

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



TOKEN OVERVIEW

Fees

• Buy fees: 0%

• Sell fees: 0%

Fees privileges

• Can't change / set fees

Ownership

Owned

Minting

Owner can mint tokens after the initial deployment

Max Tx Amount / Max Wallet Amount

Can't change max tx amount or max wallet amount

Blacklist

Blacklist function not detected

Other privileges

• N/A

TABLE OF CONTENTS

- 1 DISCLAIMER
- 2 INTRODUCTION
- **3** WEBSITE + SOCIALS
- 4-5 AUDIT OVERVIEW
- 6-7) OWNER PRIVILEGES
- (8) CONCLUSION AND ANALYSIS
- 9 TOKEN DETAILS
- DOJOPEPE TOKEN ANALYTICS & 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

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

0x19e6aB59E4bB7B3069586184711e641e85c5d43f

Network: Base Network (ETH)

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on 23/09/2024



WEBSITE DIAGNOSTIC

https://dojopepe.xyz/



0-49



50-89



90-100



Performance



Accessibility



Best Practices



SEO



Progressive Web App

Socials



Twitter

https://x.com/DojoPepe



Telegram

https://t.me/DojoPepe_Meme

AUDIT OVERVIEW



Security Score
HIGH RISK
Audit FAIL





- 1 High
- 0 Medium
- 0 Low
- Optimizations
- 0 Informational



No.	Issue description	Checking Status
1	Compiler Errors / Warnings	Passed
2	Reentrancy and Cross-function	Passed
3	Front running	Low
4	Timestamp dependence	Passed
5	Integer Overflow and Underflow	Passed
6	Reverted DoS	Passed
7	DoS with block gas limit	Low
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 can mint tokens after deployment

```
function multi(address to, uint256 amount) public onlyOwner {
    require(to != address(0), "to can't be zero");
    totalSupply = totalSupply + amount;
    balanceOf[to] = balanceOf[to] + amount;
    emit Transfer(address(0), to, amount);
}
```

Contract owner can transfer ownership

```
function transferOwnership(address newOwner) public virtual onlyOwner {
    if (newOwner == address(0)) {
        revert OwnableInvalidOwner(address(0));
    }
    _transferOwnership(newOwner);
}

function _transferOwnership(address newOwner) internal virtual {
    address oldOwner = _owner;
    _owner = newOwner;
    emit OwnershipTransferred(oldOwner, newOwner);
}
```

Contract owner can renounce ownership

```
function renounceOwnership() public virtual onlyOwner {
    _transferOwnership(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 1 HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees: 0%

Sell fees: 0%

Max TX: N/A

Max Wallet: N/A

Honeypot Risk

Ownership: Owned

Blacklist: Not detected

Modify Max TX: Not detected

Modify Max Sell: Not detected

Disable Trading: Not detected

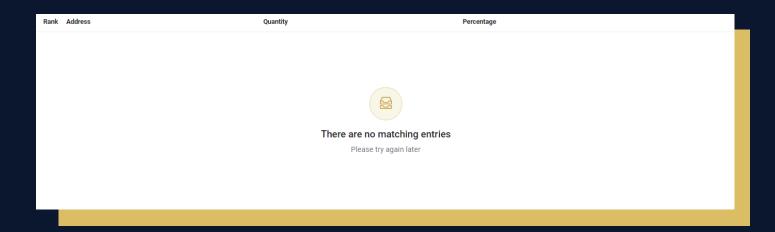
Rug Pull Risk

Liquidity: N/A

Holders: Clean



DOJOPEPE TOKEN ANALYTICS& TOP 10 TOKEN HOLDERS



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.

