



TechRate
AUDIT COMPANY

Smart Contract Security Audit

Audit Details



Audited project

CacaDragon



Deployer address

0x04008809ab2c5f672e707404f96eb470a4a15bee



Client contacts:

CacaDragon team



Blockchain

Ethereum



Project website:

<https://www.cacadragon.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 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 CacaDragon to perform an audit of smart contracts:

<https://etherscan.io/address/0xae727b5242b662bc0b9e71b2e24546b21e931251#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 19.02.2022

Contract name	CacaDragon
Contract address	0xaE727b5242B662bC0B9e71B2E24546B21E931251
Total supply	99,000,000,000,000,000,000,000
Token ticker	CDR
Decimals	9
Token holders	92
Transactions count	1,191
Top 100 holders dominance	99.87%
Liquidity fee	5
Reward fee	2
Total fees	478672248796375975887621503100
Uniswap V2 pair	0x15b2c030e206a0ccf37a7b2fddfd597eea8badb
Contract deployer address	0x04008809ab2c5f672e707404f96eb470a4a15bee
Contract's current owner address	0x04008809ab2c5f672e707404f96eb470a4a15bee

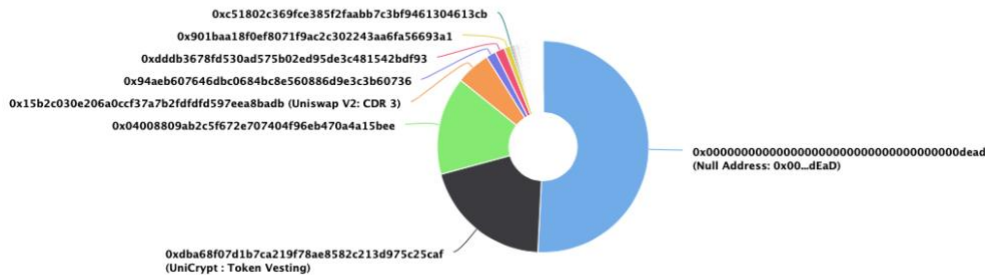
CacaDragon Token Distribution

The top 100 holders collectively own 99.87%
(98,875,480,641,237,000,000,000.00 Tokens) of CacaDragon

Token Total Supply: 99,000,000,000,000,000.00 Token | Total Token Holders: 92

CacaDragon Top 100 Token Holders

Source: Etherscan.io



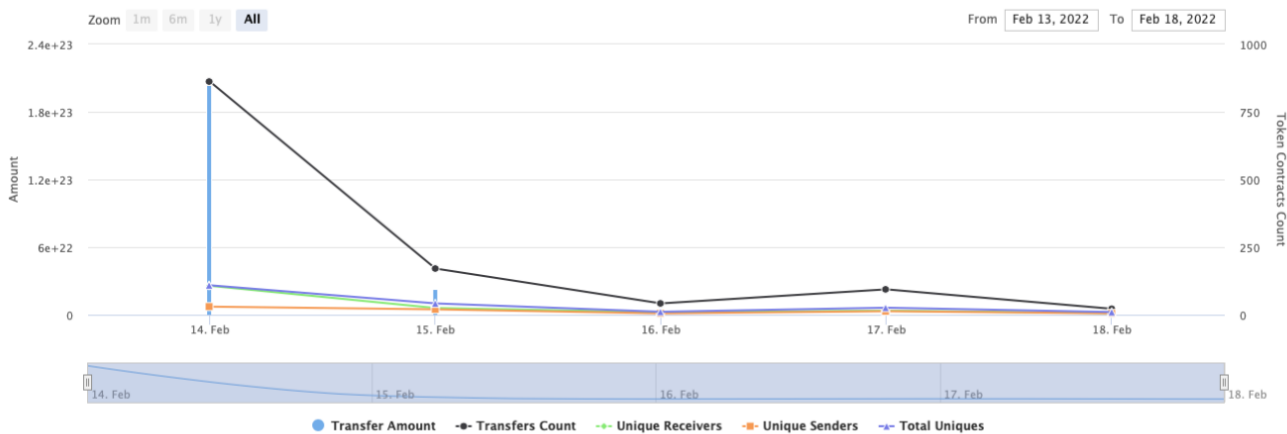
(A total of 98,875,480,641,237,000,000,000.00 tokens held by the top 100 accounts from the total supply of 99,000,000,000,000,000.00 token)

CacaDragon Contract Interaction Details



Time Series: Token Contract Overview

Mon 14, Feb 2022 - Fri 18, Feb 2022

Token Contract 0xae727b5242b662bc0b9e71b2e24546b21e931251 (CacaDragon)
Source: Etherscan.io



CacaDragon Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x00...dEaD	50,289,454,384,676,200,000,000.419648768	50.7974%
2	 UniCrypt : Token Vesting	19,805,232,577,677,800,000,000.625964724	20.0053%
3	0x04008809ab2c5f672e707404f96eb470a4a15bee	14,850,000,000,000,000,000	15.0000%
4	 Uniswap V2: CDR 3	5,202,100,255,155,270,000,000.002675775	5.2546%
5	0x94aeb607646dbc0684bc8e560886d9e3c3b60736	1,467,632,640,177,240,000,000.131237539	1.4825%
6	0xdddb3678fd530ad575b02ed95de3c481542bdf93	1,467,632,640,177,240,000,000.131237539	1.4825%
7	0x901baa18f0ef8071f9ac2c302243aa6fa56693a1	948,377,530,358,444,000,000.725776324	0.9580%
8	0xc51802c369fce385f2faabb7c3bf9461304613cb	309,106,275,108,170,000,000.083533101	0.3122%
9	0x6fdca21d72a09af45fabf2db577e3ac59de79d7b	281,708,426,517,067,000,000.451102129	0.2846%
10	0x5ccc35317809f1009839e2bb8463f40d66e6317d	212,126,484,166,342,000,000.7098422	0.2143%



Contract functions details

- + [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
- + Context
 - [Int] _msgSender
 - [Int] _msgData
- + [Lib] Address
 - [Int] isContract
 - [Int] sendValue #
 - [Int] functionCall #
 - [Int] functionCall #
 - [Int] functionCallWithValue #
 - [Int] functionCallWithValue #
 - [Prv] _functionCallWithValue #
- + Ownable (Context)
 - [Int] <Constructor> #
 - [Pub] owner
 - [Pub] renounceOwnership #
 - modifiers: onlyOwner
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
 - [Pub] geUnlockTime
 - [Pub] lock #
 - modifiers: onlyOwner
 - [Pub] unlock #
- + [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 #
 - [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 #
- + CacaDragon (Context, IERC20, Ownable)
 - [Pub] <Constructor> #
 - [Pub] name
 - [Pub] symbol
 - [Pub] decimals
 - [Pub] totalSupply
 - [Pub] balanceOf
 - [Pub] transfer #
 - [Pub] allowance
 - [Pub] approve #
 - [Pub] transferFrom #
 - [Pub] increaseAllowance #
 - [Pub] decreaseAllowance #
 - [Pub] isExcludedFromReward
 - [Pub] totalFees
 - [Pub] deliver #
 - [Pub] reflectionFromToken
 - [Pub] tokenFromReflection
 - [Pub] excludeFromReward #
 - modifiers: onlyOwner
 - [Ext] includeInReward #
 - modifiers: onlyOwner
 - [Prv] _transferBothExcluded #
 - [Pub] excludeFromFee #
 - modifiers: onlyOwner
 - [Pub] includeInFee #
 - modifiers: onlyOwner
 - [Ext] setRewardFeePercent #
 - modifiers: onlyOwner
 - [Ext] setLiquidityFeePercent #
 - modifiers: onlyOwner
 - [Ext] setMarketingFeePercent #
 - modifiers: onlyOwner
 - [Ext] setDevFeePercent #
 - modifiers: onlyOwner
 - [Ext] setBurnFeePercent #
 - modifiers: onlyOwner
 - [Ext] setMarketingWallet #
 - modifiers: onlyOwner
 - [Ext] setDevWallet #
 - modifiers: onlyOwner
 - [Ext] setMaxWalletPercent #
 - modifiers: onlyOwner
 - [Ext] setMaxWalletPercent2 #
 - modifiers: onlyOwner
 - [Pub] setSwapAndLiquifyEnabled #
 - modifiers: onlyOwner
 - [Pub] setNewRouter #
 - modifiers: onlyOwner
 - [Ext] <Fallback> (\$)
 - [Prv] _reflectFee #

- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] calculateRewardFee
- [Prv] calculateLiquidityFee
- [Prv] calculateMarketingFee
- [Prv] calculateDevFee
- [Prv] calculateBurnFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Prv] _approve #
- [Int] setExtraTaxes #
- [Prv] _transfer #
- [Pub] enableTrading #
 - modifiers: onlyOwner
- [Prv] swapAndLiquify #
 - modifiers: lockTheSwap
- [Prv] swapTokensForEth #
- [Prv] addLiquidity #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Pub] setAntiBotSystemEnable #
 - modifiers: onlyOwner
- [Pub] setBotSettingTime #
 - modifiers: onlyOwner
- [Pub] setBotFeeMultiplier #
 - modifiers: onlyOwner
- [Pub] excludeAntibot #
 - modifiers: onlyOwner
- [Pub] isBot

(\$) = 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.	Low issues
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.	Medium issue
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

1. Liquidity fee issue

Issue:

- In the function `_transfer()` changes liquidity fee when sender address is a bot address. But there is no logic to restore default value of liquidity fee. So after any bot sell all transfers with fee after that will be with increased fee value.

Recommendation:

Add logic to restore default liquidity fee when fee is taking.

✓ Low Severity Issues

2. Out of gas

Issue:

- The function `includeInReward()` uses the loop to find and remove addresses from the `_excluded` list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.
- 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.

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

- Owner can exclude from the fee.
- Owner can change fees.
- Owner can change `_marketingWallet` and `_devWallet`.
- Owner can change `_maxWalletAmount`.
- Owner can change router address.
- Owner can enable trading.
- Owner can enable/disable `antibotSystemEnable`.
- Owner can change `timeDetectBotSeconds` and `timeAntiBot`.
- Owner can change `_botIncreaseFee`.
- Owner can remove bot addresses.
- Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.

Conclusion

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

Liquidity locking details provided by the team:

<https://app.unicrypt.network/amm/uni-v2/token/0xaE727b5242B662bC0B9e71B2E24546B21E931251>

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.



[Techrate1](#)



[Techrate](#)



[Techrate audits](#)