Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

October, 2021

Audit Details

Audited project

Ecochaintoken

Deployer address

0x80de7EE11f9eBF129F87b0F5668BBD578A0FD356

Client contacts:

Ecochaintoken team

Blockchain

Binance Smart Chain

Project website:

https://ecochaintoken.finance/

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 Ecochaintoken to perform an audit of smart contracts:

https://bscscan.com/address/0x6bfd4ca8ec078d613ed6a5248eb2c7a0d5c38b7b#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

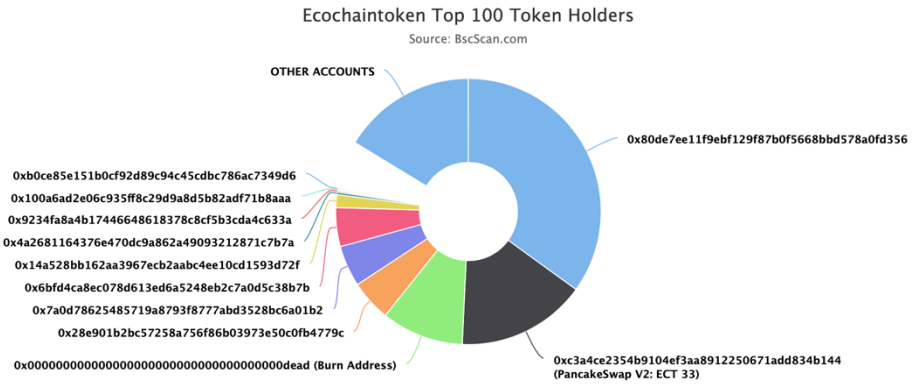
Token contract details for 05.10.2021

Contract name	Ecochaintoken
Contract address	0x6Bfd4cA8eC078d613eD6a5248Eb2c7a0d5c38b7b
Total supply	100,000,000,000,000
Token ticker	Ecochaintoken
Decimals	9
Token holders	9,806
Transactions count	137,921
Top 100 holders dominance	83.68%
Contract deployer address	0x80de7EE11f9eBF129F87b0F5668BBD578A0FD356
Contract’s current owner address	0x80de7EE11f9eBF129F87b0F5668BBD578A0FD356

Ecochaintoken Token Distribution

The top 100 holders collectively own 83.68% (83,683,442,112,132.00 Tokens) of Ecochaintoken

Token Total Supply: 100,000,000,000,000.00 Token | Total Token Holders: 9,806

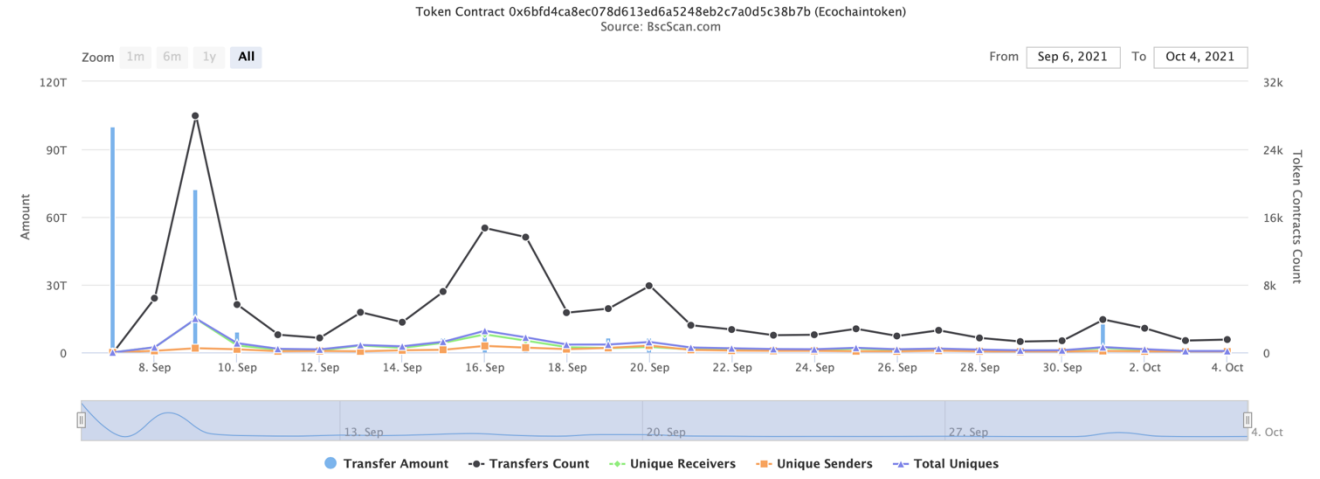


(A total of 83,683,442,112,132.00 tokens held by the top 100 accounts from the total supply of 100,000,000,000,000.00 token)

Ecochaintoken Contract Interaction Details

Time Series: Token Contract Overview

Tue 7, Sept 2021 - Mon 4, Oct 2021



Ecochaintoken Top 10 Token Holders

Rank	Address	Quantity	Percentage
1	0x80de7ee11f9ebf129f87b0f5668bbd578a0fd356	34,969,485,936,715.37919764	34.9695%
2	PancakeSwap V2: ECT 33	15,789,226,204,165.880954953	15.7892%
3	Burn Address	10,000,000,000,000	10.0000%
4	0x28e901b2bc57258a756f86b03973e50c0fb4779c	5,000,010,000,000	5.0000%
5	0x7a0d78625485719a8793f8777abd3528bc6a01b2	5,000,000,000,000	5.0000%
6	0x6bfd4ca8ec078d613ed6a5248eb2c7a0d5c38b7b	4,726,027,540,719.917491084	4.7260%
7	0x14a528bb162aa3967ecb2aabc4ee10cd1593d72f	1,553,533,407,111.21061544	1.5535%
8	0x4a2681164376e470dc9a862a49093212871c7b7a	305,376,752,228.269772538	0.3054%
9	0x9234fa8a4b17446648618378c8cf5b3cda4c633a	173,041,233,771.8078312	0.1730%
10	0x100a6ad2e06c935ff8c29d9a8d5b82adf71b8aaa	155,085,112,003.801795277	0.1551%

Contract functions details

+ [Int] IBEP20
  - [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] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] geUnlockTime
  - [Pub] lock #
    - modifiers: onlyOwner
  - [Pub] unlock #

+ [Int] IPancakeFactory
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #

- [Ext] setFeeToSetter #

+ [Int] IPancakePair
 - [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] IPancakeRouter01
 - [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] IPancakeRouter02 (IPancakeRouter01)
 - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
 - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #

  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Lib] Utils
  - [Int] swapTokensForEth #
  - [Int] swapETHForTokens #
  - [Int] addLiquidity #

+ ReentrancyGuard
  - [Pub] <Constructor> #

+ Ecochaintoken (Context, IBEP20, Ownable, ReentrancyGuard)
  - [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
  - [Ext] startTrading #
    - modifiers: onlyOwner
  - [Pub] totalFees
  - [Pub] deliver #
  - [Pub] reflectionFromToken
  - [Pub] tokenFromReflection
  - [Pub] excludeFromReward #
    - modifiers: onlyOwner
  - [Ext] includeInReward #
    - modifiers: onlyOwner
  - [Pub] excludeFromFee #
    - modifiers: onlyOwner
  - [Pub] includeInFee #
    - modifiers: onlyOwner
  - [Pub] setMaxTxPercent #
    - modifiers: onlyOwner
  - [Pub] setMinTokenNumberToSell #
    - modifiers: onlyOwner
  - [Pub] setExcludeFromMaxTx #
    - modifiers: onlyOwner
  - [Ext] setTaxFeePercent #
    - modifiers: onlyOwner
  - [Ext] setLiquidityFeePercent #
    - modifiers: onlyOwner
  - [Ext] setMarketFeePercent #
    - modifiers: onlyOwner
  - [Ext] setDevFeePercent #
    - modifiers: onlyOwner
  - [Pub] setSwapAndLiquifyEnabled #

    - modifiers: onlyOwner
  - [Ext] setReflectionFees #
    - modifiers: onlyOwner
  - [Ext] setMarketAddress #
    - modifiers: onlyOwner
  - [Ext] setDevAddress #
    - modifiers: onlyOwner
  - [Ext] setPancakeRouter #
    - modifiers: onlyOwner
  - [Ext] <Fallback> ($)
  - [Int] totalFeePerTx
  - [Prv] _reflectFee #
  - [Prv] _getRate
  - [Prv] _getCurrentSupply
  - [Int] _takePoolFee #
  - [Int] _takeMarketFee #
  - [Int] _takeDevFee #
  - [Prv] removeAllFee #
  - [Prv] restoreAllFee #
  - [Pub] isExcludedFromFee
  - [Prv] _approve #
  - [Prv] _transfer #
  - [Prv] _tokenTransfer #
  - [Prv] _transferStandard #
  - [Prv] _transferToExcluded #
  - [Prv] _transferFromExcluded #
  - [Prv] _transferBothExcluded #
  - [Prv] swapAndLiquify #

($) = 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];
            _rOwned[account] = _tOwned[account].mul(_getRate());
            _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:

Check that the excluded array length is not too big.

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

- Owner can start trading.

```
function startTrading() external onlyOwner {
    _tradingOpen = true;
    _launchTime = block.timestamp;
}
```

- Owner include in and exclude from reward.

```
function excludeFromReward(address account) public onlyOwner {
    require(!_isExcluded[account], "Account is already excluded");
    if (_rOwned[account] > 0) {
        _tOwned[account] = tokenFromReflection(_rOwned[account]);
    }
    _isExcluded[account] = true;
    _excluded.push(account);
}

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];
            _rOwned[account] = _tOwned[account].mul(_getRate());
            _tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- Owner can include in and exclude from fee.

```
function excludeFromFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = true;
}

function includeInFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = false;
}
```

- Owner can change the maximum transaction amount and set address to avoid this maximum.

```
// for 1% input 100
function setMaxTxPercent(uint256 maxTxAmount) public onlyOwner {
    _maxTxAmount = _tTotal.mul(maxTxAmount).div(10000);
}
function setExcludeFromMaxTx(address _address, bool value) public onlyOwner {
    _isExcludedFromMaxTx[_address] = value;
}
```

- Owner can change minimum number of tokens to sell.

```
function setMinTokenNumberToSell(uint256 _amount) public onlyOwner {
    minTokenNumberToSell = _amount;
}
```

- Owner can change the tax, liquidity, market and dev fee.

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

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

function setMarketFeePercent(uint256 marketFee) external onlyOwner {
    _marketFee = marketFee;
}

function setDevFeePercent(uint256 devFee) external onlyOwner {
    _devFee = devFee;
}
```

- Owner can change pancake router.

```
function setPancakeRouter(IPancakeRouter02 _pancakeRouter) external onlyOwner {
    pancakeRouter = _pancakeRouter;
}
```

- Owner can change fees and fee receivers addresses.

```
function setFees(
    uint256 _ecosystemFee,
    uint256 _liquidityFee,
    uint256 _buyBackFee,
    uint256 _marketingFee,
    uint256 _feeDenominator
) external onlyOwner {
    ecosystemFee = _ecosystemFee;
    liquidityFee = _liquidityFee;
    buyBackFee = _buyBackFee;
    marketingFee = _marketingFee;
    totalFee = ecosystemFee.add(liquidityFee).add(marketingFee).add(buyBackFee);
    feeDenominator = _feeDenominator;
    require(totalFee < feeDenominator / 4);
}

function setFeeReceivers(
    address _autoLiquidityReceiver,
    address _ecosystemFeeReceiver,
    address _marketingFeeReceiver,
    address _buyBackFeeReceiver
) external onlyOwner {
    autoLiquidityReceiver = _autoLiquidityReceiver;
    ecosystemFeeReceiver = _ecosystemFeeReceiver;
    marketingFeeReceiver = _marketingFeeReceiver;
    buyBackFeeReceiver = _buyBackFeeReceiver;
}
```

- Owner can enable / disable swap and liquify.

```
function setSwapAndLiquifyEnabled(bool _state) public onlyOwner {
    swapAndLiquifyEnabled = _state;
    emit SwapAndLiquifyEnabledUpdated(_state);
}
```

- Owner can enable / disable reflection fee.

```
function setReflectionFees(bool _state) external onlyOwner {
    reflectionFeesdiabled = _state;
}
```

- Owner can change market and dev address.

```
function setMarketAddress(address payable _marketAddress) external onlyOwner {
    marketWallet = _marketAddress;
}

function setDevAddress(address payable _devAddress) external onlyOwner {
    devWallet = _devAddress;
}
```

Conclusion

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

Liquidity locking details are provided by the team:
https://dxsale.app/app/v3/dxlockview?id=0&add=0x80de7EE11f9eBF129F87b0F5668BBD578A0FD356&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.