freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

TruthGPT

$TRUTH

10/03/2023

TOKEN OVERVIEW

Fees

- Buy fees: 10%
- Sell fees: 10%

Fees privileges

- Can change fees up to 10%

Ownership

- Owned

Minting

- No mint function

Max Tx Amount / Max Wallet Amount

- Can change max tx amount (with threshold)

Blacklist

- Blacklist function not detected

Other privileges

- Can exclude / include from fees

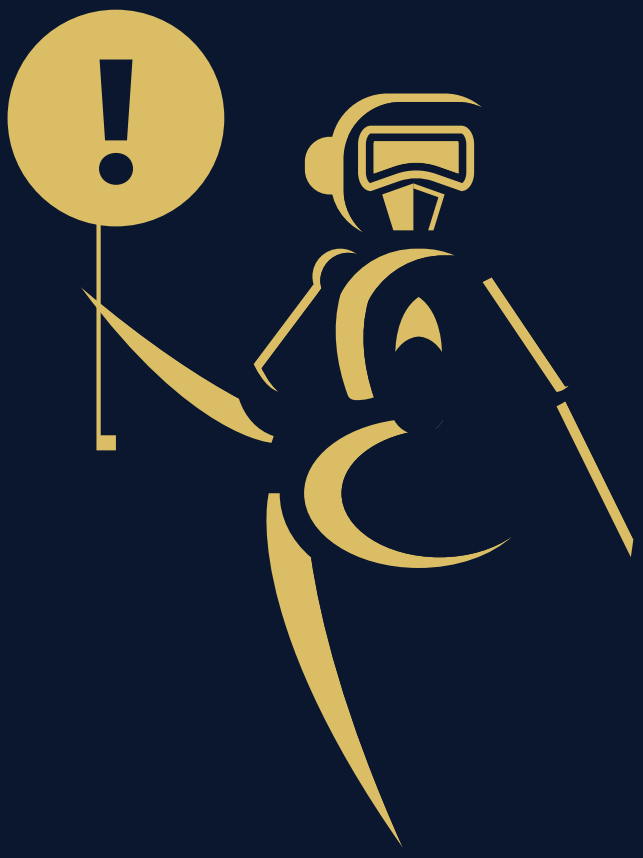
TABLE OF CONTENTS

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

0x2abDB5903171071ac29cC0779d7EFDF0FaF14228

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 10/03/2023

AUDIT OVERVIEW

94

Security Score

98

Static Scan
Automatic scanning for common vulnerabilities

92

ERC Scan
Automatic checks for ERC's conformance

0 High

2 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't exclude an address from transactions
- Contract owner can exclude/include wallet from tax

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

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

- Contract owner can exclude/include wallet from rewards

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

function includeInReward(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];
        _tOwned[account] = 0;
        _isExcluded[account] = false;
        _excluded.pop();
        break;
      }
    }
}
```

- Contract owner can change swap settings

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

Contract owner can change marketingWallet address

Current value:

marketingWallet: 0xe190575dfb5b0b74a7cfc307f64f4d92b139f016

```
function setMarketingWallet(address payable newWallet) external onlyOwner() {
        marketingWallet = newWallet;
}
```

Contract owner can change max tx amount (with threshold)

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

Contract owner can change fees up to 10%

```
function setFeePercent(uint256 taxFee, uint256 liquidityFee, uint256 marketingFee, uint256 burnFee) external onlyOwner() {
        require(taxFee.add(liquidityFee).add(marketingFee).add(burnFee) <= 10, "tax too high");
        _taxFee = taxFee;
        _liquidityFee = liquidityFee;
        _marketingFee = marketingFee;
        _burnFee = burnFee;
}
```

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;
}
```

Contract owner can renounce ownership

```
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:	10%
Sell fees:	10%
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

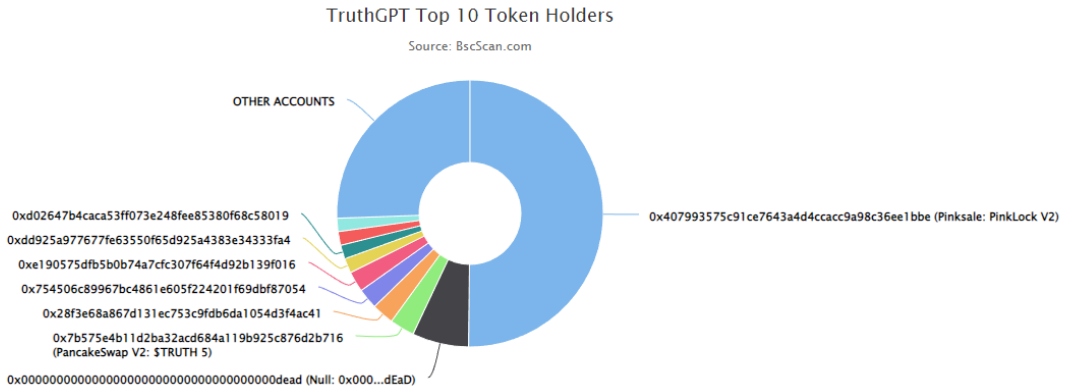
Rug Pull Risk

Liquidity:	N/A
Holders:	Clean

TRUTH TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 74.44% (744,409,183.89 Tokens) of TruthGPT

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 3,479



(A total of 744,409,183.89 tokens held by the top 10 accounts from the total supply of 1,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Pinksale: PinkLock V2	501,837,362.214492507688475028	50.1837%
2	Null: 0x000...dEaD	68,586,947.673410405776254418	6.8587%
3	PancakeSwap V2: $TRUTH 5	30,013,698.851411455317220011	3.0014%
4	0x28f3e68a867d131ec753c9fdb6da1054d3f4ac41	26,682,509.893274224632132427	2.6683%
5	0x754506c89967bc4861e605f224201f69dbf87054	25,068,988.874945190182203453	2.5069%
6	0xe190575dfb5b0b74a7cfc307f64f4d92b139f016	24,889,260.72768215537758983	2.4889%
7	0xdd925a977677fe63550f65d925a4383e34333fa4	17,800,298.827298333553507405	1.7800%
8	0xd02647b4caca53ff073e248fee85380f68c58019	16,890,813.303588021007040458	1.6891%
9	0x90ac5253b2b20013a215f9091de7f5bf53b8e566	16,422,667.734798436468699048	1.6423%
10	0x953519c19c6612c0e63518a75ea757af7d922f07	16,216,635.79082135115766972	1.6217%

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.