



# SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



**Duality ETH**  
\$DUAL

**29/06/2023**



# TOKEN OVERVIEW

---

## Fees

- Buy fees: N/A
- Sell fees: N/A

## Fees privileges

- Can't change / set fees

## Ownership

- Owned

## Minting

- No mint function

## Max Tx Amount / Max Wallet Amount

- Can't change max tx amount or wallet amount

## Blacklist

- No blacklist function

## Other privileges

- Owner can burn tokens
-

# TABLE OF CONTENTS

- 1 **DISCLAIMER**
- 2 **INTRODUCTION**
- 3 **WEBSITE + SOCIALS**
- 4-5 **AUDIT OVERVIEW**
- 6 **OWNER PRIVILEGES**
- 7 **CONCLUSION AND ANALYSIS**
- 8 **TOKEN DETAILS**
- 9 **DUAL TOKEN ANALYTICS &  
TOP 10 TOKEN HOLDERS**
- 10 **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 **Duality ETH** (Customer) to conduct a Smart Contract Code Review and Security Analysis.

**0xc9FaF9D1A624561aFc8b4fdA745A88fD84f261E3**

Network: **Ethereum (ETH)**

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on **29/06/2023**



# WEBSITE DIAGNOSTIC

<https://dualityeth.xyz/>



0-49



50-89



90-100



Performance



Accessibility



Best  
Practices



SEO



Progressive  
Web App

## Socials



Twitter

<https://twitter.com/DualityEthereum>



Telegram

<https://t.me/dualtokenproject>

# 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

```
function burn(uint256 amount) public virtual {  
    _burn(_msgSender(), amount);  
}
```

- Contract owner can transfer ownership

```
function transferOwnership(address newOwner) public virtual onlyOwner {  
    require(newOwner != address(0), "Ownable: new owner is the zero address");  
    _transferOwnership(newOwner);  
}
```

- Contract owner can renounce ownership

```
function renounceOwnership() public virtual onlyOwner {  
    _transferOwnership(address(0));  
}
```

# 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:	N/A
Sell fees:	N/A
Max TX:	N/A
Max Sell:	N/A

## Honeypot Risk

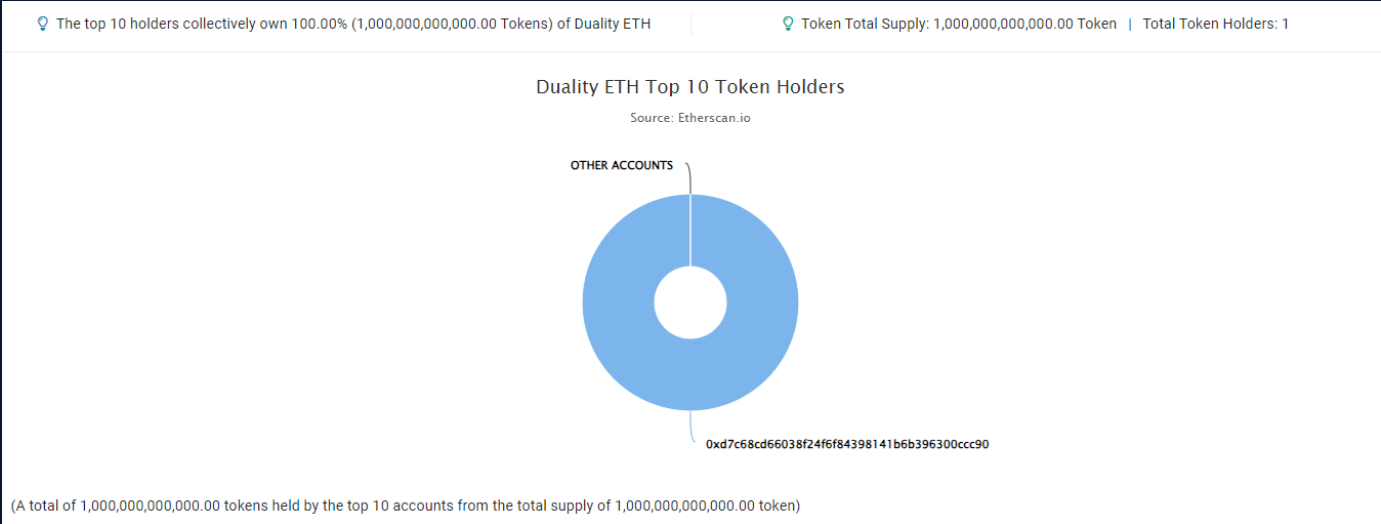
Ownership:	Owned
Blacklist:	Not detected
Modify Max TX:	Not detected
Modify Max Sell:	Not detected
Disable Trading:	Not detected

## Others

Liquidity:	N/A
Holders:	100% unlocked tokens



# DUAL TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS



Rank	Address	Quantity (Token)	Percentage
1	0xD7c68c...300cCc90	1,000,000,000,000	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.

