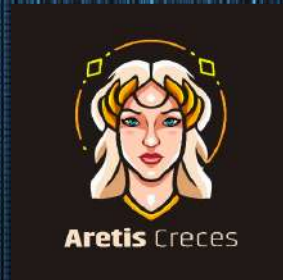




# **RugFreeCoins Audit**



## **Aretis Creces Token**

### **Smart Contract Security Audit**

**July 4, 2022**

# Contents

|                                     |    |
|-------------------------------------|----|
| Audit details                       | 1  |
| Disclaimer                          | 2  |
| Background                          | 3  |
| About the project                   | 4  |
| Target market and the concept       | 8  |
| Potential to grow with score points | 9  |
| Total Points                        | 9  |
| Contract details                    | 10 |
| Contract code function details      | 11 |
| Contract description table          | 13 |
| Security issue checking status      | 21 |
| Owner privileges                    | 22 |
| Audit conclusion                    | 25 |



# Audit details



**Audited project**  
Aretis Creces Token



**Contract Address**  
0xd87fe049573dc3b03785157ae2991e75da08e81d



**Client contact**  
Aretis Creces Team



**Blockchain**  
Binance smart chain



**Project website**  
Aretis.io

# Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Rugfreecoins and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Rugfreecoins) owe no duty of care towards you or any other person, nor does Rugfreecoins make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Rugfreecoins hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Rugfreecoins hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Rugfreecoins, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

# Background

Rugfreecoins was commissioned by the Aretis Creces Team to perform an audit of the smart contract.

**<https://bscscan.com/address/0xd87fe049573dc3b03785157ae2991e75da08e81d>**

The focus of this audit is to verify that the smart contract is secure, resilient, and working according to the specifications.

The information in this report should be used to understand the risk exposure of the smart contract, project feasibility, and long-term sustainability, and as a guide to improving the security posture of the smart contract by remediating the issues that were identified.

# About the project

Aretis Creces is a token built on the Binance Smart Chain that is with an innovative investment use case the main purpose of which is to seek out constant revenue sources, and **auto-staking protocol backed by Defi 3.0 yield farming** on Binance. Aretis Creces token will bring an unparalleled, fixed APY of **266,968.29%** while imposing profound ease, simplicity, and accessibility upon all Aretis Creces holders. Each transaction, purchase incurs a 12% fee, and sale incurs a 16% fee.

## Features

- **10% of the fee when buying** in \$ARIS tokens is deposited into the DAO Rewards Wallet and is distributed to users who contribute to Aretis Creces.
- The additional component included under the sustainability section is a **liquidity fee of 2% when buying**, which is a redistribution mechanism that ensures the trading pool always has sufficient liquidity.
- **3% of every sell trade fee** is stored in the Anti-Risk Fund which will be used to maintain the Aretis Creces.
- The **sustainability fee of 5% for marketing**, is what allows Aretis Creces Token to hold the aforementioned promise. Tokens will be swapped into BUSD-T and will be sent to the marketing wallet. This way, Aretis Creces Token will have enough funds to promote the coin and spend for future development without selling tokens as the traditional way.
- **The 6% of sell trade fees** will be allocated to Aretis Creces NFT Holders.
- **2% of every sell trade fee** of \$ARIS will be automatically burned to the Fire Pit.

# ROADMAP

## 2022 Q2

- Web Deployment
- Whitepaper launch
- DApp Development
- DApp V1 Dashboard
- Social Media launch
- Marketing Campaign
- Bounty Campaign
- IDO marketing
- Contract Audit
- IDO Sale
- CoinMarketCap/CoinGecko listing
- Contest campaigns
- 5,000 Token Holders
- 15,000 Token Holders
- 10 Million Market Cap

## 2022 Q3

- 25,000 Token Holders
- 50,000 Token Holders
- 100 Million Market Cap
- DApp v2 Dashboard - Deployment
- ACP-Swap Beta
- Cross-chain Integration
- More Partnerships
- Merchandise Launch

## 2022 Q4

- 100,000 Token Holders
- ACP-Swap Official Launch
- 250,000 Token Holders
- 500 Million Market Cap
- 1 Billion Market Cap
- SocialFi Development
- Big Marketing Campaign

## **2023+**

- Smart Contracts v2 Deployment
- Migration to v2
- 2 Billion Market Cap
- 500,000+ token holders
- 8 Billion Market Cap
- 2 Million Token Holders
- Expand to DEX Platform
- Become a leading top 10 Market Cap cryptocurrency



# Tokenomics

## **12% fee when buying**

- 10% of trade goes to the DAO reward wallet.
- 2% of trade goes to the liquidity pool.

## **16% fee when selling**

- 6% of trade goes to the NFT holders wallet
- 5% of trade goes to the marketing wallet.
- 3% of trade goes to the Anti-risk fund wallet.
- 2% of trade goes to the burn wallet.

# Target market and the concept

## Target market

- Anyone who's interested in the Crypto space with long-term investment plans.
- Anyone who's ready to earn a passive income by holding tokens.
- Anyone who's interested in trading tokens.
- Anyone who's ready in receiving automatic staking and compound rewards every 10 minutes.
- Anyone who's interested in receiving fixed interest in 10 minutes and **266,968.29%** per year.
- Anyone who's interested in taking part with Aretis Creces Dao platform earns rewards.
- Anyone who's interested in holding or trading NFTs and earning rewards.
- Anyone who's interested in taking part in the future plans of the Aretis Creces token.
- Anyone who's interested in making financial transactions with any other party using Aretis Creces Token as the currency.

# Potential to grow with score points

|              |   |               |
|--------------|---|---------------|
| 1.           | Project efficiency                      | 9/10          |
| 2.           | Project uniqueness                      | 9/10          |
| 3            | Information quality                     | 9/10          |
| 4            | Service quality                         | 9/10          |
| 5            | System quality                          | 9/10          |
| 6            | Impact on the community                 | 9/10          |
| 7            | Impact on the business                  | 9/10          |
| 8            | Preparing for the future                | 9/10          |
| 9            | Smart contract security                 | 10/10         |
| 10           | Smart contract functionality assessment | 10/10         |
| Total Points |   | <b>9.2/10</b> |

# Contract details

## Token contract details for 4<sup>th</sup> July 2022

|                                  |  |
|----------------------------------|--|
| Contract name                    | Aretis Creces Protocol                     |
| Contract address                 | 0xD87FE049573Dc3B03785157ae2991E75Da08E81d |
| Token supply                     | 166,666,666                                |
| Token ticker                     | ARIS                                       |
| Decimals                         | 8  |
| Token holders                    | 2  |
| Transaction count                | 2  |
| ArisDao address                  | 0xf03332b067581714bd8aa4b60af802dec3d89804 |
| Auto Liquidity Receiver          | 0xb26ff0922f54a759901b2377e5809a8b70667d9c |
| Firepit                          | 0xd32a0987a0f439dbdaabbb3717932381f00f7b83 |
| Treasury Receiver                | 0x64a62893d5a3b481e466247dd587b60087f7f2e3 |
| Contract deployer address        | 0xB4f03315c0f0E556325a3BE1C9A3c5A1FaFD8826 |
| Contract's current owner address | 0xb4f03315c0f0e556325a3be1c9a3c5a1fafd8826 |

# Contract code function details

| No | Category                              | Item   | Result                  |
|----|---------------------------------------|--|-------------------------|
| 1  | Coding conventions                    | BRC20 Token standards                            | pass                    |
|    |                                       | compile errors                                   | pass                    |
|    |                                       | Compiler version security                        | pass                    |
|    |                                       | visibility specifiers                            | pass                    |
|    |                                       | Gas consumption                                  | pass                    |
|    |                                       | SafeMath features                                | pass                    |
|    |                                       | Fallback usage                                   | pass                    |
|    |                                       | tx.origin usage                                  | pass                    |
|    |                                       | deprecated items                                 | pass                    |
|    |                                       | Redundant code                                   | pass                    |
|    |                                       | Overriding variables                             | pass                    |
| 2  | Function call audit                   | Authorization of function call                   | pass                    |
|    |                                       | Low level function (call/delegate call) security | pass                    |
|    |                                       | Returned value security                          | pass                    |
|    |                                       | Selfdestruct function security                   | pass                    |
| 3  | Business security                     | Access control of owners                         | High Cenralisation Risk |
|    |                                       | Business logics                                  | pass                    |
|    |                                       | Business implementations                         | pass                    |
| 4  | Integer overflow/underflow            |  | pass                    |
| 5  | Reentrancy                            |  | pass                    |
| 6  | Exceptional reachable state           |  | pass                    |
| 7  | Transaction ordering dependence       |  | pass                    |
| 8  | Block properties dependence           |  | pass                    |
| 9  | Pseudo random number generator (PRNG) |  | pass                    |
| 10 | DoS (Denial of Service)               |  | pass                    |











|           |   |  |             |
|-----------|---|--|-------------|
| <b>11</b> | <b>Token vesting<br/>implementation</b> |  | <b>pass</b> |
| <b>12</b> | <b>Fake deposit</b>                     |  | <b>pass</b> |
| <b>13</b> | <b>Event security</b>                   |  | <b>pass</b> |
















# Contract description table

The below table represents the summary of the contracts and methods in the token contract. We scanned the whole contract and listed down all the Interfaces, functions, and implementations with their visibility and mutability.











| Contract    | Type          | Bases      |            |           |
|-------------|---------------|------------|------------|-----------|
| L           | Function Name | Visibility | Mutability | Modifiers |
|             |               |            |            |           |
| SafeMathInt | Library       |            |            |           |
| L           | mul           | Internal 🔒 |            |           |
| L           | div           | Internal 🔒 |            |           |
| L           | sub           | Internal 🔒 |            |           |
| L           | add           | Internal 🔒 |            |           |
| L           | abs           | Internal 🔒 |            |           |
|             |               |            |            |           |
| SafeMath    | Library       |            |            |           |
| L           | add           | Internal 🔒 |            |           |
| L           | sub           | Internal 🔒 |            |           |
| L           | sub           | Internal 🔒 |            |           |
| L           | mul           | Internal 🔒 |            |           |
| L           | div           | Internal 🔒 |            |           |
| L           | div           | Internal 🔒 |            |           |
| L           | mod           | Internal 🔒 |            |           |

| <b>IERC20</b>                | <b>Interface</b> |            |   |      |
|------------------------------|------------------|------------|---|------|
| L                            | totalSupply      | External ! |   | NO ! |
| L                            | balanceOf        | External ! |   | NO ! |
| L                            | allowance        | External ! |   | NO ! |
| L                            | transfer         | External ! |    | NO ! |
| L                            | approve          | External ! |    | NO ! |
| L                            | transferFrom     | External ! |    | NO ! |
|                              |                  |            |   |      |
| <b>IPancakeSwap<br/>Pair</b> | <b>Interface</b> |            |   |      |
| L                            | name             | External ! |   | NO ! |
| L                            | symbol           | External ! |   | NO ! |
| L                            | decimals         | External ! |   | NO ! |
| L                            | totalSupply      | External ! |   | NO ! |
| L                            | balanceOf        | External ! |   | NO ! |
| L                            | allowance        | External ! |   | NO ! |
| L                            | approve          | External ! |  | NO ! |
| L                            | transfer         | External ! |  | NO ! |
| L                            | transferFrom     | External ! |  | NO ! |
| L                            | DOMAIN_SEPARATOR | External ! |   | NO ! |
| L                            | PERMIT_TYPEHASH  | External ! |   | NO ! |





































|                            |                      |            |   |      |
|----------------------------|----------------------|------------|---|------|
| L                          | nonces               | External ! |   | NO ! |
| L                          | permit               | External ! |    | NO ! |
| L                          | MINIMUM_LIQUIDITY    | External ! |   | NO ! |
| L                          | factory              | External ! |   | NO ! |
| L                          | token0               | External ! |   | NO ! |
| L                          | token1               | External ! |   | NO ! |
| L                          | getReserves          | External ! |   | NO ! |
| L                          | price0CumulativeLast | External ! |   | NO ! |
| L                          | price1CumulativeLast | External ! |   | NO ! |
| L                          | kLast                | External ! |   | NO ! |
| L                          | mint                 | External ! |  | NO ! |
| L                          | burn                 | External ! |  | NO ! |
| L                          | swap                 | External ! |  | NO ! |
| L                          | skim                 | External ! |  | NO ! |
| L                          | sync                 | External ! |  | NO ! |
| L                          | initialize           | External ! |  | NO ! |
|                            |                      |            |   |      |
| <b>IPancakeSwap Router</b> | <b>Interface</b>     |            |   |      |
| L                          | factory              | External ! |   | NO ! |
| L                          | WETH                 | External ! |   | NO ! |
| L                          | addLiquidity         | External ! |  | NO ! |

|   |   |            |   |      |
|---|---|------------|---|------|
| L | addLiquidityETH   | External ! |    | NO ! |
| L | removeLiquidity   | External ! |    | NO ! |
| L | removeLiquidityETH  | External ! |    | NO ! |
| L | removeLiquidityWithPermit                                 | External ! |    | NO ! |
| L | removeLiquidityETHWithPermit                              | External ! |    | NO ! |
| L | swapExactTokensForTokens                                  | External ! |    | NO ! |
| L | swapTokensForExactTokens                                  | External ! |    | NO ! |
| L | swapExactETHForTokens                                     | External ! |    | NO ! |
| L | swapTokensForExactETH                                     | External ! |    | NO ! |
| L | swapExactTokensForETH                                     | External ! |    | NO ! |
| L | swapETHForExactTokens                                     | External ! |  | NO ! |
| L | quote   | External ! |   | NO ! |
| L | getAmountOut  | External ! |   | NO ! |
| L | getAmountIn   | External ! |   | NO ! |
| L | getAmountsOut   | External ! |   | NO ! |
| L | getAmountsIn  | External ! |   | NO ! |
| L | removeLiquidityETHSupportingFeeOnTransferTokens           | External ! |  | NO ! |
| L | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! |  | NO ! |
| L | swapExactTokensForTokensSupportingFeeOnTransferTokens     | External ! |  | NO ! |
| L | swapExactETHForTokensSupportingFeeOnTransferTokens        | External ! |  | NO ! |





|                             |  |  |   |           |
|-----------------------------|--|--|---|-----------|
| L                           | swapExactTokensForETHSupportingFeeOnTransferTokens | External !   |    | NO !      |
|                             |  |  |   |           |
| <b>IpancakeSwap Factory</b> | <b>Interface</b>                                   |  |   |           |
| L                           | feeTo  | External !   |   | NO !      |
| L                           | feeToSetter  | External !   |   | NO !      |
| L                           | getPair  | External !   |   | NO !      |
| L                           | allPairs   | External !   |   | NO !      |
| L                           | allPairsLength                                     | External !   |   | NO !      |
| L                           | createPair   | External !   |    | NO !      |
| L                           | setFeeTo   | External !   |    | NO !      |
| L                           | setFeeToSetter                                     | External !   |  | NO !      |
|                             |  |  |   |           |
| <b>Ownable</b>              | <b>Implementation</b>                              |  |   |           |
| L                           |  | Public !   |  | NO !      |
| L                           | owner  | Public !   |   | NO !      |
| L                           | isOwner  | Public !   |   | NO !      |
| L                           | renounceOwnership                                  | Public !   |  | onlyOwner |
| L                           | transferOwnership                                  | Public !   |  | onlyOwner |
| L                           | _transferOwnership                                 | Internal  |  |           |
|                             |  |  |   |           |
| <b>ERC20Detailed</b>        | <b>Implementation</b>                              | <b>IERC20</b>  |   |           |
| L                           |  | Public !   |  | NO !      |

|                 |                       |                                |   |                       |
|-----------------|-----------------------|--------------------------------|---|-----------------------|
| L               | name                  | Public !                       |   | NO !                  |
| L               | symbol                | Public !                       |   | NO !                  |
| L               | decimals              | Public !                       |   | NO !                  |
|                 |                       |                                |   |                       |
| <b>IArisDAO</b> | <b>Interface</b>      |                                |   |                       |
| L               | getRelations          | External !                     |   | NO !                  |
| L               | setDaoReward          | External !                     | ● | NO !                  |
|                 |                       |                                |   |                       |
| <b>IRouter</b>  | <b>Interface</b>      |                                |   |                       |
| L               | swapBack              | External !                     | ● | NO !                  |
| L               | addLiquidity          | External !                     | ● | NO !                  |
|                 |                       |                                |   |                       |
| <b>Aretis</b>   | <b>Implementation</b> | <b>ERC20 Detailed, Ownable</b> |   |                       |
| L               |                       | Public !                       | ● | ERC20Detailed Ownable |
| L               | manualRebase          | External !                     | ● | NO !                  |
| L               | rebase                | Internal 🔒                     | ● |                       |
| L               | setStartTradingTime   | Public !                       | ● | onlyOwner             |
| L               | transfer              | External !                     | ● | validRecipient        |
| L               | transferFrom          | External !                     | ● | validRecipient        |
| L               | _basicTransfer        | Internal 🔒                     | ● |                       |
| L               | _transferFrom         | Internal 🔒                     | ● |                       |

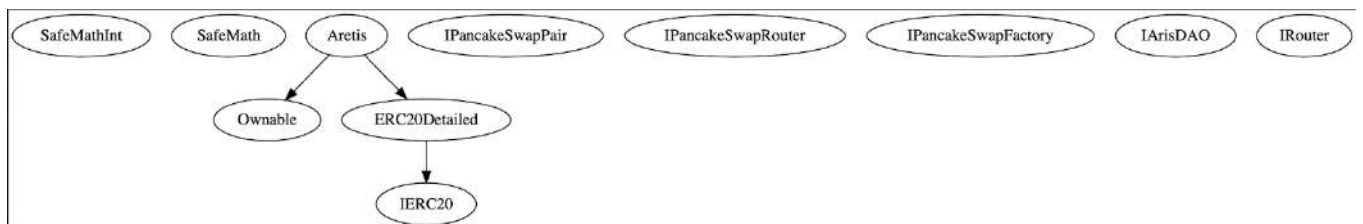
|   |                          |  |   |  |
|---|--------------------------|--|---|--|
| L | takeFee                  | Internal    |    |  |
| L | addLiquidity             | Internal    |    | swapping   |
| L | swapBack                 | Internal    |    | swapping   |
| L | shouldTakeFee            | Internal    |   |  |
| L | shouldRebase             | Internal    |   |  |
| L | shouldAddLiquidity       | Internal    |   |  |
| L | shouldSwapBack           | Internal    |   |  |
| L | setAutoRebase            | External    |    | onlyOwner  |
| L | setAutoSwapBack          | External    |    | onlyOwner  |
| L | setAutoLiquidityInterval | External   |   | onlyOwner  |
| L | setAutoAddLiquidity      | External  |  | onlyOwner  |
| L | setArisDaoAddress        | External  |  | onlyOwner  |
| L | setArisTreasuryAddress   | External  |  | onlyOwner  |
| L | allowance                | External  |   | NO  |
| L | decreaseAllowance        | External  |  | NO  |
| L | increaseAllowance        | External  |  | NO  |
| L | approve                  | External  |  | NO  |
| L | checkFeeExempt           | External  |   | NO  |
| L | getCirculatingSupply     | Public    |   | NO  |
| L | isNotInSwap              | External  |   | NO  |
| L | manualSync               | External  |  | NO  |

|   |                 |  |   |           |
|---|-----------------|--|---|-----------|
| L | setFeeReceivers | External !   |  | onlyOwner |
| L | setWhitelist    | External !   |  | onlyOwner |
| L | setBlacklist    | External !   |  | onlyOwner |
| L | totalSupply     | External !   |   | NO !      |
| L | balanceOf       | External !   |   | NO !      |
| L | isContract      | Internal  |   |           |

## Legend

| Symbol   | Meaning                   |
|--|---------------------------|
|   | Function can modify state |
|  | Function is payable       |

## Inheritance Hierarchy



# Security issue checking status

- ❖ **High severity issues**

No High severity issues found

- ❖ **Medium severity issues**

No medium severity issues found

- ❖ **Low severity issues**

No low severity issues found

- ❖ **Centralization Risk**

- ❖ Owner can change the trading start time anytime, so the owner can disable trading by changing this value to featured time

```
ftrace | funcSig
function setStartTradingTime(uint256 _time↑) public onlyOwner {
    startTradingTime = _time↑;
    if (_time↑ > 0) {
        lastAddLiquidityTime = _time↑;
        if (lastRebasedTime == 0) {
            lastRebasedTime = _time↑;
        }
    }
}
```



# Owner privileges

- ❖ The owner can enable/disable autorebase

```
ftrace | funcSig
function setAutoRebase(bool _flag↑) external onlyOwner {
    if (_flag↑) {
        _autoRebase = _flag↑;
        _lastRebasedTime = block.timestamp;
    } else {
        _autoRebase = _flag↑;
    }
}
```

- ❖ The owner can enable/disable auto swap back

```
ftrace | funcSig
function setAutoSwapBack(bool _flag↑) external onlyOwner {
    _autoSwapBack = _flag↑;
}
```

- ❖ The owner can change LP adding time interval

```
ftrace | funcSig
function setAutoLiquidityInterval(uint256 _minutes↑) external onlyOwner {
    require(_minutes↑ > 0, "invalid time");
    _autoLiquidityInterval = _minutes↑ * 1 minutes;
}
```

- ❖ The owner can enable/disable auto liquidity adding

```
ftrace | funcSig
function setAutoAddLiquidity(bool _flag↑) external onlyOwner {
    if (_flag↑) {
        _autoAddLiquidity = _flag↑;
        _lastAddLiquidityTime = block.timestamp;
    } else {
        _autoAddLiquidity = _flag↑;
    }
}
```

- ❖ The owner can change DAO and treasury address

```
ftrace | funcSig
function setArisDaoAddress(address _address↑) external onlyOwner {
    require(_address↑ != address(0), "invalid address");

    arisDaoAddress = _address↑;
    isFeeExempt[arisDaoAddress] = true;
}

ftrace | funcSig
function setArisTreasuryAddress(address _address↑) external onlyOwner {
    require(_address↑ != address(0), "invalid address");
    treasuryReceiver = _address↑;
    isFeeExempt[treasuryReceiver] = true;
    allowedFragments[treasuryReceiver][address(router)] = uint256(-1);
}
```

- ❖ The owner can change lp receiver and firepit address

```
ftrace | funcSig
function setFeeReceivers(address _autoLiquidityReceiver↑, address _firePit↑)
    external
    onlyOwner
{
    autoLiquidityReceiver = _autoLiquidityReceiver↑;
    firePit = _firePit↑;
}
```

- ❖ The owner can exclude wallets from fees( once exclude, can not include again) and can blacklist wallet from the contract

```
ftrace | funcSig
function setWhitelist(address[] memory _addrs↑) external onlyOwner {
    for (uint256 i = 0; i < _addrs↑.length; i++) {
        _isFeeExempt[_addrs↑[i]] = true;
    }
}

ftrace | funcSig
function setBlacklist(address _address↑, bool _flag↑) external onlyOwner {
    blacklist[_address↑] = _flag↑;
}
```

# Audit conclusion

RugFreeCoins team has performed in-depth testings, line by line manual code review, and automated audit of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, manipulations, and hacks. According to the smart contract audit.

Smart contract functional Status: **PASSED**

Number of risk issues: **1**

Solidity code functional issue level: **PASSED**

Number of owner privileges: **7**

Centralization risk correlated to the active owner: **HIGH**

Smart contract active ownership: **YES**