freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Oasis Metaverse
$OASIS

12/10/2023

TOKEN OVERVIEW

Fees

• **Buy fees:**   **5%**

• **Sell fees:**   **5%**

Fees privileges

• **Can change fees up to 5%**

Ownership

• **Owned**

Minting

• **No mint function**

Max Tx Amount / Max Wallet Amount

• **Can change max tx amount (with limitations)**

Blacklist

• **Blacklist function not detected**

Other privileges

• **Can exclude / include from fees**

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

0xF0Dc9fc0669f068e04aD79f7d70618D3f9Aad439

Network: **Ethereum (ETH)**

This report presents the findings of the security assessment of
Customer's smart contract and its code review conducted on **12/10/2023**

WEBSITE DIAGNOSTIC

https://oasismeta.org/

0-49   50-89   90-100

95   **98**   **96**   **94**   **NA**

Performance   Accessibility   Best   SEO   Progressive
                              Practices   Web App

Socials

Twitter   Telegram

https://twitter.com/oasismetaerc20   https://t.me/OasisVerification

AUDIT OVERVIEW

94

Security Score

96 Static Scan
Automatic scanning for common vulnerabilities

92 ERC Scan
Automatic checks for ERC's conformance

0 High

0 Medium

0 Low

0 Optimizations

0 Informational

No.	Issue description	Checking Status
1	Compiler Errors / Warnings	Passed
2	Reentrancy and Cross-function	Passed
3	Front running	Low
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 includeInFee(address account) external onlyOwner {
    _isExcludedFromFee[account] = false;
}

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

● **Contract owner can lock ownership by setting the current owner address to zero for a specified period, during which the contract cannot be accessed or modified by the owner.**

```solidity
function lock(uint256 time) public virtual onlyOwner {
    _previousOwner = _owner;
    _owner = address(0);
    _lockTime = block.timestamp + time;
    emit OwnershipTransferred(_owner, address(0));
}

function unlock() public virtual {
    require(_previousOwner == msg.sender, "You don't have permission to unlock");
    require(block.timestamp > _lockTime, 'Contract is locked until 7 days');
    emit OwnershipTransferred(_owner, _previousOwner);
    _owner = _previousOwner;
}
```

● **Contract owner can change swap settings**

```solidity
function setNumTokensSellToAddToLiquidity(uint256 newAmount) external onlyOwner {
    numTokensSellToAddToLiquidity = newAmount;
}

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

● Contract owner can change fees up to 5%

```solidity
function setFeePercent(uint256 taxFee) external onlyOwner {
    require(taxFee <= 5, 'Tax is too high');
    _taxFee = taxFee;
}
```

● Contract owner can change marketingWallet address

Current value:

marketingWallet: 0xCcCc32445a4ea1c43Cf4A8d508F967F6A43bAC30

```solidity
function setMarketingWallet(address payable newWallet) external onlyOwner {
    require(newWallet != address(0), 'invalid address');
    marketingWallet = newWallet;
}
```

● Contract owner can change max tx amount (with threshold)

```solidity
function setMaxTxAmount(uint256 maxTxAmount) external onlyOwner {
    _maxTxAmount = maxTxAmount;
    require(_maxTxAmount > totalSupply().div(400), 'value too low');
}
```

● Contract owner can transfer ownership

```solidity
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

```solidity
function renounceOwnership() public virtual onlyOwner {
    emit OwnershipTransferred(_owner, address(0));
    _owner = 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 no HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees: 5%

Sell fees: 5%

Max TX: 1,000,000,000

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
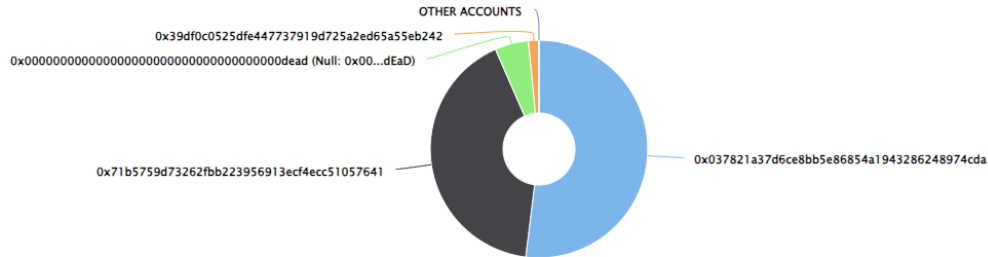
Holders: Clean

OASIS TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00% (100,000,000.00 Tokens) of Oasis Metaverse   Token Total Supply: 100,000,000.00 Token | Total Token Holders: 4

Oasis Metaverse Top 10 Token Holders
Source: Etherscan.io

OTHER ACCOUNTS
0x39df0c0525dfe447737919d725a2ed65a55eb242
0x000000000000000000000000000000000000dead (Null: 0x00...dEaD)
0x71b5759d73262fbb223956913ecf4ecc51057641
0x037821a37d6ce8bb5e86854a1943286248974cda

(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	0x037821...48974Cda	51,957,500	51.9575%
2	0x71B575...51057641	41,500,000	41.5000%
3	Null: 0x00...dEaD	5,000,000	5.0000%
4	0x39df0C...A55eb242	1,542,500	1.5425%

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.