freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

SAVE THE PEOPLE

$STP

25/01/2022

TABLE OF CONTENTS

1 DISCLAIMER

2 INTRODUCTION

3-4 WEBSITE DIAGNOSTIC

5-6 AUDIT OVERVIEW

7 OWNER PRIVILEGES

8 CONCLUSION AND ANALYSIS

9 TOKEN DETAILS

10 SAVE THE PEOPLE TOKEN DISTRIBUTION & TOP 10 TOKEN HOLDERS

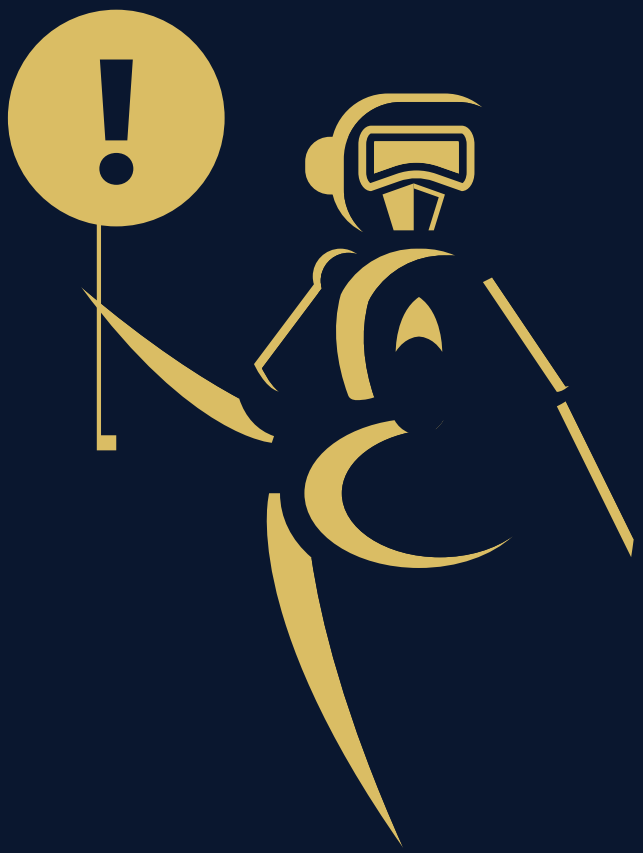
11 TECHNICAL DISCLAIMER

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
SAVE THE PEOPLE (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x01AD76511ccccbD82e73Ec2260DD668BbD3B3af5

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 25/01/2022

WEBSITE DIAGNOSTIC

https://savethepeople.io/


0-49


50-89


90-100

Performance

Accessibility

Best Practices

SEO

Progressive Web App

Metrics

First Contentful Paint
2.7 s

Time to interactive
3.6 s

Speed Index
3.8 s

Total Blocking Time
80 ms

Large Contentful Paint
4.6 s

Cumulative Layout Shift
0.016

WEBSITE IMPROVEMENTS

- Reduce unused JavaScript
- Reduce unused CSS
- Reduce initial server response time
- Image elements do not have explicit width and height
- Avoid enormous network payloads Total size was 5,600 KiB
- Form elements do not have associated labels
- Lists do not contain only <li> elements and script supporting elements
- Heading elements are not in a sequentially-descending order

AUDIT OVERVIEW

97

Security Score

96

Static Scan
Automatic scanning for common vulnerabilities

98

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	Passed
4	Timestamp dependence	Passed
5	Integer Overflow and Underflow	Passed
6	Reverted DoS	Passed
7	DoS with block gas limit	Passed
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 exclude/include wallet from reward

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

    function includeAccount(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];
                uint256 currentRate = _getRate();
                _rOwned[account] = _tOwned[account].mul(currentRate);
                _tOwned[account] = 0;
                _isExcluded[account] = false;
                _excluded.pop();
                break;
            }
        }
    }
```

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;
    }
```

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 issue during the first review.

TOKEN DETAILS

Details

Buy fees:	7%
Sell fees:	7%
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

SAVE THE PEOPLE TOKEN DISTRIBUTION & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00% (1,000,000,000.00 Tokens) of SAVE THE PEOPLE

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 1

(A total of 1,000,000,000.00 tokens held by the top 10 accounts from the total supply of 1,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xc7404d44f1731033c0bd266afc07fe4fb654b5cc	1,000,000,000	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.