



TechRate
AUDIT COMPANY

Smart Contract Security Audit

TechRate

June, 2021

Audit Details



Audited project

ORON



Deployer address

0x73a6f76fe249de1d8c5c59439f73acc204c563a8



Client contacts:

ORON team



Blockchain

Binance Smart Chain



Project website:

<https://oronfinance.net>

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 ORON to perform an audit of smart contracts:

<https://bscscan.com/address/0x7177a01e444cf50703bde5e9ae32d2c677ef60e8#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 29.08.2021

| | |
|----------------------------------|--|
| Contract name | ORON |
| Contract address | 0x7177A01e444cf50703bDe5e9Ae32D2C677EF60E8 |
| Total supply | 483,000,000,000 |
| Token ticker | ORN |
| Decimals | 9 |
| Token holders | 209 |
| Transactions count | 708 |
| Top 100 holders dominance | 95.99% |
| Liquidity fee | 10 |
| Tax fee | 1 |
| Total fees | 6055554547083829116 |
| Uniswap V2 pair | 0x3025cf5fe68e6e77e4f2d98e42a15bd87621ebf5 |
| Contract deployer address | 0x73a6f76fe249de1d8c5c59439f73acc204c563a8 |
| Contract's current owner address | 0x73a6f76fe249de1d8c5c59439f73acc204c563a8 |

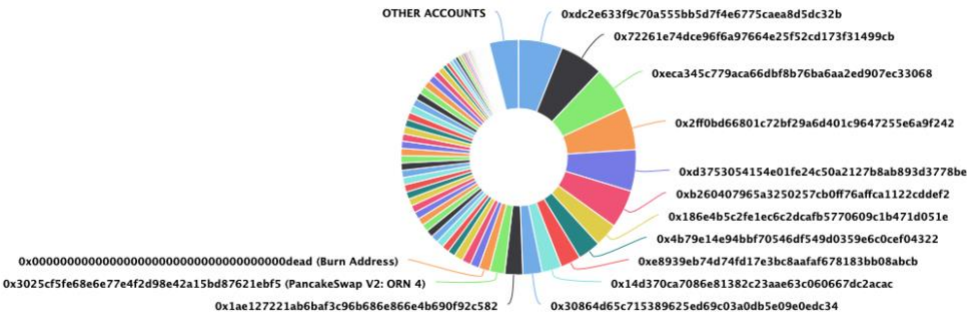
ORON Token Distribution

The top 100 holders collectively own 95.99% (463,613,702,641.07 Tokens) of ORON

Token Total Supply: 483,000,000,000.00 Token | Total Token Holders: 210

ORON Top 100 Token Holders

Source: BscScan.com



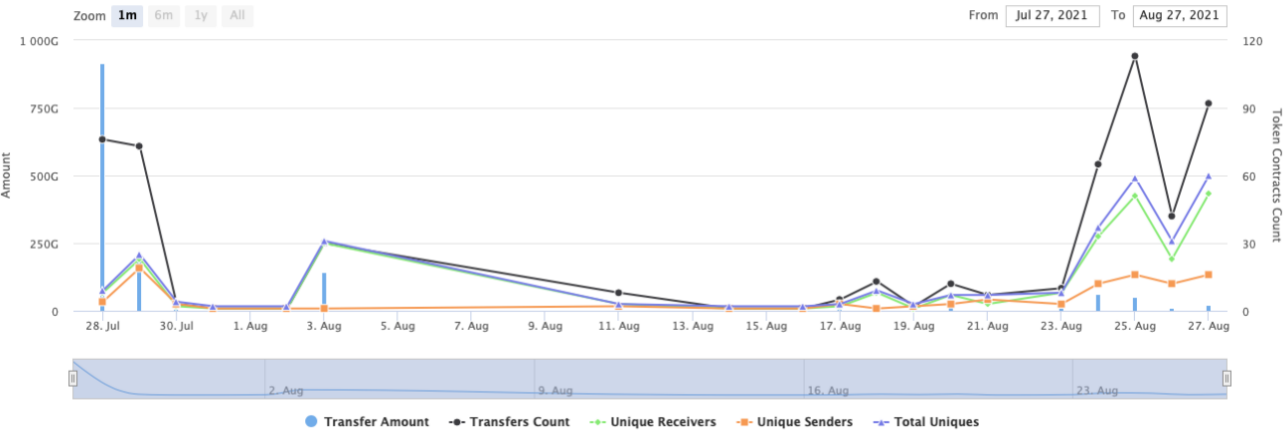
(A total of 463,613,702,641.07 tokens held by the top 100 accounts from the total supply of 483,000,000,000.00 token)

ORON Contract Interaction Details

Time Series: Token Contract Overview

Wed 28, Jul 2021 - Fri 27, Aug 2021



Token Contract 0x7177a01e444cf50703bde5e9ae32d2c677ef60e8 (ORON)
Source: BscScan.com



ORON Top 10 Token Holders

| Rank | Address | Quantity (Token) | Percentage |
|------|--|--------------------------|------------|
| 1 | 0xdc2e633f9c70a555bb5d7f4e6775caea8d5dc32b | 29,283,739,160.719409415 | 6.0629% |
| 2 | 0x72261e74dce96f6a97664e25f52cd173f31499cb | 28,966,212,875.925258198 | 5.9971% |
| 3 | 0xec345c779aca66dbf8b76ba6aa2ed907ec33068 | 28,901,851,376.128300692 | 5.9838% |
| 4 | 0x2ff0bd66801c72bf29a6d401c9647255e6a9f242 | 28,686,377,029.193155798 | 5.9392% |
| 5 | 0xd3753054154e01fe24c50a2127b8ab893d3778be | 27,545,179,854.5336053 | 5.7029% |
| 6 | 0xb260407965a3250257cb0ff76affca1122cddef2 | 25,343,152,096.662760903 | 5.2470% |
| 7 | 0x186e4b5c2fe1ec6c2dcafb5770609c1b471d051e | 15,582,362,883.944796671 | 3.2262% |
| 8 | 0x4b79e14e94bbf70546df549d03596c0cef04322 | 15,100,662,683.36935277 | 3.1264% |
| 9 | 0xe8939eb74d74fd17e3bc8aafa678183bb08abcb | 13,396,626,263.331256529 | 2.7736% |
| 10 | 0x14d370ca7086e81382c23aae63c060667dc2acac | 13,098,301,383.717838556 | 2.7119% |

ORON LP Token Holders

| Rank | Address | Quantity | Percentage |
|------|--|----------------------|-----------------|
| 1 |  0x3f4d6bf08cb7a003488ef082102c2e6418a4551e | 28.5873 | <u>78.7054%</u> |
| 2 | 0x14d370ca7086e81382c23aae63c060667dc2acac | 4.158032441261693262 | <u>11.4477%</u> |
| 3 | 0x1ae127221ab6ba3c96b686e866e4b690f92c582 | 1.179852980697157397 | <u>3.2483%</u> |
| 4 | 0x72261e74dce96f6a97664e25f52cd173f31499cb | 1.093197950613666243 | <u>3.0098%</u> |
| 5 | 0xbb28f1174dee563845cbb7183c79406d43622a78 | 0.83670394319895415 | <u>2.3036%</u> |
| 6 | 0x00e88ca793c084c1f10bc063b0aa776c8bc579f0 | 0.380993727155337266 | <u>1.0489%</u> |
| 7 | 0x8cc7bc33f5188b1fb683bedc4dbffa77b136833b | 0.085760940100736375 | <u>0.2361%</u> |
| 8 | 0x73a6f76fe249de1d8c5c59439f73acc204c563a8 | 0.000039855257605672 | <u>0.0001%</u> |
| 9 |  0x00 | 0.0000000000000001 | <u>0.0000%</u> |



Contract functions details

- + [Int] IERC20
 - [Ext] totalSupply
 - [Ext] balanceOf
 - [Ext] transfer #
 - [Ext] allowance
 - [Ext] approve #
 - [Ext] transferFrom #
- + [Lib] SafeMath
 - [Int] tryAdd
 - [Int] trySub
 - [Int] tryMul
 - [Int] tryDiv
 - [Int] tryMod
 - [Int] add
 - [Int] sub
 - [Int] mul
 - [Int] div
 - [Int] mod
 - [Int] sub
 - [Int] div
 - [Int] mod
- + Context
 - [Int] _msgSender
 - [Int] _msgData
- + [Lib] Address
 - [Int] isContract
 - [Int] sendValue #
 - [Int] functionCall #
 - [Int] functionCall #
 - [Int] functionCallWithValue #
 - [Int] functionCallWithValue #
 - [Int] functionStaticCall
 - [Int] functionStaticCall
 - [Int] functionDelegateCall #
 - [Int] functionDelegateCall #
 - [Prv] _verifyCallResult
- + Ownable (Context)
 - [Pub] <Constructor> #
 - [Pub] owner
 - [Pub] renounceOwnership #
 - modifiers: onlyOwner
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
 - [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 #

+ CoinToken (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] setDevFeePercent #
 - modifiers: onlyOwner
- [Ext] setLiquidityFeePercent #
 - modifiers: onlyOwner
- [Pub] setMaxTxPercent #
 - modifiers: onlyOwner
- [Pub] setDevWalletAddress #
 - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
 - modifiers: onlyOwner
- [Ext] <Fallback> (\$)
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues

- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] _takeDev #
- [Prv] calculateTaxFee
- [Prv] calculateDevFee
- [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 #
- [Ext] setRouterAddress #
 - modifiers: onlyOwner
- [Ext] setNumTokensSellToAddToLiquidity #
 - modifiers: onlyOwner

(\$) = 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(!_excluded[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, dev and liquidity fee.

```
ftrace | funcSig
function setTaxFeePercent(uint256 taxFee↑) external onlyOwner() {
    _taxFee = taxFee↑;
}

ftrace | funcSig
function setDevFeePercent(uint256 devFee↑) external onlyOwner() {
    _devFee = devFee↑;
}

ftrace | funcSig
function setLiquidityFeePercent(uint256 liquidityFee↑) external onlyOwner() {
    _liquidityFee = liquidityFee↑;
}
```

- Owner can change the maximum transaction amount.

```
function setMaxTxPercent(uint256 maxTxPercent↑) public onlyOwner {
    _maxTxAmount = maxTxPercent↑ * 10 ** _decimals;
}
```

- Owner can exclude from the fee.

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

- Owner can change dev address.

```
function setDevWalletAddress(address _addr↑) public onlyOwner {
    _devWalletAddress = _addr↑;
}
```

- Owner can change router address.

```
function setRouterAddress(address newRouter↑) external onlyOwner {
    IUniswapV2Router02 _uniswapV2Router = IUniswapV2Router02(newRouter↑);
    _uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory()).createPair(address(this), _uniswapV2Router.WETH());
    _uniswapV2Router = _uniswapV2Router;
}
```

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

```
function setNumTokensSellToAddToLiquidity(uint256 amountToUpdate↑) external onlyOwner {
    _numTokensSellToAddToLiquidity = amountToUpdate↑;
}
```


- 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 = 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(block.timestamp > _lockTime, "Contract is locked.");
    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 are provided by the team:

<https://deeplock.io/lock/0x3025cf5fe68e6e77E4f2D98E42A15Bd87621EBF5>

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.