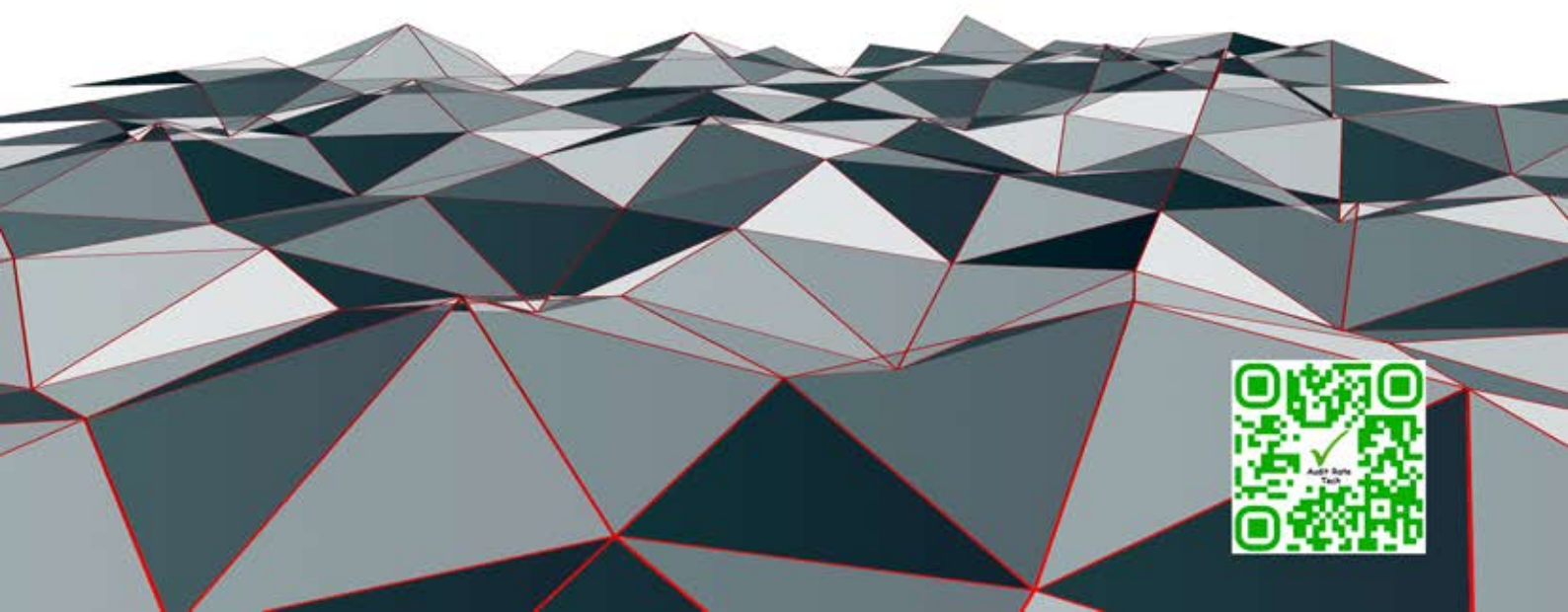
Smart Contract Security Audit

AUDIT RATE TECH

for

VeMoon



Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and AUDIT RATE TECH and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (AUDIT RATE TECH) owe no duty of care towards you or any other person, nor does AUDIT RATE TECH make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and AUDIT RATE TECH hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, AUDIT RATE TECH hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against AUDIT RATE TECH, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

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 details:

Audited project: VeMoon

Total supply: 1,000,000,000

Token ticker: VMN

Decimals: 9

Contract address: 0xD396DB1A47140deD604E8E9646716f2e38a0b18a

Languages: Solidity (Smart contract)

Platforms and Tools: Remix IDE, Truffle, Truffle Team, Ganache, Solhint, VScode, Mythril, Contract Library

Compiler Version: v0.8.12+commit.f00d7308

Optimization Enabled: Yes with 200 runs

Contract Deployer Address: 0x8BB6219Cd4Fe78b8385a34095ee0c76eb7877a16

Blockchain: Binance Smart Chain

Project website: https://vemoon.io/

The audit items and results:

(Other unknown security vulnerabilities are not included in the audit responsibility scope)

Audit Result: Passed

Audit Date: April 1, 2022

Audit Team: AUDIT RATE TECH

https://www.auditrate.tech

Introduction

This Audit Report mainly focuses on the overall security of VeMoon Smart Contract.
With this report, we have tried to ensure the reliability and correctness of their smart contract by complete and rigorous assessment of their system's architecture and the smart contract codebase.

Auditing Approach and Methodologies applied

The AUDIT RATE TECH team has performed rigorous testing of the project starting with analyzing the code design patterns in which we reviewed the smart contract architecture to ensure it is structured and safe use of third-party smart contracts and libraries.
Our team then performed a formal line by line inspection of the Smart Contract to find any potential issue like race conditions, transaction-ordering dependence, timestamp dependence, and denial of service attacks.
In the Unit testing Phase, we coded/conducted custom unit tests written for each function in the contract to verify that each function works as expected.
In Automated Testing, we tested the Smart Contract with our in-house developed tools to identify vulnerabilities and security flaws.
The code was tested in collaboration of our multiple team members and this included -

- Testing the functionality of the Smart Contract to determine proper logic has been followed throughout the whole process.
- Analyzing the complexity of the code in depth and detailed, manual review of the code, lineby-line.
- Deploying the code on testnet using multiple clients to run live tests.
- Analyzing failure preparations to check how the Smart Contract performs in case of any bugs and vulnerabilities.
- Checking whether all the libraries used in the code are on the latest version.
- Analyzing the security of the on-chain data.

Audit Goals

The focus of the audit was to verify that the Smart Contract System is secure, resilient and working according to the specifications. The audit activities can be grouped in the following three categories:
Security
Identifying security related issues within each contract and the system of contract.
Sound Architecture
Evaluation of the architecture of this system through the lens of established smart contract best practices and general software best practices.
Code Correctness and Quality
A full review of the contract source code. The primary areas of focus include:

- Accuracy
- Readability
- Sections of code with high complexity
- Quantity and quality of test coverage

Issue Categories

Every issue in this report was assigned a severity level from the following:
High level severity issues
Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.
Medium level severity issues
Issues on this level could potentially bring problems and should eventually be fixed.
Low level severity issues
Issues on this level are minor details and warnings that can remain unfixed but would be better fixed at some point in the future.

Manual Audit:

For this section the code was tested/read line by line by our developers. We also used Remix IDE's JavaScript VM and Kovan networks to test the contract functionality.

Automated Audit

Remix Compiler Warnings
It throws warnings by Solidity's compiler. If it encounters any errors the contract cannot be compiled and deployed. No issues found.

Number of issues per severity

Critical	High	Medium	Low	Note
0	0	0	3	0

Issues Checking Status

№	Issue description.	Checking status
1	Compiler warnings.	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.	Low
10	Methods execution permissions.	Passed
11	Economy model.	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 Zeppelin module.	Passed
21	Fallback function security.	Passed

Owner privileges

169 renounceOwnership
174 transferOwnership
188 lock
612 setRouterAddressAndCreatePair
619 setRouterAddress
625 setPairAddress
630 setLiquidityAddress
663 excludeFromReward
673 includeInReward
994 excludeFromFee
998 includeInFee
1016 setTaxFeePercent
1020 setVaultFeePercent
1024 setBuyFee
1030 setSellFee
1036 setBuySellDevFee
1041 setLiquidityFeePercent
1045 setBuyMaxTxAmount
1049 setSellMaxTxAmount
1053 setTriggerAmount
1058 setNumTokensSellToAddToBuyBack
1062 setMarketingAddress
1067 setCharityAddress
1072 setSwapAndLiquifyEnabled
1077 setBusdAddress
1081 setCharityAndMarketingFee
1088 setDevFee
1099 changeRouterVersion
1118 transferForeignToken
1125 manualSwapAndLiquifyBNB
1130 manualSwapAndLiquifyTokens
1180 SweepStuck

Owner can set fees without limit

```
    function setTaxFeePercent(uint256 taxFee) external onlyOwner() {
    _taxFee = taxFee;   }
function setVaultFeePercent(uint256 vaultFee) external onlyOwner() {
    _vaultFee = vaultFee;   }
  function setBuyFee(uint256 buyTaxFee, uint256 buyVaultFee, uint256 buyLiquidityFee) external onlyOwner {
    _buyTaxFee = buyTaxFee; _buyVaultFee = buyVaultFee; _buyLiquidityFee = buyLiquidityFee;   }
  function setSellFee(uint256 sellTaxFee, uint256 sellVaultFee, uint256 sellLiquidityFee) external onlyOwner {
    _sellTaxFee = sellTaxFee; _sellVaultFee = sellVaultFee;  _sellLiquidityFee = sellLiquidityFee;   }
  function setBuySellDevFee(uint256 _newBuyFee, uint256 _newSellFee) external onlyOwner{
    _buyDevFee = _newBuyFee;  _sellDevFee = _newSellFee; }
    function setLiquidityFeePercent(uint256 liquidityFee) external onlyOwner {
    _liquidityFee = liquidityFee;  }
```

No mint function found

Owner can set max tx amount without limit

```
  function setBuyMaxTxAmount(uint256 bMaxTxAmount) external onlyOwner {
    _bMaxTxAmount = bMaxTxAmount;   }
  function setSellMaxTxAmount(uint256 sMaxTxAmount) external onlyOwner {
    _sMaxTxAmount = sMaxTxAmount;   }
```

Owner cannot pause trading

! Out of gas
Issue:
includeInReward()
The function includeInReward() also uses the loop for evaluating total supply. It also could be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.
Recommendation:
Check that the excluded array length is not too big.
! Out of gas
Issue:
getRate()
The function getRate also uses the loop for evaluating reflect rate. It also could be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.
Recommendation:
Check that the array length is not too big.
! Out of gas
Issue:
getCurrentSupply()
The function getCurrentSupply also uses the loop for evaluating total supply. It also could be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.
Recommendation:
Check that the excluded array length is not too big.

Note:
Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner. The analysis of the contract does not give complete security and includes only the analysis that is indicated in the report. We do not analyze locked tokens or LP tokens, the presence of KYC in other companies, and so on. Also, our audit is not a recommendation for investment. All responsibility for the loss of investment lies with you!

Website Audit

Address	https://vemoon.io/
Domain registration	1 years
Domain	Clean
Web server	LiteSpeed
The server is located	United States
Server response time	1.09 sec
SSL certificate	Yes
JavaScript errors	Not found
Typos, or grammatical errors	Not found
Issues with loading elements, code, or stylesheets	Not found
Malware	Not found
Injected spam	Not found
Internal server errors	Not found
Popups	Not found
Blocking files	Not found
Mobile Friendly	Yes
Compress CSS files	Optimized
Compress JS files	Optimized
Image compression	Optimized
Visible content	Optimized
Social Media/contacts	Yes
Roadmap	Yes

Top Token Holders

At the time of the audit

The top 3 holders collectively own 100.00% (1,000,000,000.00 Tokens) of VeMoon

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 1

(A total of 1,000,000,000.00 tokens held by the top 3 accounts from the total supply of 1,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x494e73fb3801cc499f7580e0c3d9eccfd743c694	1,000,000,000	100.0000%

KYC/Doxx

Verified by Audit Rate Tech

THANK YOU!