Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

June, 2021

Audit Details

Audited project

Addax

Deployer address

0x6AAcdA0733c7E405489D3544f8Eaa4D0f8A6B92E

Client contacts:

Addax team

Blockchain

Binance Smart Chain

Project website:

https://addaxtoken.com/

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 Addax to perform an audit of smart contracts:

https://bscscan.com/address/0xce666d0e507c5f2afe0671ee29a99cfa97954c48#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.

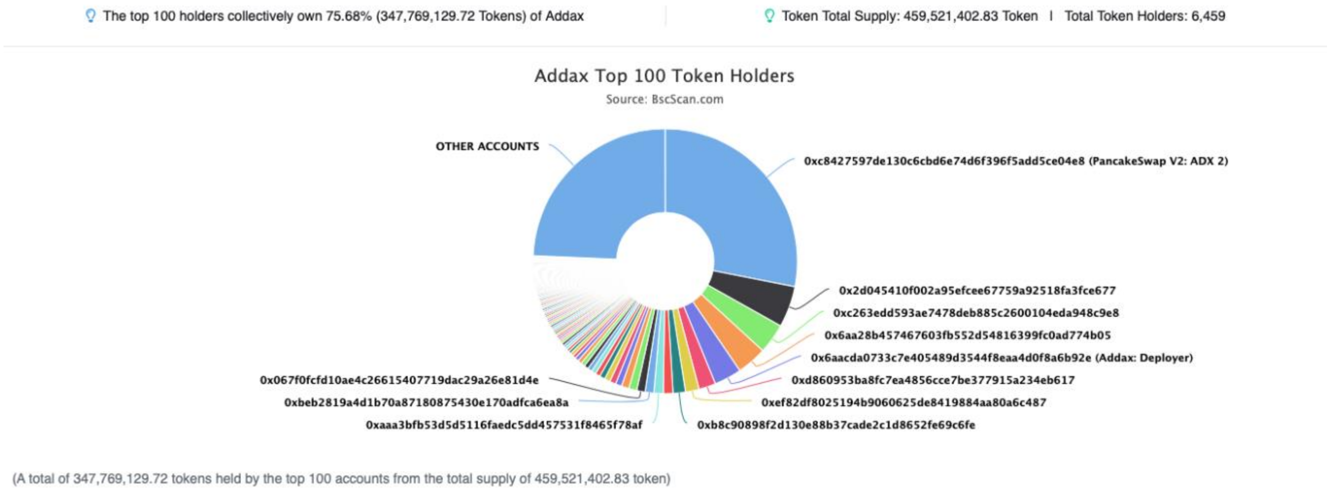
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 04.06.2021

Contract name	Addax
Contract address	0xce666D0e507C5F2Afe0671Ee29A99cfa97954c48
Total supply	459,521,402.831715
Token ticker	ADX
Decimals	9
Token holders	6,458
Transactions count	19,547
Top 100 holders dominance	75.68%
Liquidity fee	500
Tax fee	200
Total fees	40478563168284011
Uniswap V2 pair	0xc8427597de130c6cbd6e74d6f396f5add5ce04e8
Contract deployer address	0x6AAcdA0733c7E405489D3544f8Eaa4D0f8A6B92E
Contract’s current owner address	0x0000000000000000000000000000000000000000

Addax Token Distribution



The top 100 holders collectively own 75.68% (347,769,129.72 Tokens) of Addax

Token Total Supply: 459,521,402.83 Token | Total Token Holders: 6,459

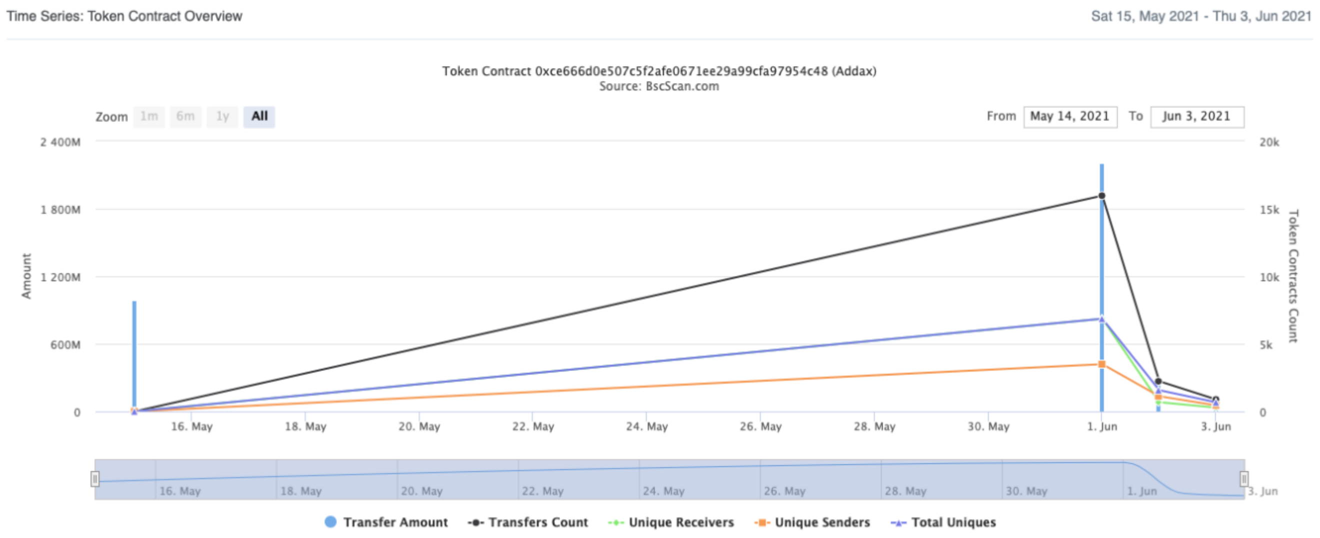
Addax Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0xc8427597de130c6cbd6e74d6f396f5add5ce04e8 (PancakeSwap V2: ADX 2)
0x2d045410f002a95efcee67759a92518fa3fce677
0xc263edd593ae7478deb885c2600104eda948c9e8
0x6aa28b457467603fb552d54816399fc0ad774b05
0x6aacda0733c7e405489d3544f8eaa4d0f8a6b92e (Addax: Deployer)
0xd860953ba8fc7ea4856cce7be377915a234eb617
0xef82df8025194b9060625de8419884aa80a6c487
0xb8c90898f2d130e88b37cade2c1d8652fe69c6fe
0x067f0fcfd10ae4c26615407719dac29a26e81d4e
0xbeb2819a4d1b70a87180875430e170adfca6ea8a
0xaaa3bfb53d5d5116faedc5dd457531f8465f78af

(A total of 347,769,129.72 tokens held by the top 100 accounts from the total supply of 459,521,402.83 token)

Addax Contract Interaction Details



Time Series: Token Contract Overview

Sat 15, May 2021 - Thu 3, Jun 2021

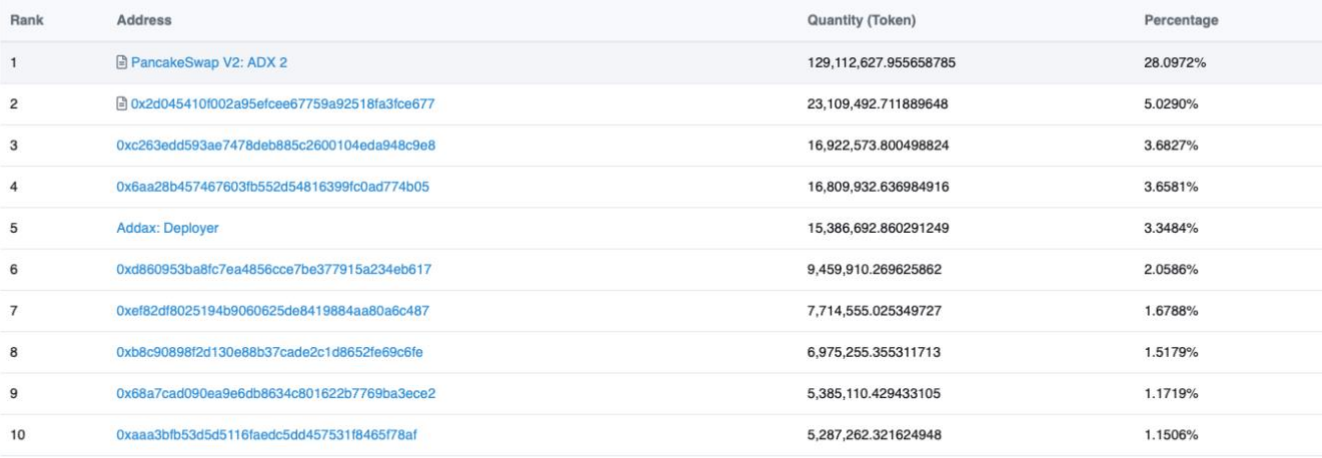
Token Contract 0xce666d0e507c5f2afe0671ee29a99cfa97954c48 (Addax)

Source: BscScan.com

Zoom 1m 6m 1y **All**

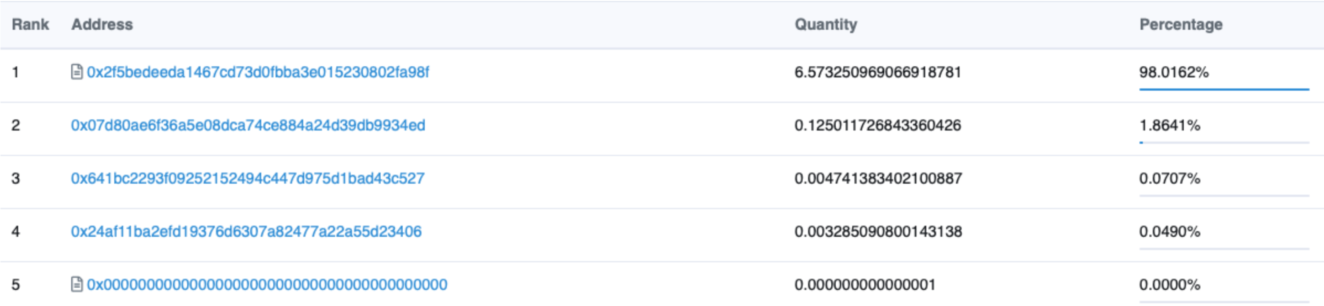
From May 14, 2021 To Jun 3, 2021

Addax Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	PancakeSwap V2: ADX 2	129,112,627.955658785	28.0972%
2	0x2d045410f002a95efcee67759a92518fa3fce677	23,109,492.711889648	5.0290%
3	0xc263edd593ae7478deb885c2600104eda948c9e8	16,922,573.800498824	3.6827%
4	0x6aa28b457467603fb552d54816399fc0ad774b05	16,809,932.636984916	3.6581%
5	Addax: Deployer	15,386,692.860291249	3.3484%
6	0xd860953ba8fc7ea4856cce7be377915a234eb617	9,459,910.269625862	2.0586%
7	0xef82df8025194b9060625de8419884aa80a6c487	7,714,555.025349727	1.6788%
8	0xb8c90898f2d130e88b37cade2c1d8652fe69c6fe	6,975,255.355311713	1.5179%
9	0x68a7cad090ea9e6db8634c801622b7769ba3ece2	5,385,110.429433105	1.1719%
10	0xaaa3bfb53d5d5116faedc5dd457531f8465f78af	5,287,262.321624948	1.1506%

Addax LP Token Holders



Rank	Address	Quantity	Percentage
1	0x2f5bedeeda1467cd73d0fbba3e015230802fa98f	6.573250969066918781	98.0162%
2	0x07d80ae6f36a5e08dca74ce884a24d39db9934ed	0.125011726843360426	1.8641%
3	0x641bc2293f09252152494c447d975d1bad43c527	0.004741383402100887	0.0707%
4	0x24af11ba2efd19376d6307a82477a22a55d23406	0.003285090800143138	0.0490%
5	0x0000000000000000000000000000000000000000	0.000000000000001	0.0000%

Contract functions details

```
 +  Context
   - [Int] _msgSender
   - [Int] _msgData

+ [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

+  Ownable (Context)
   - [Pub] <Constructor> #
   - [Pub] owner
   - [Pub] renounceOwnership #
      - modifiers: onlyOwner
   - [Pub] transferOwnership #
      - modifiers: onlyOwner
   - [Pub] getUnlockTime
   - [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 #

 +  Addax (Context, IBEP20, Ownable)
    - [Pub] <Constructor> #
       - modifiers: Ownable
    - [Ext] <Fallback> ($)
    - [Pub] name
```

- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Prv] _approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Pub] excludeFromReward #
  - modifiers: onlyOwner
- [Ext] includeInReward #
  - modifiers: onlyOwner
- [Pub] totalFees
- [Pub] totalBurn
- [Pub] excludeFromFee #
  - modifiers: onlyOwner
- [Pub] includeInFee #
  - modifiers: onlyOwner
- [Ext] setTaxFeePercent #
  - modifiers: onlyOwner
- [Ext] setLiquidityFeePercent #
  - modifiers: onlyOwner
- [Ext] setBurnFeePercent #
  - modifiers: onlyOwner
- [Ext] setMaxTxPercent #
  - modifiers: onlyOwner
- [Ext] setMinLiquidityPercent #
  - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
  - modifiers: onlyOwner
- [Pub] isExcludedFromFee
- [Pub] isExcludedFromReward
- [Ext] setIsExcludedFromSwapAndLiquify #
  - modifiers: onlyOwner
- [Ext] setUniswapRouter #
  - modifiers: onlyOwner
- [Ext] setUniswapPair #
  - modifiers: onlyOwner
- [Prv] _transfer #
- [Prv] swapAndLiquify #
  - modifiers: lockTheSwap
- [Prv] swapTokensForBnb #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferBothExcluded #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _reflectFee #
- [Prv] _getTValues

- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] takeTransactionFee #

($) = 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

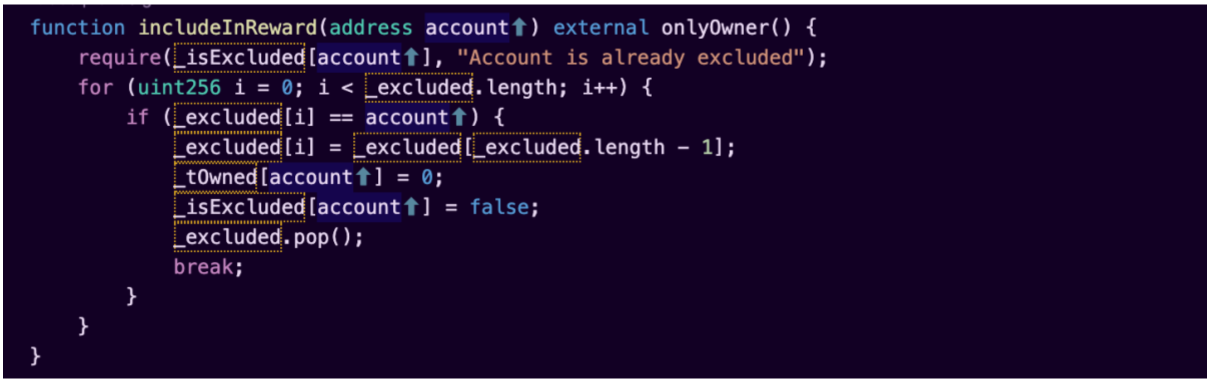
No medium severity issues found.

Low Severity Issues

1. Out of gas

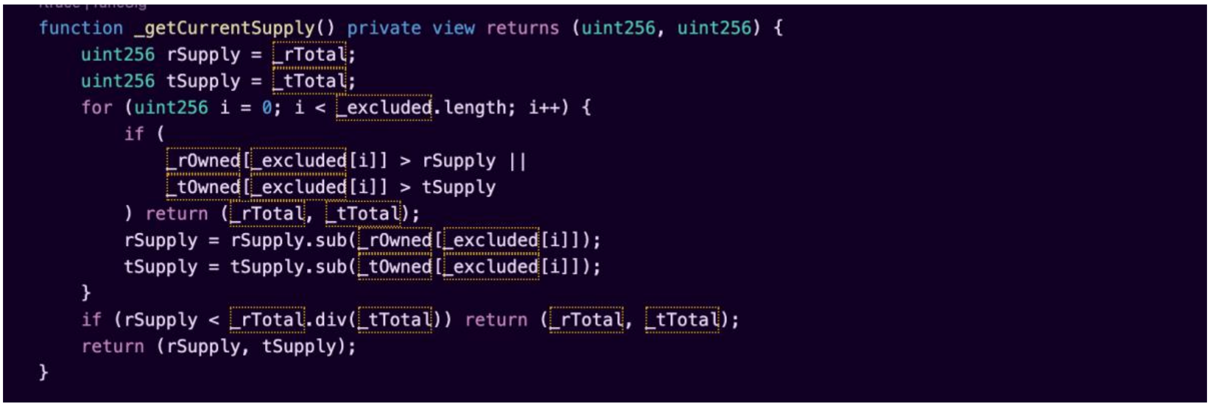
Issue:

- 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.



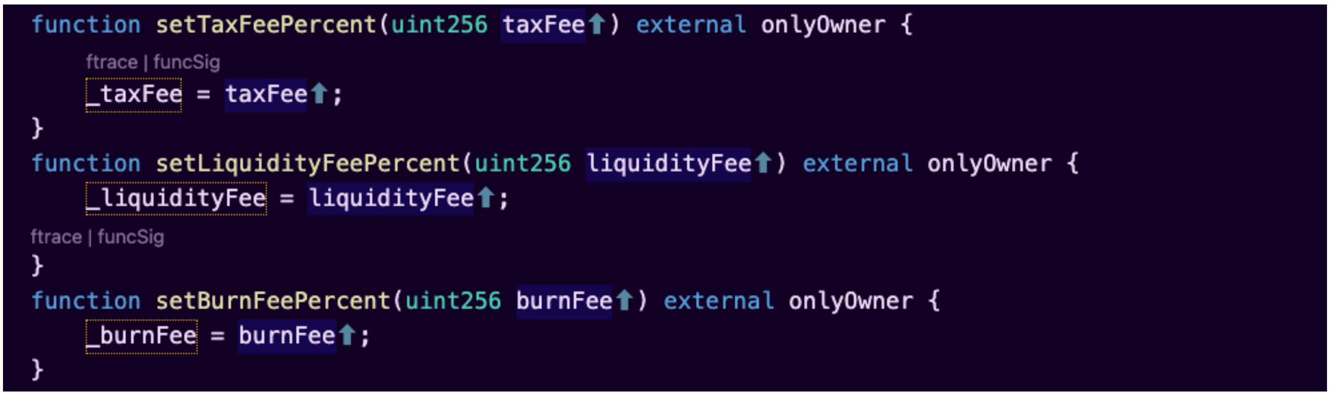
```
function _getCurrentSupply() private view returns (uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (
            _rOwned[_excluded[i]] > rSupply ||
            _tOwned[_excluded[i]] > tSupply
      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

Check that the excluded array length is not too big.

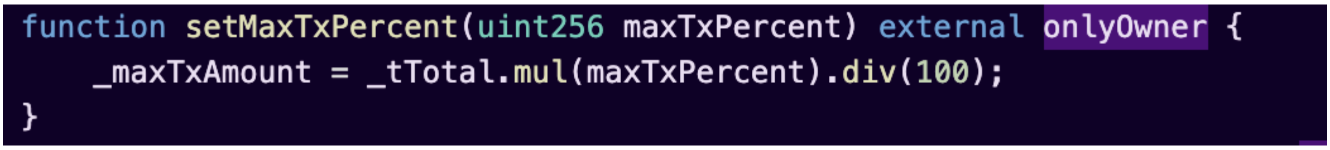
Owner privileges (In the period when the owner is not renounced)

- Owner can change the tax, burn and liquidity fee.



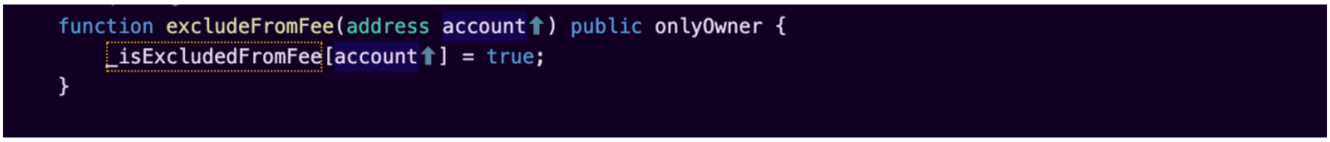
```
function setTaxFeePercent(uint256 taxFee) external onlyOwner {
        ftrace | funcSig
        _taxFee = taxFee;
}
function setLiquidityFeePercent(uint256 liquidityFee) external onlyOwner {
        _liquidityFee = liquidityFee;
ftrace | funcSig
}
function setBurnFeePercent(uint256 burnFee) external onlyOwner {
        _burnFee = burnFee;
}
```

- Owner can change the maximum transaction amount.



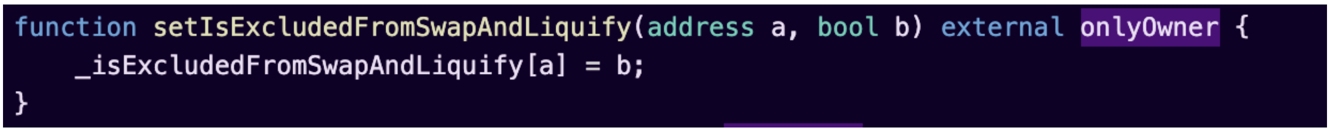
```
function setMaxTxPercent(uint256 maxTxPercent) external onlyOwner {
    _maxTxAmount = _tTotal.mul(maxTxPercent).div(100);
}
```

- Owner can exclude from the fee.



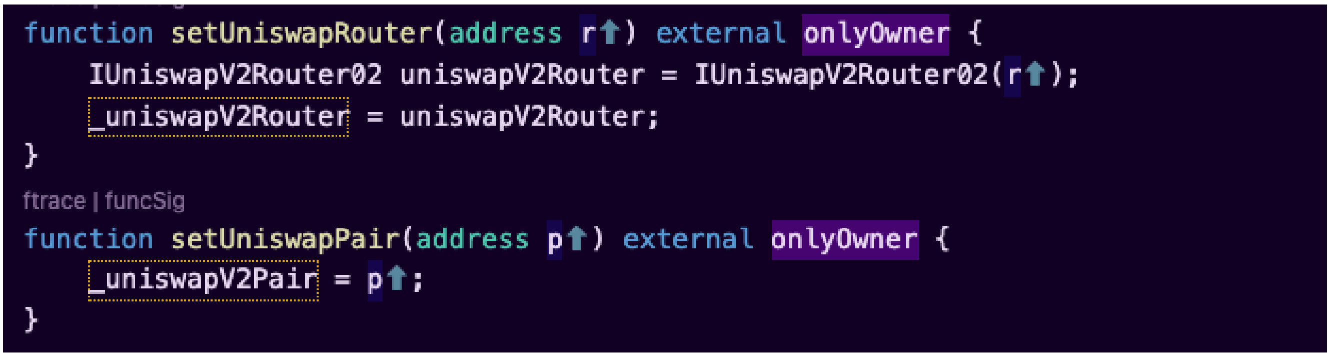
```
function excludeFromFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = true;
}
```

- Owner can include & exclude from swapAndLiquify (swapAndLiquify won't be called).



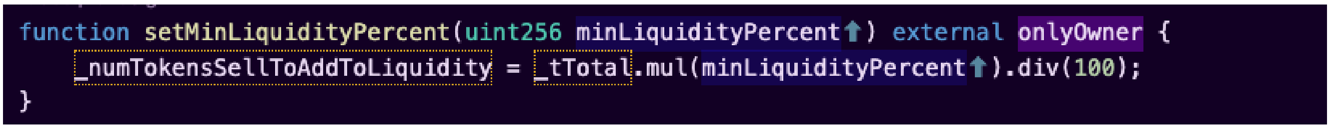
```
function setIsExcludedFromSwapAndLiquify(address a, bool b) external onlyOwner {
    _isExcludedFromSwapAndLiquify[a] = b;
}
```

- Owner can change uniswap router & pair.



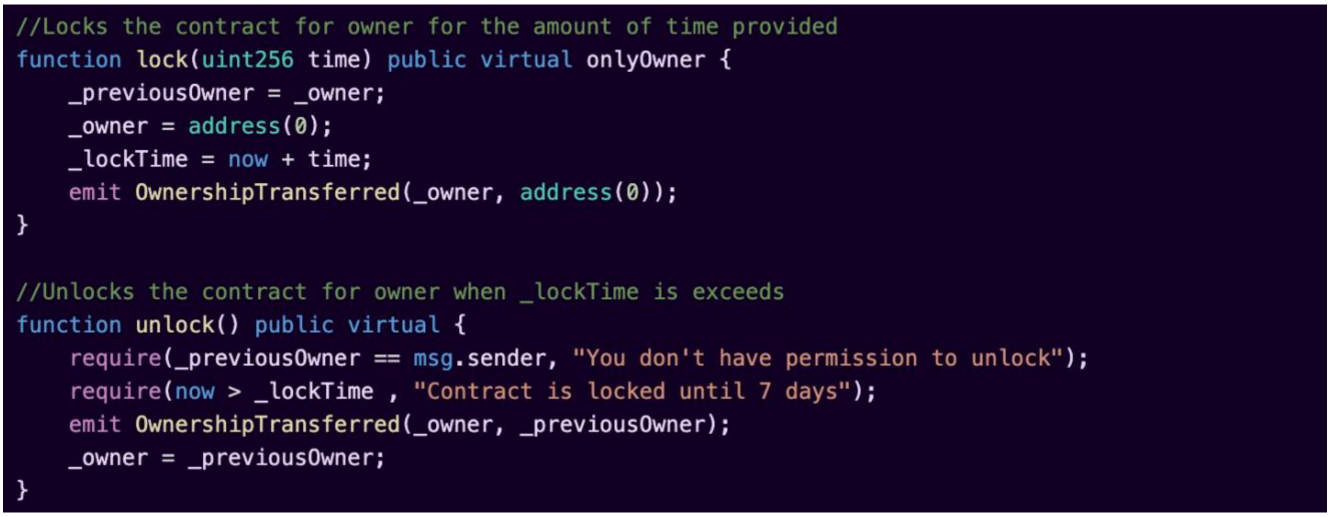
```
function setUniswapRouter(address r) external onlyOwner {
    IUniswapV2Router02 uniswapV2Router = IUniswapV2Router02(r);
    _uniswapV2Router = uniswapV2Router;
}
ftrace | funcSig
function setUniswapPair(address p) external onlyOwner {
    _uniswapV2Pair = p;
}
```

- Owner can change number of tokens to add to liquidity.



```
function setMinLiquidityPercent(uint256 minLiquidityPercent⬆) external onlyOwner {
    _numTokensSellToAddToLiquidity = _tTotal.mul(minLiquidityPercent⬆).div(100);
}
```

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

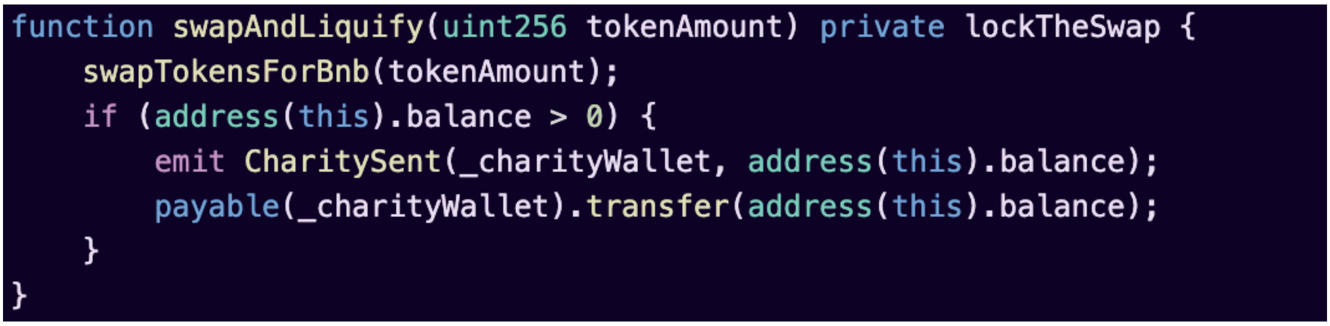


```
//Locks the contract for owner for the amount of time provided
function lock(uint256 time) public virtual onlyOwner {
    _previousOwner = _owner;
    _owner = address(0);
    _lockTime = now + time;
    emit OwnershipTransferred(_owner, address(0));
}

//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;
}
```

Notes

- swapAndLiquify() function sends all swap balance to charity wallet.



```
function swapAndLiquify(uint256 tokenAmount) private lockTheSwap {
    swapTokensForBnb(tokenAmount);
    if (address(this).balance > 0) {
        emit CharitySent(_charityWallet, address(this).balance);
        payable(_charityWallet).transfer(address(this).balance);
    }
}
```

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/pages/dxlockview?id=1250&add=0&type=lpdefi&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.