

# SMART CONTRACT

---

## Security Audit Report

Project: DeadMemes Token  
Website: [deadmemestoken.com](http://deadmemestoken.com)  
Platform: Ethereum  
Language: Solidity  
Date: May 10th, 2023

# Table of contents

Introduction .....	4
Project Background .....	4
Audit Scope .....	4
Claimed Smart Contract Features .....	5
Audit Summary .....	6
Technical Quick Stats .....	7
Code Quality .....	8
Documentation .....	8
Use of Dependencies .....	8
AS-IS overview .....	9
Severity Definitions .....	10
Audit Findings .....	11
Conclusion .....	13
Our Methodology .....	14
Disclaimers .....	16
Appendix	
• Code Flow Diagram .....	17
• Slither Results Log .....	18
• Solidity static analysis .....	19
• Solhint Linter .....	20

THIS IS SECURITY AUDIT REPORT DOCUMENT AND WHICH MAY CONTAIN INFORMATION WHICH IS CONFIDENTIAL. WHICH INCLUDES ANY POTENTIAL VULNERABILITIES AND MALICIOUS CODES WHICH CAN BE USED TO EXPLOIT THE SOFTWARE. THIS MUST BE REFERRED INTERNALLY AND ONLY SHOULD BE MADE AVAILABLE TO THE PUBLIC AFTER ISSUES ARE RESOLVED.

# Introduction

EtherAuthority was contracted by the DeadMemes team to perform the Security audit of the DeadMemes Token smart contract code. The audit has been performed using manual analysis as well as using automated software tools. This report presents all the findings regarding the audit performed on May 10th, 2023.

**The purpose of this audit was to address the following:**

- Ensure that all claimed functions exist and function correctly.
- Identify any security vulnerabilities that may be present in the smart contract.

## Project Background

- DeadMemes is a standard ERC20 token, having functions like approve, transferFrom, transfer, decreaseAllowance, etc.

## Audit scope

<b>Name</b>	<b>Code Review and Security Analysis Report for DeadMemes Token Smart Contract</b>
<b>Platform</b>	<b>Ethereum / Solidity</b>
<b>File</b>	DeadMeme.sol
<b>File MD5 Hash</b>	718BAF4A5E22804ABC00F84CCF9311EE
<b>Audit Date</b>	May 10th, 2023

## Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
<b>Tokenomics:</b> <ul style="list-style-type: none"><li>• Name: DeadMemes</li><li>• Symbol: DEADMEMES</li><li>• Decimals: 18</li><li>• Total Supply: 420.690 Trillion</li><li>• No more minting possible</li></ul>	<b>YES, This is valid.</b>

## Audit Summary

According to the standard audit assessment, Customer's solidity based smart contracts are "**Secured**". This token contract does not contain any owner control, which does make it fully decentralized.



We used various tools like Slither, Solhint and Remix IDE. At the same time this finding is based on critical analysis of the manual audit.

All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Audit overview section. General overview is presented in AS-IS section and all identified issues can be found in the Audit overview section.

**We found 0 critical, 0 high, 0 medium and 0 low and 1 very low level issues.**

**Investors Advice:** Technical audit of the smart contract does not guarantee the ethical nature of the project. Any owner controlled functions should be executed by the owner with responsibility. All investors/users are advised to do their due diligence before investing in the project.

## Technical Quick Stats

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Passed
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Passed
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Passed
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	N/A
	Fallback function misuse	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Features claimed	Passed
	Other programming issues	Passed
Code Specification	Function visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Unused code	Passed
Gas Optimization	"Out of Gas" Issue	Passed
	High consumption 'for/while' loop	Passed
	High consumption 'storage' storage	Passed
	Assert() misuse	Passed
Business Risk	The maximum limit for mintage not set	Passed
	"Short Address" Attack	Passed
	"Double Spend" Attack	Passed

**Overall Audit Result: PASSED**

## Code Quality

This audit scope has 1 smart contract. Smart contract contains Libraries, Smart contracts, inherits and Interfaces. This is a compact and well written smart contract.

The libraries in the DeadMemes Token are part of its logical algorithm. A library is a different type of smart contract that contains reusable code. Once deployed on the blockchain (only once), it is assigned a specific address and its properties / methods can be reused many times by other contracts in the DeadMemes Token.

The DeadMemes team has **not** provided scenario and unit test scripts, which would have helped to determine the integrity of the code in an automated way.

Code parts are **not** well commented on in the smart contracts. Ethereum's NatSpec commenting style is used, which is a good thing.

## Documentation

We were given a DeadMemes Token smart contract code in the form of a file. The hash of that code is mentioned above in the table.

As mentioned above, code parts are not **well** commented. But the logic is straightforward. So it is easy to quickly understand the programming flow as well as complex code logic. Comments are very helpful in understanding the overall architecture of the protocol.

Another source of information was its official website: <https://deadmemestoken.com> which provided rich information about the project architecture and tokenomics.

## Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure that are based on well known industry standard open source projects.

Apart from libraries, its functions are not used in external smart contract calls.



# AS-IS overview

## Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	balanceOf	external	Passed	No Issue
3	transfer	external	Passed	No Issue
4	allowance	read	Passed	No Issue
5	approve	external	Passed	No Issue
6	transferFrom	external	Passed	No Issue
7	increaseAllowance	external	Passed	No Issue
8	decreaseAllowance	external	Passed	No Issue
9	_transfer	internal	Passed	No Issue
10	_mint	internal	Passed	No Issue
11	_approve	internal	Passed	No Issue
12	_spendAllowance	internal	Passed	No Issue
13	name	external	Passed	No Issue
14	symbol	external	Passed	No Issue
15	decimals	write	Passed	No Issue
16	totalSupply	external	Passed	No Issue

## Severity Definitions

Risk Level	Description
<b>Critical</b>	Critical vulnerabilities are usually straightforward to exploit and can lead to token loss etc.
<b>High</b>	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial
<b>Medium</b>	Medium-level vulnerabilities are important to fix; however, they can't lead to tokens lose
<b>Low</b>	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution
<b>Lowest / Code Style / Best Practice</b>	Lowest-level vulnerabilities, code style violations and info statements can't affect smart contract execution and can be ignored.

# Audit Findings

## Critical Severity

No Critical severity vulnerabilities were found.

## High Severity

No high severity vulnerabilities were found.

## Medium

No medium severity vulnerabilities were found.

## Low

No Low severity vulnerabilities were found.

## Very Low / Informational / Best practices:

(1) The `_msgData` function is missing in Context contract:

```
8
9  /**
10 * @dev Provides information about the current execution context, including the
11 * sender of the transaction and its data. While these are generally available
12 * via msg.sender and msg.data, they should not be accessed in such a direct
13 * manner, since when dealing with meta-transactions the account sending and
14 * paying for execution may not be the actual sender (as far as an application
15 * is concerned).
16 *
17 * This contract is only required for intermediate, library-like contracts.
18 */
19 abstract contract Context {
20     function _msgSender() internal view virtual returns (address) {
21         return msg.sender;
22     }
23
24     function _msgData() internal view virtual returns (bytes calldata) {
25         return msg.data;
26     }
27 }
```

The `_msgData` function is missing in the Context contract. which is used to get the transaction data.

**Resolution:** We suggest using an open zeppelin context contract to mitigate potential risk.

## Centralization

The DeadMemes Token smart contract does not have any ownership control, hence it is 100% decentralized.

# Conclusion

We were given a contract code in the form of a file and we have used all possible tests based on given objects as files. We have observed 1 low severity issue in the token smart contract. But those issues are not critical ones. So, **it's good to go for the mainnet deployment.**

Since possible test cases can be unlimited for such smart contracts protocol, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high-level description of functionality was presented in the As-is overview section of the report.

The audit report contains all found security vulnerabilities and other issues in the reviewed code.

The security state of the reviewed smart contract, based on standard audit procedure scope, is **"Secured"**.

# Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

## **Manual Code Review:**

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

## **Vulnerability Analysis:**

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

## **Documenting Results:**

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

## **Suggested Solutions:**

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.

# Disclaimers

## EtherAuthority.io Disclaimer

EtherAuthority team has analyzed this smart contract in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only. We also suggest conducting a bug bounty program to confirm the high level of security of this smart contract.

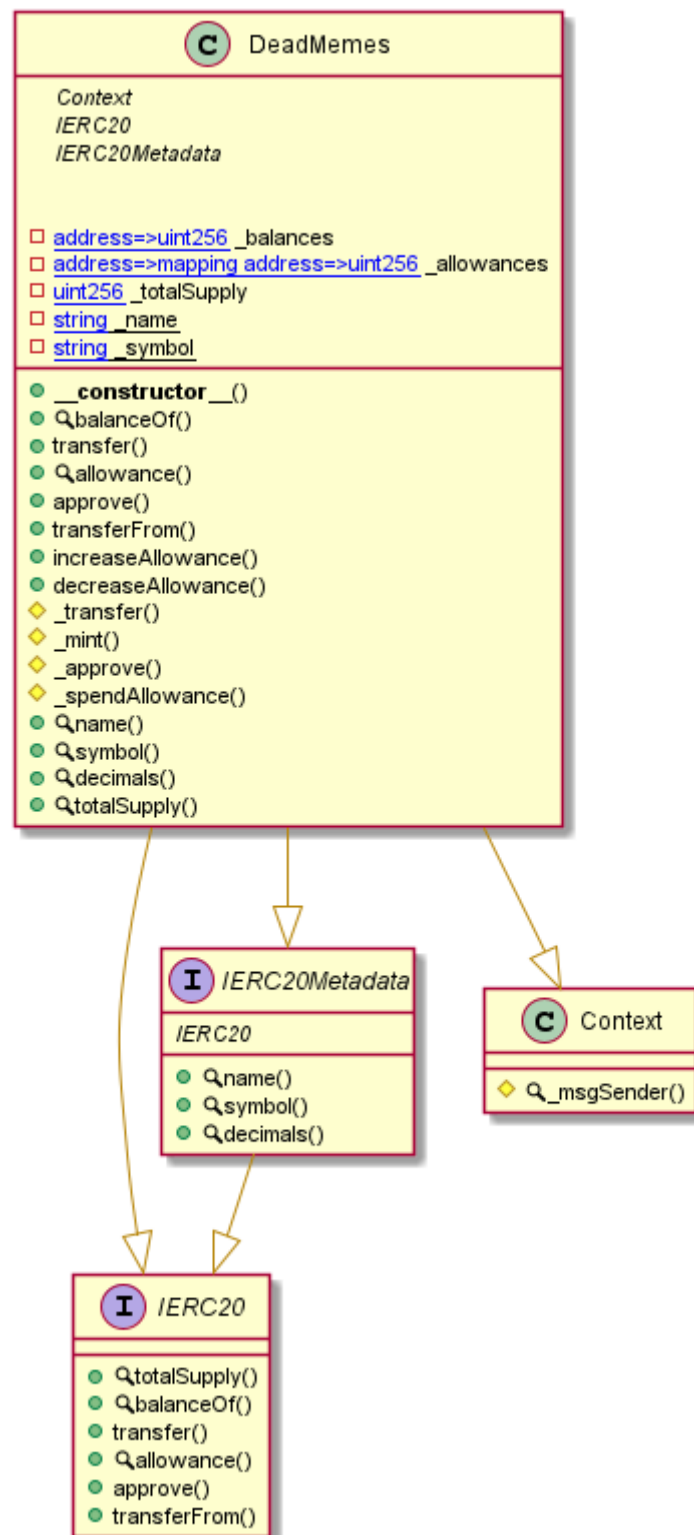
## Technical Disclaimer

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 their own vulnerabilities that can lead to hacks. Thus, the audit can't guarantee explicit security of the audited smart contracts.



# Appendix

## Code Flow Diagram - DeadMemes Token



# Slither Results Log

## Slither Log >> DeadMemes.sol

```
Pragma version0.8.19 (DeadMemes.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.16
solc-0.8.19 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Constant DeadMemes.name (DeadMemes.sol#53) is not in UPPER_CASE_WITH_UNDERSCORES
Constant DeadMemes._symbol (DeadMemes.sol#54) is not in UPPER_CASE_WITH_UNDERSCORES
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

DeadMemes.constructor() (DeadMemes.sol#56-58) uses literals with too many digits:
- _mint(msg.sender,4206900000000000 * 10 ** decimals()) (DeadMemes.sol#57)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
DeadMemes.sol analyzed (4 contracts with 84 detectors), 5 result(s) found
```

# Solidity Static Analysis

DeadMemes.sol

## Gas & Economy

### Gas costs:

Gas requirement of function DeadMemes.transfer is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)

Pos: 66:4:

## Miscellaneous

### Constant/View/Pure functions:

IERC20.transfer(address,uint256) : Potentially should be constant/view/pure but is not.

[more](#)

Pos: 16:4:

### No return:

IERC20.totalSupply(): Defines a return type but never explicitly returns a value.

Pos: 12:4:

### Similar variable names:

DeadMemes.\_mint(address,uint256) : Variables have very similar names "account" and "amount".

Pos: 152:43:

### Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

[more](#)

Pos: 170:12:

# Solhint Linter

## DeadMemes.sol

```
DeadMemes.sol:121:18: Error: Parse error: missing ';' at '{'  
DeadMemes.sol:137:18: Error: Parse error: missing ';' at '{'  
DeadMemes.sol:149:18: Error: Parse error: missing ';' at '{'  
DeadMemes.sol:174:22: Error: Parse error: missing ';' at '{'
```

### Software analysis result:

These software reported many false positive results and some are informational issues. So, those issues can be safely ignored.



This is a private and confidential document. No part of this document should be disclosed to third party without prior written permission of EtherAuthority.

**Email: [audit@EtherAuthority.io](mailto:audit@EtherAuthority.io)**