✓ | - |
| | transferFromAndCall | External | ✓ | - |
| | approveAndCall | External | ✓ | - |
| | approveAndCall | External | ✓ | - |
| | | | | |
| FrockProxy | Implementation | ERC1967Proxy | | |
| | <Constructor> | Public | Payable | ERC1967Proxy |
| | getImplementation | External | | - |
| | getAdmin | External | | - |
| | changeAdmin | External | ✓ | - |
| | | | | |
| FrockTokenV1 | Implementation | TokenBasic | | |
| | setReflection | External | ✓ | onlyRole |
| | setTreasury | External | ✓ | onlyRole |
| | setMarketing | External | ✓ | onlyRole |
| | setPercentage | External | ✓ | onlyRole |
| | transfer | Public | ✓ | - |
| | transferFrom | Public | ✓ | - |
| | _taxDeduction | Internal | ✓ | |
| | | | | |
| TokenBasic | Implementation | Initializable, UUPSUpgradeable, ERC20CappedUpgradeable, ERC20BurnableUpgradeable, ERC20PermitUpgradeable, ERC1363Upgradeable, AccessControlUpgradeable, SafeTokenRecoverUpgradeable, PausableUp | | |

| | | | | |
|--|----------------------|--|---|-------------|
| | | gradeable, ERC20Snap shotUpgrad eable | | |
| | initialize | Public | ✓ | initializer |
| | excludeFromFees | Public | ✓ | onlyRole |
| | setBlacklist | Public | ✓ | onlyRole |
| | decimals | Public | | - |
| | _authorizeUpgrade | Internal | ✓ | |
| | _mint | Internal | ✓ | |
| | _beforeTokenTransfer | Internal | ✓ | |
| | pause | External | ✓ | onlyRole |
| | unpause | External | ✓ | onlyRole |
| | paused | Public | | - |
| | supportsInterface | Public | | - |
| | snapshot | Public | ✓ | onlyRole |

Contract Flow



Summary

There are some functions that can be abused by the owner, like manipulating fees and blacklisting contracts. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

Disclaimer

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment.

Coinscope team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed.

The Coinscope team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Coinscope receive a payment to manipulate those results or change the awarding badge that we will be adding in our website.

Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token.

The Coinscope team disclaims any liability for the resulting losses.

About Coinscope

Coinscope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

Coinscope is aiming to make crypto discoverable and efficient globally. It provides all the essential tools to assist users draw their own conclusions.



The Coinscope.co team

<https://www.coinscope.co>