



# SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



**EEZY COIN**  
\$EEZY

**16/03/2022**



# 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 **EEZY 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 Honey pot etc )



# INTRODUCTION

**FreshCoins** (Consultant) was contracted by **EEZY COIN** (Customer) to conduct a Smart Contract Code Review and Security Analysis.

**TLCAQRbtZzCQuGEC4sred11WYmYk7D2ISM**

Network: **TRON (TRX)**

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on **16/03/2022**



# WEBSITE DIAGNOSTIC

<https://trx.eezycoin.io/>



0-49



50-89



90-100



Performance



Accessibility



Best  
Practices



SEO



Progressive  
Web App

## Metrics



First Contentful Paint

**2.2 s**



Time to interactive

**8.2 s**



Speed Index

**3.4 s**



Total Blocking Time

**3,005 ms**



Large Contentful Paint

**7.9 s**



Cumulative Layout Shift

**0.019**

# WEBSITE IMPROVEMENTS

---

Reduce unused JavaScript

---

Reduce unused CSS

---

Ensure text remains visible during webfont load

---

Avoid enormous network payloads Total size was 14,582 KiB

---

Reduce JavaScript execution time 10.3 s

---

Reduce the impact of third-party code Third-party code blocked the main thread for 3,5k ms

---

Ensure text remains visible during webfont load

---

Image elements do not have explicit width and height

---

Image elements do not have [alt] attributes

---

Background and foreground colors do not have a sufficient contrast ratio

---

List items (<li>) are not contained within <ul> or <ol> parent elements.

---

Heading elements are not in a sequentially-descending order

---

Document does not have a meta description

---

Links do not have a discernible name

---

# 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	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 disable trading.

---

Contract owner can't exclude an address from transactions.

---

Contract owner can't set / change buy & sell taxes.

---

Contract owner can't change swap settings.

---

Contract owner can't change tx amount.

---

Contract owner can burn tokens from any wallet

```
function burnFrom(address _from, uint256 _value) public returns (bool success) {  
    require(_balances[_from] >= _value);  
    require(_value <= _allowed[_from][msg.sender]);  
    _balances[_from] -= _value;  
    _allowed[_from][msg.sender] -= _value;  
    totalSupply -= _value;  
    emit Burn(_from, _value);  
    return true;  
}
```

```
function burn(uint256 _value) public returns (bool success) {  
    require(_balances[msg.sender] >= _value);  
    _balances[msg.sender] -= _value;  
    totalSupply -= _value;  
    emit Burn(msg.sender, _value);  
    return true;  
}
```

Contract owner can transfer ownership

```
function transferOwnership(address _newOwner) public onlyOwner {  
    newOwner = _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: N/A

Sell fees: N/A

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



# EEZY TOKEN DISTRIBUTION & TOP 10 TOKEN HOLDERS

## Asset Breakdown by Holders

■ Top 1~10 holders:97.85% ■ Top 11~50 holders:0.67% ■ Top 51~100 holders:0.42% ■ Top 101~500 holders:0.76% ■ Top 501~∞ holders:0.30%

Rank	Address	Quantity	Percentage
1	TNjUr3ZjuTin3i9UgBBvc2R4PBajrYcgqD	242,458,292.301323	96.983317%
2	TVCEgjB1t5rJLee9fAHue1rXT99vYErMxr	1,028,615.216648	0.411446%
3	SC TLCAQRbtZzCQuGEC4sred11WYmYk7D21SM	227,518	0.091007%
4	TY3NPVFwhMCjGhTQwbwKwmtQEY8M3mAgSo	209,372.6402	0.083749%
5	TRbdgZAmCYpeS5UsopV8is1qgf7fmmZAL	151,824.9999	0.06073%
6	TJgHg5mCbrxwfrmg5NsuCjVSxLa68TN2VF	127,833.333267	0.051133%
7	TMQTR4UpDvZv1741qSvasdnvdmquUepY5r	117,396.0415	0.046958%
8	TBGVyrx9aGZyQCnKJqrD4BEtjQkbAAL265	109,566.687707	0.043827%
9	TBzv7VpPABmLv6JkhxrT7NHWrnFVvYptx	97,325	0.03893%
10	TVp3ZAXwqgJTaGp4A1wqhjWuaCXNyU85md	96,242.023643	0.038497%

# 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.

