

SMART CONTRACT SECURITY AUDIT MS MOONA REWARDS



SMART CONTRACT AUDIT | TEAM KYC | PROJECT EVALUATION

RELENTLESSLY SECURING THE PUBLIC BLOCKCHAIN | MADE IN CANADA 

Summary

| | |
|---|--|
| Auditing Firm | InterFi Network |
| Architecture | InterFi "Echelon" Auditing Standard |
| Smart Contract Audit Approved By | Chris Blockchain Specialist at InterFi Network |
| Project Overview Approved BY | Albert Project Specialist at InterFi Network |
| Platform | Solidity |
| Audit Check (Mandatory) | Static, Software, Auto Intelligent & Manual Analysis |
| Project Check (Optional) | KYC, Website & Socials Analysis (Not Applicable) |
| Consultation Request Date | October 07, 2021 |
| Report Date | October 09, 2021 (Fast-tracked) |

Audit Summary

Smart Contract Security Audit

InterFi team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit:

- ❖ **Ms Moona Rewards' smart contract source codes has **LOW RISK SEVERITY**.**
- ❖ **Ms Moona Rewards has successfully **PASSED** the smart contract audit.**

For the detailed understanding of risk severity, source code vulnerability, and functional test, kindly refer to the audit.



Table Of Contents

Project Information

| | |
|----------------|---|
| Overview | 4 |
|----------------|---|

InterFi “Echelon” Audit Standard

| | |
|------------------------------------|---|
| Audit Scope & Methodology | 7 |
| InterFi’s Risk Classification..... | 9 |

Smart Contract Risk Assessment

| | |
|--------------------------------|----|
| Contract Overview | 10 |
| Static Analysis..... | 11 |
| Software Analysis | 16 |
| Manual Analysis..... | 21 |
| SWC Attacks..... | 23 |
| Risk Status & Radar Chart..... | 25 |

Report Summary

| | |
|-------------------------|----|
| Auditor’s Verdict | 26 |
|-------------------------|----|

Legal Advisory

| | |
|----------------------------|----|
| Important Disclaimer | 27 |
| About InterFi Network..... | 28 |



Project Overview

InterFi was consulted by Ms Moona Rewards on October 07, 2021 to conduct a smart contract security audit of their token source code and ICO source code.

Moona aims to make a platform that constantly grows until it can achieve a fully decentralized status where the development fund's rewards will be turned off entirely and ownership renounced. Basically, moona's goal is to build a sustainable ecosystem composed of consumers and merchants.

| | |
|-------------------|---|
| Project | MS MOONA REWARDS |
| Blockchain | Binance Smart Chain Mainnet / Binance Blockchain Explorer |
| Language | Solidity |
| Contract | 0xe157020a326651e957f9cDe7366A1D5fdBC039c5 |
| Website | https://moona.finance/ |
| Twitter | https://twitter.com/MoonaRewards |
| Telegram | https://t.me/moona_rewards |
| Reddit | https://www.reddit.com/r/MsMoonaRewards/ |
| Discord | https://discord.com/invite/hmgAz9DcBq |
| Instagram | https://www.instagram.com/moonarewards/ |



Public logo



Solidity Source Code On InterFi GitHub

<https://github.com/interfinetwork/audited-codes/blob/main/Moona.sol>

GitHub Commits

Solidity source code committed at: a36cdf010e129b56c562ef8658fbc7ed75ceeb59



Contract Source Code On Blockchain (BscScan Verified With Exact Match)

<https://bscscan.com/address/0xe157020a326651e957f9cDe7366A1D5fdBC039c5#code>

Contract Name: MoonaToken

Compiler Version: v0.7.6+commit.7338295f

Optimization Enabled: Yes with 200 runs

Files Under Scope (Solidity Multiple Files Format)

- ❖ MoonaToken.sol
- ❖ Context.sol
- ❖ DividendPayingToken.sol
- ❖ DividendPayingTokenInterface.sol
- ❖ DividendPayingTokenOptionalInterface.sol
- ❖ ERC20.sol
- ❖ IERC20.sol
- ❖ IERC20Metadata.sol
- ❖ IterableMapping.sol
- ❖ IUniswapV2Pair.sol
- ❖ IUniswapV2Router.sol
- ❖ IUniswapV2Factory.sol
- ❖ MoonaRewardsTracker.sol
- ❖ Ownable.sol
- ❖ RewardsContract.sol
- ❖ SafeMath.sol
- ❖ SafeMathInt.sol
- ❖ SafeMathUint.sol

Smart Contract
Security Audit



Audit Scope & Methodology

The scope of this report is to audit the smart contract source code of Ms Moona Rewards (Moona).

The source code can be viewed in its entirety on

<https://github.com/interfinetwork/audited-codes/blob/main/Moona.sol>

InterFi has scanned the contract and reviewed the project for common vulnerabilities, exploits, hacks, and back-doors. Below is the list of commonly known smart contract vulnerabilities, exploits, and hacks:

Category

Smart Contract Vulnerabilities

- ❖ Re-entrancy (RE)
- ❖ Unhandled Exceptions (UE)
- ❖ Transaction Order Dependency (TO)
- ❖ Integer Overflow (IO)
- ❖ Unrestricted Action (UA)
- ❖ Ownership Takeover
- ❖ Gas Limit and Loops

Source Code Review

- ❖ Deployment Consistency
- ❖ Repository Consistency
- ❖ Data Consistency
- ❖ Token Supply Manipulation
- ❖ Access Control and Authorization
- ❖ Operations Trail and Event Generation

Functional Assessment

- ❖ Assets Manipulation
- ❖ Liquidity Access



InterFi's Echelon Audit Standard

The aim of InterFi's "Echelon" standard is to analyze the smart contract and identify the vulnerabilities and the hacks in the smart contract. Mentioned are the steps used by ECHELON-1 to assess the smart contract:

1. Solidity smart contract source code reviewal:
 - ❖ Review of the specifications, sources, and instructions provided to InterFi to make sure we understand the size, scope, and functionality of the smart contract.
 - ❖ Manual review of code, which is the process of reading source code line-byline to identify potential vulnerabilities.
2. Static, Manual, and Automated AI analysis:
 - ❖ Test coverage analysis, which is the process of determining whether the test cases are covering the code and how much code is exercised when we run those test cases.
 - ❖ Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts

Automated 3P frameworks used to assess the smart contract vulnerabilities

- ❖ Slither
- ❖ Consensys MythX
- ❖ Consensys Surya
- ❖ Open Zeppelin Code Analyzer
- ❖ Solidity Code Compiler



InterFi's Risk Classification

Smart contracts are generally designed to manipulate and hold funds denominated in ETH/BNB. This makes them very tempting attack targets, as a successful attack may allow the attacker to directly steal funds from the contract. Below are the typical risk levels of a smart contract:

Vulnerable: A contract is vulnerable if it has been flagged by a static analysis tool as such. As we will see later, this means that some contracts may be vulnerable because of a false-positive.

Exploitable: A contract is exploitable if it is vulnerable and the vulnerability could be exploited by an external attacker. For example, if the "vulnerability" flagged by a tool is in a function which requires to own the contract, it would be vulnerable but not exploitable.

Exploited: A contract is exploited if it received a transaction on the main network which triggered one of its vulnerabilities. Therefore, a contract can be vulnerable or even exploitable without having been exploited.

| Risk severity | Meaning |
|-------------------|--|
| ! Critical | This level vulnerabilities could be exploited easily, and can lead to asset loss, data loss, asset manipulation, or data manipulation. They should be fixed right away. |
| ! High | This level vulnerabilities are hard to exploit but very important to fix, they carry an elevated risk of smart contract manipulation, which can lead to critical risk severity |
| ! Medium | This level vulnerabilities are should be fixed, as they carry an inherent risk of future exploits, and hacks which may or may not impact the smart contract execution. |
| ! Low | This level vulnerabilities can be ignored. They are code style violations, and informational statements in the code. They may not affect the smart contract execution |







Smart Contract – Overview

Contract information



| Query | Result |
|-------------------------|--|
| Name | Ms. Moona Rewards |
| Symbol | MOONA |
| Decimals | 18 |
| Total Supply | 16,000,000,000 |
| Owner | 0x1d9361ffbd96226143d6a8358da4b026563951b1 |
| Rewards Token | CAKE |
| Liquidity Fee | 3 |
| Rewards Fee | 8 |
| Liquidity Wallet | 0x1d9361ffbd96226143d6a8358da4b026563951b1 |
| Marketing Wallet | 0x2b95ea2171ab3b1aef48ed1a9939181118437771 |
| Rewards Wallet | 0x7302a9f7efaa1fad0314d7dee9e2db955d038865 |
| Rewards Tracker | 0x7ef74bf85176dd6bff9ffc14ee63d17d54d4dcf6 |
| BOT Wallet | 0x426e3be2cc72f2cdcaf4e55104dc7af8a0565388 |
| Uniswap pair | 0xf1fdf25e7478d2d217168f8dfdecf395a42aff0d |
| Uniswap Router | 0x10ed43c718714eb63d5aa57b78b54704e256024e |



Smart Contract – Static Analysis

| Symbol | Meaning |
|---|--------------------------|
|  | Function can be modified |
|  | Function is payable |
|  | Function is locked |
|  | Function can be accessed |
| ! | Important functionality |

```

| ++MoonaToken++ | Implementation | ERC20, Ownable |||
| | <Constructor> | Public ! |  | ERC20 |
| | <Receive Ether> | External ! |  | NO ! |
| | rewardsAdd | Public ! |  | onlyOwner |
| | rewardsSend | Public ! |  | onlyOwner |
| | rewardsTime | Public ! |  | onlyOwner |
| | excludeFromFees | Public ! |  | onlyOwner |
| | _setAutomatedMarketMakerPair | Private  |  | |
| | withdrawETH | Public ! |  | onlyOwner |
| | elonSet | External ! |  | onlyOwner |
| | updateGasForProcessing | Public ! |  | onlyOwner |
| | getTotalRewardsDistributed | External ! | | NO ! |
| | getAccountRewardsInfo | Public ! | | NO ! |
| | processRewardsTracker | External ! |  | NO ! |
| | claim | External ! |  | NO ! |
| | checkRewardTokenShares | External ! | | NO ! |
| | updateHolderRewardsOffset | External ! |  | onlyOwner |
| | updateSingleHolderRewardsOffset | External ! |  | onlyOwner |
| | clearHolderRewardsOffset | External ! |  | onlyOwner |
| | seeOffset | External ! | | NO ! |
| | changeMinimumBalanceToReceiveRewards | Public ! |  | onlyOwner |
| | _transfer | Internal  |  | |
| | swapAndLiquify | Private  |  | |
| | swapTokensForEth | Private  |  | |
| | addLiquidity | Private  |  | |
| | swapAndSendDividends | Private  |  | |
| | changeUserCustomToken | External ! |  | NO ! |
| | resetUserCustomToken | External ! |  | NO ! |
| | seeUserCustomToken | External ! | | NO ! |
| | changeRewardsToken | External ! |  | NO ! |

```



```

| L | viewRewardsToken | External ! | |NO ! |
| L | viewRewardsTokenCount | External ! | |NO ! |
| L | viewRewardsPercentage | External ! | |NO ! |
| L | viewRewardsTokens | External ! | |NO ! |
| L | getLastRewardsTokens | Public ! | |NO ! |
| L | changeRewardsPercentage | External ! | ● | onlyOwner |
| L | changeUserClaimTokenPercentage | External ! | ● |NO ! |
| L | seeUserClaimTokenPercentage | External ! | |NO ! |
| L | viewUserCustomClaimTokenPercentage | External ! | |NO ! |
| L | resetUserClaimTokenPercentage | External ! | ● |NO ! |
| L | seeUserRewardsSetup | Public ! | |NO ! |
| L | changeUserRewardsSetup | Public ! | ● |NO ! |
| L | seeTxCountRewards | Public ! | |NO ! |
| L | changeBotWallet | Public ! | ● | onlyOwner |
| L | viewBotWallet | Public ! | |NO ! |
|||||
| **Context** | Implementation | |||
| L | _msgSender | Internal 🔒 | | |
| L | _msgData | Internal 🔒 | | |
|||||
| **DividendPayingToken** | Implementation | ERC20, Ownable, DividendPayingTokenInterface,
DividendPayingTokenOptionalInterface |||
| L | <Constructor> | Public ! | ● | ERC20 |
| L | <Receive Ether> | External ! | 💰 |NO ! |
| L | distributeDividends | Public ! | 💰 |NO ! |
| L | withdrawDividend | Public ! | ● |NO ! |
| L | _withdrawDividendOfUser | Internal 🔒 | ● | |
| L | getRewardsRatio | Internal 🔒 | | |
| L | setRewardsPercentage | External ! | ● | onlyOwner |
| L | setUserClaimTokenPercentage | Public ! | ● |NO ! |
| L | viewUserClaimTokenPercentage | Public ! | |NO ! |
| L | clearUserClaimTokenPercentage | External ! | ● |NO ! |
| L | getCurrentRewardsToken | Public ! | |NO ! |
| L | setBotWallet | Public ! | ● | onlyOwner |
| L | setRewardsToken | Public ! | ● |NO ! |
| L | getRewardsTokensCount | External ! | |NO ! |
| L | getRewardsTokens | External ! | |NO ! |
| L | getLastRewardsTokens | Public ! | |NO ! |
| L | swapEthForCustomToken | Internal 🔒 | ● | |
| L | updateUserCustomToken | Public ! | ● |NO ! |
| L | clearUserCustomToken | Public ! | ● |NO ! |
| L | viewUserCustomToken | Public ! | |NO ! |
| L | viewUserRewardsSetup | External ! | |NO ! |
| L | setUserRewardsSetup | External ! | ● |NO ! |
| L | dividendOf | Public ! | |NO ! |
| L | withdrawableDividendOf | Public ! | |NO ! |
| L | withdrawnDividendOf | Public ! | |NO ! |
| L | accumulativeDividendOf | Public ! | |NO ! |
| L | _transfer | Internal 🔒 | ● | |
| L | _mint | Internal 🔒 | ● | |

```



```

| L | _burn | Internal | 🔒 | 🔴 | |
| L | _setBalance | Internal | 🔒 | 🔴 | |
| L | checkShares | Public | ! | | NO ! |
| | | |
| **DividendPayingTokenInterface** | Interface | | |
| L | dividendOf | External | ! | | NO ! |
| L | distributeDividends | External | ! | 🏧 | NO ! |
| L | withdrawDividend | External | ! | 🔴 | NO ! |
| | | |
| **DividendPayingTokenOptionalInterface** | Interface | | |
| L | withdrawableDividendOf | External | ! | | NO ! |
| L | withdrawnDividendOf | External | ! | | NO ! |
| L | accumulativeDividendOf | External | ! | | NO ! |
| | | |
| **ERC20** | Implementation | Context, IERC20, IERC20Metadata | | |
| L | <Constructor> | Public | ! | 🔴 | NO ! |
| L | name | Public | ! | | NO ! |
| L | symbol | Public | ! | | NO ! |
| L | decimals | Public | ! | | NO ! |
| L | totalSupply | Public | ! | | NO ! |
| L | balanceOf | Public | ! | | NO ! |
| L | transfer | Public | ! | 🔴 | NO ! |
| L | allowance | Public | ! | | NO ! |
| L | approve | Public | ! | 🔴 | NO ! |
| L | transferFrom | Public | ! | 🔴 | NO ! |
| L | increaseAllowance | Public | ! | 🔴 | NO ! |
| L | decreaseAllowance | Public | ! | 🔴 | NO ! |
| L | _transfer | Internal | 🔒 | 🔴 | |
| L | _mint | Internal | 🔒 | 🔴 | |
| L | _burn | Internal | 🔒 | 🔴 | |
| L | _approve | Internal | 🔒 | 🔴 | |
| L | _beforeTokenTransfer | Internal | 🔒 | 🔴 | |
| | | |
| **IERC20** | Interface | | |
| L | totalSupply | External | ! | | NO ! |
| L | balanceOf | External | ! | | NO ! |
| L | transfer | External | ! | 🔴 | NO ! |
| L | allowance | External | ! | | NO ! |
| L | approve | External | ! | 🔴 | NO ! |
| L | transferFrom | External | ! | 🔴 | NO ! |
| | | |
| **IERC20Metadata** | Interface | IERC20 | | |
| L | name | External | ! | | NO ! |
| L | symbol | External | ! | | NO ! |
| L | decimals | External | ! | | NO ! |
| | | |
| **IterableMapping** | Library | | |
| L | get | Public | ! | | NO ! |
| L | getIndexOfKey | Public | ! | | NO ! |
| L | getKeyAtIndex | Public | ! | | NO ! |

```



```

| L | size | Public ! | |NO ! |
| L | set | Public ! | ● |NO ! |
| L | remove | Public ! | ● |NO ! |
| | | |
| **IUniswapV2Factory** | Interface | | |
| L | feeTo | External ! | |NO ! |
| L | feeToSetter | External ! | |NO ! |
| L | getPair | External ! | |NO ! |
| L | allPairs | External ! | |NO ! |
| L | allPairsLength | External ! | |NO ! |
| L | createPair | External ! | ● |NO ! |
| L | setFeeTo | External ! | ● |NO ! |
| L | setFeeToSetter | External ! | ● |NO ! |
| | | |
| **IUniswapV2Pair** | Interface | | |
| L | name | External ! | |NO ! |
| L | symbol | External ! | |NO ! |
| L | decimals | External ! | |NO ! |
| L | totalSupply | External ! | |NO ! |
| L | balanceOf | External ! | |NO ! |
| L | allowance | External ! | |NO ! |
| L | approve | External ! | ● |NO ! |
| L | transfer | External ! | ● |NO ! |
| L | transferFrom | External ! | ● |NO ! |
| L | DOMAIN_SEPARATOR | External ! | |NO ! |
| L | PERMIT_TYPEHASH | External ! | |NO ! |
| L | nonces | External ! | |NO ! |
| L | permit | External ! | ● |NO ! |
| L | MINIMUM_LIQUIDITY | External ! | |NO ! |
| L | factory | External ! | |NO ! |
| L | token0 | External ! | |NO ! |
| L | token1 | External ! | |NO ! |
| L | getReserves | External ! | |NO ! |
| L | price0CumulativeLast | External ! | |NO ! |
| L | price1CumulativeLast | External ! | |NO ! |
| L | kLast | External ! | |NO ! |
| L | mint | External ! | ● |NO ! |
| L | burn | External ! | ● |NO ! |
| L | swap | External ! | ● |NO ! |
| L | skim | External ! | ● |NO ! |
| L | sync | External ! | ● |NO ! |
| L | initialize | External ! | ● |NO ! |
| | | |
| **MoonaRewardsTracker** | Implementation | Ownable, DividendPayingToken | |
| L | <Constructor> | Public ! | ● | DividendPayingToken |
| L | _transfer | Internal 🔒 | | |
| L | withdrawDividend | Public ! | |NO ! |
| L | excludeFromDividends | External ! | ● | onlyOwner |
| L | getAccount | Public ! | |NO ! |
| L | canAutoClaim | Private 🔒 | | |

```



```

| L | updateMoonaBalance | External ! | ● | onlyOwner |
| L | updateSingleHolderShares | External ! | ● | onlyOwner |
| L | updateHolderShares | External ! | ● | onlyOwner |
| L | clearShares | Public ! | ● | onlyOwner |
| L | setMinimumBalanceToReceiveDividends | External ! | ● | onlyOwner |
| L | setBalance | Public ! | ● | onlyOwner |
| L | viewOffset | Public ! | | NO ! |
| L | process | Public ! | ● | NO ! |
| L | processAccount | Public ! | ● | onlyOwner |
| | | | |
| **Ownable** | Implementation | Context | | |
| L | <Constructor> | Public ! | ● | NO ! |
| L | owner | Public ! | | NO ! |
| L | transferOwnership | Public ! | ● | onlyOwner |
| | | | |
| **RewardsContract** | Implementation | Ownable | | |
| L | <Constructor> | Public ! | ● | NO ! |
| L | adder | External ! | ● | onlyOwner |
| L | statusFind | External ! | | onlyOwner |
| L | swapTokensForEthMarketing | External ! | ● | onlyOwner |
| L | withdrawToMarketing | External ! | ● | onlyOwner |
| | | | |
| **SafeMath** | Library | | | |
| L | add | Internal 🔒 | | |
| L | sub | Internal 🔒 | | |
| L | sub | Internal 🔒 | | |
| L | mul | Internal 🔒 | | |
| L | div | Internal 🔒 | | |
| L | div | Internal 🔒 | | |
| | | | |
| **SafeMathInt** | Library | | | |
| L | mul | Internal 🔒 | | |
| L | div | Internal 🔒 | | |
| L | sub | Internal 🔒 | | |
| L | add | Internal 🔒 | | |
| L | toUint256Safe | Internal 🔒 | | |
| | | | |
| **SafeMathUint** | Library | | | |
| L | toInt256Safe | Internal 🔒 | | |

```



Smart Contract – Software Analysis

Callout functions – Sighash

| Sighash | | Function Signature |
|----------|----|--|
| ===== | | |
| 20589707 | => | getAccountRewardsInfo(address) |
| 39509351 | => | increaseAllowance(address,uint256) |
| 43509138 | => | div(int256,int256) |
| 44591001 | => | updateMoonaBalance(address,uint256) |
| 55867375 | => | changeRewardsToken(address) |
| 793347eb | => | rewardsAdd(address) |
| 10e645f8 | => | rewardsSend(uint256) |
| f3bf6bad | => | rewardsTime(uint256,uint256,uint256) |
| c0246668 | => | excludeFromFees(address,bool) |
| a7f7b36f | => | _setAutomatedMarketMakerPair(address,bool) |
| 4782f779 | => | withdrawETH(address,uint256) |
| b4673917 | => | elonSet(uint256) |
| 871c128d | => | updateGasForProcessing(uint256) |
| e7c52d44 | => | getTotalRewardsDistributed() |
| c325c97d | => | processRewardsTracker(uint256) |
| 4e71d92d | => | claim() |
| 9ba2511f | => | checkRewardTokenShares(address) |
| 131b11a2 | => | updateHolderRewardsOffset(address,uint256[]) |
| 21bb7f5d | => | updateSingleHolderRewardsOffset(address,uint256) |
| f7560b35 | => | clearHolderRewardsOffset(address) |
| 633e1b65 | => | seeOffset(address) |
| c387acde | => | changeMinimumBalanceToReceiveRewards(uint256) |
| 30e0789e | => | _transfer(address,address,uint256) |
| 173865ad | => | swapAndLiquify(uint256) |
| b28805f4 | => | swapTokensForEth(uint256) |
| 9cd441da | => | addLiquidity(uint256,uint256) |
| 818c19dc | => | swapAndSendDividends(uint256) |
| be7ab214 | => | changeUserCustomToken(address,address) |
| 89e5c747 | => | resetUserCustomToken(address) |
| 2c43147e | => | seeUserCustomToken(address) |
| de27e4d0 | => | viewRewardsToken() |
| a7b31f4e | => | viewRewardsTokenCount() |
| 64ce420e | => | viewRewardsPercentage() |
| 1aefb0af | => | viewRewardsTokens() |
| 38656d0b | => | getLastRewardsTokens(uint256) |
| 93da3995 | => | changeRewardsPercentage(uint256) |
| d71d124e | => | changeUserClaimTokenPercentage(address,uint256) |
| 9338a9e3 | => | seeUserClaimTokenPercentage(address) |
| 49dea86b | => | viewUserCustomClaimTokenPercentage(address) |
| aa84e7f3 | => | resetUserClaimTokenPercentage(address) |
| 721260d3 | => | seeUserRewardsSetup(address) |
| 11b613d2 | => | changeUserRewardsSetup(address,address,uint256) |
| c2a1fd8d | => | seeTxCountRewards() |




```

57da4f85 => changeBotWallet(address)
cbdf39c4 => viewBotWallet()
119df25f => _msgSender()
8b49d47e => _msgData()
03c83302 => distributeDividends()
6a474002 => withdrawDividend()
373de4aa => _withdrawDividendOfUser(address)
2be12493 => getRewardsRatio(address,uint256)
4caeb3dc => setRewardsPercentage(uint256)
d7f386e6 => setUserClaimTokenPercentage(address,uint256)
210393d1 => viewUserClaimTokenPercentage(address)
8dc690ca => clearUserClaimTokenPercentage(address)
7aef2521 => getCurrentRewardsToken()
f5dc097a => setBotWallet(address)
de320cc1 => setRewardsToken(address)
d487393d => getRewardsTokensCount()
499e2319 => getRewardsTokens()
b8977ec1 => swapEthForCustomToken(address,uint256)
4fd2af55 => updateUserCustomToken(address,address)
bc25b7f0 => clearUserCustomToken(address)
dc610dd4 => viewUserCustomToken(address)
c75a1c5f => viewUserRewardsSetup(address)
4c897584 => setUserRewardsSetup(address,address,uint256)
91b89fba => dividendOf(address)
a8b9d240 => withdrawableDividendOf(address)
aafd847a => withdrawnDividendOf(address)
27ce0147 => accumulativeDividendOf(address)
4e6ec247 => _mint(address,uint256)
6161eb18 => _burn(address,uint256)
ab86e0a6 => _setBalance(address,uint256)
8d5ceeca => checkShares(address)
06fdde03 => name()
95d89b41 => symbol()
313ce567 => decimals()
18160ddd => totalSupply()
70a08231 => balanceOf(address)
a9059cbb => transfer(address,uint256)
dd62ed3e => allowance(address,address)
095ea7b3 => approve(address,uint256)
23b872dd => transferFrom(address,address,uint256)
a457c2d7 => decreaseAllowance(address,uint256)
104e81ff => _approve(address,address,uint256)
cad3be83 => _beforeTokenTransfer(address,address,uint256)
268d8e2e => get(Map,address)
b45dad3d => getIndexOfKey(Map,address)
7596720f => getKeyAtIndex(Map,uint256)
b1b533f3 => size(Map)
6b06f325 => set(Map,address,uint256)
0eac8729 => remove(Map,address)
017e7e58 => feeTo()

```



```

094b7415 => feeToSetter()
e6a43905 => getPair(address,address)
1e3dd18b => allPairs(uint256)
574f2ba3 => allPairsLength()
c9c65396 => createPair(address,address)
f46901ed => setFeeTo(address)
a2e74af6 => setFeeToSetter(address)
3644e515 => DOMAIN_SEPARATOR()
30adf81f => PERMIT_TYPEHASH()
7ecebe00 => nonces(address)
d505accf => permit(address,address,uint256,uint256,uint8,bytes32,bytes32)
ba9a7a56 => MINIMUM_LIQUIDITY()
c45a0155 => factory()
0dfe1681 => token0()
d21220a7 => token1()
0902f1ac => getReserves()
5909c0d5 => price0CumulativeLast()
5a3d5493 => price1CumulativeLast()
7464fc3d => kLast()
6a627842 => mint(address)
89afcb44 => burn(address)
022c0d9f => swap(uint256,uint256,address,bytes)
bc25cf77 => skim(address)
fff6cae9 => sync()
485cc955 => initialize(address,address)
ad5c4648 => WETH()
e8e33700 => addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256)
f305d719 => addLiquidityETH(address,uint256,uint256,uint256,address,uint256)
baa2abde => removeLiquidity(address,address,uint256,uint256,uint256,address,uint256)
02751cec => removeLiquidityETH(address,uint256,uint256,uint256,address,uint256)
2195995c =>
removeLiquidityWithPermit(address,address,uint256,uint256,uint256,address,uint256,bool,uint8,bytes3
2,bytes32)
ded9382a =>
removeLiquidityETHWithPermit(address,uint256,uint256,uint256,address,uint256,bool,uint8,bytes32,byt
es32)
38ed1739 => swapExactTokensForTokens(uint256,uint256,address[],address,uint256)
8803dbee => swapTokensForExactTokens(uint256,uint256,address[],address,uint256)
7ff36ab5 => swapExactETHForTokens(uint256,address[],address,uint256)
4a25d94a => swapTokensForExactETH(uint256,uint256,address[],address,uint256)
18cbafe5 => swapExactTokensForETH(uint256,uint256,address[],address,uint256)
fb3bdb41 => swapETHForExactTokens(uint256,address[],address,uint256)
ad615dec => quote(uint256,uint256,uint256)
054d50d4 => getAmountOut(uint256,uint256,uint256)
85f8c259 => getAmountIn(uint256,uint256,uint256)
d06ca61f => getAmountsOut(uint256,address[])
1f00ca74 => getAmountsIn(uint256,address[])
af2979eb =>
removeLiquidityETHSupportingFeeOnTransferTokens(address,uint256,uint256,uint256,address,uint256)

```



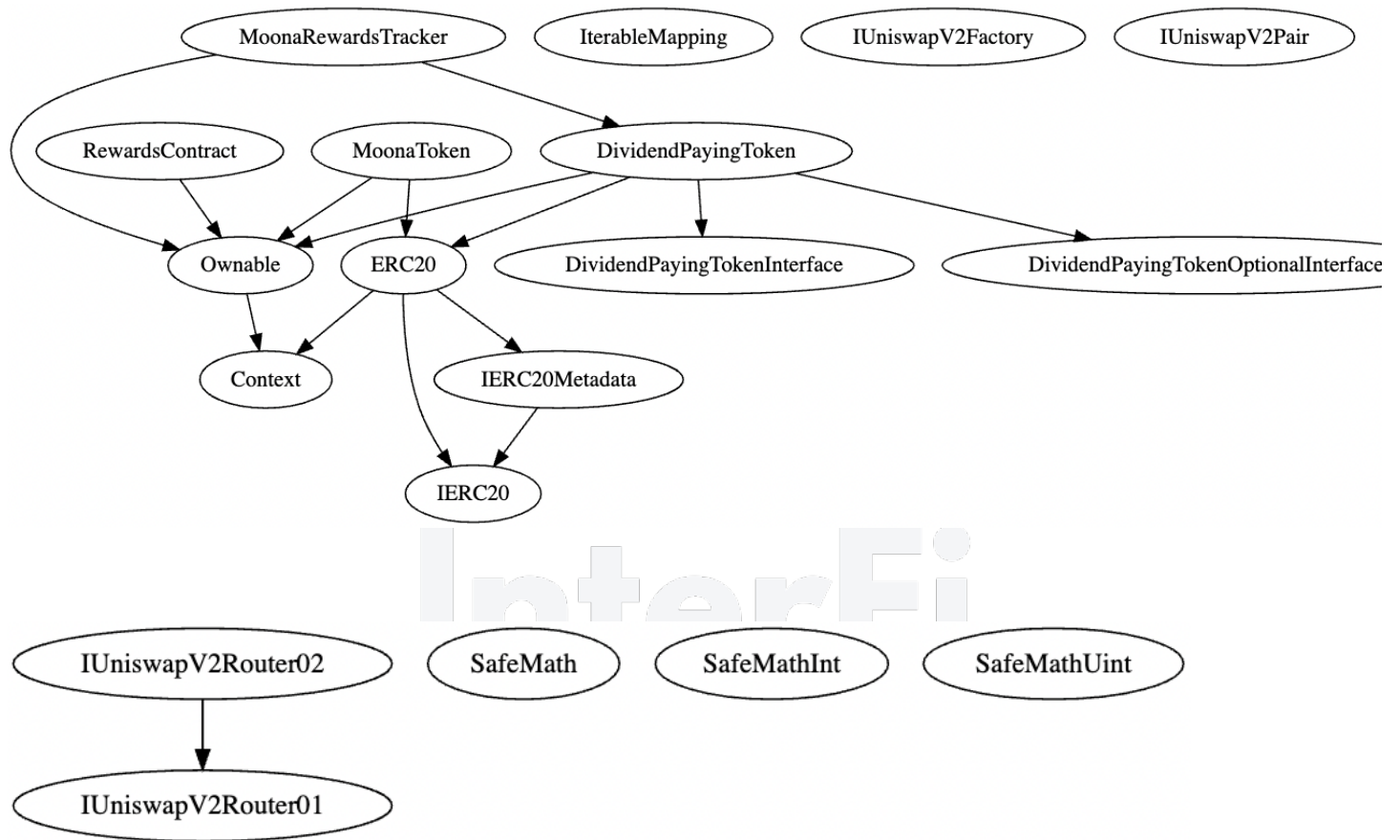
```

5b0d5984 =>
removeLiquidityETHWithPermitSupportingFeeOnTransferTokens(address,uint256,uint256,uint256,address,u
int256,bool,uint8,bytes32,bytes32)
5c11d795 =>
swapExactTokensForTokensSupportingFeeOnTransferTokens(uint256,uint256,address[],address,uint256)
b6f9de95 => swapExactETHForTokensSupportingFeeOnTransferTokens(uint256,address[],address,uint256)
791ac947 =>
swapExactTokensForETHSupportingFeeOnTransferTokens(uint256,uint256,address[],address,uint256)
31e79db0 => excludeFromDividends(address)
fbcbc0f1 => getAccount(address)
77fdb837 => canAutoClaim(uint256)
20ed4506 => updateSingleHolderShares(address,uint256)
b2faae00 => updateHolderShares(address,uint256[])
da3d2953 => clearShares(address)
8d4c2326 => setMinimumBalanceToReceiveDividends(uint256)
9eda069f => setBalance(address)
8a6d6a33 => viewOffset(address)
ffb2c479 => process(uint256)
bc4c4b37 => processAccount(address,bool)
8da5cb5b => owner()
f2fde38b => transferOwnership(address)
45ae8409 => adder(address)
985c7560 => statusFind(address)
0ff12c38 => swapTokensForEthMarketing(uint256)
4c749dba => withdrawToMarketing(uint256)
771602f7 => add(uint256,uint256)
b67d77c5 => sub(uint256,uint256)
e31bdc0a => sub(uint256,uint256,string)
c8a4ac9c => mul(uint256,uint256)
a391c15b => div(uint256,uint256)
b745d336 => div(uint256,uint256,string)
bbe93d91 => mul(int256,int256)
adefc37b => sub(int256,int256)
a5f3c23b => add(int256,int256)
744f7c7d => toUint256Safe(int256)
e823b9bf => toInt256Safe(uint256)

```



Callout functions – Inheritance Graph



2



Smart Contract – Manual Analysis

| Function | Description | Tested | Verdict |
|---------------------|---|--------|---------------|
| TotalSupply | provides information about the total token supply | Yes | Passed |
| BalanceOf | provides account balance of the owner's account | Yes | Passed |
| Transfer | executes transfers of a specified number of tokens to a specified address | Yes | Passed |
| TransferFrom | executes transfers of a specified number of tokens from a specified address | Yes | Passed |
| Approve | allow a spender to withdraw a set number of tokens from a specified account | Yes | Passed |
| Allowance | returns a set number of tokens from a spender to the owner | Yes | Passed |
| burn | executes transfers of a specified number of tokens to a burn address | NA | NA |

Verified

Active smart contract owner privileges constitute an elevated impact to smart contract's safety and security.

- ❖ Active Owner: 0x1d9361ffbd96226143d6a8358da4b026563951b1
- ❖ Owner can mint tokens at token launch.
- ❖ Owner can-not lock or burn user assets.
- ❖ Owner can-not lock or pause the smart contract.



Important Information

Ms Moona Rewards Token smart contract utilizes the “SafeMath” to prevent known vulnerabilities.

```
string private _name = 'Ms Moona Rewards';
string private _symbol = 'MoonaToken';
uint8 private _decimals = 18;

library SafeMath {
function add(uint256 a, uint256 b) internal pure returns (uint256) {
    uint256 c = a + b;
    require(c >= a, 'SafeMath: addition overflow');

    return c;
}
function sub(uint256 a, uint256 b) internal pure returns (uint256) {
    return sub(a, b, 'SafeMath: subtraction overflow');
}
uint256 c = a * b;
require(c / a == b, 'SafeMath: multiplication overflow');

    return c;
}
function mod(uint256 a, uint256 b) internal pure returns (uint256) {
    require(b > 0, "SafeMath: modulo by zero");
    return a % b;
}
function mod(uint256 a, uint256 b) internal pure returns (uint256) {
    return mod(a, b, 'SafeMath: modulo by zero');
}
```

Ms Moona Rewards smart contract has low severity issues which may not create any functional vulnerability.

❖ "Expected identifier, got 'Payable'"



Smart Contract – SWC Attacks

| SWC ID | Description | Verdict |
|---------|--------------------------------------|---------|
| SWC-101 | Integer Overflow and Underflow | Passed |
| SWC-102 | Outdated Compiler Version | ! Low |
| SWC-103 | Floating Pragma | Passed |
| SWC-104 | Unchecked Call Return Value | Passed |
| SWC-105 | Unprotected Ether Withdrawal | Passed |
| SWC-106 | Unprotected SELFDESTRUCT 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 |

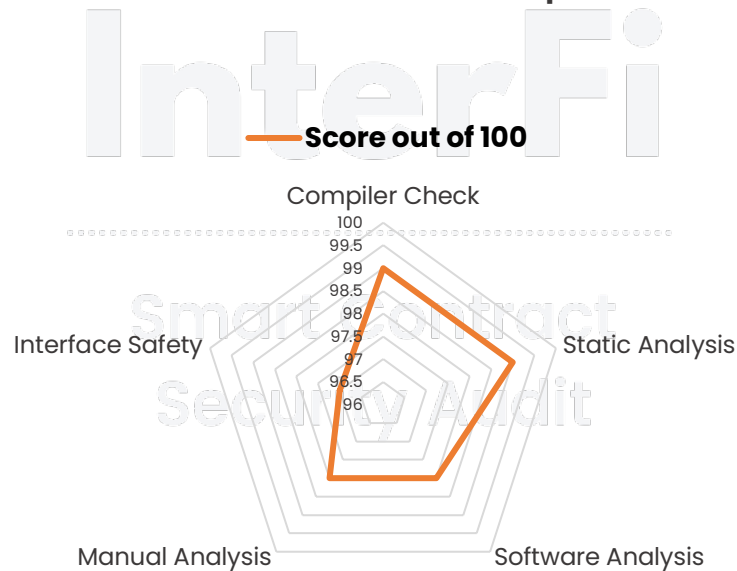


| | | |
|----------------|---|---------------|
| SWC-119 | Shadowing State Variables | Passed |
| SWC-120 | Weak Sources of Randomness from Chain Attributes | Passed |
| SWC-121 | Missing Protection against Signature Replay Attacks | Passed |
| SWC-122 | Lack of Proper Signature Verification | Passed |
| 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 hardcoded gas amount | Passed |
| SWC-135 | Code With No Effects (Irrelevant/Dead Code) | ! Low |
| SWC-136 | Unencrypted Private Data On-Chain | Passed |



Smart Contract - Risk Status & Radar Chart

| Risk Severity | Status |
|-------------------|---|
| ! Critical | None critical severity issues identified |
| ! High | None high severity issues identified |
| ! Medium | None medium severity issues identified |
| ! Low | 1 Low severity issues identified |
| Passed | 41 functions and instances verified and passed |



Compiler Check 99

Static Analysis 97

Software Analysis 98

Manual Analysis 98

Interface Safety 97



Auditor's Verdict

InterFi team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks.

Ms Moona Rewards' token smart contract source codes has LOW RISK SEVERITY.

Ms Moona Rewards has successfully PASSED the smart contract audit.

InterFi

Smart Contract
Security Audit

General Note:

- ❖ Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's safety and security.
- ❖ Owner or developer KYC isn't checked and verified due to out of scope.
- ❖ Project's liquidity pair isn't checked and verified due to out of scope.
- ❖ Project website is not checked due to out of scope. The website hasn't been reviewed for SSL and lighthouse report.



Important Disclaimer

InterFi Network provides contract auditing and project verification services for blockchain projects. The purpose of the audit is to analyse the on-chain smart contract source code, and to provide basic overview of the project. **This report should not be transmitted, disclosed, referred to, or relied upon by any person for any purposes without InterFi's prior written consent.**

InterFi provides the easy-to-understand assessment of the project, and the smart contract (otherwise known as the source code). The audit makes no statements or warranties on the security of the code. It also cannot be considered as an enough assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While we have used all the data at our disposal to provide the transparent analysis, it is important to note that you should not rely on this report only – we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts. **Be aware that smart contracts deployed on a blockchain aren't resistant from 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, InterFi 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.

This report should not be considered as an endorsement or disapproval of any project or team.

The information provided on this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. Do conduct your own due diligence and consult your financial advisor before making any investment decisions.



About InterFi Network

InterFi Network provides intelligent blockchain solutions. InterFi is developing an ecosystem that is seamless and responsive. Some of our services: Blockchain Security, Token Launchpad, NFT Marketplace, etc. **InterFi's mission is to interconnect multiple services like Blockchain Security, DeFi, Gaming, and Marketplace under one ecosystem that is seamless, multi-chain compatible, scalable, secure, fast, responsive, and easy-to-use.**

InterFi is built by a decentralized team of UI experts, contributors, engineers, and enthusiasts from all over the world. Our team currently consists of 6+ core team members, and 10+ casual contributors. **InterFi provides manual, static, and automatic smart contract analysis, to ensure that project is checked against known attacks and potential vulnerabilities.**

To learn more, visit <https://interfi.network>

To view our audit portfolio, visit <https://github.com/interfinetwork>.....

To book an audit, message <https://t.me/interfiaudits>





@INTERFINETWORK

RELENTLESSLY SECURING THE PUBLIC BLOCKCHAIN | MADE IN CANADA 🇨🇦