TechRate

AUDIT COMPANY

Smart Contract Security Audit

Audit Details

Audited project

LOL

Deployer address

0x57bc1f8ef14418d2c824b650f2aedd2c873fee56

Client contacts:

LOL team

Blockchain

Ethereum

Project website:

https://lol.one

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 LOL to perform an audit of smart contracts:

https://etherscan.io/address/0xf91ac30e9b517f6d57e99446ee44894e6c22c032#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 15.11.2021

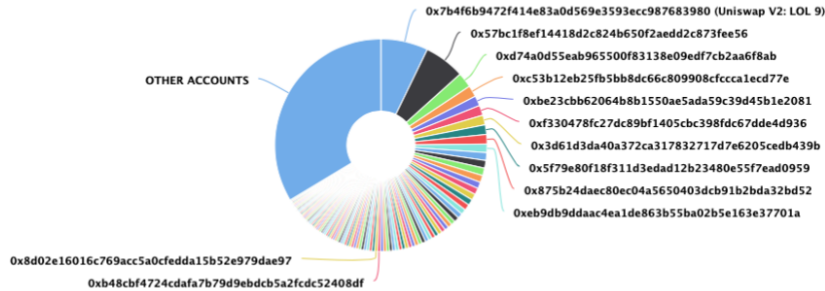|	
Contract name	LOL
Contract address	0xf91AC30E9b517f6D57e99446ee44894e6C22C032
Total supply	1,000,000,000,000
Token ticker	LOL
Decimals	9
Token holders	1,065
Transactions count	3,106
Top 100 holders dominance	66.38%
B/S Liquidity fee	1/1
B/S Tax fee	2/2
Total fees	74103197002881402005
Uniswap V2 pair	0x7b4f6b9472f414e83a0d569e3593ecc987683980
Contract deployer address	0x57bc1f8ef14418d2c824b650f2aedd2c873fee56
Contract's current owner address	0x57bc1f8ef14418d2c824b650f2aedd2c873fee56

LOL Token Distribution

LOL Top 100 Token Holders
Source: Etherscan.io

0x7b4f6b9472f414e83a0d569e3593ecc987683980 (Uniswap V2: LOL 9)
0x57bc1f8ef14418d2c824b650f2aedd2c873fee56
0xd74a0d55eab965500f83138e09edf7cb2aa6f8ab
0xc53b12eb25fb5bb8dc66c809908cfccca1ecd77e
0xbe23cbb62064b8b1550ae5ada59c39d45b1e2081
0xf330478fc27dc89bf1405cbc398fdc67dde4d936
0x3d61d3da40a372ca317832717d7e6205cedb439b
0x5f79e80f18f311d3edad12b23480e55f7ead0959
0x875b24daec80ec04a5650403dcb91b2bda32bd52
0xeb9db9ddaac4ea1de863b55ba02b5e163e37701a

OTHER ACCOUNTS

0x8d02e16016c769acc5a0cfedda15b52e979dae97
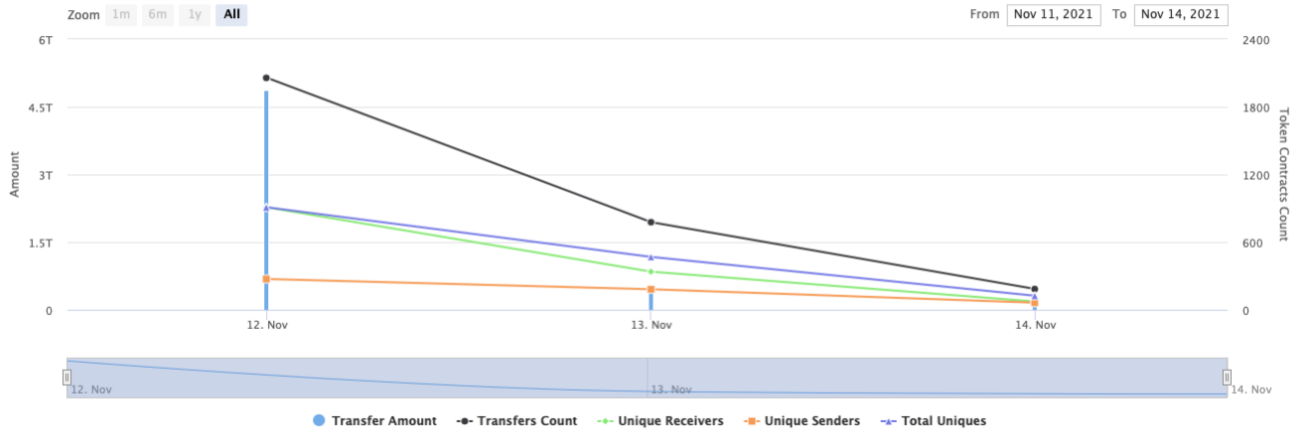0xb48cbf4724cdafa7b79d9ebdcb5a2fcdc52408df

(A total of 663,763,653,406.34 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

LOL Contract Interaction Details

Time Series: Token Contract Overview   Fri 12, Nov 2021 - Sun 14, Nov 2021

Token Contract 0xf91ac30e9b517f6d57e99446ee44894e6c22c032 (LOL)
Source: Etherscan.io

LOL Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	📄 Uniswap V2: LOL 9	71,916,653,710.891925187	7.1917%
2	0x57bc1f8ef14418d2c824b650f2aedd2c873fee56	61,708,139,620.512870359	6.1708%
3	0xd74a0d55eab965500f83138e09edf7cb2aa6f8ab	22,948,879,147.99182953	2.2949%
4	0xc53b12eb25fb5bb8dc66c809908cfccca1ecd77e	17,357,449,727.065744735	1.7357%
5	0xbe23cbb62064b8b1550ae5ada59c39d45b1e2081	15,291,324,617.35101452	1.5291%
6	0xf330478fc27dc89bf1405cbc398fdc67dde4d936	15,191,934,612.927920826	1.5192%
7	0x3d61d3da40a372ca317832717d7e6205cedb439b	14,933,407,024.187474497	1.4933%
8	0x5f79e80f18f311d3edad12b23480e55f7ead0959	14,640,507,701.164801458	1.4641%
9	0x875b24daec80ec04a5650403dcb91b2bda32bd52	14,434,242,075.746430558	1.4434%
10	0xeb9db9ddaac4ea1de863b55ba02b5e163e37701a	12,889,548,366.194048475	1.2890%

Contract functions details

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

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

+ **[Lib]** SafeMath
 - [Int] add
 - [Int] sub
 - [Int] sub
 - [Int] mul
 - [Int] div
 - [Int] div
 - [Int] mod
 - [Int] mod

+ **[Lib]** Address
 - [Int] isContract
 - [Int] sendValue #
 - [Int] functionCall #
 - [Int] functionCall #
 - [Int] functionCallWithValue #
 - [Int] functionCallWithValue #
 - **[Prv]** _functionCallWithValue #

+ **Ownable** (Context)
 - **[Pub]** <Constructor> #
 - **[Pub]** owner
 - **[Pub]** renounceOwnership #
  - modifiers: onlyOwner
 - **[Pub]** transferOwnership #
  - modifiers: onlyOwner
 - **[Pub]** getUnlockTime
 - **[Pub]** getTime

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

+ [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]** burn **#**
- **- [Ext]** swap **#**
- **- [Ext]** skim **#**
- **- [Ext]** sync **#**
- **- [Ext]** initialize **#**

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

+ **LOL** (Context, IERC20, Ownable)
 - **[Pub]** <Constructor> (**$**)
 - **[Ext]** name
 - **[Ext]** symbol
 - **[Ext]** decimals
 - **[Ext]** totalSupply
 - **[Pub]** balanceOf
 - **[Ext]** transfer **#**
 - **[Ext]** allowance
 - **[Pub]** approve **#**
 - **[Ext]** transferFrom **#**
 - **[Ext]** increaseAllowance **#**
 - **[Ext]** decreaseAllowance **#**
 - **[Ext]** isExcludedFromReward
 - **[Ext]** totalFees
 - **[Ext]** removeLimits **#**
   - modifiers: onlyOwner
 - **[Ext]** disableTransferDelay **#**
   - modifiers: onlyOwner
 - **[Pub]** excludeFromMaxTransaction **#**
   - modifiers: onlyOwner
 - **[Int]** enableTrading **#**
   - modifiers: onlyOwner
 - **[Ext]** launch **#**
   - modifiers: onlyOwner
 - **[Ext]** minimumTokensBeforeSwapAmount
 - **[Pub]** setAutomatedMarketMakerPair **#**
   - modifiers: onlyOwner
 - **[Prv]** _setAutomatedMarketMakerPair **#**
 - **[Ext]** setGasPriceLimit **#**
   - modifiers: onlyOwner
 - **[Ext]** reflectionFromToken
 - **[Pub]** tokenFromReflection
 - **[Pub]** excludeFromReward **#**
   - modifiers: onlyOwner
 - **[Pub]** includeInReward **#**
   - modifiers: onlyOwner
 - **[Prv]** _approve **#**
 - **[Prv]** _transfer **#**
 - **[Prv]** swapBack **#**
   - modifiers: lockTheSwap
 - **[Ext]** forceSwapBack **#**
   - modifiers: onlyOwner
 - **[Prv]** swapTokensForETH **#**
 - **[Prv]** addLiquidity **#**
 - **[Prv]** _tokenTransfer **#**
 - **[Prv]** _transferStandard **#**
 - **[Prv]** _transferToExcluded **#**
 - **[Prv]** _transferFromExcluded **#**
 - **[Prv]** _transferBothExcluded **#**
 - **[Prv]** _reflectFee **#**
 - **[Prv]** _getValues
 - **[Prv]** _getTValues
 - **[Prv]** _getRValues

- **[Prv]** _getRate
- **[Prv]** _getCurrentSupply
- **[Prv]** _takeLiquidity **#**
- **[Prv]** calculateTaxFee
- **[Prv]** calculateLiquidityFee
- **[Prv]** removeAllFee **#**
- **[Prv]** restoreAllFee **#**
- **[Ext]** isExcludedFromFee
- **[Ext]** removeBoughtEarly **#**
  - modifiers: onlyOwner
- **[Ext]** excludeFromFee **#**
  - modifiers: onlyOwner
- **[Ext]** includeInFee **#**
  - modifiers: onlyOwner
- **[Ext]** setBuyFee **#**
  - modifiers: onlyOwner
- **[Ext]** setSellFee **#**
  - modifiers: onlyOwner
- **[Ext]** setMarketingAddress **#**
  - modifiers: onlyOwner
- **[Pub]** setLiquidityAddress **#**
  - modifiers: onlyOwner
- **[Pub]** setSwapAndLiquifyEnabled **#**
  - modifiers: onlyOwner
- **[Ext]** <Fallback> **($)**
- **[Ext]** transferForeignToken **#**
  - modifiers: onlyOwner
- **[Ext]** withdrawStuckETH **#**
  - 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.

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

- **Owner can remove limits and disable transfer delay.**
- **Owner can exclude from the maximum transaction amount restriction.**
- **Owner can enable trading.**
- **Owner can launch contract (set basic settings, liquidity, enable trading).**
- **Owner can include in automatedMarketMakerPairs array.**
- **Owner can change gas restriction value.**
- **Owner can manually call swapBack() function.**
- **Owner can remove boughtEarly addresses.**
- **Owner can exclude from the fee.**
- **Owner can change fees.**
- **Owner can change marketing and liquidity addresses.**
- **Owner can withdraw contract ERC20 tokens and ETHs.**

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 are provided by the team:
https://app.unicrypt.network/amm/uni-v2/pair/0x7b4f6b9472f414e83a0d569e3593ecc987683980

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.