

TechRate
June, 2022



SMART CONTRACTS SECURITY AUDIT REPORT



Techrate_audits



Techrate



Techrate1

Audit Details



Audited project

PYRAVEUM



Deployer address

0x586a7f20182957c8080afc153295e418b3a166d4



Client contacts:

PYRAVEUM team



Blockchain

Binance Smart Chain



Project website:

<https://pyraveum.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 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 PYRAVEUM to perform an audit of smart contracts:

<https://bscscan.com/address/0xf15931dfc50ace0625a0c662ad0b3b95f4ba1863#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 16.06.2022

Contract name PYRAVEUM

Contract address 0xF15931dfC50Ace0625A0C662Ad0B3B95f4ba1863

Total supply 120,000,000

Token ticker PYR

Decimals 9

Token holders 472

Transactions count 10,551

Top 100 holders dominance 79.39%

Marketing wallet 0x586a7f20182957c8080afc153295e418b3a166d4

Team wallet 0x586a7f20182957c8080afc153295e418b3a166d4

Liquidity fee buy/sell 3/3

Uniswap V2 pair 0x5659798633298196ee8e9501ba3eb81b43a6769f

Contract deployer address 0x586a7f20182957c8080afc153295e418b3a166d4

Owner address 0x586a7f20182957c8080afc153295e418b3a166d4

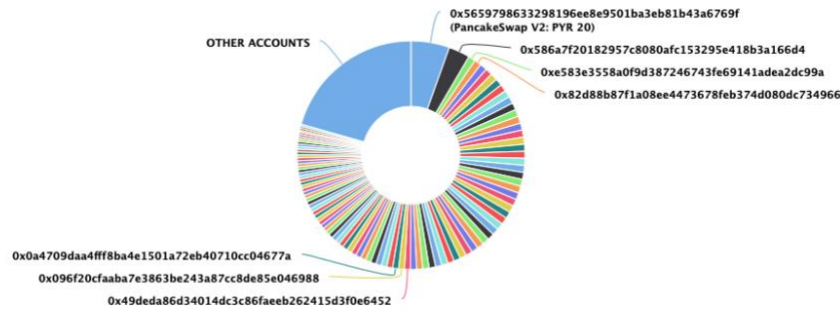
PYRAVEUM Token Distribution

The top 100 holders collectively own 79.39% (95,268,860.53 Tokens) of PYRAVEUM

Token Total Supply: 120,000,000.00 Token | Total Token Holders: 472

PYRAVEUM Top 100 Token Holders

Source: BscScan.com



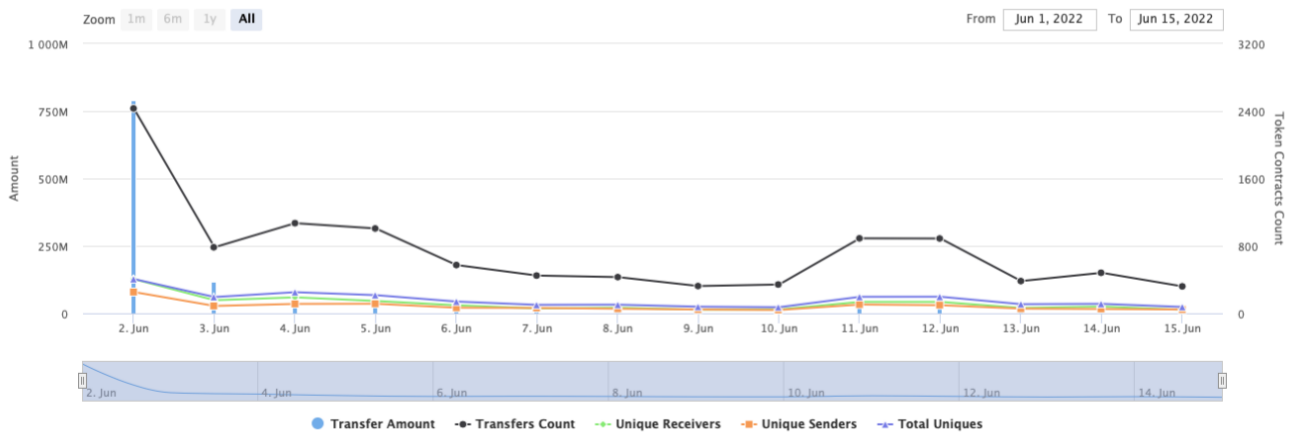
(A total of 95,268,860.53 tokens held by the top 100 accounts from the total supply of 120,000,000.00 token)

PYRAVEUM Contract Interaction Details


Time Series: Token Contract Overview

Thu 2, Jun 2022 - Wed 15, Jun 2022




Token Contract 0xf15931dfc50ace0625a0c662ad0b3b95f4ba1863 (PYRAVEUM)
Source: BscScan.com



PYRAVEUM Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	 PancakeSwap V2: PYR 20	6,541,148.857016377	5.4510%
2	0x586a7f20182957c8080afc153295e418b3a166d4	3,628,954.837191816	3.0241%
3	0xe583e3558a0f9d387246743fe69141adea2dc99a	1,200,000	1.0000%
4	0x82d88b87f1a08ee4473678feb374d080dc734966	1,199,999.668136526	1.0000%
5	0x631de63b6020574c8e4c6251f05c9d50a40af740	1,199,999.42747793	1.0000%
6	0x0e311693744e2407c68375e9beee1634757afd8	1,199,998.8	1.0000%
7	0x8274c34b2fdb90de7f40d7fd65f3502d8644964d	1,199,997	1.0000%
8	0xc5a36b191fe43204ebe534b6acc4e017a76abb49	1,199,990.860130029	1.0000%
9	0x38177f7856f71a5570c3d290041ec5665f17743e	1,199,981.694917431	1.0000%
10	0xc1a398504549543bc2d91725e41f1cdd6d49c477	1,199,978.858927126	1.0000%

PYRAVEUM Top LP token Holders

Rank	Address	Quantity	Percentage
1	 0x407993575c91ce7643a4d4ccacc9a98c36ee1bbe	0.363726688124733024	95.7889%
2	0x586a7f20182957c8080afc153295e418b3a166d4	0.006458923012930323	1.7010%
3	0x0cf9528fbdbf5d586993acf5d8509aefe7140006	0.005287897907028324	1.3926%
4	0x10348bce7dc6cabdfbda3654540c5af5d3a21c78	0.002724624551807469	0.7175%
5	 0x0ed943ce24baebf257488771759f9b482c39706	0.001518928917571048	0.4000%
6	 Null Address: 0x000...000	0.0000000000000001	0.0000%

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] waiveOwnership #
 - modifiers: onlyOwner
- [Pub] transferOwnership #
 - modifiers: onlyOwner
- [Pub] getTime

+ [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] 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 #
- + PYRAVEUM (Context, IERC20, Ownable)
- [Pub] <Constructor> #
 - [Pub] name
 - [Pub] symbol
 - [Pub] decimals
 - [Pub] totalSupply
 - [Pub] balanceOf
 - [Pub] allowance
 - [Pub] increaseAllowance #
 - [Pub] decreaseAllowance #
 - [Pub] minimumTokensBeforeSwapAmount
 - [Pub] approve #
 - [Prv] _approve #
 - [Pub] setMarketPairStatus #
 - modifiers: onlyOwner
 - [Ext] setIsTxLimitExempt #
 - modifiers: onlyOwner
 - [Pub] setIsExcludedFromFee #
 - modifiers: onlyOwner
 - [Ext] setBuyTaxes #
 - modifiers: onlyOwner
 - [Ext] setSellTaxes #
 - modifiers: onlyOwner
 - [Ext] setDistributionSettings #
 - modifiers: onlyOwner

- [Ext] setMaxTxAmount #
 - modifiers: onlyOwner
- [Ext] enableDisableWalletLimit #
 - modifiers: onlyOwner
- [Ext] setIsWalletLimitExempt #
 - modifiers: onlyOwner
- [Ext] setWalletLimit #
 - modifiers: onlyOwner
- [Ext] setNumTokensBeforeSwap #
 - modifiers: onlyOwner
- [Ext] setMarketingWalletAddress #
 - modifiers: onlyOwner
- [Ext] setTeamWalletAddress #
 - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
 - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyByLimitOnly #
 - modifiers: onlyOwner
- [Pub] getCirculatingSupply
- [Prv] transferToAddressETH #
- [Pub] changeRouterVersion #
 - modifiers: onlyOwner
- [Ext] <Fallback> (\$)
- [Pub] transfer #
- [Pub] transferFrom #
- [Prv] _transfer #
- [Int] _basicTransfer #
- [Prv] swapAndLiquify #
 - modifiers: lockTheSwap
- [Prv] swapTokensForEth #
- [Prv] addLiquidity #
- [Int] takeFee #

(\$) = 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.	Low issues
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. waiveOwnership issue

Issue:

- The function `waiveOwnership()` transfers ownership to `0x7B228194608803b1246eBC9289f049873a64bC2E` address but emits transferring to `0x00000000000000000000000000000000dEaD` address.

Recommendation:

Correct event emitting.

Notes:

- `changeRouterVersion()` function do not include back to limits old addresses.
- `setSellTaxes()` function has spelling mistake.

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

- Owner can change the marketing, team and liquidity fees.
- Owner can change the maximum transaction amount.
- Owner can exclude from the fee and maxTX.
- Owner can change marketing and team wallets.
- Owner can change minimum number of tokens before swap.
- Owner can change router address.
- Owner can change swap and liquify settings.
- Owner can include in isMarketPair array.
- Owner can enable/disable wallet limit, exclude from it and change this limit value.

Contract	Type	Bases		
L	Function Name	Visibility	Mutability	Modifiers
PYRAVEUM	Implementation	Context, IERC20, Ownable		
L	approve	Public !		NO!
L	setMarketPairStatus	Public !		onlyOwner
L	setIsTxLimitExempt	External !		onlyOwner
L	setIsExcludedFromFee	Public !		onlyOwner
L	setBuyTaxes	External !		onlyOwner
L	setSellTaxes	External !		onlyOwner
L	setDistributionSettings	External !		onlyOwner
L	setMaxTxAmount	External !		onlyOwner
L	enableDisableWalletLimit	External !		onlyOwner
L	setIsWalletLimitExempt	External !		onlyOwner
L	setWalletLimit	External !		onlyOwner
L	setNumTokensBeforeSwap	External !		onlyOwner
L	setMarketingWalletAddress	External !		onlyOwner
L	setTeamWalletAddress	External !		onlyOwner
L	setSwapAndLiquifyEnabled	Public !		onlyOwner
L	setSwapAndLiquifyByLimitOnly	Public !		onlyOwner
L	changeRouterVersion	Public !		onlyOwner
L	transfer	Public !		NO!
L	transferFrom	Public !		NO!

Legend

Symbol Meaning



Function can modify state



Function is payable

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 are NOT provided by the team.

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.