

TechRate
July, 2022



SMART CONTRACTS SECURITY AUDIT REPORT



Techrate_audits



Techrate



Techrate1

Audit Details



Audited project

colR Coin



Deployer address

0x5292d370c0ff8caab4ebb13959ac5aaf8855e25e



Client contacts:

@colRverse



Blockchain

Ethereum



Project website:

<http://colrverse.io>

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 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 colR Coin to perform an audit of smart contracts:

<https://etherscan.io/address/0x14b40ad2eba6c1b31db2ba817b07578afb414415#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 02.08.2022

Contract name colR Coin

Contract address 0x14b40AD2EBA6c1B31db2bA817b07578AFB414415

Total supply 100,000,000

Token ticker \$colR

Decimals 18

Token holders 211

Transactions count 3,375

Top 100 holders dominance 94.86%

Liquidity fee 10

Marketing fee 40

Floor fee 20

Uniswap V2 pair 0xacffa9649bb201b48fcbbfa72a1857479a340d3

Contract deployer address 0x5292d370c0ff8caab4ebb13959ac5aaf8855e25e

Owner address 0x5292d370c0ff8caab4ebb13959ac5aaf8855e25e

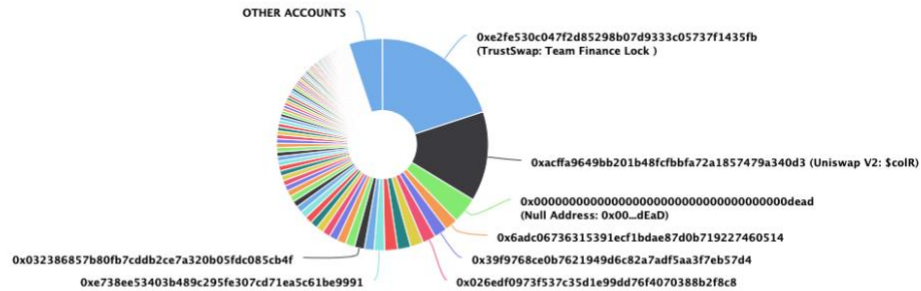
colR Coin Token Distribution

The top 100 holders collectively own 94.86% (94,861,803.67 Tokens) of colR Coin

Token Total Supply: 100,000,000.00 Token | Total Token Holders: 211

colR Coin Top 100 Token Holders

Source: Etherscan.io



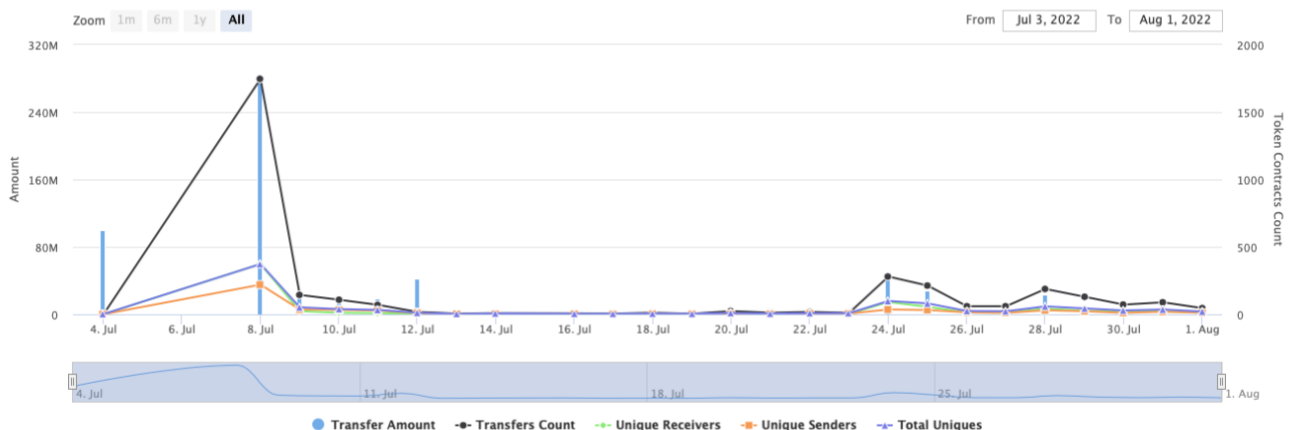
(A total of 94,861,803.67 tokens held by the top 100 accounts from the total supply of 100,000,000.00 token)

colR Coin Contract Interaction Details

Time Series: Token Contract Overview

Mon 4, Jul 2022 - Mon 1, Aug 2022

Token Contract 0x14b40ad2eba6c1b31db2ba817b07578afb414415 (colR Coin)
Source: Etherscan.io



colR Coin Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	TrustSwap: Team Finance Lock	20,000,000	20.0000%
2	Uniswap V2: \$colR	13,709,492.222428953478947874	13.7095%
3	Null Address: 0x00...dEaD	4,003,304.8	4.0033%
4	0x6adc06736315391ecf1bdae87d0b719227460514	2,000,000	2.0000%
5	0x39f9768ce0b7621949d6c82a7adf5aa3f7eb57d4	1,999,385.083874206050654605	1.9994%
6	0x026edf0973f537c35d1e99dd76f4070388b2f8c8	1,999,181.334170097381321905	1.9992%
7	0x957647be0920c43de599cd71c4c6460730dead81	1,998,091.620680715629824432	1.9981%
8	0x8a941e486772d8187b87f313a5676140842ca2b1	1,992,585.112485323248511769	1.992%
9	0x13021a4e6c9083a6cd63c37d7483db8e5781c70	1,978,441.294748535770194517	1.9784%
10	0xe738ee53403b489c295fe307cd71ea5c61be9991	1,600,000	1.6000%

colR Coin LP Token Holders

Rank	Address	Quantity	Percentage
1	Unicrypt : Liquidity Lockers	18,245.263284553919902619	<div>93.8689%</div>
2	0x5292d370c0ff8caab4ebb13959ac5aaf8855e25e	821.25601523147762649	<div>4.2252%</div>
3	0xa7577f841d95b1331954c936d71fe45ba2f62fe5	370.452749069098057402	<div>1.9059%</div>
4	<> ryoshit.eth	0.00000000000005	<div>0.0000%</div>
5	Null Address: 0x000...000	0.000000000000001	<div>0.0000%</div>

Contract functions details

+ [Int] IERC20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ [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

+ Context

- [Int] _msgSender
- [Int] _msgData

+ [Lib] Address

- [Int] isContract
- [Int] sendValue #
- [Int] functionCall #
- [Int] functionCall #
- [Int] functionCallWithValue #
- [Int] functionCallWithValue #
- [Int] functionStaticCall
- [Int] functionStaticCall
- [Int] functionDelegateCall #
- [Int] functionDelegateCall #
- [Prv] _verifyCallResult

+ Ownable (Context)

- [Pub] <Constructor> #
 - [Pub] owner
 - [Pub] renounceOwnership #
 - modifiers: onlyOwner
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
- + LockToken (Ownable)
- [Pub] <Constructor> #
 - [Ext] openTrade #
 - modifiers: onlyOwner
 - [Ext] includeToWhiteList #
 - modifiers: onlyOwner
- + [Int] IERC20Metadata (IERC20)
- [Ext] name
 - [Ext] symbol
 - [Ext] decimals
- + ERC20 (Context, Ownable, IERC20, IERC20Metadata)
- [Pub] <Constructor> #
 - [Pub] name
 - [Pub] symbol
 - [Pub] decimals
 - [Pub] totalSupply
 - [Pub] balanceOf
 - [Pub] transfer #
 - [Pub] allowance
 - [Pub] approve #
 - [Pub] transferFrom #
 - [Pub] increaseAllowance #
 - [Pub] decreaseAllowance #
 - [Int] _transfer #
 - [Int] _mint #
 - [Int] _burn #
 - [Int] _approve #
 - [Int] _beforeTokenTransfer #
- + [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] mint #
 - [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 #

DF1408

65

76C6

5C780

29C4CADB

C4

87C9C

31B2A384

DF1

65

- [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 #
- + TOKEN (ERC20, LockToken)
- [Pub] <Constructor> #
 - modifiers: ERC20
 - [Pub] excludeFromFee #
 - modifiers: onlyOwner
 - [Pub] includeInFee #
 - modifiers: onlyOwner
 - [Ext] setLiquidityFeePercent #
 - modifiers: onlyOwner
 - [Ext] setMarketingFeePercent #
 - modifiers: onlyOwner
 - [Ext] setFloorFeePercent #
 - modifiers: onlyOwner
 - [Ext] setMarketingWalletAddress #
 - modifiers: onlyOwner
 - [Ext] setFloorWalletAddress #
 - modifiers: onlyOwner
 - [Ext] setNumTokensSellToAddToLiquidity #
 - modifiers: onlyOwner
 - [Ext] setMaxBalance #
 - modifiers: onlyOwner
 - [Ext] setRouterAddress #
 - modifiers: onlyOwner
 - [Ext] setSwapAndLiquifyEnabled #
 - modifiers: onlyOwner
 - [Ext] <Fallback> (\$)
 - [Ext] withdrawStuckedFunds #
 - modifiers: onlyOwner
 - [Ext] withdrawStuckedTokens #
 - modifiers: onlyOwner

- [Pub] isExcludedFromFee
- [Int] _transfer #
 - modifiers: open
- [Prv] swapBack #
- [Prv] swapTokensForEth #
- [Prv] addLiquidity #
- [Ext] airdrop #
 - 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:





















- Old owner is not removed from exemptions after transferring ownership.

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



- Owner can whitelist addresses to transfer.
- Owner can open trading.
- Owner can exclude addresses from fees.
- Owner can change fees.
- Owner can change fee receivers addresses.
- Owner can withdraw contract ERC20 and native tokens.
- Owner can change numTokensSellToAddToLiquidity.
- Owner can change _maxWalletBalance.
- Owner can change router address.
- Owner can enable/disable swapAndLiquifyEnabled.
- Owner can multitransfer.

Testnet deployment

Contracts Description Table

Contract	Type	Bases	Visibility	Mutability	Modifiers
L	Function Name				
LockToken	Implementation	Ownable			
L	openTrade	External	!		onlyOwner
L	includeToWhiteList	External	!		onlyOwner
ERC20	Implementation	Context, Ownable, IERC20, IERC20Metadata			
L	transfer	Public	!		NO!
L	approve	Public	!		NO!
L	transferFrom	Public	!		NO!
L	increaseAllowance	Public	!		NO!
L	decreaseAllowance	Public	!		NO!
TOKEN	Implementation	ERC20, LockToken			
L	excludeFromFee	Public	!		onlyOwner
L	includeInFee	Public	!		onlyOwner
L	setLiquidityFeePercent	External	!		onlyOwner
L	setMarketingFeePercent	External	!		onlyOwner
L	setFloorFeePercent	External	!		onlyOwner
L	setMarketingWalletAddress	External	!		onlyOwner
L	setFloorWalletAddress	External	!		onlyOwner
L	setNumTokensSellToAddToLiquidity	External	!		onlyOwner
L	setMaxBalance	External	!		onlyOwner
L	setRouterAddress(PAIR EXIST)	External	!		onlyOwner
L	setSwapAndLiquifyEnabled	External	!		onlyOwner
L	withdrawStuckedFunds	External	!		onlyOwner
L	withdrawStuckedTokens	External	!		onlyOwner

Legend

Symbol	Meaning
	Function can modify state
	Function is payable

Conclusion

Smart contracts do not contain high severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details are provided by the team:

<https://app.unicrypt.network/amm/uni-v2/pair/0xacffa9649bb201b48fcfbfa72a1857479a340d3>

Security score: 88.

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.