Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

December, 2021

Audit Details

Audited project

ZamoLaws

Deployer address

0x9acb3ca313516d367838e77be370d8104361682b

Client contacts:

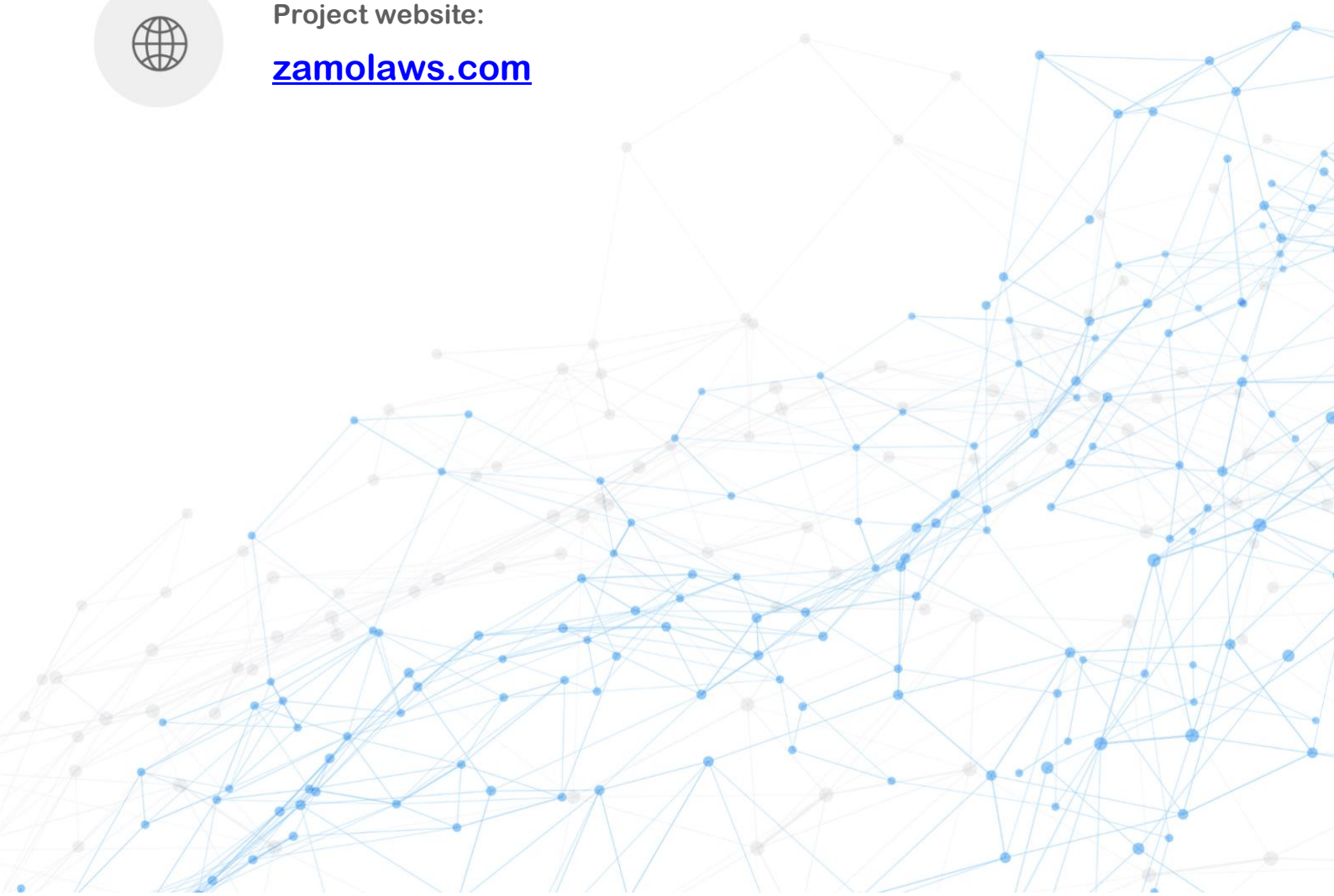
ZamoLaws team

Blockchain

Ethereum

Project website:

zamolaws.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 ZamoLaws to perform an audit of smart contracts:

https://etherscan.io/address/0xb7888f20642f6bcab295b48a8a20bede0f4a3c49#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

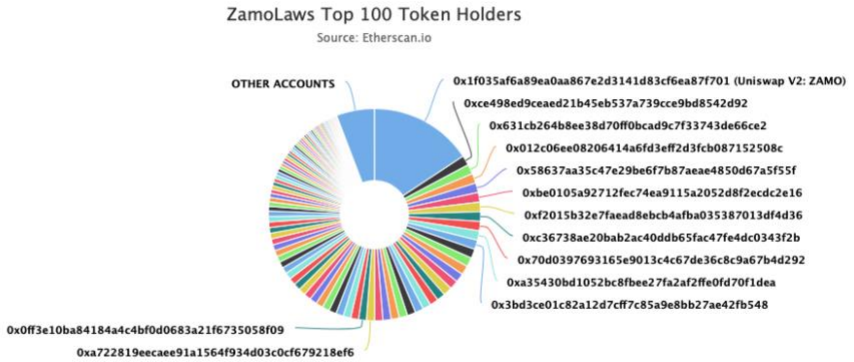
Token contract details for 29.12.2021

Contract name	ZamoLaws
Contract address	0xB7888f20642F6Bcab295B48a8a20beDe0f4a3c49
Total supply	1,000,000,000,000
Token ticker	ZAMO
Decimals	9
Token holders	199
Transactions count	286
Top 100 holders dominance	94.20%
Max wallet size	25000000000000000000
Max TX amount	5000000000000000000
Development address	0x23d94b332f6f89cbd3555c645736a0bd52c70c68
Uniswap V2 pair	0x1f035af6a89ea0aa867e2d3141d83cf6ea87f701
Contract deployer address	0x9acb3ca313516d367838e77be370d8104361682b
Contract's current owner address	0x9acb3ca313516d367838e77be370d8104361682b

ZamoLaws Token Distribution

The top 100 holders collectively own 94.20% (942,000,603,092.60 Tokens) of ZamoLaws

Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 199

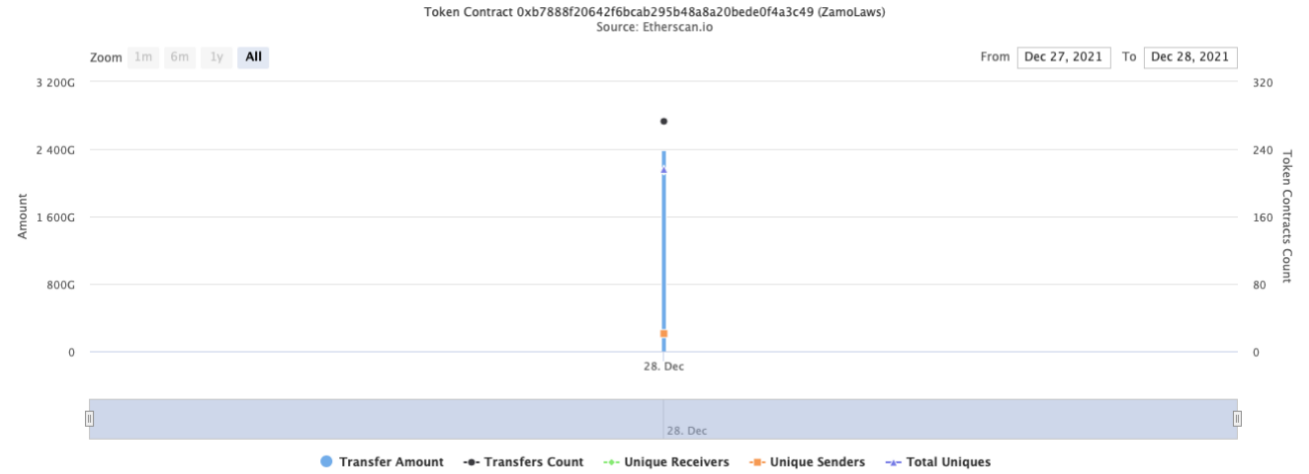


(A total of 942,000,603,092.60 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

ZamoLaws Contract Interaction Details

Time Series: Token Contract Overview

Tue 28, Dec 2021 - Tue 28, Dec 2021



ZamoLaws Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Uniswap V2: ZAMO	157,237,785,740.74116124	15.7238%
2	0xce498ed9ceaed21b45eb537a739cce9bd8542d92	14,964,073,604	1.4964%
3	0x631cb264b8ee38d70ff0bcad9c7f33743de66ce2	14,824,850,972	1.4825%
4	0x012c06ee08206414a6fd3eff2d3fcb087152508c	14,728,991,959	1.4729%
5	0x58637aa35c47e29be6f7b87aeae4850d67a5f55f	14,669,764,790	1.4670%
6	0xbe0105a92712fec74ea9115a2052d8f2ecdc2e16	14,624,426,756	1.4624%
7	0xf2015b32e7faead8ebcb4afba035387013df4d36	14,615,369,938	1.4615%
8	0xc36738ae20bab2ac40ddb65fac47fe4dc0343f2b	14,539,393,595	1.4539%
9	0x70d0397693165e9013c4c67de36c8c9a67b4d292	14,284,041,834	1.4284%
10	0xa35430bd1052bc8fbee27fa2af2ffe0fd70f1dea	14,276,401,104	1.4276%

Contract functions details

+ Context
  - [Int] _msgSender

+ [Int] IERC20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

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

+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div

+ [Int] IUniswapV2Factory
  - [Ext] createPair #

+ [Int] IUniswapV2Router02
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidityETH ($)

+ ZamoLaws (Context, IERC20, Ownable)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] developmentWallet
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Prv] tokenFromReflection
  - [Prv] removeAllFee #
  - [Prv] restoreAllFee #

- [Prv] _approve #
- [Prv] _transfer #
- [Prv] swapTokensForEth #
  - modifiers: lockTheSwap
- [Ext] setMinSwapTokensThreshold #
- [Prv] sendETHToFee #
- [Pub] setTrading #
  - modifiers: onlyOwner
- [Ext] manualswap #
- [Ext] manualsend #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _takeTeam #
- [Prv] _reflectFee #
- [Ext] <Fallback> ($)
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Pub] toggleSwap #
  - modifiers: onlyOwner
- [Ext] setMaxTxnAmount #
- [Ext] setMaxWalletSize #
- [Ext] lowerBuyTeamFee #
- [Ext] lowerSellTeamFee #

($) = 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/disable trading.
- Owner can enable/disable swap.
- Development address can change _swapTokensAtAmount.
- Development address can withdraw contract ETHs.
- Development address can manually swap and send amount to fee.
- Development address can change max TX amount.
- Development address can change _maxWalletSize.
- Development address can lower _taxFeeOnBuy and _taxFeeOnSell.

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 are provided by the team:
https://app.unicrypt.network/amm/uni-v2/pair/0x1f035af6a89ea0aa867e2d3141d83cf6ea87f701

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.