



# Smart Contract Security Audit

## Audit details:

Audited project:	PurpleMonster
Deployer address	0x9ff3f268c5e0756eae1e2843522d2ff5793bcb2f
Blockchain:	Binance Smart Chain
Project website:	Not provided

# 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 PurpleMonster to perform an audit of smart contracts:

- <https://bscscan.com/address/0xd66c5C66Cef05a0fd2F20d087D4DAd3fB48E10Be#code>
- <https://bscscan.com/address/0xC46889ec6d0DeAffbfF6545621F82a3e6e0D73A5#code>
- <https://www.bscscan.com/address/0xf6583D313A3A74A9dcbf4989bC73b9771dA29A0c#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.

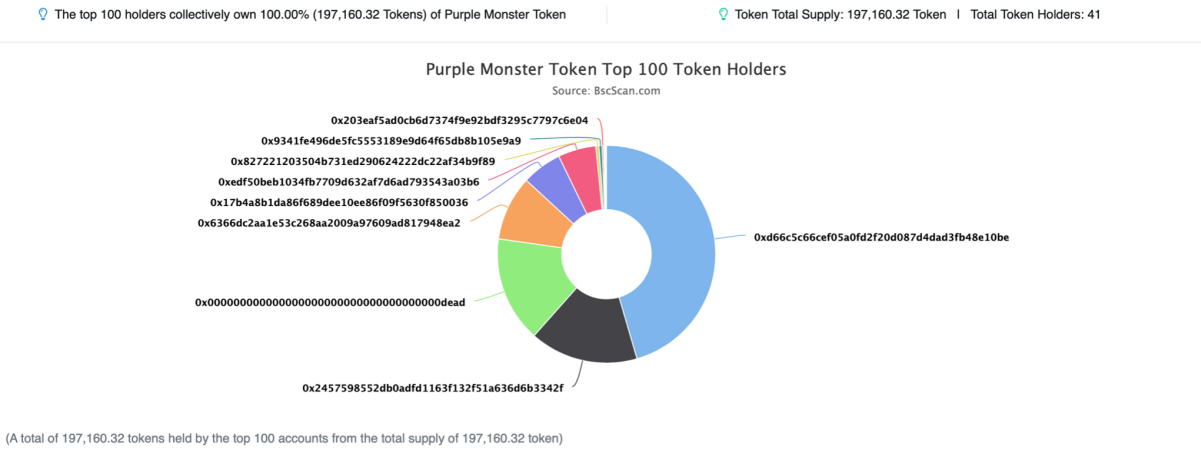
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

# Contracts details






Token contract details for 18.05.2021.

Contract name:	PurpleMonsterToken
Compiler version:	v0.8.0+commit.c7dfd78e
Contract address:	0xC46889ec6d0DeAffbfF6545621F82a3e6e0D73A5
Total supply:	197160318444108185482608
Token ticker:	PMOT
Decimals:	18
Token holders:	41
Transactions count:	3721
Contract deployer address:	0x9ff3f268c5e0756eae1e2843522d2ff5793bcb2f
Contract's current owner address:	0xd66c5c66cef05a0fd2f20d087d4dad3fb48e10be

# PurpleMonster tokens distribution



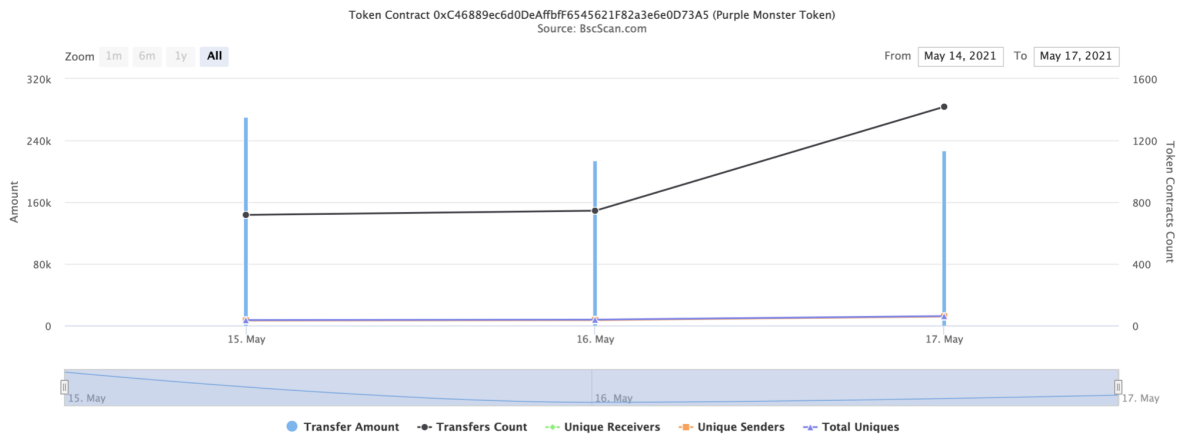
# PurpleMonster top 10 token holders

Rank	Address	Quantity (Token)	Percentage
1	 <a href="#">0xd66c5c66cef05a0fd2f20d087d4dad3fb48e10be</a>	89,694.985343341079114632	45.4934%
2	 <a href="#">0x2457598552db0adfd1163f132f51a636d6b3342f</a>	31,669.791932292514469986	16.0630%
3	<a href="#">0x00000000000000000000000000000000dead</a>	31,000.0656	15.7233%
4	 <a href="#">0x6366dc2aa1e53c268aa2009a97609ad817948ea2</a>	18,942.55705666619914674	9.6077%
5	 <a href="#">0x17b4a8b1da86f689dee10ee86f09f5630f850036</a>	11,648.613121703439375791	5.9082%
6	 <a href="#">0xedf50beb1034fb7709d632af7d6ad793543a03b6</a>	11,131.27711497768621956	5.6458%
7	<a href="#">0x827221203504b731ed29062422dc22af34b9f89</a>	903.225267160472112404	0.4581%
8	<a href="#">0x9341fe496de5fc5553189e9d64f65db8b105e9a9</a>	864.729422420090436236	0.4386%
9	<a href="#">0x203eaf5ad0cb6d7374f9e92bdf3295c7797c6e04</a>	462.332405700114652309	0.2345%
10	<a href="#">0x46bb5a41aa0d97ea45d33fba84d22bd4d44b3ca</a>	250	0.1268%

# PurpleMonster transactions

Time Series: Token Contract Overview

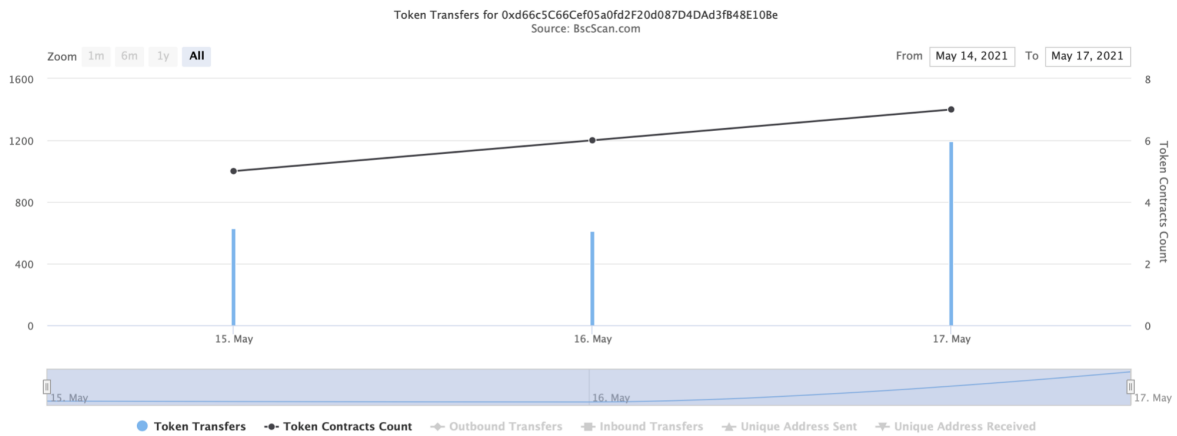
Sat 15, May 2021 - Mon 17, May 2021



# PurpleMonsterMasterChef transactions

Time Series: Address Token (BEP-20) Transfers

Sat 15, May 2021 - Mon 17, May 2021



Pro-Tip: Click on the chart data points to view more

## MasterChef contract details for 18.05.2021.

Contract name:	PurpleMonsterMasterChef
Compiler version:	v0.8.0+commit.c7dfd78e
Contract address:	0xd66c5C66Cef05a0fd2F20d087D4DAd3fB48E10Be
Deployer address:	0x9ff3f268c5e0756eae1e2843522d2ff5793bcb2f
Fee address:	0x64e054b9a1dee07a0949a31db9d7ca0c8bfd100d
Token NFT address:	0xf6583d313a3a74a9dcbf4989bc73b9771da29a0c
Token contract address:	0xc46889ec6d0deaffbfff6545621f82a3e6e0d73a5
Token per block:	1000000000000000000
Contract owner address:	0x9ff3f268c5e0756eae1e2843522d2ff5793bcb2f
Pool length:	7
Start block:	0
Total alloc point:	3900
Bonus multiplier:	1

# MasterChef functions outline

## + [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

## + [Int] IERC165

- [Ext] supportsInterface

## + ERC165 (IERC165)

- [Pub] supportsInterface

## + [Lib] Strings

- [Int] toString
- [Int] toHexString
- [Int] toHexString

## + 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 #
- [Priv] \_verifyCallResult

## + [Lib] SafeERC20



- [Int] safeTransfer #
  - [Int] safeTransferFrom #
  - [Int] safeApprove #
  - [Int] safeIncreaseAllowance #
  - [Int] safeDecreaseAllowance #
  - [Prv] \_callOptionalReturn #
- + [Int] IERC20
    - [Ext] totalSupply
    - [Ext] balanceOf
    - [Ext] transfer #
    - [Ext] allowance
    - [Ext] approve #
    - [Ext] transferFrom #
- + [Int] IERC721Metadata (IERC721)
    - [Ext] name
    - [Ext] symbol
    - [Ext] tokenURI
- + [Int] IERC721Enumerable (IERC721)
    - [Ext] totalSupply
    - [Ext] tokenOfOwnerByIndex
    - [Ext] tokenByIndex
- + ERC721URIStorage (ERC721)
    - [Pub] tokenURI
    - [Int] \_setTokenURI #
    - [Int] \_burn #
- + [Int] IERC721Receiver
    - [Ext] onERC721Received #
- + [Int] IERC721 (IERC165)
    - [Ext] balanceOf
    - [Ext] ownerOf
    - [Ext] safeTransferFrom #
    - [Ext] transferFrom #
    - [Ext] approve #
    - [Ext] getApproved
    - [Ext] setApprovalForAll #
    - [Ext] isApprovedForAll
    - [Ext] safeTransferFrom #
- + ERC721 (Context, ERC165, IERC721, IERC721Metadata)
    - [Pub] <Constructor> #
    - [Pub] supportsInterface

- [Pub] balanceOf
- [Pub] ownerOf
- [Pub] name
- [Pub] symbol
- [Pub] tokenURI
- [Int] \_baseURI
- [Pub] approve #
- [Pub] getApproved
- [Pub] setApprovalForAll #
- [Pub] isApprovedForAll
- [Pub] transferFrom #
- [Pub] safeTransferFrom #
- [Pub] safeTransferFrom #
- [Int] \_safeTransfer #
- [Int] \_exists
- [Int] \_isApprovedOrOwner
- [Int] \_safeMint #
- [Int] \_safeMint #
- [Int] \_mint #
- [Int] \_burn #
- [Int] \_transfer #
- [Int] \_approve #
- [Prv] \_checkOnERC721Received #
- [Int] \_beforeTokenTransfer #

#### + ReentrancyGuard

- [Pub] <Constructor> #

#### + Ownable (Context)

- [Pub] <Constructor> #
- [Pub] owner
- [Pub] renounceOwnership #
  - modifiers: onlyOwner
- [Pub] transferOwnership #
  - modifiers: onlyOwner

#### + PurpleMonsterToken (BEP20)

- [Pub] mint #
  - modifiers: onlyOwner

#### + [Int] IBEP20

- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Ext] balanceOf

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

+ BEP20 (Context, IBEP20, Ownable)

- [Pub] <Constructor> #
- [Ext] getOwner
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] mint #
  - modifiers: onlyOwner
- [Int] \_transfer #
- [Int] \_mint #
- [Int] \_burn #
- [Int] \_approve #
- [Int] \_burnFrom #

+ PurpleMonNFT (ERC721URIStorage, IERC721Enumerable, Ownable)

- [Pub] <Constructor> #
  - modifiers: ERC721
- [Pub] PaymentAddress
- [Pub] setPrice #
  - modifiers: onlyOwner
- [Pub] buySingles (\$)
- [Int] \_baseURI
- [Pub] setPaymentAddress #
  - modifiers: onlyOwner
- [Pub] getPrice
- [Pub] getRarityRemainingSupply
- [Pub] getTokenIssuedCount
- [Pub] getRarityTotalSupply
- [Pub] getUserNftTokens
- [Pub] getUserNftTokensForRarity
- [Pub] getRarityOfTokenId
- [Pub] supportsInterface
- [Pub] tokenOfOwnerByIndex
- [Pub] totalSupply

- [Pub] tokenByIndex
  - [Int] \_beforeTokenTransfer #
  - [Prv] \_addTokenToOwnerEnumeration #
  - [Prv] \_addTokenToAllTokensEnumeration #
  - [Prv] \_removeTokenFromOwnerEnumeration #
  - [Prv] \_removeTokenFromAllTokensEnumeration #
- + PurpleMonsterMasterChef (Ownable, IERC721Receiver, ReentrancyGuard)
- [Pub] <Constructor> #
  - [Ext] poolLength
  - [Pub] add #
    - modifiers: onlyOwner,nonDuplicated
  - [Pub] set #
    - modifiers: onlyOwner
  - [Pub] getMultiplier
  - [Ext] pendingPurpleMonster
  - [Ext] pendingPurpleMonsterNFT
  - [Pub] massUpdateNftPools #
  - [Pub] massUpdatePools #
  - [Pub] updateNftPool #
  - [Pub] updatePool #
  - [Prv] confirmAllTokensRarity
  - [Pub] depositNft #
    - modifiers: nonReentrant
  - [Pub] deposit #
    - modifiers: nonReentrant
  - [Pub] withdrawNft #
    - modifiers: nonReentrant
  - [Pub] withdraw #
    - modifiers: nonReentrant
  - [Pub] GetTokenIdsStakedByUser
  - [Pub] emergencyWithdrawNfts #
    - modifiers: nonReentrant
  - [Pub] emergencyWithdraw #
    - modifiers: nonReentrant
  - [Int] safePurpleMonsterTransfer #
  - [Ext] setFeeAddress #
  - [Ext] updateEmissionRate #
    - modifiers: onlyOwner
  - [Ext] updateEmissionRateNft #
    - modifiers: onlyOwner
  - [Ext] onERC721Received

(\$) = 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. Block gas limit

Issue:

The `updateEmissionRate` function can fail due to the block gas limit if the pool size is too big.

## Owner privileges

- ☐ Owner can change the price in the PurpleMonNFT contract.
- ☐ Owner can change the payment address in the PurpleMonNFT contract.
- ☐ Owner can change the pool details in the MasterChef contract.

## Conclusion

Smart contracts contain low severity issues and owner privileges! Audited only the contracts listed above.

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.*