



## SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



**FlexDefi**  
\$FDE



**13/01/2022**



# TABLE OF CONTENTS

- 1 DISCLAIMER
- 2 INTRODUCTION
- 3-4 WEBSITE DIAGNOSTIC
- 5-6 AUDIT OVERVIEW
- 7-8 OWNER PRIVILEGES
- 9 CONCLUSION AND ANALYSIS
- 10 TOKEN DETAILS
- 11 FLEXDEFI TOKEN DISTRIBUTION & TOP 10 TOKEN HOLDERS
- 12 TECHNICAL DISCLAIMER



# DISCLAIMER

The information provided on this analysis document is only for general information and should not be used as a reason to invest.

FreshCoins Team will take no payment for manipulating the results of this audit.

The score and the result will stay on this project page information on our website <https://freshcoins.io>

FreshCoins Team does not guarantees that a project will not sell off team supply, or any other scam strategy ( RUG or Honeypot etc )



# INTRODUCTION

FreshCoins (Consultant) was contracted by FlexDefi (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x153625fb8849f0e7d4ca2ecec52e39be4307dd49

Network: Binance Smart Chain (BSC)

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on 13/01/2022



# WEBSITE DIAGNOSTIC

<https://www.flexdefi.network/>



0-49



50-89



90-100



Performance



Accessibility



Best Practices



SEO



Progressive  
Web App

## Metrics



First Contentful Paint

**3.2 s**



Time to interactive

**7.4 s**



Speed Index

**6.2 s**



Total Blocking Time

**550 ms**



Large Contentful Paint

**3.8 s**



Cumulative Layout Shift

**0**

# WEBSITE IMPROVEMENTS

---

Eliminate render-blocking resources

---

Reduce unused CSS

---

Reduce initial server response time

---

Reduce unused JavaScript

---

Ensure text remains visible during webfont load

---

Reduce the impact of third-party code Third-party code blocked the main thread for 870 ms

---

Background and foreground colors do not have a sufficient contrast ratio.

---

Links do not have a discernible name

---

Some elements have a `[tabindex]` value greater than 0

---

# AUDIT OVERVIEW



**Security Score**



**Static Scan**  
Automatic scanning for common vulnerabilities



**ERC Scan**  
Automatic checks for ERC's conformance



**High**



**Medium**



**Low**



**Optimizations**



**Informational**



No.	Issue description	Checking Status
1	Compiler Errors / Warnings	Passed
2	Reentrancy and Cross-function	Passed
3	Front running	Passed
4	Timestamp dependence	Passed
5	Integer Overflow and Underflow	Passed
6	Reverted DoS	Passed
7	DoS with block gas limit	Passed
8	Methods execution permissions	Passed
9	Exchange rate impact	Passed
10	Malicious Event	Passed
11	Scoping and Declarations	Passed
12	Uninitialized storage pointers	Passed
13	Design Logic	Passed
14	Safe Zeppelin module	Passed

# OWNER PRIVILEGES

Contract owner can't exclude an address from transactions.

Contract owner can mint tokens after initial contract deploy

```
function mint(uint256 amount) public onlyOwner returns (bool) {
    _mint(_msgSender(), amount);
    return true;
}
```

Contract owner can exclude/include wallet address from fee

```
function setExcludeTaxFee(address _add, bool value) public onlyOperator {
    require(whitelistTaxFee[_add] != value, "Same value !");
    whitelistTaxFee[_add] = value;
}
```

Contract owner can renounce ownership

```
function renounceOwnership() public virtual onlyOwner {
    emit OwnershipTransferred(_owner, address(0));
    _owner = address(0);
}
```

Contract owner can transfer ownership

```
function transferOwnership(address newOwner) public virtual onlyOwner {
    require(newOwner != address(0), "Ownable: new owner is the zero address");
    emit OwnershipTransferred(_owner, newOwner);
    _owner = newOwner;
}
```

Contract owner can change swap settings

```
function updateSwapAndLiquifyEnabled(bool _enabled) public onlyOperator {
    emit SwapAndLiquifyEnabledUpdated(msg.sender, _enabled);
    swapAndLiquifyEnabled = _enabled;
}
```

Contract owner can change burn rate

```
function updateBurnRate(uint16 _burnRate) public onlyOperator {
    require(_burnRate <= 190, "FlexDefi::updateBurnRate: Burn rate must not exceed the maximum rate.");
    emit BurnRateUpdated(msg.sender, burnRate, _burnRate);
    burnRate = _burnRate;
}
```

## Contract owner can change the fees

```
function updateTransferTaxRate(uint16 _transferTaxRate) public onlyOperator {  
    require(_transferTaxRate <= MAXIMUM_TRANSFER_TAX_RATE, "FlexDefi::updateTransferTaxRate: Transfer  
tax rate must not exceed the maximum rate.");  
    emit TransferTaxRateUpdated(msg.sender, transferTaxRate, _transferTaxRate);  
    transferTaxRate = _transferTaxRate;  
}
```

## Contract owner can change max tx amount

```
function updateMaxTransferAmountRate(uint16 _maxTransferAmountRate) public onlyOperator {  
    require(_maxTransferAmountRate <= 10000, "FlexDefi::updateMaxTransferAmountRate: Max transfer  
amount rate must not exceed the maximum rate.");  
    emit MaxTransferAmountRateUpdated(msg.sender, maxTransferAmountRate, _maxTransferAmountRate);  
    maxTransferAmountRate = _maxTransferAmountRate;  
}
```

# CONCLUSION AND ANALYSIS



Smart Contracts within the scope were manually reviewed and analyzed with static tools.



Audit report overview contains all found security vulnerabilities and other issues in the reviewed code.



Found no issue during the first review.

# TOKEN DETAILS

## Details

Buy fees:	3%
Sell fees:	3%
Max TX:	N/A
Max Sell:	N/A

## Honeypot Risk

Ownership:	Owned
Blacklist:	Not detected
Modify Max TX:	Detected
Modify Max Sell:	Not detected
Disable Trading:	Not detected

## Rug Pull Risk

Liquidity:	N/A
Holders:	Clean



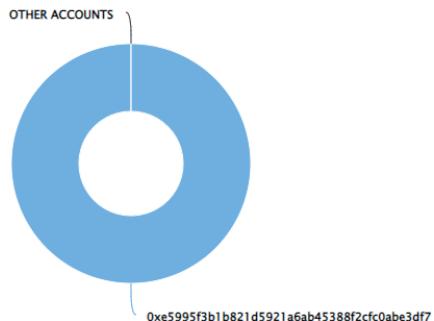
# FLEXDEFI TOKEN DISTRIBUTION & TOP 10 TOKEN HOLDERS

 The top 10 holders collectively own 100.00% (100,000,000.00 Tokens) of FlexDefi

 Token Total Supply: 100,000,000.00 Token | Total Token Holders: 1

FlexDefi Top 10 Token Holders

Source: BscScan.com



(A total of 100,000,000.00 tokens held by the top 10 accounts from the total supply of 100,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xe5995f3b1b821d5921a6ab45388f2fc0abe3df7	100,000,000.0000000001	100.0000%

# TECHNICAL DISCLAIMER

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have its vulnerabilities that can lead to hacks. The audit can't guarantee the explicit security of the audited project / smart contract.

