SAFUAUDIT
SMART CONTRACT AUDITING

DOGESTAR

SMART CONTRACT AUDIT

February 22, 2022

INTRODUCTION

Client	DogeStar
Language	Solidity
Contract address	0xB1eEb750fAb190CE97Aee9e65497e609042DaED7
Website	https://dogestar.net/
Telegram	https://t.me/Dogestarofficial
Twitter	https://twitter.com/Dogexstar

Description

DogeStar is a community of crypto enthusiasts who want to make NFT much cooler. The project has a mixed utility (hold and earn to play and earn) with a small collection of NFTs.

TABLE OF CONTENTS

01 INTRODUCTION

Introduction 02

Approach 04

Risk classification 05

02 ABSTRACT

Abstract 06

03 SWC ATTACKS

SWC Attacks 07

04 MANUAL ANALYSIS

Manual analysis 09

Important Snippets 10

05 WEBSITE

Website audit 11

06 CONCLUSIONS

Disclaimer 12

Audit Results 13

Summary 14

Approach

Audit Details

Our comprehensive audit report provides a full overview of the audited system's architecture, smart contract codebase, and details on any vulnerabilities found within the system.

Audit Goals

The audit goal is to ensure that the project is built to protect investors and users, preventing potentially catastrophic vulnerabilities after launch, that lead to scams and rugpulls.

,

Code Quality

Our analysis includes both automatic tests and manual code analysis for the following aspects:

- Exploits
- Back-doors
- Vulnerability
- Accuracy
- Readability

Tools

- Remix IDE
- MythX, Mythril
- SWC Registry
- Open Zeppelin Code Analyzer
- Solidity Code Complier

RISK CLASSIFICATION

CRITICAL

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

MEDIUM

Issues on this level could potentially bring problems and should eventually be fixed.

MINOR

Issues on this level are minor details and warning that can remain unfixed but would be better fixed at some point in the future

INFORMATIONAL

Information level is to offer suggestions for improvement of efficacity or security for features with a risk free factor.

ABSTRACT

Fees	Ownership	Mint function
Buy Fees: 10% Sell Fees: 10%	Owned	No mint function found

Owner can set fees	Max Tx amount	Pause
Owner can set fees up to 100%	Owner can set max tx amount but not to 0	Owner can pause trading

SWC Attacks

SWC ID	Description	
SWC-100	Function Default Visibility	Passed
SWC-101	Integer Overflow and Underflow	Passed
SWC-102	Outdated Compiler Version	Passed
SWC-103	Floating Pragma	Passed
SWC-104	Unchecked Call Return Value	Passed
SWC-105	Unprotected Ether Withdrawal	Passed
SWC-106	Unprotected SELF-DESTRUCT Instruction	Passed
SWC-107	Re-entrancy	Passed
SWC-108	State Variable Default Visibility	Passed
SWC-109	Uninitialized Storage Pointer	Passed
SWC-110	Assert Violation	Passed
SWC-111	Use of Deprecated Solidity Functions	Passed
SWC-112	Delegate Call to Untrusted Callee	Passed
SWC-113	DoS with Failed Call	Passed
SWC-114	Transaction Order Dependence	Passed
SWC-115	Authorization through tx.origin	Passed

SWC-116	Block values as a proxy for time	**Passed**
SWC-117	Signature Malleability	**Passed**
SWC-118	Incorrect Constructor Name	**Passed**
SWC-119	Shadowing State Variables	**Passed**
SWC-120	Weak Sources of Randomness from Chain Attributes	**Passed**
SWC-121	Missing Protection against Signature Replay Attacks	**Passed**
SWC-122	Lack of Proper Signature Verification	**Passed**
SWC-123	Requirement Violation	**Passed**
SWC-124	Write to Arbitrary Storage Location	**Passed**
SWC-125	Incorrect Inheritance Order	**Passed**
SWC-126	Insufficient Gas Griefing	**Passed**
SWC-127	Arbitrary Jump with Function Type Variable	**Passed**
SWC-128	DoS With Block Gas Limit	**Passed**
SWC-129	Typographical Error	**Passed**
SWC-130	Right-To-Left-Override control character (U+202E)	**Passed**
SWC-131	Presence of unused variables	**Passed**
SWC-132	Unexpected Ether balance	**Passed**
SWC-133	Hash Collisions With Multiple Variable Length Arguments	**Passed**
SWC-134	Message call with the hardcoded gas amount	**Passed**
SWC-135	Code With No Effects (Irrelevant/Dead Code)	**Passed**
SWC-136	Unencrypted Private Data On-Chain	**Passed**

MANUAL ANALYSIS

The contract is verified to check if functions do and work as they should and malicious code is not inserted.

	Tested	Result
Transfer	Yes	**Passed**
Total Supply	Yes	**Passed**
Buy Back	Yes	**Passed**
Burn	Yes	**N/A**
Mint	Yes	**N/A**
Rebase	Yes	**N/A**
Pause	Yes	**Low**
Blacklist	Yes	**N/A**
Lock	Yes	**N/A**
Max Transaction	Yes	**Passed**
Transfer Ownership	Yes	**Passed**
Renounce Ownership	Yes	**Passed**

MANUAL AUDIT

Important snippets

Owner can stop trading

```
function tradingStatus(bool _status) public onlyOwner {
    tradingOpen = _status;
}
```

Owner can set taxes up to 100%

```
function setFees(uint256 _liquidityFee, uint256 _reflectionFee, uint256 _marketingFee,
uint256 _buybackFee, uint256 _devFee, uint256 _feeDenominator)
 external authorized {
    liquidityFee = _liquidityFee;
    reflectionFee = _reflectionFee;
    marketingFee = _marketingFee;
    buybackFee = _buybackFee;
    devFee = _devFee;
    totalFee = _liquidityFee.add(_reflectionFee).add(_marketingFee).add(_buybackFee).add(_devFee);
    feeDenominator = _feeDenominator;
}
```

Owner can set max transaction limit but not to 0

```
function setTxLimit(uint256 amount) external authorized {
    require(amount >= _totalSupply / 1000);
    _maxTxAmount = amount;
}
```

WEBSITE

Website	https://dogestar.net/
Domain Registry	http://www.lws.fr/
Domain Expiry Date	2023-01-29
Response Code	500
SSL Checker and HTTPS Test	Passed
Deprecated HTML tags	Low
Robots.txt	Passed
Sitemap Test	Low
SEO Friendly URL	Passed
Responsive Test	Low
JS Error Test	Passed
Console Errors Test	Passed
Site Loading Speed Test	2.4 seconds
HTTP2 Test	Passed
Safe Browsing Test	Passed

DISCLAIMER

SafuAudit.com is not a financial institution and the information provided on this website does not constitute investment advice, financial advice, trading advice or any other sort of advice. You should not treat any of the website's content as such. Investing in crypto assets carries a high level of risk and does not hold guarantees for not sustaining financial loss due to their volatility.

Accuracy of Information

SafuAudit will strive to ensure accuracy of information listed on this website although it will not hold any responsibility for any missing or wrong information. SafuAudit provides all information as is. You understand that you are using any and all information available here at your own risk. Any use or reliance on our content and services is solely at your own risk and discretion.

The purpose of the audit is to analyse the on-chain smart contract source code, and to provide basic overview of the project.

While we have used all the information available to us for this straightforward investigation, you should not rely on this report only — we recommend proceeding with several independent audits Be aware that smart contracts deployed on a blockchain aren't secured enough against external vulnerability, or a hack. Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's safety and security. Therefore, SafuAudit does not guarantee the explicit security of the audited smart contract. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

AUDIT RESULTS

CRITICAL

No critical severity issues have been found.

MEDIUM

No medium severity issues have been found.

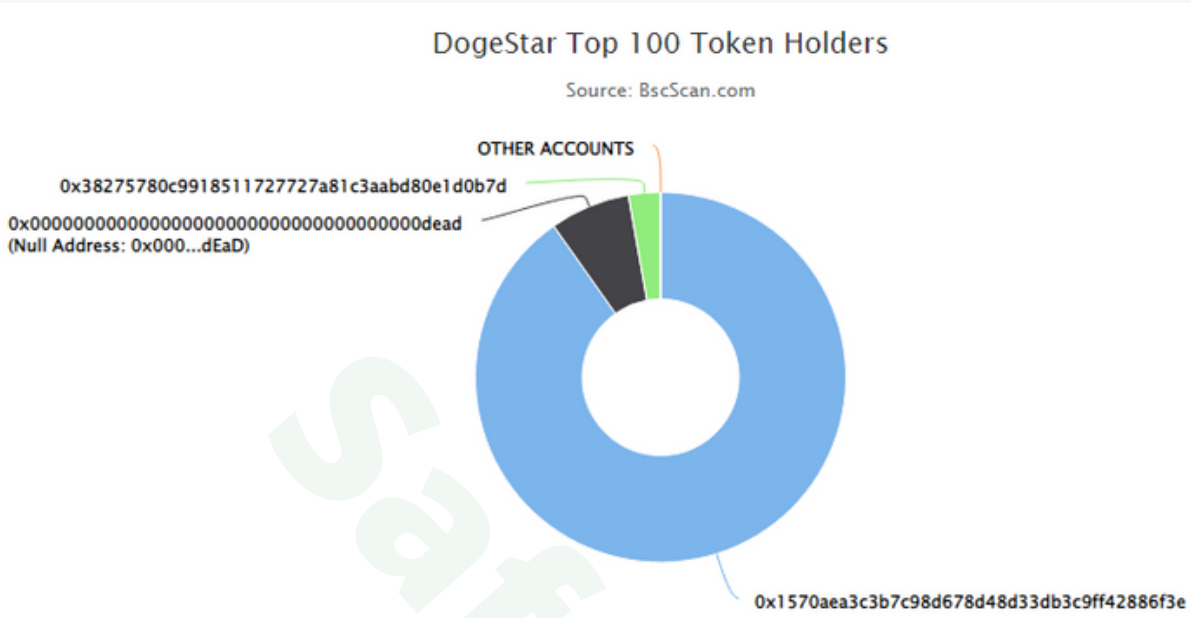
MINOR

1. Owner can Pause trading - can be fixed with some limits added
2. Owner can set fees up to 100% - can be fixed with upper limits added

INFORMATIONAL

The standard audit model does not offer suggestions and consulting for improvements of efficacity.

SUMMARY



Rank	Address	Quantity (Token)	Percentage
1	0x1570aea3c3b7c98d678d48d33db3c9ff42886f3e	902,250,000	90.2250%
2	Null Address: 0x000...dEaD	70,000,000	7.0000%
3	0x38275780c9918511727727a81c3aabd80e1d0b7d	27,750,000	2.7750%

Conclusion

Project DogeStar does not contain any severe issues. SafuAudit has tested the security based on manual and automated tests. Please note that we don't offer any warranties for business model.