freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

SDAO

$SDAO

13/10/2022

TOKEN OVERVIEW

Fees

- Buy fees: 3%
- Sell fees: 3%

Fees privileges

- Can set buy fees up to 10% and sell fees up to 10%

Ownership

- Owned

Minting

- No mint function

Max Tx Amount / Max Wallet Amount

- Can set max tx amount and/or wallet limitations with threshold

Blacklist

- No blacklist function

Other privileges

- Can exclude from fees and tx limitations

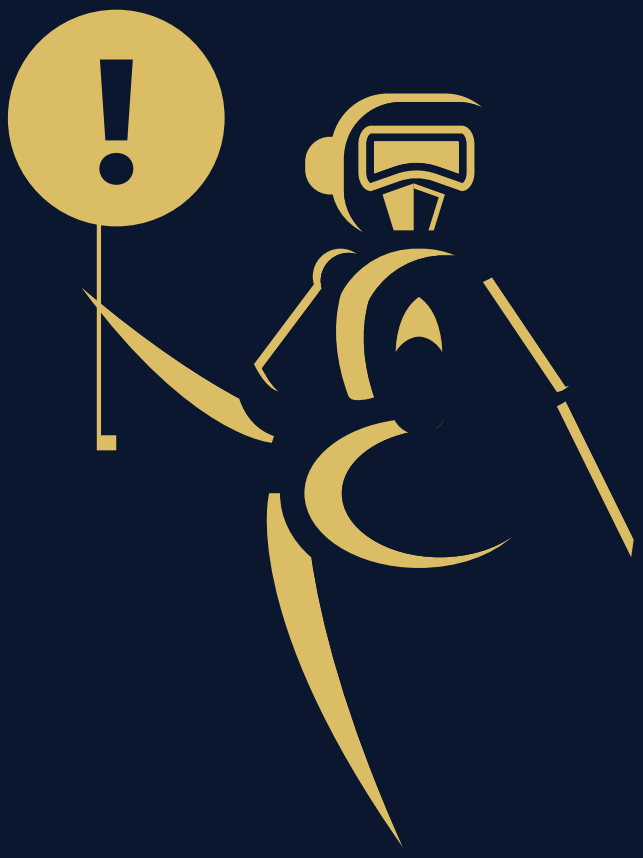
TABLE OF CONTENTS

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

0x07dbEF0F356623168e6279788507Bd98dd9D6304

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 13/10/2022

AUDIT OVERVIEW

86

Security Score

90

Static Scan
Automatic scanning for common vulnerabilities

82

ERC Scan
Automatic checks for ERC's conformance

0 High

2 Medium

1 Low

0 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(s) from fees

```
function excludeFromFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = true;
}

function includeInFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = false;
}

function setFromFees(address[] memory accounts, bool[] memory flags) public onlyOwner {
    require(accounts.length == flags.length);
    for (uint256 i = 0; i < accounts.length; i++) {
      _isExcludedFromFee[accounts[i]] = flags[i];
    }
}
```

- Contract owner can change sell limitations (without threshold)

```
function setMinToken(uint256 _minTokenNumberToSell) public onlyOwner {
    minTokenNumberToSell = _minTokenNumberToSell;
}

function setSellAmountRate(uint256[5] memory _sellAmountRate) public onlyOwner {
    sellAmountRate = _sellAmountRate;
}

function setSellLimit(bool _sellLimit) public onlyOwner {
    sellLimit = _sellLimit;
}

function setSellLimit(bool _sellInterval) public onlyOwner {
    sellInterval = _sellInterval;
}
```

- Contract owner can change swap settings

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

Contract owner can withdraw tokens from smart contract

```
function takeToken(address token, address recipient, uint256 amount) public onlyOwner {
    IERC20(token).transfer(recipient, amount);
}

function takeBNB(address recipient, uint256 amount) public onlyOwner {
    payable(recipient).transfer(amount);
}
```

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;
}
```

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:	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:	Detected
Disable Trading:	Not detected

Others

Liquidity:	N/A
Holders:	Clean

SDAO TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 99.80% (99,802,255.00 Tokens) of RAVE TOKEN

Token Total Supply: 100,000,000.00 Token | Total Token Holders: 27

(A total of 99,802,255.00 tokens held by the top 10 accounts from the total supply of 100,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xab85177a8723240ce27af755741cf9d0483083c9	98,000,000	98.0000%
2	0x482ebaf547c71ce84d02480beccbaf805733e018	1,499,641	1.4996%
3	0x1261e60ad19387646e8065808973889ada348270	79,335	0.0793%
4	0x6a0b4e731df6e7f16592bacb888d29c968de68dd	43,470	0.0435%
5	0x4c5922cfcd4b863bf389eb05f571fe88471505b1	41,034	0.0410%
6	0x0d6987c543e4c1f8bda704fcd68d830aa59ce76e	37,334	0.0373%
7	0x2c97409a953295fbd366f1f364eaf334a9f744b6	25,627	0.0256%
8	0xd5eb39874380ee958fd93ca62ec8d623ef7b7960	25,480	0.0255%
9	0x00ac400c24fd492c94ec4e8dc532d896cdb18744	25,167	0.0252%
10	0x6d9b999d2d1f6bd90d7454e095b75333bbf82400	25,167	0.0252%

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.