# SMC AUDITORS

# DoubleMoon
# Smart Contract Audit

SMCAuditors

https://smcauditors.com / info@smcauditors.com

10th of August 2021

*This document is the audit of the DoubleMoon smart contract performed by SMCAuditors.*

# 1. Executive Summary

This report was written to provide a security audit for DoubleMoon (https://doublemoon.finance) smart contract. DoubleMoon is a deflationary token on Binance Smart Chain with a burning function and yield generating features. SMCAuditors conducted the audit focusing on whether DoubleMoon smart contract is designed and implemented without any security vulnerabilities. The contract is listed below with its link.

- DoubleMoon
  - https://bscscan.com/token/0x0314e5a39806C30D67B869EE1bCDABee7e08dE74

We have run extensive static analysis of the codebase as well as standard security assessment utilising industry approved tools. There are no critical/high level issues with

the currently deployed token contract. Our low and medium level findings are available in the next section.

# 2. Audit Findings

## Low Level Findings

- ❖ *includeInReward()* and *_getCurrentSupply* functions use a loop to find and remove addresses from the _excluded list. Function will be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list. You can use *EnumerableSet* instead of array or not use long arrays.

## Medium Level Findings

- ❖ Ownership of the token is not renounced and the owner can change the token tax fee, liquidity fee, marketing fee and commission amounts. These changes may have negative effects if not set correctly or maliciously set. Consider setting these amounts right once and then renouncing ownership.

# 3. Conclusion

In this audit, we thoroughly analyzed the DoubleMoon token smart contract. Our identified issues are promptly confirmed and taken into consideration.

# 4. Disclaimer

This report is not advice on investment, nor does it guarantee adequacy of a business model and/or a bug-free code. This report should be used only to discuss known technical problems. It will be necessary to resolve addressed issues and conduct thorough tests to ensure the safety of the smart contract.