



Smart Contract Security Audit

TechRate
July, 2021

Audit Details



Audited project

CryptoDogs



Deployer address

0xA769c41BfAB24cDa456c4EFeD58d51054F881869



Client contacts:

CryptoDogs team



Blockchain

Binance Smart Chain





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 CryptoDogs to perform an audit of smart contracts:

 $\frac{\text{https://bscscan.com/address/0xc4f7891486d21d711e07dfce9bda89f5ae8b2d98\#cod}{\underline{e}}$

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.

.

101000001

100000001111101100101

100 11011

11001000100000

001000110101

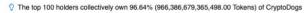
0010011101

Contracts Details

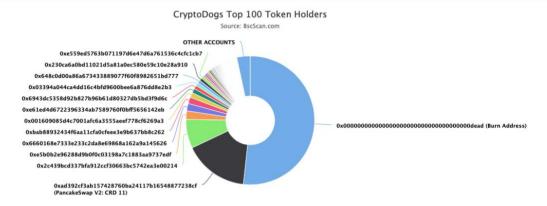
Token contract details for 22.07.2021

Contract name	CryptoDogs
Contract address	0xc4f7891486D21d711E07DFcE9BDA89f5Ae8b2D9 8
Total supply	1,000,000,000,000
Token ticker	CRD
Decimals	9
Token holders	7,850
Transactions count	15,799
Top 100 holders dominance	96.64%
Liquidity fee	9
Tax fee	5
Total fees	44139283487589394756866
Uniswap V2 pair	0xad392cf3ab157428760ba24117b16548877238cf
Contract deployer address	0xA769c41BfAB24cDa456c4EFeD58d51054F88186 9
Contract's current owner address	0xa769c41bfab24cda456c4efed58d51054f881869

CryptoDogs Token Distribution

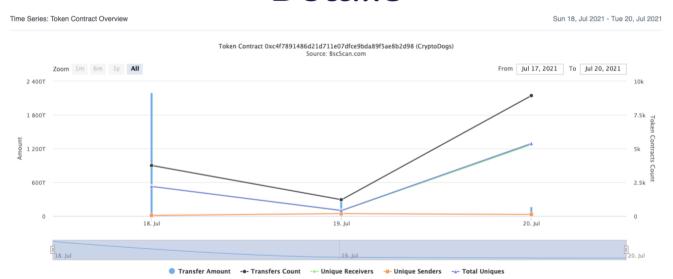


Token Total Supply: 1,000,000,000,000,000.00 Token | Total Token Holders: 7,85



(A total of 966,386,679,365,498.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000,000 token)

CryptoDogs Contract Interaction Details



CryptoDogs Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Burn Address	517,208,652,305,345.331759438	51.7209%
2	□ PancakeSwap V2: CRD 11	162,834,800,577,507.792435174	16.2835%
3	0x2c439bcd337bfa912ccf30663bc5742ea3e00214	72,468,728,312,560.303474839	7.2469%
4	0xe5b0b2e96288d9b0f0c03198a7c1883aa9737edf	21,286,903,932,234.906639067	2.1287%
5	0x6660168e7333e233c2da8e69868a162a9a145626	18,525,925,248,597.0125441	1.8526%
6	0xbab88932434f6aa11cfa0cfeee3e9b637bb8c262	16,530,279,364,820.733676282	1.6530%
7	0x001609085d4c7001afc6a3555aeef778cf6269a3	12,050,082,542,919.998517004	1.2050%
8	0xe61ed4d6722396334ab7589760f0bff5656142eb	11,357,253,750,422.421753114	1.1357%
9	0x6943dc5358d92b827b96b61d80327db5bd3f9d6c	8,789,245,662,723.41836975	0.8789%
10	0x03394a044ca4dd16c4bfd9600bee6a876dd8e2b3	8,081,474,032,569.503217828	0.8081%

CryptoDogs LP Token Holders

Rank	Address	Quantity	Percentage
1		9,002.339988493594	90.6549%
2	CryptoDogs: Deployer	877.713502721607979921	8.8387%
3	0x07d80ae6f36a5e08dca74ce884a24d39db9934ed	42.709812200879018132	0.4301%
4	0x8cc7bc33f5188b1fb683bedc4dbffa77b136833b	7.081447892625507892	0.0713%
5	0xde608e1d1db7a0fc7c57d9e37f938c1d0e671069	0.494024610095028737	0.0050%
6	<u> </u>	0.00000000000001	0.0000%

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) - [Pub] owner - [Pub] renounceOwnership # - modifiers: onlvOwner - [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 #
- + CryptoDogs (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] setTaxFeePercent #
 - modifiers: onlyOwner
 - [Ext] setLiquidityFeePercent #
 - modifiers: onlyOwner
 - [Pub] setNumTokensSellToAddToLiquidity #
 - modifiers: onlyOwner
 - [Pub] setMaxTxPercent#
 - modifiers: onlyOwner
 - [Pub] setSwapAndLiquifyEnabled #
 - modifiers: onlyOwner
 - [Ext] <Fallback> (\$)
 - [Prv] reflectFee #
 - [Prv] _getValues
 - [Prv] _getTValues
 - [Prv] _getRValues
 - [Prv] _getRate
 - [Prv] _getCurrentSupply
 - [Prv] _takeLiquidity #
 - [Pub] claimTokens #
 - modifiers: onlyOwner
 - [Prv] calculateTaxFee
 - [Prv] calculateLiquidityFee
 - [Prv] removeAllFee #
 - [Prv] restoreAllFee #
 - [Pub] isExcludedFromFee

- [Prv] _approve #
- [Prv] _transfer #
- [Prv] swapAndLiquify #
 - modifiers: lockTheSwap
- [Prv] swapTokensForEth #
- [Prv] addLiquidity #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- (\$) = 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.	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
 - 1. 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 change the tax and liquidity fee.

```
function setTaxFeePercent(uint256 taxFee) external onlyOwner() {
    _taxFee = taxFee;
}

function setLiquidityFeePercent(uint256 liquidityFee) external onlyOwner() {
    _liquidityFee = liquidityFee;
}
```

Owner can change the maximum transaction amount.

Owner can exclude from the fee.

```
function excludeFromFee(address account 1) public onlyOwner {
        [isExcludedFromFee(account 1) = true;
}
```

Owner can claim all tokens from contract balance.

```
ftrace|funcSig
function claimTokens() public onlyOwner {
         payable(_owner).transfer(address(this).balance);
}
```

Owner can change numTokensSellToAddToLiquidity.

```
ftrace|funcSig
function setNumTokensSellToAddToLiquidity(uint256 swapNumber1) public onlyOwner {
    numTokensSellToAddToLiquidity = swapNumber1 * 10 ** _decimals;
}
```

 Owner can lock and unlock. By the way, using these functions the owner could leave as owner even after the ownership was renounced.

```
//Locks the contract for owner for the amount of time provided
function lock(uint256 time) public virtual onlyOwner {
    _previousOwner = _owner;
    _owner = address(0);
    _lockTime = now + time;
    emit OwnershipTransferred(_owner, address(0));
}

//Unlocks the contract for owner when _lockTime is exceeds
function unlock() public virtual {
    require(_previousOwner == msg.sender, "You don't have permission to unlock");
    require(now > _lockTime , "Contract is locked until 7 days");
    emit OwnershipTransferred(_owner, _previousOwner);
    _owner = _previousOwner;
}
```

Conclusion

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

Liquidity locking details provided by the team: https://dxsale.app/app/v2 9/dxlockview?id=0&add=0xA769c41BfAB 24cDa456c4EFeD58d51054F881869&type=lplock&chain=BSC

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.

