

A low-angle, upward-looking photograph of several tall skyscrapers, creating a sense of height and urban density. The image is overlaid with a semi-transparent blue filter.

SMART CONTRACT SECURITY AUDIT

Final report

Plan: Simple

Mongoose
December 2023

TABLE OF CONTENTS

1. Introduction	3
2. Analyzed Contracts	3
3. Audit Process	3
3.1 Auto-analysis	3
3.2 Expert audit	3
4. Known issues checked	4
5. Issue Classification	6
6. Issues	6
6.1 High risk issues	6
6.2 Medium risk issues	6
6.3 Low risk issues	6
7. Conclusion	7
8. Disclaimer	8

INTRODUCTION

The report has been prepared for Mongoose.

MONGOOSE, a meme coin, was initially created following a humorous speech by US Congressman Brad Sherman in 2021. The token has antibot protection mechanism, takes fees on transfers and adds them to liquidity. Addresses can be excluded from fees by the token owner.

Name	Mongoose
Audit date	2023-12-15 - 2023-12-15
Language	Solidity
Platform	Ethereum

ANALYZED CONTRACTS

Name	Address
Mongoose	0x47f7b78436d5d93fa36953fd6540b397d305c0df

AUDIT PROCESS

Our audit structure consists of two stages:

Auto-analysis

- Our automated tools allow us to scan smart contract code and find potential issues
- We hand pick and verify all the issues found by the tools

Expert audit

- Manual analysis of potential issues and vulnerabilities

- Contract code is reviewed thoroughly

KNOWN ISSUES CHECKED

Title	Result
Unencrypted Private Data On-Chain	✓ passed
Code With No Effects	✓ passed
Message call with hardcoded gas amount	✓ passed
Typographical Error	✓ passed
DoS With Block Gas Limit	✓ passed
Presence of unused variables	✓ passed
Incorrect Inheritance Order	✓ passed
Requirement Violation	✓ passed
Weak Sources of Randomness from Chain Attributes	✓ passed
Shadowing State Variables	✓ passed
Incorrect Constructor Name	✓ passed

Block values as a proxy for time	✓ passed
----------------------------------	----------

Authorization through tx.origin	✓ passed
---------------------------------	----------

DoS with Failed Call	✓ passed
----------------------	----------

Delegatecall to Untrusted Callee	✓ passed
----------------------------------	----------

Use of Deprecated Solidity Functions	✓ passed
--------------------------------------	----------

Assert Violation	✓ passed
------------------	----------

State Variable Default Visibility	✓ passed
-----------------------------------	----------

Reentrancy	✓ passed
------------	----------

Unprotected SELFDESTRUCT Instruction	✓ passed
--------------------------------------	----------

Unprotected Ether Withdrawal	✓ passed
------------------------------	----------

Unchecked Call Return Value	✓ passed
-----------------------------	----------

Floating Pragma	✓ passed
-----------------	----------

Outdated Compiler Version	✓ passed
---------------------------	----------

Integer Overflow and Underflow	✓ passed
--------------------------------	----------

Function Default Visibility	✓ passed
-----------------------------	----------

ISSUE CLASSIFICATION

High risk	Issues leading to assets theft, locking or any other loss of assets or leading to contract malfunctioning.
Medium risk	Issues that can trigger a contract failure of malfunctioning.
Low risk	Issues that do not affect contract functionality. For example, unoptimised gas usage, outdated or unused code, code style violations, etc.

ISSUES

High risk issues

No issues were found

Medium risk issues

No issues were found

Low risk issues

No issues were found

CONCLUSION

Mongoose Mongoose contract was audited. No risk issues were found.

DISCLAIMER

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without RapidLabs prior written consent.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts RapidLabs to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.



RAPID LABS

YOUR PROJECT SECURED

RL@RAPIDLABS.FINANCE

RAPIDLABS.FINANCE