SMART CONTRACT AUDIT

ZOKYO.

Dec 7th, 2021 | v. 1.0

PASS

Zokyo Security Team has concluded that this smart contract passes security qualifications to be listed on digital asset exchanges.

SCORE

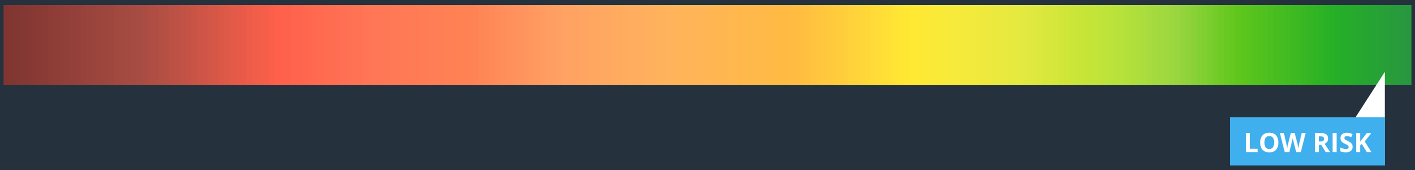
100

TECHNICAL SUMMARY

This document outlines the overall security of the Dogelon Mars smart contracts, evaluated by Zokyo's Blockchain Security team.

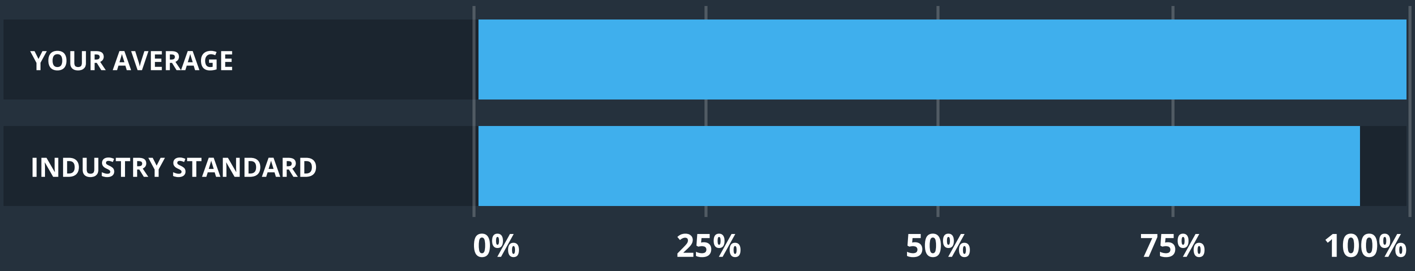
The scope of this audit was to analyze and document the Dogelon Mars smart contract codebase for quality, security, and correctness.

Contract Status



There were no critical issues found during the audit.

Testable Code



The testable code is 100%, which is above the industry standard of 95%.

It should be noted that this audit is not an endorsement of the reliability or effectiveness of the contract, rather limited to an assessment of the logic and implementation. In order to ensure a secure contract that's able to withstand the Ethereum network's fast-paced and rapidly changing environment, we at Zokyo recommend that the Dogelon Mars team put in place a bug bounty program to encourage further and active analysis of the smart contract.

TABLE OF CONTENTS

Auditing Strategy and Techniques Applied . . . 3

Summary . . . 5

Structure and Organization of Document . . . 6

Complete Analysis . . . 7

Code Coverage and Test Results for all files . . . 9

Tests written by Zokyo Secured team . . . 9

AUDITING STRATEGY AND TECHNIQUES APPLIED

The Smart contract's source code was taken from the Dogelon Mars archive file.

Repository:
https://etherscan.io/address/0x761d38e5ddf6ccf6cf7c55759d5210750b5d60f3#code

Last commit:
bd78e0627583afe5bf944d6c0eae1e653390c000

Contract under the scope:
Dogelon (ELON)

Throughout the review process, care was taken to ensure that the token contract:

- Implements and adheres to existing Token standards appropriately and effectively;
- Documentation and code comments match logic and behavior;
- Distributes tokens in a manner that matches calculations;
- Follows best practices in efficient use of gas, without unnecessary waste;
- Uses methods safe from reentrance attacks;
- Is not affected by the latest vulnerabilities;
- Whether the code meets best practices in code readability, etc.

Zokyo's Security Team has followed best practices and industry-standard techniques to verify the implementation of Dogelon Mars smart contracts. To do so, the code is reviewed line-by-line by our smart contract developers, documenting any issues as they are discovered. Part of this work includes writing a unit test suite using the Truffle testing framework. In summary, our strategies consist largely of manual collaboration between multiple team members at each stage of the review:

1. Due diligence in assessing the overall code quality of the codebase.
2. Cross-comparison with other, similar smart contracts by industry leaders.
3. Testing contract logic against common and uncommon attack vectors.
4. Thorough, manual review of the codebase, line-by-line.

SUMMARY

Zokyo auditing team has run a deep investigation of the Dogelon Mars smart contract. During the auditing process, there were no issues found. The contract is in excellent condition. It is well written and structured.

Based on the conducted audit, we give a score of 100 to the aforementioned contract.

Zokyo auditing team can state that the contract is full production-ready and bear no security or operational risk.

STRUCTURE AND ORGANIZATION OF DOCUMENT

For ease of navigation, sections are arranged from most critical to least critical. Issues are tagged “Resolved” or “Unresolved” depending on whether they have been fixed or addressed. Furthermore, the severity of each issue is written as assessed by the risk of exploitation or other unexpected or otherwise unsafe behavior:

● Critical

The issue affects the ability of the contract to compile or operate in a significant way.

● High

The issue affects the ability of the contract to compile or operate in a significant way.

● Medium

The issue affects the ability of the contract to operate in a way that doesn’t significantly hinder its behavior.

● Low

The issue has minimal impact on the contract’s ability to operate.

● Informational

The issue has no impact on the contract’s ability to operate.

COMPLETE ANALYSIS

During the auditing process (both manual part and testing part) no issues were identified.

	Dogelon (ELON)
Re-entrancy	Pass
Access Management Hierarchy	Pass
Arithmetic Over/Under Flows	Pass
Unexpected Ether	Pass
Delegatecall	Pass
Default Public Visibility	Pass
Hidden Malicious Code	Pass
Entropy Illusion (Lack of Randomness)	Pass
External Contract Referencing	Pass
Short Address/ Parameter Attack	Pass
Unchecked CALL Return Values	Pass
Race Conditions / Front Running	Pass
General Denial Of Service (DOS)	Pass
Uninitialized Storage Pointers	Pass
Floating Points and Precision	Pass
Tx.Origin Authentication	Pass
Signatures Replay	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass

CODE COVERAGE AND TEST RESULTS FOR ALL FILES

Tests written by Zokyo Security team

As part of our work assisting Dogelon Mars in verifying the correctness of their contract code, our team was responsible for writing integration tests using the Truffle testing framework.

Tests were based on the functionality of the code, as well as a review of the Dogelon Mars contract requirements for details about issuance amounts and how the system handles these.

Code Coverage

The resulting code coverage (i.e., the ratio of tests-to-code) is as follows:

FILE	% STMTS	% BRANCH	% FUNCS	% LINES	UNCOVERED LINES
contracts\	100.00	100.00	100.00	100.00	
DOGELON.sol	100.00	100.00	100.00	100.00	
All files	**100.00**	**100.00**	**100.00**	**100.00**	

Test Results

```
Contract: Dogelon
  constructor
    ✓ should deploy with correct token name (142ms)
    ✓ should deploy with the correct token symbol (140ms)
    ✓ should mint tokens to owner correctly (138ms)
  Functions:
    transfer
      ✓ should transfer tokens correctly (1053ms)
      ✓ should revert if the sender is a zero address (2013ms)
      ✓ should revert if the recipient is a zero address (901ms)
      ✓ should revert if the transfer amount exceeds the sender's balance (1032ms)
    transferFrom
      ✓ should transfer tokens correctly (1786ms)
      ✓ should revert if the sender is a zero address (266ms)
      ✓ should revert if the recipient is a zero address (156ms)
      ✓ should revert if the transfer amount exceeds the sender's balance (259ms)
    approve
      ✓ should approve tokens correctly (215ms)
      ✓ should revert if approve to the zero address (260ms)
    allowance
      ✓ should return allowance tokens correctly (89ms)
      ✓ should increase allowance correctly (281ms)
      ✓ should decrease allowance correctly (343ms)
      ✓ should revert if subtracted amount more than current allowance (266ms)

  17 passing (12s)
```

We are grateful to have been given the opportunity to work with the Dogelon Mars team.

The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them.

Zokyo's Security Team recommends that the Dogelon Mars team put in place a bug bounty program to encourage further analysis of the smart contract by third parties.

ZOKYO.