freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Fibonacci Coin
$FIBO

31/07/2023

TOKEN OVERVIEW

Fees

• **Buy fees:** **7%**

• **Sell fees:** **7%**

Fees privileges

• **Can change sell fees up to 20% and buy fees up to 20%**

Ownership

• **Owned**

Minting

• **No mint function**

Max Tx Amount / Max Wallet Amount

• **Can change max tx amount and max wallet amount (with threshold)**

Blacklist

• **Blacklist function not detected**

Other privileges

• **Can exclude / include from fees**

• **Can exclude / include from rewards**

TABLE OF CONTENTS

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
Fibonacci Coin (Customer) to conduct a Smart Contract Code Review and
Security Analysis.

0x42878032D5aB5A166f7Fa96e00F06caE86f07fD8

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 31/07/2023

WEBSITE DIAGNOSTIC

https://fibocoin.com/

0-49   50-89   90-100

96   **96**   **94**   **92**   **NA**

Performance   Accessibility   Best
Practices   SEO   Progressive
Web App

Socials

Twitter

https://twitter.com/fibo_coin

Telegram

https://t.me/fibonacci_coin_portal

AUDIT OVERVIEW

91

Security Score

98

Static Scan
Automatic scanning for common vulnerabilities

89

ERC Scan
Automatic checks for ERC's conformance

0 High

0 Medium

0 Low

1 Optimizations

0 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	Low
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 mint tokens after initial contract deploy**

● **Contract owner can't exclude an address from transactions**

● **Contract owner can exclude/include wallet from tax**

```solidity
function excludeFromFees(address account, bool excluded) public onlyOwner {
    require(_isExcludedFromFee[account] != excluded, "FLOC: Account is already the value of 'excluded'");
    _isExcludedFromFee[account] = excluded;
}
```

● **Contract owner can exclude/include wallet from rewards**

```solidity
function excludeFromReward(address account) public onlyOwner() {
    require(!_isExcluded[account], "Account is already excluded");
    if(_rOwned[account] > 0) {
        _tOwned[account] = tokenFromReflection(_rOwned[account]);
    }
    _isExcluded[account] = true;
    _excluded.push(account);
}

function includeInReward(address account) external onlyOwner() {
    require(_isExcluded[account], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

● **Contract owner can change swap settings**

```solidity
function setSwapAndLiquifyEnabled(bool _enabled) public onlyOwner {
    swapAndLiquifyEnabled = _enabled;
    emit SwapAndLiquifyEnabledUpdated(_enabled);
}

function setNumTokensSellToAddToLiquidity(uint256 newAmt) external onlyOwner() {
    numTokensSellToAddToLiquidity = newAmt*10**_decimals;
}
```

Contract owner can change buy fees up to 20% and sell fees up to 20%

```solidity
function setBuyFeePercent(uint256 taxFee, uint256 MarketingFee, uint256 liquidityFee, uint256 lotteryfee)
external onlyOwner() {
    _buyTaxFee = taxFee;
    _buyMarketingFee = MarketingFee;
    _buyLiquidityFee = liquidityFee;
    _buyLotteryFee = lotteryfee;
    require(_buyTaxFee + _buyLotteryFee + _buyLiquidityFee + _buyMarketingFee <= 20, "Must keep at 20%
or less");
}

function setSellFeePercent(uint256 taxFee, uint256 MarketingFee, uint256 liquidityFee, uint256 lotteryfee)
external onlyOwner() {
    _sellTaxFee = taxFee;
    _sellMarketingFee = MarketingFee;
    _sellLiquidityFee = liquidityFee;
    _sellLotteryFee = lotteryfee;
    require(_sellTaxFee + _sellLotteryFee + _sellLiquidityFee + _sellMarketingFee <= 20, "Must keep at 20%
or less");
}
```

Contract owner can change lotteryWallet and marketingWallet addresses

Current values:

lotteryWallet: 0x9db954c41092fb55a8e08fc670c4ddaf79990af5

marketingWallet: 0x1b32e44023fb932355790ca09695c909d70d1a63

```solidity
function setlotteryWallet(address payable newWallet) external onlyOwner() {
    lotteryWallet = newWallet;
}

function setMarketingWallet(address payable newWallet) external onlyOwner() {
    marketingWallet = newWallet;
}
```

Contract owner has ability to retrieve any token held by the contract

Native tokens excluded

```solidity
function removeStuckToken(address _address) external onlyOwner {
    require(_address != address(this), "Can't withdraw tokens destined for liquidity");
    require(IERC20(_address).balanceOf(address(this)) > 0, "Can't withdraw 0");

    IERC20(_address).transfer(owner(), IERC20(_address).balanceOf(address(this)));
}

function withdrawStuckBNB() external onlyOwner{
    require (address(this).balance > 0, "Can't withdraw negative or zero");
    payable(owner()).transfer(address(this).balance);
}
```

● Contract owner can change max wallet and max tx amount limitations

With threshold

```
function setMaxWalletToken(uint256 _maxWallet) external onlyOwner {
    maxWalletToken = _maxWallet * (10**18);
    require(maxWalletToken >= totalSupply() * 5 / 1000, "cant set max wallet less then 0.5%");
}

function setMaxTxAmount(uint256 newAmount) external onlyOwner() {
    _maxTxAmount = newAmount * (10**18);
    require(_maxTxAmount >= totalSupply() * 5 / 1000, "cant set max trx less then 0.5%");
}
```

● 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 renounce ownership

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

● L01: Missing Zero Address Check
FibonacciCoin: setlotteryWallet
FibonacciCoin: setMarketingWallet

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. The risk can be prevented by temporarily locking the contract or renouncing ownership.

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 HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees:	7%
Sell fees:	7%
Max TX:	11,235,813,213,456
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

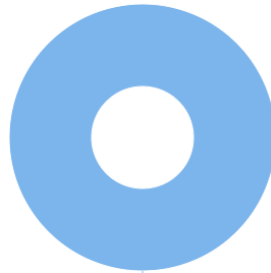|	
Liquidity:	N/A
Holders:	100% unlocked tokens

FIBO TOKEN ANALYTICS
& TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00% (1,123,581,321,345,590.00 Tokens) of Fibonacci Coin

Token Total Supply: 1,123,581,321,345,589.00 Token | Total Token Holders: 1

Fibonacci Coin Top 10 Token Holders

Source: BscScan.com

0xf7a0020fa223ba28383b3506a4993a7197872eea

(A total of 1,123,581,321,345,590.00 tokens held by the top 10 accounts from the total supply of 1,123,581,321,345,589.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xf7a0020fa223ba28383b3506a4993a7197872eea	1,123,581,321,345,589	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.