



# SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



**Diamond Holders**  
**\$DAH**

**26/12/2021**

# 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 **DIAMOND HOLDERS 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 **Diamond Holders** (Customer) to conduct a Smart Contract Code Review and Security Analysis.

**0x8654c77297ebC444a592ae2Cb047E33FF34b89b9**

**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 **26/12/2021**



# WEBSITE DIAGNOSTIC

<https://diamondholders.site/>



0-49



50-89



90-100



Performance



Accessability



Best  
Practices



SEO



Progressive  
Web App

## Metrics



First Contentful Paint

1.8 s



Time to interactive

2.1 s



Speed Index

6.0 s



Total Blocking Time

20 ms



Large Contentful Paint

16.1 s



Cumulative Layout Shift

0

## Issues found

---

Properly size images

---

Reduce initial server response time

---

Reduce unused CSS

---

Serve static assets with an efficient cache policy

---

Ensure text remains visible during webfont load

---

Image elements do not have explicit width and height

---

Avoid enormous network payloads

---

Background and foreground colors do not have a sufficient contrast ratio.

---

# 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	Passsed
2	Reentrancy and Cross-function	Passsed
3	Front running	Passsed
4	Timestamp dependence	Passsed
5	Integer Overflow and Underflow	Passsed
6	Reverted DoS	Passsed
7	DoS with block gas limit	Low
8	Methods execution permissions	Passsed
9	Exchange rate impact	Passsed
10	Malicious Event	Passsed
11	Scoping and Declarations	Passsed
12	Uninitialized storage pointers	Passsed
13	Design Logic	Passsed
14	Safe Zeppeling module	Passsed



# 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.

---



# 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 **1** low issue during the first review.

# TOKEN DETAILS

## Details

Buy fees: 0%

Sell fees: 0%

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

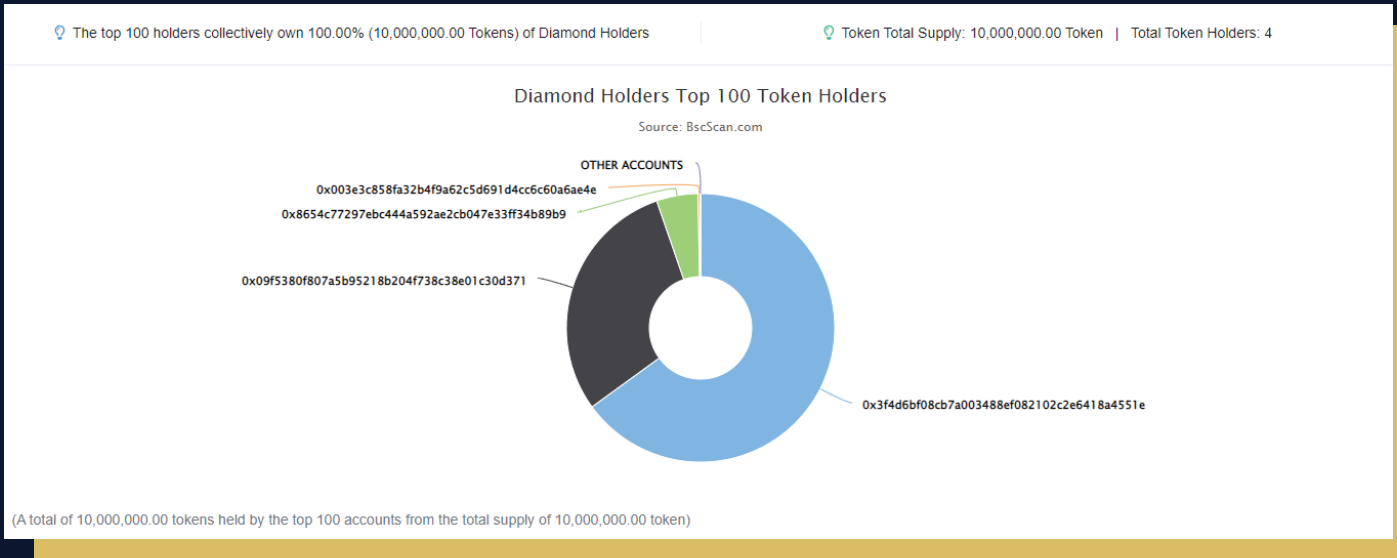
## Rug Pull Risk

Liquidity: N/A

Holders: Clean



# DIAMOND HOLDERS TOKEN DISTRIBUTION & TOP 10 TOKEN HOLDERS



Rank	Address	Quantity (Token)	Percentage
1	<a href="#">0x3f4d6bf08cb7a003488ef082102c2e6418a4551e</a>	6,500,000	65.0000%
2	<a href="#">0x09f5380f807a5b95218b204f738c38e01c30d371</a>	2,970,600	29.7060%
3	<a href="#">0x8654c77297ebc444a592ae2cb047e33ff34b89b9</a>	500,000	5.0000%
4	<a href="#">0x003e3c858fa32b4f9a62c5d691d4cc6c60a6ae4e</a>	29,400	0.2940%

# 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.

