



SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



OPTIMUS GROKS
\$OPGROKS

24/12/2023



TOKEN OVERVIEW

Fees

- Buy fees: 6%
- Sell fees: 6%

Fees privileges

- Can't change fees

Ownership

- Owned

Minting

- No mint function

Max Tx Amount / Max Wallet Amount

- Can't change max tx amount and / or max wallet amount

Blacklist

- Blacklist function not detected

Other privileges

- Can exclude / include from fees
 - Contract owner has to call enableTrading function to enable trade
-

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

OPGROKS TOKEN 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 **OPTIMUS GROKS** (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0xBdea6832976422D6717de58106750E78A896b18

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 **24/12/2023**



WEBSITE DIAGNOSTIC

<https://optimusgroks.ai/>



0-49



50-89



90-100



Performance



Accessibility



Best
Practices



SEO



Progressive
Web App

Socials



Twitter

<https://twitter.com/optimusgroks>



Telegram

<https://t.me/OPGROKS>

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 wallet from tax

```
function excludeFromFee(address account, bool isExcluded) public onlyOwner {  
    require(isExcludedFromFee[account] != isExcluded, "The wallet is already has that value.");  
    isExcludedFromFee[account] = isExcluded;  
    emit excludeStatus(account, isExcluded);  
}
```

- Contract owner can whitelist wallet address

```
function setWhitelistBuySell(address _user, bool _wl) external onlyOwner {  
    require(whitelistBuySell[_user] != _wl, "The wallet is already has that value.");  
    whitelistBuySell[_user] = _wl;  
    emit whitelistStatus(_user, _wl);  
}
```

- Contract owner has to call **enableTrading** function to enable trade

Please note that any wallet whitelisted or owner wallet retains the ability to engage in trading, even in situations where trading has been disabled

```
function enableTrading() external onlyOwner {  
    tradingActive = true;  
}  
  
_transferFrom function line 1076  
.  
.  
.  
require(isNotLockBuySell(from), "OPTIMUS GROKS: Lock");  
.  
.  
.
```

After enabling trading, the initial five transactions must not exceed 240,240,000 tokens

uint256 public firstTrade = 240240000 * 1e9;

```
if(from == swapPair && count < 5) {  
    count = count + 1;  
    require(amount <= firstTrade, "Exceed the maximum limit");  
}
```

● Contract owner can transfer 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);
}
```

● Contract owner can renounce ownership

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

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 1 HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees: 6%

Sell fees: 6%

Max TX: N/A

Max Sell: N/A

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



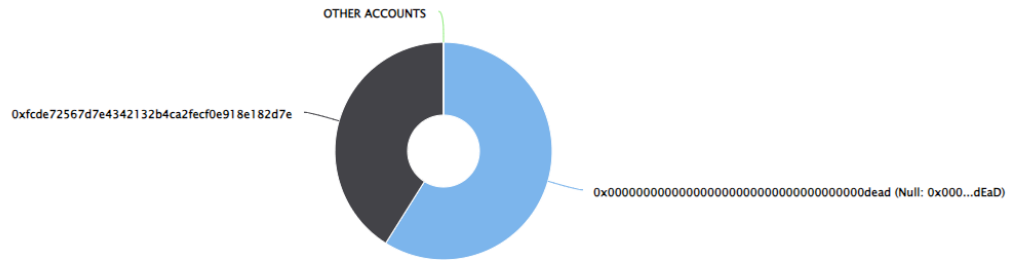
OPGROKS TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

💡 The top 10 holders collectively own 100.00% (420,000,000,000.00 Tokens) of OPTIMUS GROKS




💡 Token Total Supply: 420,000,000,000.00 Token | Total Token Holders: 2

OPTIMUS GROKS Top 10 Token Holders

Source: BscScan.com



(A total of 420,000,000,000.00 tokens held by the top 10 accounts from the total supply of 420,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Null: 0x000...dEaD 	247,501,673,999.7	58.9290%
2	 0xfcdE72...8e182D7E 	172,498,326,000.3	41.0710%

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.

