



TechRate
AUDIT COMPANY

Smart Contract Security Audit

Audit Details



Audited project

ElonTusk



Deployer address

0x2c423c3cd4792f8768d2232c84dcd6d4073a0ab4



Client contacts:

ElonTusk team



Blockchain

Ethereum



Project website:

<https://elontuskerc20.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 ElonTusk to perform an audit of smart contracts:

<https://etherscan.io/address/0x943498b40d90c1000ca36f06010d970ccc47197f#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 07.10.2021

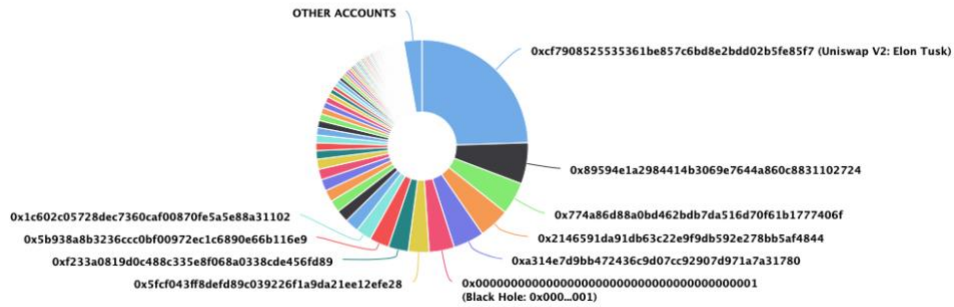
Contract name	ElonTusk
Contract address	0x943498B40d90C1000cA36f06010d970CcC47197f
Total supply	1,000,000,000,000,000,000
Token ticker	Elon Tusk
Decimals	9
Token holders	196
Transactions count	585
Top 100 holders dominance	97.24%
Contract deployer address	0x2c423c3cd4792f8768d2232c84dcd6d4073a0ab4
Contract's current owner address	0x00

ElonTusk Token Distribution

💡 The top 100 holders collectively own 97.24% (972,448,371,099,089,000.00 Tokens) of ELONTUSK

💡 Token Total Supply: 1,000,000,000,000,000.00 Token | Total Token Holders: 196

ELONTUSK Top 100 Token Holders
Source: Etherscan.io



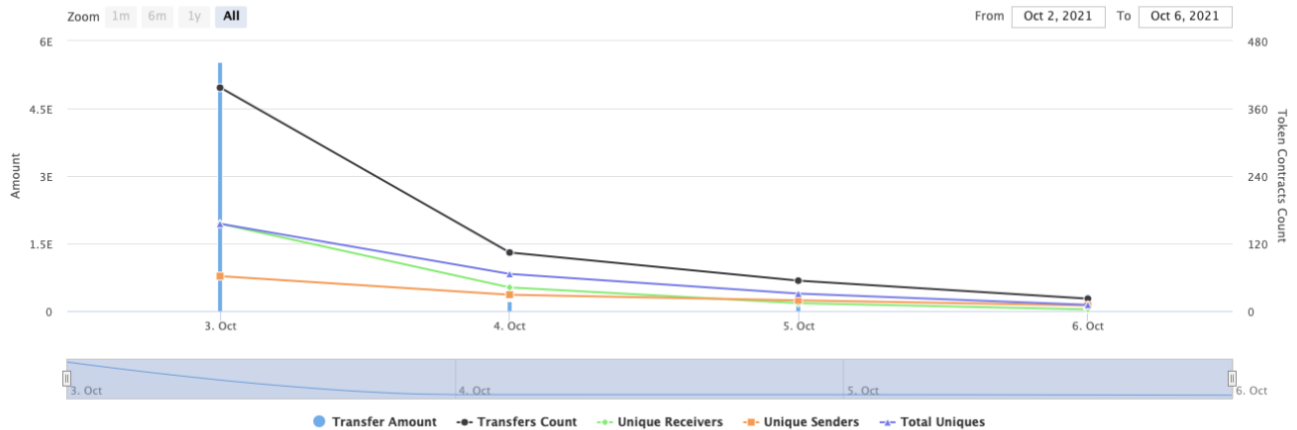
(A total of 972,448,371,099,089,000.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000.00 token)

ElonTusk Contract Interaction Details


Time Series: Token Contract Overview

Sun 3, Oct 2021 - Wed 6, Oct 2021

Token Contract 0x943498b40d90c1000ca36f06010d970ccc47197f (ELONTUSK)
Source: Etherscan.io



ElonTusk Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	 Uniswap V2: Elon Tusk	244,860,816,145,237,000.097550616	24.4861%
2	0x89594e1a2984414b3069e7644a860c8831102724	62,540,577,320,036,800.406300567	6.2541%
3	0x774a86d88a0bd462bdb7da516d70f61b1777406f	49,322,160,720,881,500.326373608	4.9322%
4	0x2146591da91db63c22e9f9db592e278bb5af4844	47,123,964,466,163,900.178045629	4.7124%
5	0xa314e7d9bb472436c9d07cc92907d971a7a31780	47,047,047,047,047,000.047047047	4.7047%
6	Black Hole: 0x000...001	38,365,513,829,270,600.009667926	3.8366%
7	0x5fcf043ff8defd89c039226f1a9da21ee12efe28	31,851,114,306,676,400.580650247	3.1851%
8	0xf233a0819d0c488c335e8f068a0338cde456fd89	30,280,509,333,514,800.713307661	3.0281%
9	0x5b938a8b3236ccc0bf00972ec1c6890e66b116e9	29,976,742,170,816,600.051997483	2.9977%
10	0x1c602c05728dec7360caf00870fe5a5e88a31102	23,526,528,755,495,100.617610275	2.3527%



Contract functions details

+ Context

- [Int] _msgSender

+ [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

+ Ownable (Context)

- [Pub] <Constructor> #
- [Pub] owner
- [Pub] renounceOwnership #
- modifiers: onlyOwner

+ [Int] IUniswapV2Factory

- [Ext] createPair #

+ [Int] IUniswapV2Router02

- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
- [Ext] factory
- [Ext] WETH
- [Ext] addLiquidityETH (\$)

+ ElonTusk (Context, IERC20, Ownable)

- [Pub] <Constructor> #
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Ext] setCooldownEnabled #
- modifiers: onlyOwner
- [Prv] tokenFromReflection
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] swapTokensForEth #

- modifiers: lockTheSwap
- [Prv] sendETHToFee #
- [Ext] openTrading #
 - modifiers: onlyOwner
- [Pub] setBots #
 - modifiers: onlyOwner
- [Pub] delBot #
 - modifiers: onlyOwner
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _takeTeam #
- [Prv] _reflectFee #
- [Ext] <Fallback> (\$)
- [Ext] manualswap #
- [Ext] manualsend #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply

(\$) = 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.	Passed
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

No low severity issues found.

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

- Owner can enable cooldown (user to user trading with time offset).

```
function setCooldownEnabled(bool onoff) external onlyOwner() {
    cooldownEnabled = onoff;
}
```

- Owner can open swap trading.

```
function openTrading() external onlyOwner() {
    require(!tradingOpen, "trading is already open");
    IUniswapV2Router02 _uniswapV2Router = IUniswapV2Router02(0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D);
    uniswapV2Router = _uniswapV2Router;
    _approve(address(this), address(uniswapV2Router), _tTotal);
    uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory()).createPair(address(this), _uniswapV2Router.WETH());
    uniswapV2Router.addLiquidityETH(value: address(this).balance)(address(this), balanceOf(address(this)), 0, 0, owner(), block.timestamp);
    swapEnabled = true;
    cooldownEnabled = true;
    _maxTxAmount = 5000000000000000 * 10**9;
    tradingOpen = true;
    IERC20(uniswapV2Pair).approve(address(uniswapV2Router), type(uint).max);
}
```

- Owner can add and remove bots (no transferring between this addresses).

```
function setBots(address[] memory bots_) public onlyOwner {
    for (uint i = 0; i < bots_.length; i++) {
        bots[bots_[i]] = true;
    }
}

function delBot(address notbot) public onlyOwner {
    bots[notbot] = false;
}
```

Conclusion

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

Liquidity locking details provided by the team:

<https://team.finance/view-coin/0x943498B40d90C1000cA36f06010d970CcC47197f?name=ELONTUSK&symbol=Elon%20Tusk>

Ownership renounce details provided by the team:

<https://etherscan.io/tx/0x666f3f6f2c86b670873dfb14572d573e6dc2df4035aa3be08fe40191be992273>

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.



[Techrate1](#)



[Techrate](#)



[Techrate_audits](#)