Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

November, 2021

Audit Details

Audited project

Zatcoin

Deployer address

0xf03e4b5ddc3a55846a2d3f8f395b31238386df97

Client contacts:

Zatcoin team

Blockchain

Binance Smart Chain

Project website:

https://zatcoin.io/home

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 Zatcoin to perform an audit of smart contracts:

https://bscscan.com/address/0x958e030E5937414B8B54e4647fb513E348Ed90E5#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

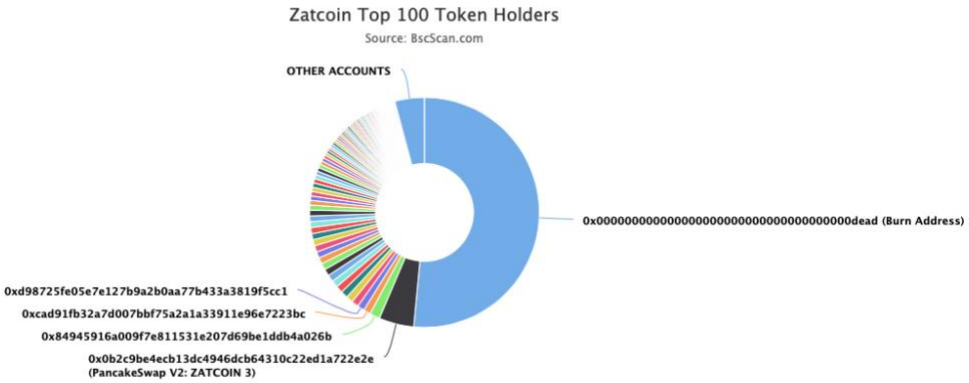
Token contract details for 14.11.2021

Contract name	Zatcoin
Contract address	0x958e030E5937414B8B54e4647fb513E348Ed90E5
Total supply	2,000,000,000
Token ticker	ZATCOIN
Decimals	7
Token holders	638
Transactions count	727
Top 100 holders dominance	95.83%
Liquidity wallet	0x84945916a009f7e811531e207d69be1ddb4a026b
Marketing wallet	0xb5592bdc5ad40c7cb5678225a310b6573ca3c43e
Total fees	8256149308478
Uniswap V2 pair	0x0b2c9be4ecb13dc4946dcb64310c22ed1a722e2e
Contract deployer address	0xf03e4b5ddc3a55846a2d3f8f395b31238386df97
Contract's current owner address	0xf03e4b5ddc3a55846a2d3f8f395b31238386df97

Zatcoin Token Distribution

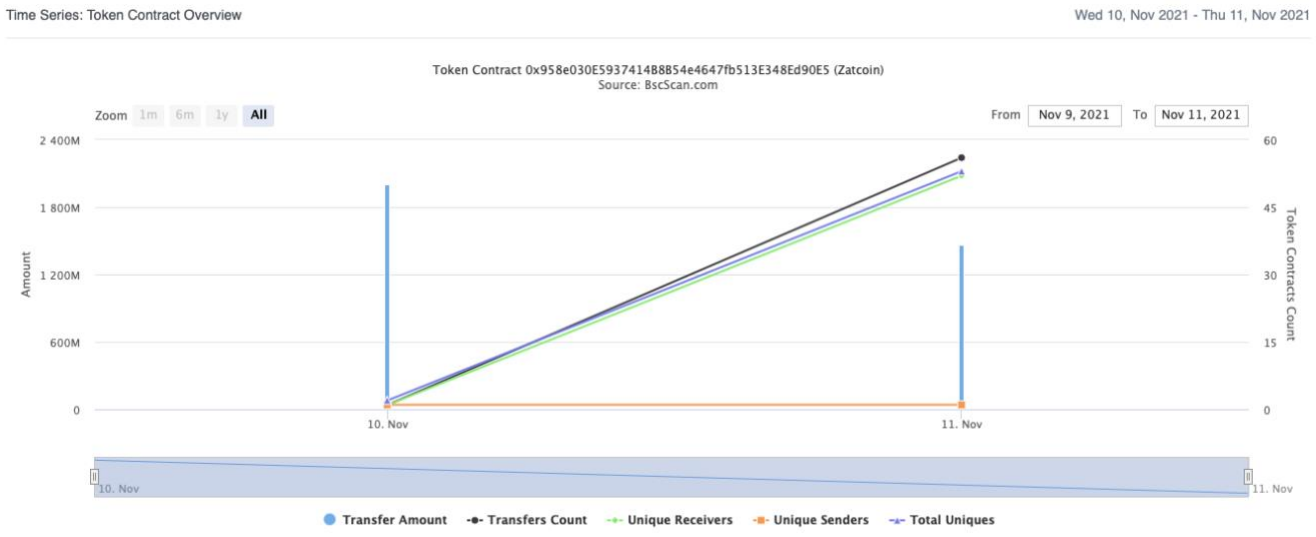
The top 100 holders collectively own 95.83% (1,916,672,887.52 Tokens) of Zatcoin

Token Total Supply: 2,000,000,000.00 Token | Total Token Holders: 638



(A total of 1,916,672,887.52 tokens held by the top 100 accounts from the total supply of 2,000,000,000.00 token)

Zatcoin Contract Interaction Details



Zatcoin Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Burn Address	1,029,915,975	51.4958%
2	PancakeSwap V2: ZATCOIN 3	98,724,435.6061306	4.9362%
3	0x84945916a009f7e811531e207d69be1ddb4a026b	28,818,274.3700048	1.4409%
4	0xcad91fb32a7d007bbf75a2a1a33911e96e7223bc	19,996,975.39	0.9998%
5	0xd98725fe05e7e127b9a2b0aa77b433a3819f5cc1	19,876,828.6565947	0.9938%
6	0xb8298214a3798710a29a4258bf83dc8637981b7a	19,870,662.61	0.9935%
7	0x80cf5e67808ea62070c4d8bf0af36b0f17282d88	19,840,183.01	0.9920%
8	0xf2e9c0eabea787743036588875445fcd7607bde1	19,807,933.76	0.9904%
9	0xb02c069f98ed5a16bcbd5a7ac3551d91134b01d0	19,795,680	0.9898%
10	0x81dcf02d043a6959765579a9254bb390fedf4527	19,599,814.07	0.9800%

Contract functions details

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

+ [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
  - [Int] mod
  - [Int] mod

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] _functionCallWithValue #

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

+ [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 #

+ Zatcoin (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] reflectionFromToken
- [Pub] tokenFromReflection
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] swapAndLiquify #
  - modifiers: lockTheSwap
- [Prv] swapTokensForBNB #
- [Prv] addLiquidity #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _transferBothExcluded #
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] calculateTaxFee
- [Prv] calculateLiquidityFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Ext] A_setMaxTxPercent #
  - modifiers: onlyOwner
- [Ext] E1_enableFees #
  - modifiers: onlyOwner
- [Pub] E2_enable_ProjectFunding #
  - modifiers: onlyOwner
- [Ext] E4_enableTrading #
  - modifiers: onlyOwner
- [Ext] F01_setMarketingFee #
  - modifiers: onlyOwner
- [Ext] F02_setBuyBackfee #
  - modifiers: onlyOwner
- [Ext] F06_setBuyTaxfee #
  - modifiers: onlyOwner
- [Ext] F02_setLiqfee #
  - modifiers: onlyOwner
- [Ext] F07_setTaxFee #

  - modifiers: onlyOwner
- [Ext] F08_setProjectFee #
  - modifiers: onlyOwner
- [Ext] F09_setSellTaxFee #
  - modifiers: onlyOwner
- [Ext] F11_setTransferTaxFee #
  - modifiers: onlyOwner
- [Ext] F12_setBuyProjectFee #
  - modifiers: onlyOwner
- [Ext] F13_setSellProjectFee #
  - modifiers: onlyOwner
- [Ext] F15_setTransferProjectFee #
  - modifiers: onlyOwner
- [Ext] F16_setExchangeTaxFee #
  - modifiers: onlyOwner
- [Ext] F17_setExchangeProjectFee #
  - modifiers: onlyOwner
- [Pub] S01_includeInFee #
  - modifiers: onlyOwner
- [Pub] S02_excludeFromFee #
  - modifiers: onlyOwner
- [Ext] S03_includeInReward #
  - modifiers: onlyOwner
- [Pub] S04_excludeFromReward #
  - modifiers: onlyOwner
- [Pub] S05_addToBlacklist #
  - modifiers: onlyOwner
- [Pub] S06_removeFromBlacklist #
  - modifiers: onlyOwner
- [Pub] S07_addAllowedExchange #
  - modifiers: onlyOwner
- [Pub] S08_removeAllowedExchange #
  - modifiers: onlyOwner
- [Pub] S09_isAllowedExchange
- [Pub] S10_addBridge #
  - modifiers: onlyOwner
- [Pub] S11_removeBridge #
  - modifiers: onlyOwner
- [Pub] W1_setMarketingWallet #
  - modifiers: onlyOwner
- [Pub] W2_setBuybackWallet #
  - modifiers: onlyOwner
- [Pub] W3_setliquidityWallet #
  - modifiers: onlyOwner
- [Pub] getAllowedBridges
- [Pub] getBridgeLiquidityFee
- [Pub] getBridgeTaxFee
- [Ext] <Fallback> ($)

($) = 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 S03_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 S03_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.

Notes:

- _maxTxAmount also checked on cases it already passed.
- addLiquidity() function is unused.

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

- Owner can change maximum transaction amount.
- Owner can enable/disable fees, ProjectFundingEnabled and trading.
- Owner can change fees.
- Owner can exclude from the fee.
- Owner can blacklist addresses.
- Owner can add addresses in AllowedExchanges array.
- Owner can change fees for addresses.
- Owner can change marketing, buyback and liquidity wallet.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details provided by the team:
https://dxsale.app/app/v3/dxlockview?id=2&add=0xf03E4b5DDc3a55846A2D3F8F395B31238386df97&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.