



TechRate
AUDIT COMPANY

Smart Contract Security Audit

Audit Details



Audited project
Parma Token



Deployer address
0x8cda2065f49be9a1ded69b7c7d60db8759d22322



Client contacts:
Parma Token team



Blockchain
Ethereum



Project website:
<https://parmatoken.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 Parma Token to perform an audit of smart contracts:

<https://etherscan.io/address/0x1a2933fba0c6e959c9a2d2c933f3f8ad4aa9f06e#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 13.02.2022

Contract name	Parma Token
Contract address	0x1A2933fbA0c6e959c9A2D2c933f3f8AD4aa9f06e
Total supply	97,942,588,182.106689112965593394
Token ticker	PARMA
Decimals	18
Token holders	1,078
Transactions count	13,416
Top 100 holders dominance	86.79%
Transfer delay enabled	True
Trading active	True
Total fees	7
Limits in effect	False
Contract deployer address	0x8cda2065f49be9a1ded69b7c7d60db8759d22322
Contract's current owner address	0x8cda2065f49be9a1ded69b7c7d60db8759d22322

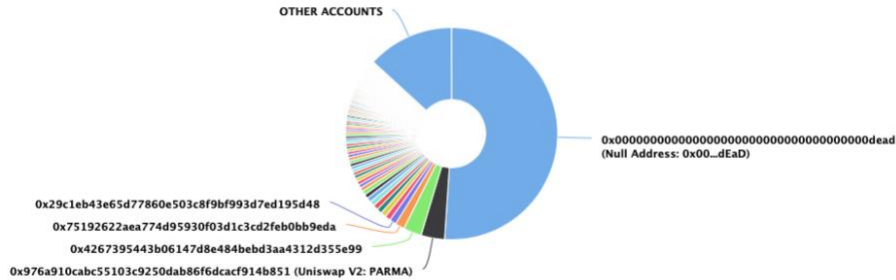
Parma Token Token Distribution

The top 100 holders collectively own 86.79% (85,007,757,719.67 Tokens) of Parma Token

Token Total Supply: 97,942,338,182.11 Token | Total Token Holders: 1,079

Parma Token Top 100 Token Holders

Source: Etherscan.io



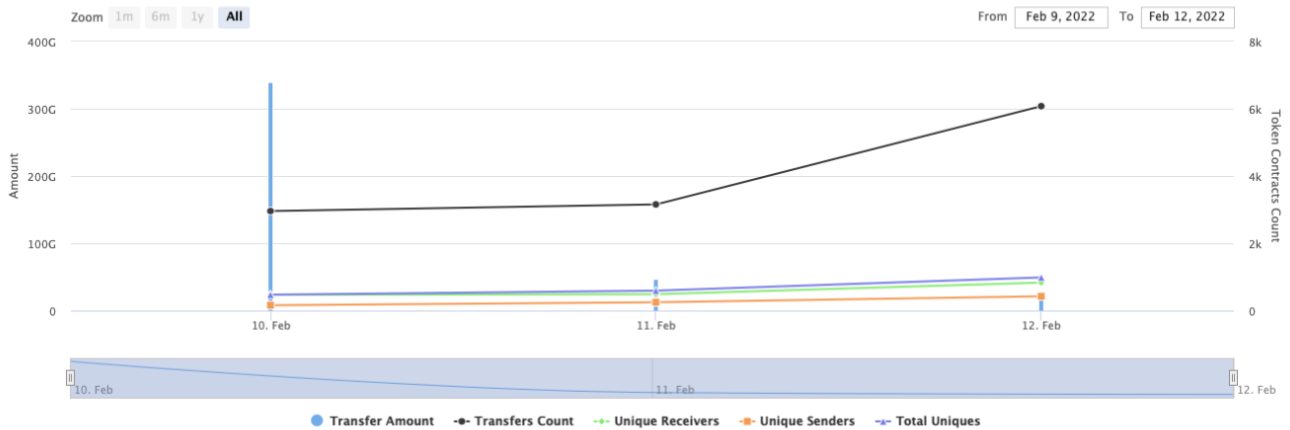
(A total of 85,007,757,719.67 tokens held by the top 100 accounts from the total supply of 97,942,338,182.11 token)

Parma Token Contract Interaction Details


Time Series: Token Contract Overview

Thu 10, Feb 2022 - Sat 12, Feb 2022

Token Contract 0x1a2933fba0c6e959c9a2d2c933f3f8ad4aa9f06e (Parma Token)
Source: Etherscan.io



Parma Token Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x00...dEaD	50,000,000,000	51.0504%
2	 Uniswap V2: PARMA	3,524,732,475.65449713956926679	3.5988%
3	0x4267395443b06147d8e484bebd3aa4312d355e99	2,706,334,873.705675000559397637	2.7632%
4	0x75192622aea774d95930f03d1c3cd2feb0bb9eda	1,405,360,307.596522670652849379	1.4349%
5	0x29c1eb43e65d77860e503c8f9bf993d7ed195d48	1,001,355,854.914395020299358642	1.0224%
6	0x3c4fa6a4c62951524762b102c1e8c788e3d16ecb	847,257,537.491003664950915904	0.8651%
7	0xc46caad3fa41ff62b3d6f72aa47d86a71e4401bd	814,803,607.37603089577132322	0.8319%
8	0x0a0871c2ea6f24149758dc5bd1136d337b7f47b8	773,702,944.731187604243301367	0.7900%
9	0xf5825c034259ae5ef2c2982220cf6abfeec8f62b	760,872,482.806262223232203573	0.7769%
10	0x5d632e54a14646063ff30d8ed555820184a020bc	734,622,946.341267950175041572	0.7501%



Contract functions details

+ Context

- [Int] _msgSender
- [Int] _msgData

+ ERC20 (Context, IERC20, IERC20Metadata)

- [Pub] <Constructor> #
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Int] _transfer #
- [Int] _mint #
- [Int] _burn #
- [Int] _approve #
- [Int] _spendAllowance #
- [Int] _beforeTokenTransfer #
- [Int] _afterTokenTransfer #

+ [Int] IERC20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ [Int] IERC20Metadata (IERC20)

- [Ext] name
- [Ext] symbol
- [Ext] decimals

+ [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 #

+ Ownable (Context)

- [Pub] <Constructor> #
 - [Pub] owner
 - [Pub] renounceOwnership #
 - modifiers: onlyOwner
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
 - [Int] _transferOwnership #
- + [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
- + PARMA (ERC20, Ownable)
- [Pub] <Constructor> #
 - modifiers: ERC20
 - [Ext] enableTrading #
 - modifiers: onlyOwner
 - [Ext] removeLimits #
 - modifiers: onlyOwner
 - [Ext] disableTransferDelay #
 - modifiers: onlyOwner
 - [Ext] updateSwapTokensAtAmount #
 - modifiers: onlyOwner
 - [Ext] updateMaxTxnAmount #
 - modifiers: onlyOwner
 - [Ext] updateMaxWalletAmount #
 - modifiers: onlyOwner
 - [Pub] excludeFromMaxTransaction #
 - modifiers: onlyOwner
 - [Ext] updateFees #
 - modifiers: onlyOwner
 - [Pub] excludeFromFees #
 - modifiers: onlyOwner
 - [Pub] setAutomatedMarketMakerPair #
 - modifiers: onlyOwner
 - [Prv] _setAutomatedMarketMakerPair #
 - [Ext] updateFeeWallet #
 - modifiers: onlyOwner
 - [Pub] isExcludedFromFees
 - [Pub] setBlacklisted #
 - modifiers: onlyOwner
 - [Pub] delBlacklisted #
 - modifiers: onlyOwner
 - [Pub] isSniper

- [Int] _transfer #
- [Prv] _swapTokensForEth #
- [Prv] _addLiquidity #
- [Prv] swapBack #
- [Ext] forceSwap #
 - modifiers: onlyOwner
- [Ext] forceSend #
 - modifiers: onlyOwner
- [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 `setBlacklisted()` and `delBlacklisted()` uses the loop add/remove blacklist addresses from list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long addresses list.

Recommendation:

Check that the array's length is not too big.

Notes:

- Dev and marketing balances goes to fee wallet.

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

- Owner can enable trading.
- Owner can remove limits.
- Owner can disable transfer delay.
- Owner can change `swapTokensAtAmount` value.
- Owner can change maximum transaction amount and max wallet.
- Owner can exclude from maximum transaction amount.
- Owner can change fees.
- Owner can include in and exclude from fees.
- Owner can include in and exclude from addresses in `automatedMarketMakerPairs` array.
- Owner can change `feeWallet` address.
- Owner can withdraw ETHs to fee wallet.
- Owner can manually swap contract tokens to ETHs and send them to fee wallet.

Conclusion

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

Liquidity locking details provided by the team:

<https://app.unicrypt.network/amm/uni-v2/pair/0x976a910cab55103c9250dab86f6dcacf914b851>

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](#)