


SMART CONTRACT SECURITY AUDIT


Final report

Plan: Simple

Dali

December 2021

 rugdog.net

 the@rugdog.net



CONTENTS

1. Introduction	3
2. Contracts checked	3
3. Audit Process	3
4. Attacks checked	4
5. Classification of issues	5
6. Issues	6
6.1 High severity issues	6
6.2 Medium severity issues	6
6.3 Low severity issues	6
7. Conclusion	7
8. Disclaimer	8

INTRODUCTION

This smart contract audit report has been prepared by the RugDog team for the Dali project. The report contains the results of a complete security assessment of the Dali Token contract

Name	Dali
Audit date	2021-12-07 - 2021-12-16
Language	Solidity
Network	Binance Smart Chain

CONTRACTS CHECKED

Name	Address
CoinToken	0xa0f67af7a704deda149823100acc51a78179d55b

AUDIT PROCESS

The code was audited by the team according to the following order:

Automated analysis

- ♦ Scanning the project's smart contracts with several publicly available automated Solidity analysis tools
- ♦ Manual confirmation of all the issues found by the tools

Manual audit

- ♦ Thorough manual analysis of smart contracts for security vulnerabilities
- ♦ Smart contracts' logic check

ATTACKS CHECKED

Title	Check 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	✗ not passed
-----------------	--------------

Outdated Compiler Version	✓ passed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

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

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

CLASSIFICATION OF ISSUES

High severity Issues leading to assets theft, locking or any other loss of assets or leading to contract malfunctioning.

Medium severity Issues that can trigger a contract failure of malfunctioning.

Low severity Issues that do now affect contract functionality. For example, unoptimised gas usage, outdated or unused code, code style violations, etc.

◆ ISSUES

High severity issues

No issues were found

Medium severity issues

No issues were found

Low severity issues

1. Floating pragma number (CoinToken)

The latest version of Solidity should be used for deployment.

◆ CONCLUSION

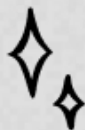
Dali CoinToken contract was audited. 1 low severity issue was found.

◆ **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 RugDog 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 RugDog 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.



WOOF!

 rugdog.net

 the@rugdog.net

