



TechRate
AUDIT COMPANY

Smart Contract Security Audit

Audit Details



Audited project

Dr. Skull



Deployer address

0x4Dac5c14BE3Ad5dc358868f78A92298880535e30



Client contacts:

Dr. Skull team



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 Dr. Skull to perform an audit of smart contracts:

<https://bscscan.com/address/0x17922598458a7f29e3ce2bf088dff2b1b474771a#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 14.08.2021

Contract name	Dr. Skull
Contract address	0x17922598458A7F29E3ce2bF088DfF2B1b474771a
Total supply	100,000,000,000,000
Token ticker	DRSL
Decimals	8
Token holders	1,055
Transactions count	1,697
Top 100 holders dominance	100.00%
Contract deployer address	0x4Dac5c14BE3Ad5dc358868f78A92298880535e30
Contract's current owner address	0x7887eab3e978e30065d12d4f268c82a645e05497

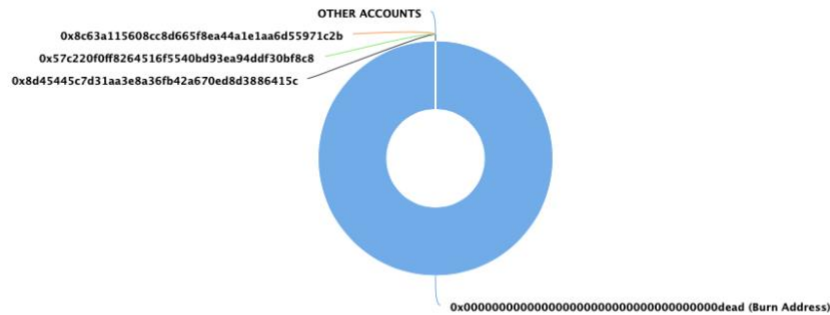
Dr. Skull Token Distribution

💡 The top 100 holders collectively own 100.00% (99,999,594,696,206.60 Tokens) of Dr. Skull

💡 Token Total Supply: 100,000,000,000,000.00 Token | Total Token Holders: 1,055

Dr. Skull Top 100 Token Holders

Source: BscScan.com



(A total of 99,999,594,696,206.60 tokens held by the top 100 accounts from the total supply of 100,000,000,000,000.00 token)

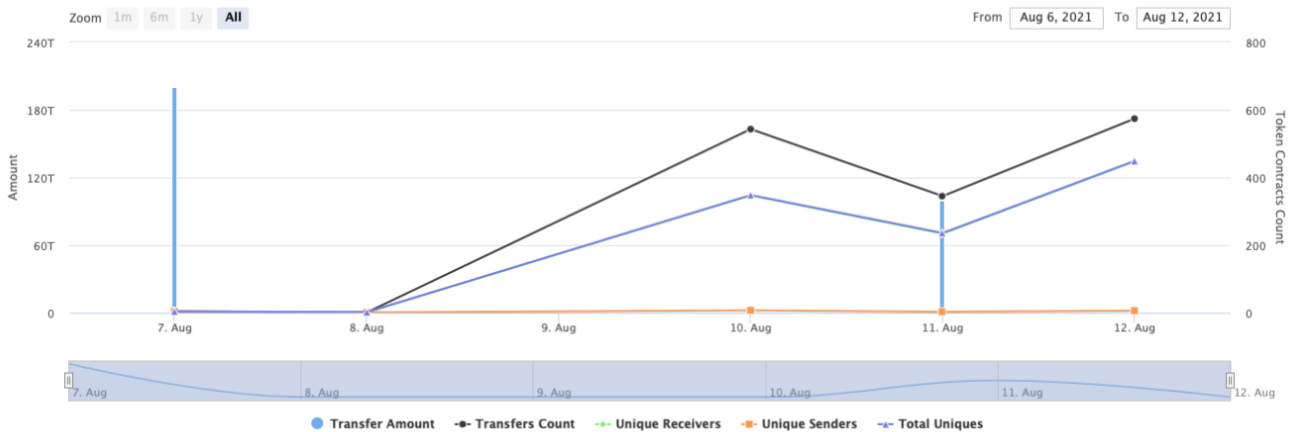
Dr. Skull Contract Interaction Details

Time Series: Token Contract Overview

Sat 7, Aug 2021 - Thu 12, Aug 2021

Token Contract 0x17922598458a7f29e3ce2bf088dff2b1b474771a (Dr. Skull)

Source: BscScan.com



Dr. Skull Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Burn Address	99,990,000,000,000	99.9900%
2	0x8d45445c7d31aa3e8a36fb42a670ed8d3886415c	8,871,170,186.23647873	0.0089%
3	0x57c220f0ff8264516f5540bd93ea94ddf30bf8c8	80,445,511.94117645	0.0001%
4	0x8c63a115608cc8d665f8ea44a1e1aa6d55971c2b	38,235,294.11764705	0.0000%
5	0x7fa0f407bdfbdea3aaa559ac2b16b930dc2517e1	30,000,000	0.0000%
6	0xacba07450146b9261192b17d2b7d04e54e665524	28,873,529.4117647	0.0000%
7	0x7968c4f7626129778d7795da2f3e93a67f2fb3c3	20,000,000	0.0000%
8	0x14fce8d8edc488266f9b6892481806b38e0e8cf6	19,823,529.41176458	0.0000%
9	0xbf792d37b282c0250c5a7972a34a6ea4e5a5e35d	15,882,352.35294117	0.0000%
10	0xad2a4418c0d94af81871f2c99484245873b426a9	14,077,393.29941175	0.0000%



Contract functions details

- + Context
 - [Int] <Constructor> #
 - [Int] _msgSender
 - [Int] _msgData
- + Ownable (Context)
 - [Int] <Constructor> #
 - [Pub] owner
 - [Pub] renounceOwnership #
 - modifiers: onlyOwner
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
 - [Int] _transferOwnership #
- + [Int] IBEP20
 - [Ext] totalSupply
 - [Ext] decimals
 - [Ext] symbol
 - [Ext] name
 - [Ext] getOwner
 - [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
 - [Int] min
 - [Int] sqrt
- + [Lib] Address
 - [Int] isContract
 - [Int] sendValue #
 - [Int] functionCall #
 - [Int] functionCall #
 - [Int] functionCallWithValue #
 - [Int] functionCallWithValue #
 - [Prv] _functionCallWithValue #
- + BEP20 (Context, IBEP20, Ownable)
 - [Pub] <Constructor> #
 - [Ext] getOwner
 - [Pub] name
 - [Pub] decimals
 - [Pub] symbol
 - [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 #
- + DRSL (BEP20)
 - [Pub] mint #
 - modifiers: onlyOwner
 - [Ext] delegates
 - [Ext] delegate #
 - [Ext] delegateBySig #
 - [Ext] getCurrentVotes
 - [Ext] getPriorVotes
 - [Int] _delegate #
 - [Int] _moveDelegates #
 - [Int] _writeCheckpoint #
 - [Int] safe32
 - [Int] getChainId

(\$) = 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.

Owner privileges

- Owner can mint any amount of tokens without any restrictions, before transferring ownership to the MasterChef.

Conclusion

Smart contracts contain owner privileges. Audited only the token of the project.

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](#)