Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

March, 2022

Audit Details

Audited project

LESLAR Metaverse

Deployer address

0x6175f6620f8257246d82a2b10195c82d998f106e

Client contacts:

LESLAR Metaverse team

Blockchain

Binance Smart Chain

Project website:

https://www.leslarmetaverse.com

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 TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate 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 TechRate 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, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, 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.

Background

TechRate was commissioned by LESLAR Metaverse to perform an audit of smart contracts:

https://bscscan.com/address/0x0F2420fC7ce2446C35CD37F514486aa88D703bC3#code

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

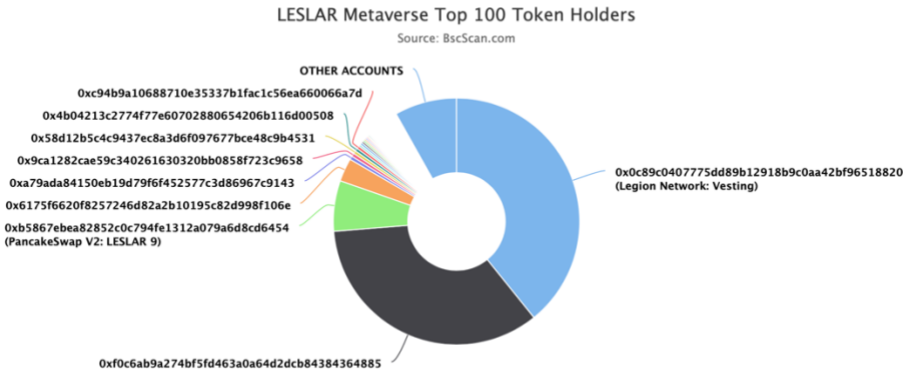
Token contract details for 10.03.2022

Contract name	LESLAR Metaverse
Contract address	0x0F2420fC7ce2446C35CD37F514486aa88D703bC3
Total supply	1,000,000,000,000
Token ticker	LESLAR
Decimals	9
Token holders	5,885
Transactions count	18,955
Top 100 holders dominance	91.85%
Sell cycle hours	24
Tax fee	3
Total fees	3
Marketing / dev / dev product shares	40 / 30 / 30
Contract deployer address	0x6175f6620f8257246d82a2b10195c82d998f106e
Contract's current owner address	0x6175f6620f8257246d82a2b10195c82d998f106e

LESLAR Metaverse Token Distribution

The top 100 holders collectively own 91.85% (918,522,999,412.32 Tokens) of LESLAR Metaverse

Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 5,885

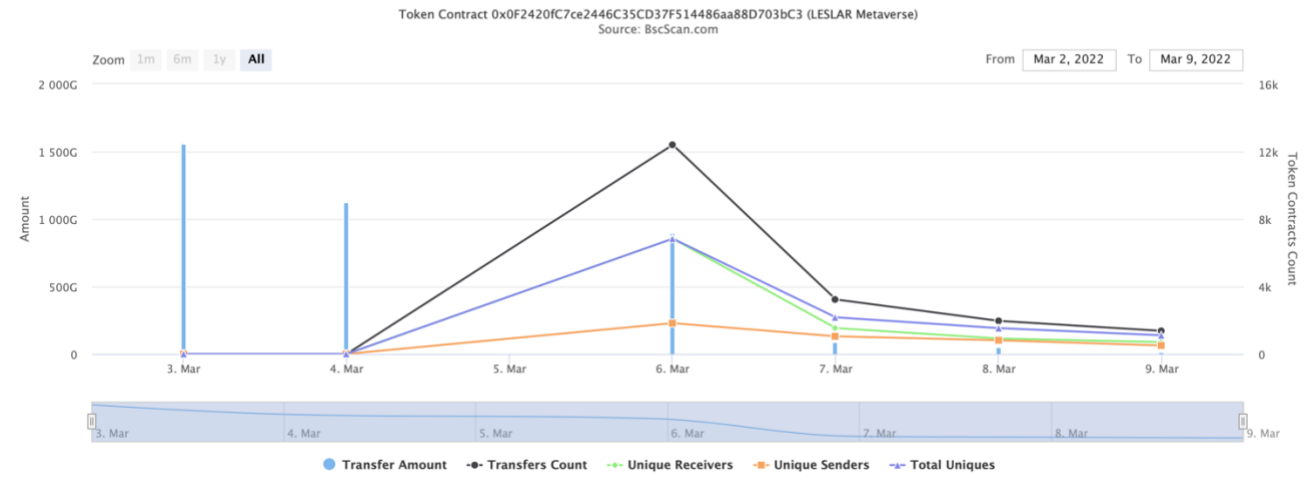


(A total of 918,522,999,412.32 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

LESLAR Metaverse Contract Interaction Details

Time Series: Token Contract Overview

Thu 3, Mar 2022 - Wed 9, Mar 2022



LESLAR Metaverse Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Legion Network: Vesting	392,000,000,000	39.2000%
2	0xf0c6ab9a274bf5fd463a0a64d2dcb84384364885	345,310,843,132.273069705	34.5311%
3	PancakeSwap V2: LESLAR 9	66,238,256,977.020017601	6.6238%
4	0x6175f6620f8257246d82a2b10195c82d998f106e	30,515,704,978.99805459	3.0516%
5	0xa79ada84150eb19d79f6f452577c3d86967c9143	4,656,144,076.122931943	0.4656%
6	0x9ca1282cae59c340261630320bb0858f723c9658	4,325,547,231.308952789	0.4326%
7	0x58d12b5c4c9437ec8a3d6f097677bce48c9b4531	3,923,466,584.6991938	0.3923%
8	0x4b04213c2774f77e60702880654206b116d00508	3,779,423,007.158880919	0.3779%
9	0xc94b9a10688710e35337b1fac1c56ea660066a7d	3,672,391,545.325383007	0.3672%
10	0x50d88d7cf9b07768a8a58dcd3ad283ff2483f1a0	2,942,599,938.524395259	0.2943%

Contract functions details

+ Supply (Tokenomics, RFI)
  - [Pub] totalCirculatingSupply

+ [Int] IUniswapV2Router02 (IUniswapV2Router01)
  - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Int] IUniswapV2Router01
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidity #
  - [Ext] addLiquidityETH ($)
  - [Ext] removeLiquidity #
  - [Ext] removeLiquidityETH #
  - [Ext] removeLiquidityWithPermit #
  - [Ext] removeLiquidityETHWithPermit #
  - [Ext] swapExactTokensForTokens #
  - [Ext] swapTokensForExactTokens #
  - [Ext] swapExactETHForTokens ($)
  - [Ext] swapTokensForExactETH #
  - [Ext] swapExactTokensForETH #
  - [Ext] swapETHForExactTokens ($)
  - [Ext] quote
  - [Ext] getAmountOut
  - [Ext] getAmountIn
  - [Ext] getAmountsOut
  - [Ext] getAmountsIn

+ [Int] IUniswapV2Pair
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transfer #
  - [Ext] transferFrom #
  - [Ext] DOMAIN_SEPARATOR
  - [Ext] PERMIT_TYPEHASH
  - [Ext] nonces
  - [Ext] permit #
  - [Ext] MINIMUM_LIQUIDITY
  - [Ext] factory
  - [Ext] token0
  - [Ext] token1
  - [Ext] getReserves
  - [Ext] price0CumulativeLast

  - [Ext] price1CumulativeLast
  - [Ext] kLast
  - [Ext] mint #
  - [Ext] burn #
  - [Ext] swap #
  - [Ext] skim #
  - [Ext] sync #
  - [Ext] initialize #

+ [Int] IUniswapV2Factory
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #
  - [Ext] setFeeToSetter #

+ Helpers

+ Pancake (Ownable)
  - [Ext] <Fallback> ($)
  - [Ext] initDEXRouter #
    - modifiers: onlyOwner
  - [Int] swapTokensForBnb #
  - [Pub] addAddressToLPs #
    - modifiers: onlyOwner
  - [Pub] removeAddressFromLPs #
    - modifiers: onlyOwner

+ TxPolice (Tokenomics, Pancake, RFI, Supply)
  - [Pub] toggleLimitExemptions #
    - modifiers: onlyOwner
  - [Ext] toggleSpecialWallets #
    - modifiers: onlyOwner
  - [Int] enforceCyclicSellLimit #
  - [Pub] maxSellAllowancePerCycle
  - [Ext] setMaxSellAllowanceMultiplier #
    - modifiers: onlyOwner
  - [Int] hasSellCycleEnded
  - [Ext] setSellCycleHours #
    - modifiers: onlyOwner
  - [Ext] disableSellLimit #
    - modifiers: onlyOwner
  - [Ext] enableSellLimit #
    - modifiers: onlyOwner
  - [Ext] sellAllowanceLeft
  - [Int] guardMaxLimits
  - [Int] canTakeFee
  - [Int] swapExcludedFromFee #
  - [Int] getTransactionType

+ Expensify (Ownable, Helpers, Tokenomics, Pancake, TxPolice)
  - [Ext] setProductDevWallet #

    - modifiers: onlyOwner,legitWallet
  - [Ext] setDevWallet #
    - modifiers: onlyOwner,legitWallet
  - [Ext] setMarketingWallet #
    - modifiers: onlyOwner,legitWallet
  - [Int] canTax
  - [Int] taxify #
    - modifiers: lockTheProcess

+ RFI (IERC20, Ownable, Tokenomics, Pancake)
  - [Pub] <Constructor> #
  - [Prv] _getValues
  - [Prv] _getTValues
  - [Prv] _getRValues
  - [Prv] _getRate
  - [Prv] _getCurrentSupply
  - [Pub] tokenFromReflection
  - [Int] rfiApprove #
  - [Int] _transfer #
  - [Prv] _tokenTransfer #
  - [Int] beforeTokenTransfer #
  - [Int] takeFee #
  - [Prv] _takeTax #
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #

+ Tokenomics (IERC20, Ownable)
  - [Ext] setTaxFee #
    - modifiers: onlyOwner,sameValue
  - [Ext] disableAllFeesTemporarily #
    - modifiers: onlyOwner
  - [Ext] restoreAllFees #
    - modifiers: onlyOwner
  - [Int] removeAllFee #
  - [Int] restoreAllFee #
  - [Int] calculateTaxFee
  - [Ext] setMinToTax #
    - modifiers: onlyOwner,supplyBounds
  - [Ext] totalSupply
  - [Ext] totalFees
  - [Ext] setAntibot #
    - modifiers: onlyOwner
  - [Pub] isBot
  - [Ext] rescueBNB #
    - modifiers: onlyOwner
  - [Ext] rescueBEP20Tokens #
    - modifiers: onlyOwner

+ [Int] IERC20Metadata (IERC20)
  - [Ext] name

  - [Ext] symbol
  - [Ext] decimals

+ [Int] IERC20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ Ownable (Context)
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Int] _transferOwnership #

+ Context
  - [Int] _msgSender
  - [Int] _msgData

+ [Lib] SafeMath
  - [Int] tryAdd
  - [Int] trySub
  - [Int] tryMul
  - [Int] tryDiv
  - [Int] tryMod
  - [Int] add
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] mod
  - [Int] sub
  - [Int] div
  - [Int] mod

+ LESLAR (IERC20Metadata, Context, Ownable, Tokenomics, RFI, TxPolice, Expensify)
  - [Pub] <Constructor> #
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals
  - [Int] beforeTokenTransfer #
  - [Int] takeFee
  - [Prv] triggerFeatures #
  - [Int] _triggerTax #
  - [Ext] triggerTax #
    - modifiers: onlyOwner

($) = payable function
= non-constant function

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
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.

Notes:

- Max transaction amount equals total supply.

Owner privileges (In the period when the owner is not renounced)

- Owner can change router address.
- Owner can add/remove addresses from lp array.
- Owner can change limit exemptions.
- Owner can change specialAddresses value.
- Owner can change maxSellAllowanceMultiplier.
- Owner can enable/disable sell limit.
- Owner can change productDevWallet and productDevShare.
- Owner can change devWallet and devShare.
- Owner can change marketingWallet and marketingShare.
- Owner can change tax fee and enable/disable fee.
- Owner can change minToTax.
- Owner can mark addresses as bots.
- Owner can withdraw ERC20 and native tokens.
- Owner can manually trigger the tax.

Conclusion

Smart contracts do not contain high severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details NOT provided by the team.

TechRate 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.