

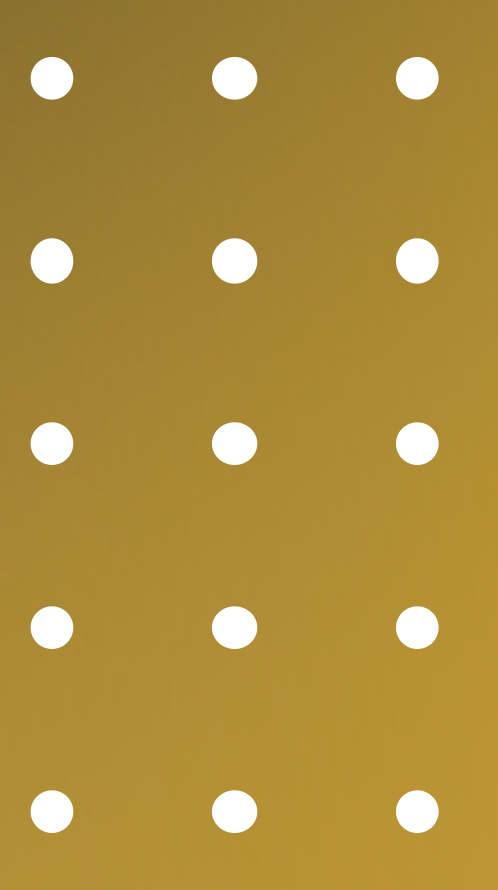


Smart Contract Security Audit Report

DOT

March 2023

Security Status

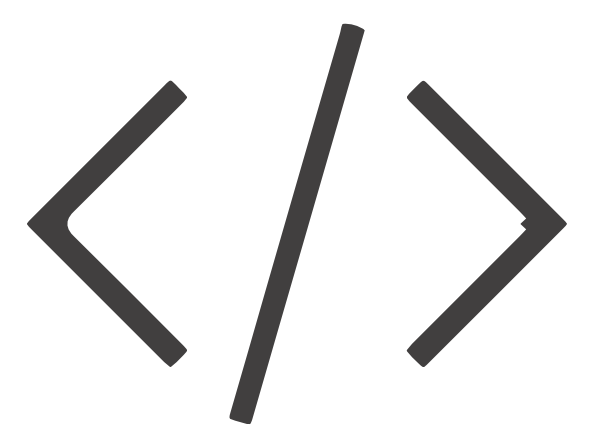


Audit Details



Audited project

DOT



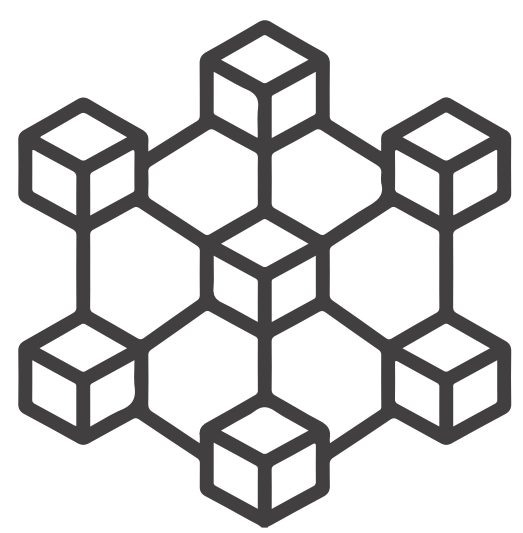
Deployer address

0x53b1ab959526811d7a304afc6bb0294e53acd53d



Client contacts

DOT Team



Blockchain

Binance smart chain



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) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe 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 HackSafe 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, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, 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.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 - Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by DOT to perform an audit of smart contracts:

- <https://bscscan.com/token/0x67fb98b7eBa501dFAa9c7b6481F48bB6b3cbbB41#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 understood 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.

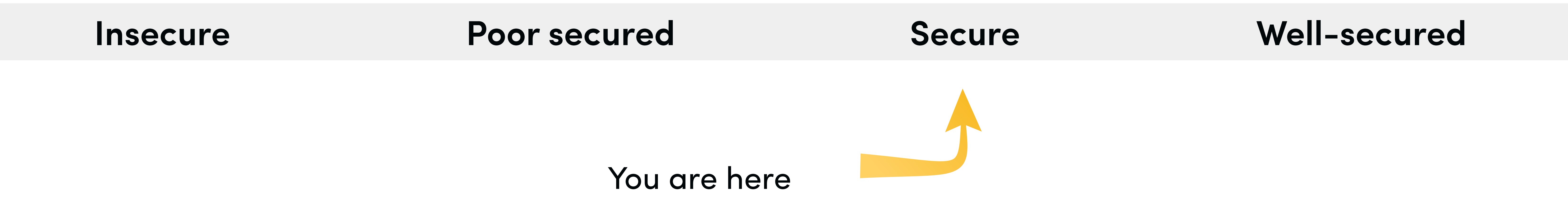
Contract Details

Token contract details for 22.03.2023

Token Type	: Exchange
Contract name	: Dot
Contract address	: 0x67fb98b7eBa501dFAa9c7b6481F48bB6b3cbbB41
Total supply	: 500,000,000
Token ticker	: DOT
Decimals	: 18
Token holders	: 2,294
Transactions count	: 3,170
Compiler version	: v0.8.6+commit.11564f7e
Contract deployer address	: 0x53b1ab959526811d7a304afc6bb0294e53acd53d
owner address	: 0x53b1ab959526811d7a304afc6bb0294e53acd53d

Audit Summary


According to the standard audit assessment, Customer`s solidity smart contracts are “**Secure**”. This token contract does contain owner control, which do not make it fully decentralized.



We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 0 medium and 0 low.

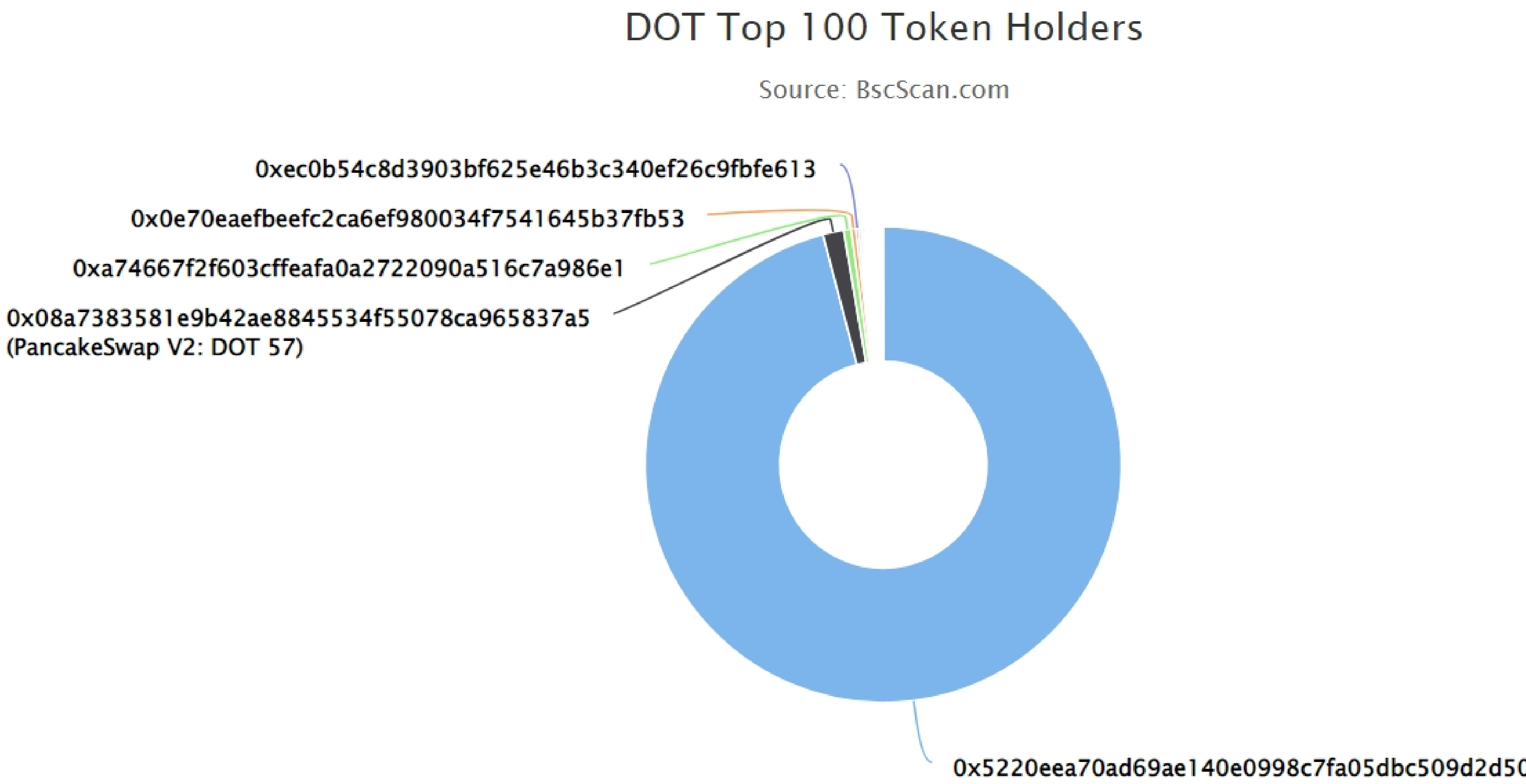
DOT TOKEN Distribution

 The top 100 holders collectively own 99.91% (499,564,661.29 Tokens) of DOT

 Token Total Supply: 500,000,000.00 Token

|

Total Token Holders: 2,294



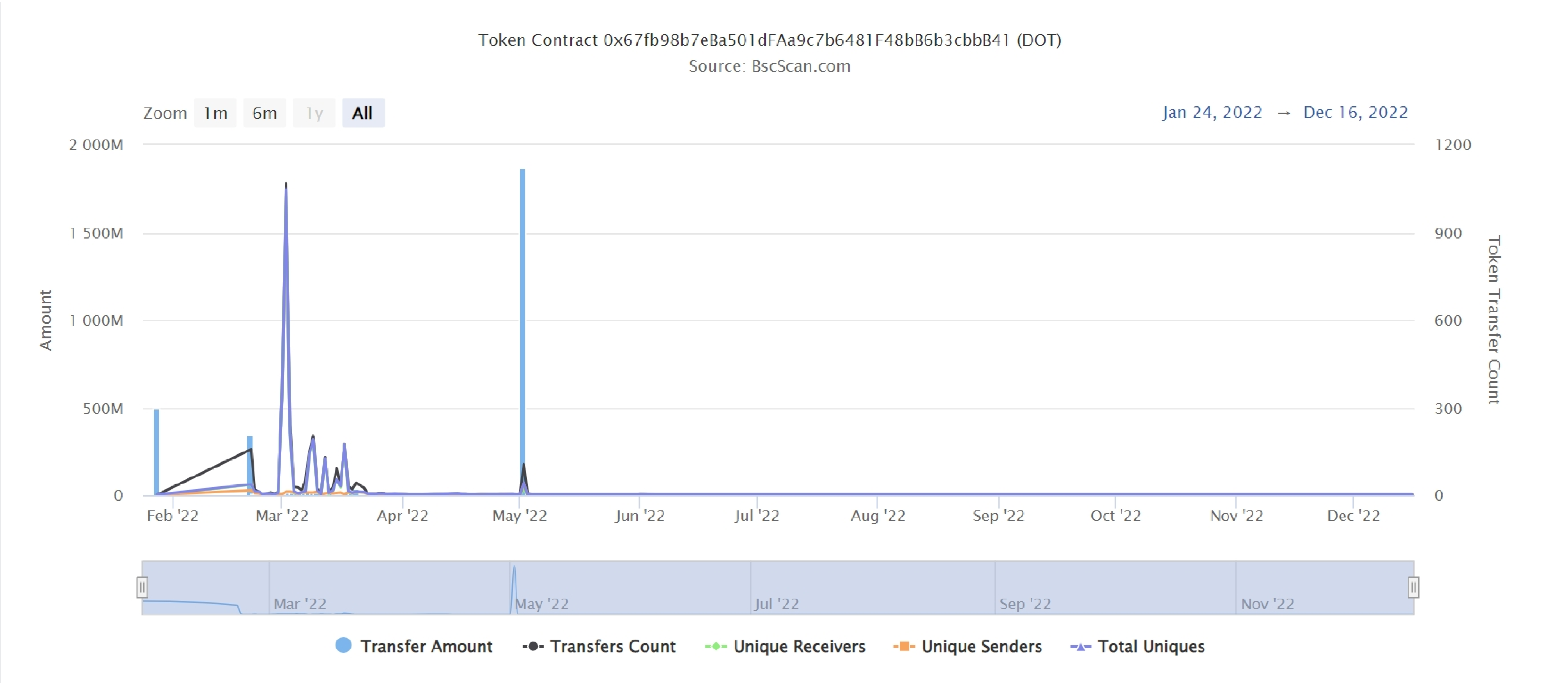
DOT Token Top 20 Token Holders

(A total of 499,564,661.29 tokens held by the top 100 accounts from the total supply of 500,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x5220eea70ad69ae140e0998c7fa05dbc509d2d50	479,573,889.21080492057185158	95.9148%
2	PancakeSwap V2: DOT 57	7,142,244.378348587859505231	1.4284%
3	0xa74667f2f603cfeafa0a2722090a516c7a986e1	2,500,000	0.5000%
4	0x0e70eaeefbeefc2ca6ef980034f7541645b37fb53	1,607,000	0.3214%
5	0xec0b54c8d3903bf625e46b3c340ef26c9fbfe613	944,643.757152293424807482	0.1889%
6	0x235f780bc740abad3ed5f83b904d0a912f768945	895,148.198006537541864872	0.1790%
7	0x3ebc1ff125dff6f4d0e80b1facae57e22de56e99	796,675.886001381388293515	0.1593%
8	0x4b71b1a3a76713824cbba579266884eb4f17f7a8	742,853.415959233506146111	0.1486%
9	0x2c042bf96071c716c2a0c1988afef9f8e97c600c	698,438.770148629832596446	0.1397%
10	0x00ce3a5747295addbe470f082fa9243fb8abd6ad	693,413.609399654188167792	0.1387%
11	0xe0676176cae44ca89159cc73542a61820699c85f	609,254.127006543607502438	0.1219%
12	0x08b73c1b005e1fc50a45fe6304256435996f2f58	582,596.104159831099509011	0.1165%
13	0x7cb166319b3fddf57eefde7cc872ddb7fafb7c36	580,392.994119886986849494	0.1161%
14	0xe1e73c2a0923bc5cf63220093ba9aa3881d5672b	576,885.881264606475678964	0.1154%
15	0x3ba1609b1319a1e0aa33ddbfa9c78d05e0cb26b1	554,751.530246410159646102	0.1110%
16	0xa779e1e231377d12e4a91548636ad2de48980a36	500,000	0.1000%
17	0xbb613e1f13eb6e95fd2da7b4074771c81c6a5f56	250,002.061086857935305479	0.0500%
18	0x5e3773713f0a20806168d633652b905ee7253f83	63,734.558224614579446123	0.0127%
19	0x6f499f0388e41431b9bd2a861587c29c4059ec28	45,029.38832059595387331	0.0090%
20	0xda7f5e97a1bc6062b06250b998ec38ad7d7f8940	31,923.413653492009989233	0.0064%

DOT TOKEN Distribution

DOT Contract Overview



Contract functions details

+Owned

- [Pub] changeOwnership #
 - modifiers: onlyOwner

+BEP20

- [Pub] balanceOf
- [Pub] transfer #
- [Pub] transferFrom #
- [Pub] approve #
- [Pub] allowance
- [Int] _mint #
- [Int] _burn #
- [Int] _beforeTokenTransfer #

+Dot (Owned, BEP20)

- [Pub] #
- [Ext] mint #
 - modifiers: onlyOwner
- [Ext] burn #
 - modifiers: onlyOwner

(\$) = payable function

= non-constant function

Issues Checking Status

No.	Title	Status
1.	Compiler error	Passed
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	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.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Too old version	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

✔ Critical Severity Issues

No critical severity issue found.

✔ High Severity Issues

No high severity issue found.

✔ Medium Severity Issues

No medium severity issue found.

✔ Low Severity Issues

No low severity issue found.

Centralization

Owner Privileges :

- DOT Contract:
 - Owner can mint any amount of tokens.
 - Owner can burn self tokens.

This smart contract has some functions which can be executed by the admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble as smart contract ownership has not been renounced.

Conclusion

Smart contract contains no medium severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe 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.