TechRate
July, 2022

SMART CONTRACTS SECURITY AUDIT REPORT

Techrate_audits Techrate Techrate1

Audit Details

Audited project

BOJI

Deployer address

0x86670ea08664556e1a1fdd18400807134894a3eb

Client contacts:

BOJI team

Blockchain

Binance Smart Chain

Project website:

www.boji.finance

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 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 BOJI to perform an audit of smart contracts:
https://bscscan.com/address/0x1b19c6bb5ea3290dc8b4cb722dee9eea7bc7b164#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

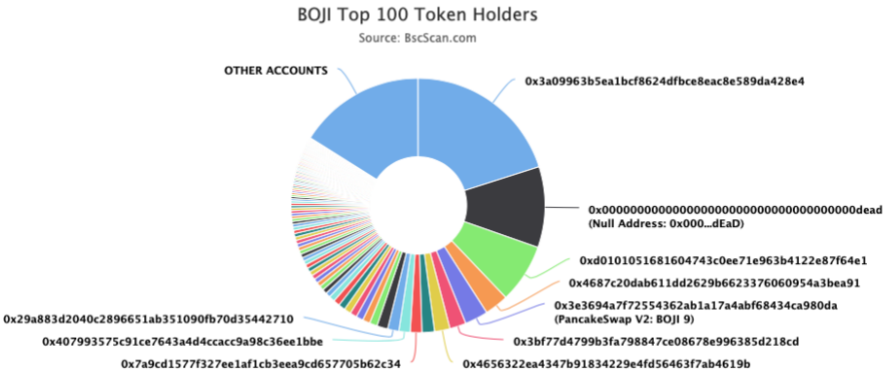
Token contract details for 03.06.2022

Contract name	BOJI
Contract address	0x1b19c6bB5ea3290dc8b4Cb722Dee9EEa7BC7B164
Total supply	700,000,000,000,000
Token ticker	BOJI
Decimals	9
Token holders	2,908
Transactions count	17,731
Top 100 holders dominance	83.93%
Total fees	19814531687589148917112
Liquidity fee	3
Tax fee	1
Team fee	6
Uniswap V2 pair	0x3e3694a7f72554362ab1a17a4abf68434ca980da
Contract deployer address	0x86670ea08664556e1a1fdd18400807134894a3eb
Owner address	0x86670ea08664556e1a1fdd18400807134894a3eb

BOJI Token Distribution

The top 100 holders collectively own 83.93% (587,481,779,978,520.00 Tokens) of BOJI

Token Total Supply: 700,000,000,000,000.00 Token | Total Token Holders: 2,908



(A total of 587,481,779,978,520.00 tokens held by the top 100 accounts from the total supply of 700,000,000,000,000.00 token)

BOJI Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0x3a09963b5ea1bcf8624dfbce8eac8e589da428e4	140,577,912,177,997.570072343	20.0826%
2	Null Address: 0x000...dEaD	72,009,190,701,791.558250162	10.2870%
3	0xd0101051681604743c0ee71e963b4122e87f64e1	52,497,580,484,384.606852835	7.4997%
4	0x4687c20dab611dd2629b6623376060954a3bea91	21,283,318,838,690.226903243	3.0405%
5	PancakeSwap V2: BOJI 9	20,798,541,918,659.573577417	2.9712%
6	0x3bf77d4799b3fa798847ce08678e996385d218cd	14,516,749,674,623.913885791	2.0738%
7	0x4656322ea4347b91834229e4fd56463f7ab4619b	13,751,466,032,581.911235266	1.9645%
8	0xe06c4dc815a615e93777ee09e73e710817ad7be9	11,098,209,725,228.902383066	1.5855%
9	0x7a9cd1577f327ee1af1cb3eea9cd657705b62c34	10,390,936,609,205.027151263	1.4844%
10	0x407993575c91ce7643a4d4ccacc9a98c36ee1bbe	10,059,028,763,204.149704866	1.4370%

BOJI LP Token Holders

Rank	Address	Quantity	Percentage
1	0xecc4c93c4ac67f88bcea4734adc80e2e4d8784c7	1,722.184113535940234556	99.4518%
2	0x0ed943ce24baebf257488771759f9bf482c39706	9.493778395980693104	0.5482%
3	Null Address: 0x000...000	0.000000000000001	0.0000%

Contract functions details

+ [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

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

+ [Int] IUniswapV2Router02 (IUniswapV2Router01)
  - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [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] 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] IUniswapV2Factory
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs

- [Ext] allPairsLength
- [Ext] createPair #
- [Ext] setFeeTo #
- [Ext] setFeeToSetter #

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

+ 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

+ BOJI (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] isExcluded
- [Ext] setExcludeFromFee #

  - modifiers: onlyOwner
- [Ext] enableDisableBuySellLimit #
  - modifiers: onlyOwner
- [Ext] _setBuySellLimit #
  - modifiers: onlyOwner
- [Pub] totalFees
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Ext] excludeAccount #
  - modifiers: onlyOwner
- [Ext] includeAccount #
  - modifiers: onlyOwner
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] swapTokensForEth #
  - modifiers: lockTheSwap
- [Prv] sendETHToTeam #
- [Ext] manualSwap #
  - modifiers: onlyOwner
- [Ext] manualSend #
  - modifiers: onlyOwner
- [Ext] setSwapEnabled #
  - modifiers: onlyOwner
- [Ext] setCooldownEnabled #
  - modifiers: onlyOwner
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _transferBothExcluded #
- [Prv] _takeTeam #
- [Prv] _reflectFee #
- [Ext] <Fallback> ($)
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _getTaxFee
- [Prv] _getMaxTxAmount
- [Pub] getMaxTxAmount

- [Pub] getNumOfTokensToExchangeForTeam
- [Pub] _getETHBalance
- [Ext] _setTaxFee #
  - modifiers: onlyOwner
- [Ext] _setTeamFee #
  - modifiers: onlyOwner
- [Ext] setLiquidityFeePercent #
  - modifiers: onlyOwner
- [Ext] _setOpsTeamWallet #
  - modifiers: onlyOwner
- [Ext] setnumOfTokensToExchangeForTeam #
  - modifiers: onlyOwner
- [Ext] _setMaxTxAmount #
  - modifiers: onlyOwner
- [Prv] _takeLiquidity #

($) = 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.

Notes:

- Old owner is not removed from exemptions after transferring ownership.

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

- Owner can change the tax, liquidity and team fee(from 1 to 7).
- Owner can change the maximum transaction amount.
- Owner can change MIN_BUY_SELL_TXN_AMOUNT.
- Owner can exclude from the fee.
- Owner can enable/disable buy/sell limit.
- Owner can change _numOfTokensToExchangeForTeam.
- Owner can manually swap and send ETH to team.
- Owner can enable/disable swap and cooldown.
- Owner can change _opsTeamWalletAddress.

Testnet deployment

Contracts Description Table

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
Ownable	Implementation	Context		
└	renounceOwnership	Public ❗	🛑	onlyOwner
└	transferOwnership	Public ❗	🛑	onlyOwner
BOJI	Implementation	Context, IERC20, Ownable		
└	transfer	Public ❗	🛑	NO❗
└	approve	Public ❗	🛑	NO❗
└	transferFrom	Public ❗	🛑	NO❗
└	increaseAllowance	Public ❗	🛑	NO❗
└	decreaseAllowance	Public ❗	🛑	NO❗
└	setExcludeFromFee	External ❗	🛑	onlyOwner
└	enableDisableBuySellLimit	External ❗	🛑	onlyOwner
└	_setBuySellLimit	External ❗	🛑	onlyOwner
└	deliver	Public ❗	🛑	NO❗
└	excludeAccount	External ❗	🛑	onlyOwner
└	includeAccount	External ❗	🛑	onlyOwner
└	manualSwap	External ❗	🛑	onlyOwner
└	manualSend	External ❗	🛑	onlyOwner
└	setSwapEnabled	External ❗	🛑	onlyOwner
└	setCooldownEnabled	External ❗	🛑	onlyOwner
└	_setTaxFee	External ❗	🛑	onlyOwner
└	_setTeamFee	External ❗	🛑	onlyOwner
└	setLiquidityFeePercent	External ❗	🛑	onlyOwner
└	_setOpsTeamWallet	External ❗	🛑	onlyOwner
└	setnumOfTokensToExchangeForTeam	External ❗	🛑	onlyOwner
└	_setMaxTxAmount	External ❗	🛑	onlyOwner

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

Conclusion

Smart contracts do not contain high 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 are provided by the team:
https://dxsale.app/app/v3_3/dxlockview?id=0&add=0x3E3694a7f72554362AB1a17a4aBf68434CA980Da&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.