



SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



Fortnite OG
\$FRT

12/11/2023

TOKEN OVERVIEW

Fees

- Buy fees: 0%
- Sell fees: 0%

Fees privileges

- Can't change / set fees

Ownership

- Owned

Minting

- No mint function

Max Tx Amount / Max Wallet Amount

- Can change max wallet amount (with threshold)

Blacklist

- Blacklist function not detected

Other privileges

- N/A
-

TABLE OF CONTENTS

1

DISCLAIMER

2

INTRODUCTION

3

WEBSITE + SOCIALS

4-5

AUDIT OVERVIEW

6-8

OWNER PRIVILEGES

9

CONCLUSION AND ANALYSIS

10

TOKEN DETAILS

11

FRT ANALYTICS &
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 **Fortnite OG** (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x92dfB764f39f4F90089F04c0B1F275AA7dF14898

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 **12/11/2023**



WEBSITE DIAGNOSTIC

<https://fortniteog.vip/>



0-49



50-89



90-100



Performance



Accessibility



Best
Practices



SEO



Progressive
Web App

Socials



Twitter

<https://twitter.com/FORTNITEOGERC>



Telegram

<https://t.me/fortniteogerc>

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	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 address from wallet limitations

```
function excludeFromMaxHoldSumList(address _address) public onlyOwner {  
    isExcludedFromMaxHoldSum[_address] = true;  
}
```

- Contract owner has ability to retrieve any token held by the contract
Native tokens not excluded

```
function withdrawTokens(address to) public onlyOwner {  
    uint currentTokenBalance = IERC20(address(this)).balanceOf(address(this));  
    _transfer(address(this), to, currentTokenBalance);  
}
```

- Contract owner can change max wallet limitations (with threshold)

```
function changeMaxHoldSum(uint _newMaxHoldSum) public onlyOwner {  
    require(_newMaxHoldSum >= (totalSupply() / 1000), "Must be at least 0.1%");  
    maxHoldSum = _newMaxHoldSum;  
}
```

- Contract owner can renounce ownership

```
function renounceOwnership() public virtual onlyOwner {  
    _transferOwnership(address(0));  
}
```

- Contract owner can renounce ownership

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

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:	0%
Sell fees:	0%
Max TX:	100,000,000
Max Sell:	100,000,000

Honeypot Risk

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

Rug Pull Risk

Liquidity:	N/A
Holders:	Clean



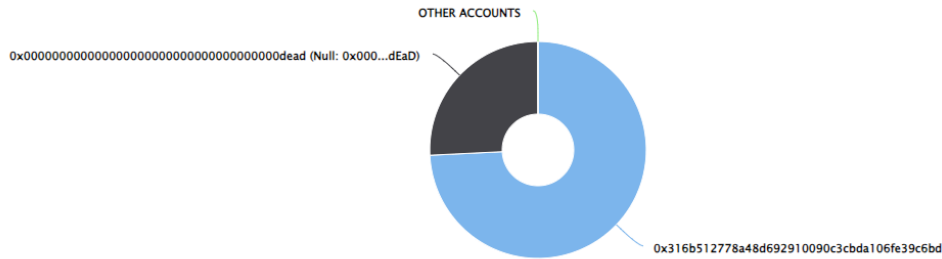
FRT TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

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

Token Total Supply: 100,000,000,000.00 Token | Total Token Holders: 2

Fortnite OG Top 10 Token Holders

Source: BscScan.com



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

Rank	Address	Quantity (Token)	Percentage
1	0x316B51...FE39c6Bd	74,225,000,000	74.2250%
2	Null: 0x000...dEaD	25,775,000,000	25.7750%

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.

