SMART CONTRACT SECURITY AUDIT

WATCHTOWER

AUDIT DETAILS

Project Name

MOONSPINY COIN

Contract address

0xda994d9a9f93f87a4f3280b392a7faf4f2aefacf

Deployer Address:

0xA40B3EF194315b09E5D93a289bf5a83F4b6CD51d

Blockchain

Binance Smart Chain

Project website:

http://Moonspiny.com

DISCLAIMER

Watchtower has completed this report to provide a summary of the Smart Contract functions, and any security, dependency or cybersecurity vulnerabilities. This is often a constrained report on our discoveries based on our investigation and understanding of the current programming versions as at the date of this report. In order to understand the full scope of our analysis, it is vital for you to review the complete report. Although we have done our best in conducting our investigation and creating this report, it is vital to note that you should not depend on this report and cannot make any claim against Watchtower or it's Subsidiaries and Team members on the premise of what has or has not been included in the report. Please remember to conduct your own independent examinations before making any investment choices. We do not provide investment advice or in any way claim to determine if the project will be successful or not.

DISCLAIMER: By perusing this report or any portion of it, you concur to the terms of this disclaimer. In the unlikely situation where you do not concur to the terms, you should immediately terminate reading this report, and erase and discard any and all duplicates of this report downloaded and/or printed by you. This report is given for data purposes as it were and on a non-reliance premise, and does not constitute speculation counsel. No one should have any right to depend on the report or its substance, and Watchtower and its members (including holding companies, shareholders, backups, representatives, chiefs, officers and other agents) Watchtower and it's subsidiaries owe no obligation of care towards you or any other person, nor does Watchtower make any guarantee or representation to any individual on the precision or completeness of the report.

ABOUT THE AUDITOR:
Watchtower is an Anti-Scam Token Utility which reviews Smart Contracts and Token information to Identify Rug Pull and Honey Pot scamming activity.
Watchtowers Development Team consists of a number of Smart Contract creators, Auditors Developers and Blockchain experts.
Watchtowers Website Scanner reviews a number of Risk factors to provide an adequate Risk summary of token projects.
In Addition to this the team also helps with Creation of Smart Contracts for legitimate projects, Audits and Promotion.

OVERVIEW

Watchtower was contracted by MOONSPINY COIN to complete a Smart Contract audit

The objective of the Audit is to achieve the following:

- Provide an Overview and Summary of the Token project.
- Review Team competency and identify risks
- Ensure that the Smart Contract functions are necessary and operate as intended.
- Identify any vulnerabilities in the Smart Contract code.

DISCLAIMER: This Audit is intended to inform about token Contract Risks, the result does not imply an endorsement or in any way provide financial advice, please do invest at your own risk.
(https://www.cryptowatchtower.io/)

SMART CONTRACT REVIEW

Contract Created on 08.02.2021

Contract name	MOONSPINY COIN
Contract address	0xda994d9a9f93f87a4f3280b392a7faf4f2aefacf
Total supply	100,000,000
Token ticker	MSY
Decimals	3
Token holders	11
Transactions count	13
Top 5 holders dominance	99.00%
Tax fee	0%
Total fees	0%
Contract deployer address	0xA40B3EF194315b09E5D93a289bf5a83F4b6CD51d
Contract's current owner address	0xA40B3EF194315b09E5D93a289bf5a83F4b6CD51d

MOONSPINNY Overview

Project Details:

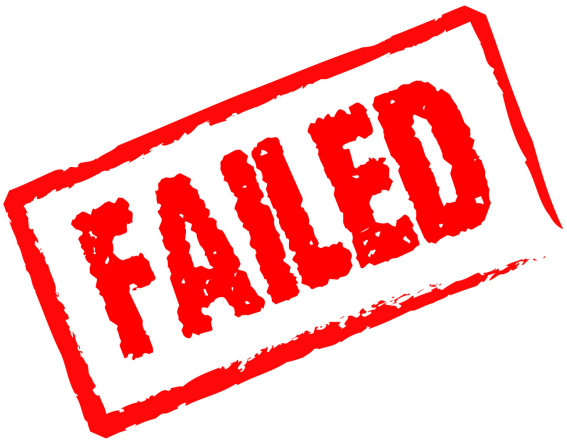
Moonspiny is a Charity token on the Binance Smart Chain. It is designed to donate monthly to community-selected charities while simultaneously providing potential rewards to investors through deflationary tokenomics fundamentals and an innovative, self- fulfilling marketing strategy feeding long term project popularity and growth.

Tokenomics:

Starting Supply: 100,000,000 (100 Million)
No Tokenomics evident in contract.
Dev claims manual burn and redistribution of 2% will be enacted.

Team Review:

The MOONSPINNY team don't seem to understand the tokenomics of their contract. The claimed burn function and redistribution are not evident in the contract!
This was raised with the Moonspiny team who claimed they would do it manually which is impossible to track. The team then closed their telegram and social media pages which leads us to believe we caught out a scam before it occurred!



CONTRACT FUNCTIONS DETAILS

FUNCTIONS (PUBLIC)

1. approve (Spender Address) - generally used to authorise the pre-sale address.
2. Transfer (To, From)
3. Transfer (From, To)

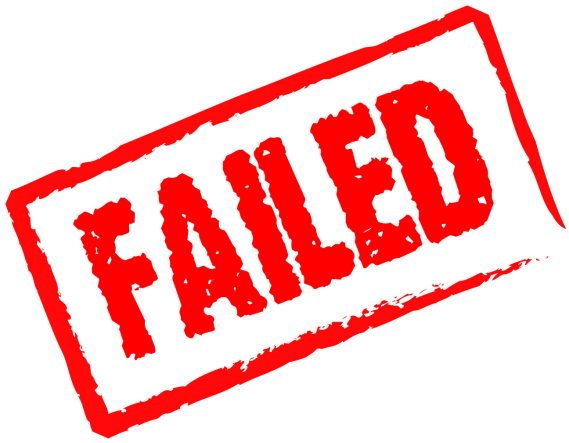
Function Risks

Upon review of Smart Contract Coding and Functions available for the Owner to change Watchtower is satisfied that no malicious coding has been found however the claimed tokenomics did not exist in the contract.

Note: The contract version and functionality is limited and provides security since the owner cannot manipulate the contract fees to cause a honeypot.
The contract effectively can be renounced as there are no functions required to be called however there is no renounce functionality either.

The contract itself was safe but Watchtower believes either the team was too inexperienced or they were attempting to scam in another way!

This audit has failed.



Imported Libraries / Interfaces

- SafeMath
- IERC20

Overview

1. ADDITION OF COMMENTS: 6
2. CALL STACK DEPTH ATTACK: 10
3. TIME STAMP DEPENDENCY: 10
4. PARTY MULTISIG BUG: 10
5. USE OF LIBRARIES/DEPENDENCIES (FROM TRUSTED SOURCES): 7
    a. TRANSACTION-ORDERING DEPENDENCY: 10
6. ACCESS CONTROL AND AUTHORIZATION: 5
7. REENTRANCY ATTACKS: 10
8. ERC/BEP STANDARD VIOLATIONS: 10
9. USAGE OF VISIBILITY LEVELS: 10

ISSUES CHECKING STATUS

Issue description	Checking status
1. Compiler errors.	Passed
2. Race conditions and Reentrancy. Cross-function race conditions.	Passed
3. Possible delays in data delivery.	Passed
4. Oracle calls.	Passed
5. Front running.	Passed
6. Timestamp dependence.	Passed
7. Integer Overflow and Underflow.	Passed
8. DoS with Revert.	Passed
9. DoS with block gas limit.	Passed
10. Methods execution permissions.	Passed

Issue description	Checking status
11. Economy model of the contract.	Passed
12. The impact of the exchange rate on the logic.	Passed
13. Private user data leaks.	Passed
14. Malicious Event log.	Passed
15. Scoping and Declarations.	Passed
16. Uninitialized storage pointers.	Passed
17. Arithmetic accuracy.	Passed
18. Design Logic.	Passed
19. Cross-function race conditions.	Passed
20. Safe Open Zeppelin contracts implementation and usage.	Passed
21. Fallback function security.	Passed

SECURITY ISSUES

High Severity Issues

No High Severity Issues found.

Medium Severity Issues

No Medium Severity issues found.

Low Severity Issues

No Low Severity issues found.

CONCLUSION

The contract seems to be a copy of https://github.com/CodeWithJoe2020/ERC20Token/blob/main/ERC20.sol
The Smart Contract Functions are safe, void of any malicious coding and the owner has limited functions access which provide confidence in the contract. There are no severity issues however it is highly recommended to update the version to 0.8.0+

NOTE: The Moonspiny team was advised their contract does not do what they claimed and they have now closed off their social media pages and disappeared.

Watchtower note:

Please check the disclaimer above and note, this Audit is intended to inform about token Contract Risks, the result does not imply an endorsement or in any way provide financial advice, please invest at your own risk.
(https://www.cryptowatchtower.io/)

Contact Us

@Watchtower_WTW

Watchtower-WTW

Watchtowercrypto