



Smart Contract Security Audit

Audit details:

Audited project:	ChesterCoin
Deployer address:	0x1636fefc825ce10db1b26fa1361c19f8cca2fb9a
Client contacts:	ChesterCoin team
Blockchain:	Binance Smart Chain
Project website:	https://chesterfinance.info

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 ChesterCoin to perform an audit of smart contracts:

- <https://bscscan.com/address/0xb74ed4112c23b7c8ef1439fa55d304d537c5599b#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 03.05.2021.

Contract name:	ChesterCoin
Contract address:	0xb74ed4112c23b7c8ef1439fa55d304d537c5599b
Total supply:	100_000_000_000_000_000_000_000_000
Token ticker:	CTRFI
Decimals:	9
Token holders:	25068
Transactions count:	61376
Top 100 holders dominance:	80.42 %
Liquidity fee:	5
Tax fee:	3
Total fees:	10_315_871_944_680_301_199_044_323
Uniswap V2 pair:	0xa4cce27a7404f4e80adb7f2b65ab5d1df07256f8
Contract deployer address:	0x1636fefc825ce10db1b26fa1361c19f8cca2fb9a
Contract's current owner address:	0x000000000000000000000000000000000000dead

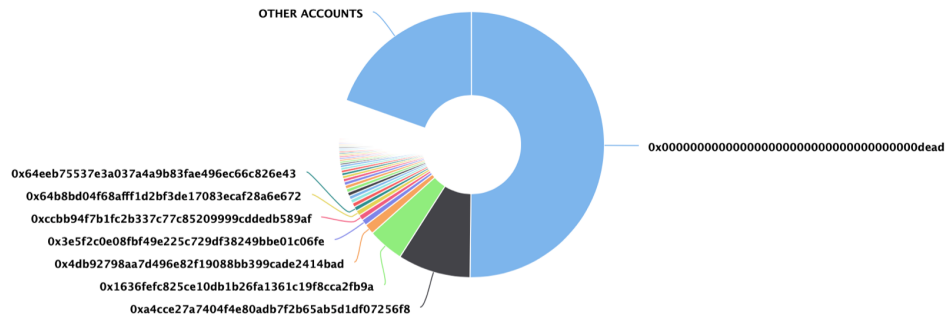
ChesterCoin token distribution

💡 The top 100 holders collectively own 80.42% (80,415,933,051,431,200.00 Tokens) of ChesterCoin

💡 Token Total Supply: 100,000,000,000,000.00 Token | Total Token Holders: 25,068

ChesterCoin Top 100 Token Holders

Source: BscScan.com



(A total of 80,415,933,051,431,200.00 tokens held by the top 100 accounts from the total supply of 100,000,000,000,000,000.00 token)

ChesterCoin contract interaction details

Time Series: Token Contract Overview


Thu 29, Apr 2021 - Sun 2, May 2021

Token Contract 0xb74ed4112c23b7c8ef1439fa55d304d537c5599b (ChesterCoin)


Source: BscScan.com



ChesterCoin top 10 token holders

Rank	Address	Quantity (Token)	Percentage
1	0x00000000000000000000000000000000dead	50,174,424,439,852,600.008997857	50.1744%
2	 0xa4cce27a7404f4e80adb7f2b65ab5d1df07256f8	8,876,165,462,406,670.925020838	8.8762%
3	0x1636fetc825ce10db1b26fa1361c19f8cca2fb9a	4,371,981,869,757,120.342478931	4.3720%
4	0x4db92798aa7d496e82f19088bb399cade2414bad	1,236,208,267,380,640.96474375	1.2362%
5	0x3e5f2c0e08fbf49e225c729df38249bbe01c06fe	757,910,667,866,010.253081519	0.7579%
6	0xcceb94f7b1fc2b337c77c85209999cdded589af	642,845,047,602,530.907444203	0.6428%
7	0x64b8bd04f68afff1d2bf3de17083ecaf28a6e672	640,005,979,258,219.829971933	0.6400%
8	0x64eeb75537e3a037a4a9b83fae496ec66c826e43	525,907,487,102,992.543792055	0.5259%
9	0x1253d14923c14bac88abb8dc198b91258d070ff6	500,013,236,706,817.773755531	0.5000%
10	0xa76ec53ef29e3e22921478e0e390cd401b57268c	486,734,410,072,687.322644495	0.4867%

ChesterCoin LP token holders

Rank	Address	Quantity	Percentage
1	0x00000000000000000000000000000000dead	56,487.166993421536048767	99.0175%
2	0x07d80ae6f36a5e08dca74ce884a24d39db9934ed	546.437887090736998723	0.9579%
3	0xed15e8aa249f0ec0f247bc3716664d409dc8d162	7.479835136884253207	0.0131%
4	0x2dbb3220c75fc29e9b4ea5800a7afc40d76e4578	2.235383501674693529	0.0039%
5	0xf833e2d39cea61f20489c086d27395e8e2f13edc	2.181718873574855563	0.0038%
6	0xcc0fca2c8183cc077d845d097169608a8e540f1a	1.166025973239895502	0.0020%
7	0x0aedb9a1f161e8f65ba3001bc83c9aaf937bbc55	0.362615591943533104	0.0006%
8	0x97b9739b2ec6120162a4c688d0bdaa1e85d2acbb	0.32386721424721493	0.0006%
9	0xc1ea4ec66d0f6ec5e8bfe4fd3037ae764453ea	0.20422897333616469	0.0004%
10	0x18f5cf9ff24be0dbcb3a0094381f0d2641aee3e1	0.073446226594814213	0.0001%
11	 0x000000000000000000000000000000000000	0.000000000000001	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)

- [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 #

+ ChesterCoin (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
- [Ext] setMaxTxPercent #
 - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
 - modifiers: onlyOwner
- [Ext] <Fallback> (\$)
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [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.

```
function includeInReward(address account) external onlyOwner() {
    require(!_isExcluded[account], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- ❑ 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.

```
function _getCurrentSupply() private view returns (uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (
            _rOwned[_excluded[i]] > rSupply ||
            _tOwned[_excluded[i]] > tSupply
        ) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

Recommendation:

Use `EnumerableSet` instead of array or do not use long arrays.

Conclusion

Smart contracts contain only low severity issues. LP pair contract security is not checked.

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.