

Smart Contract Security Audit Report

TERK

February 2023

Security Status



www.hacksafe.io



Audit Details



Audited project

TERK



Deployer address

0x1a00a6f01390d4b67fa39915a36b4087724b87fa



Client contacts

TERK 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 TERK to perform an audit of smart contracts:

- <https://bscscan.com/token/0x53035E4e14fb3f82C02357B35d5cC0C5b53928B4#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.

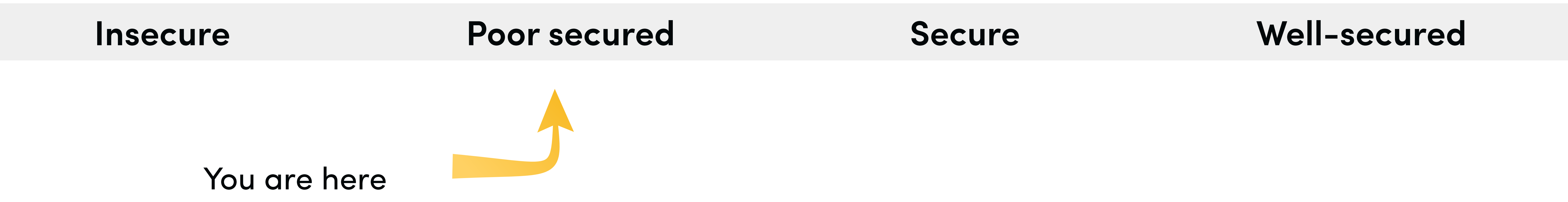
Contract Details

Token contract details for 21.02.2023

Token Type	: MEME
Contract name	: Terkehh
Contract address	: 0x53035E4e14fb3f82C02357B35d5cC0C5b53928B4
Total supply	: 210,000,000,000
Token ticker	: Terk
Decimals	: 18
Token Holders	: 1,636,886
Transactions count	: 1,987,454
Compiler version	: v0.6.12+commit.27d51765
Contract deployer address	: 0x1a00a6f01390d4b67fa39915a36b4087724b87fa
Owner address	: 0x1a00a6f01390d4b67fa39915a36b4087724b87fa

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **“Poor 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, 1 medium and 1 low.

TERK Token Distribution

 The top 100 holders collectively own 8.71% (18,287,259,720.29 Tokens) of Terk

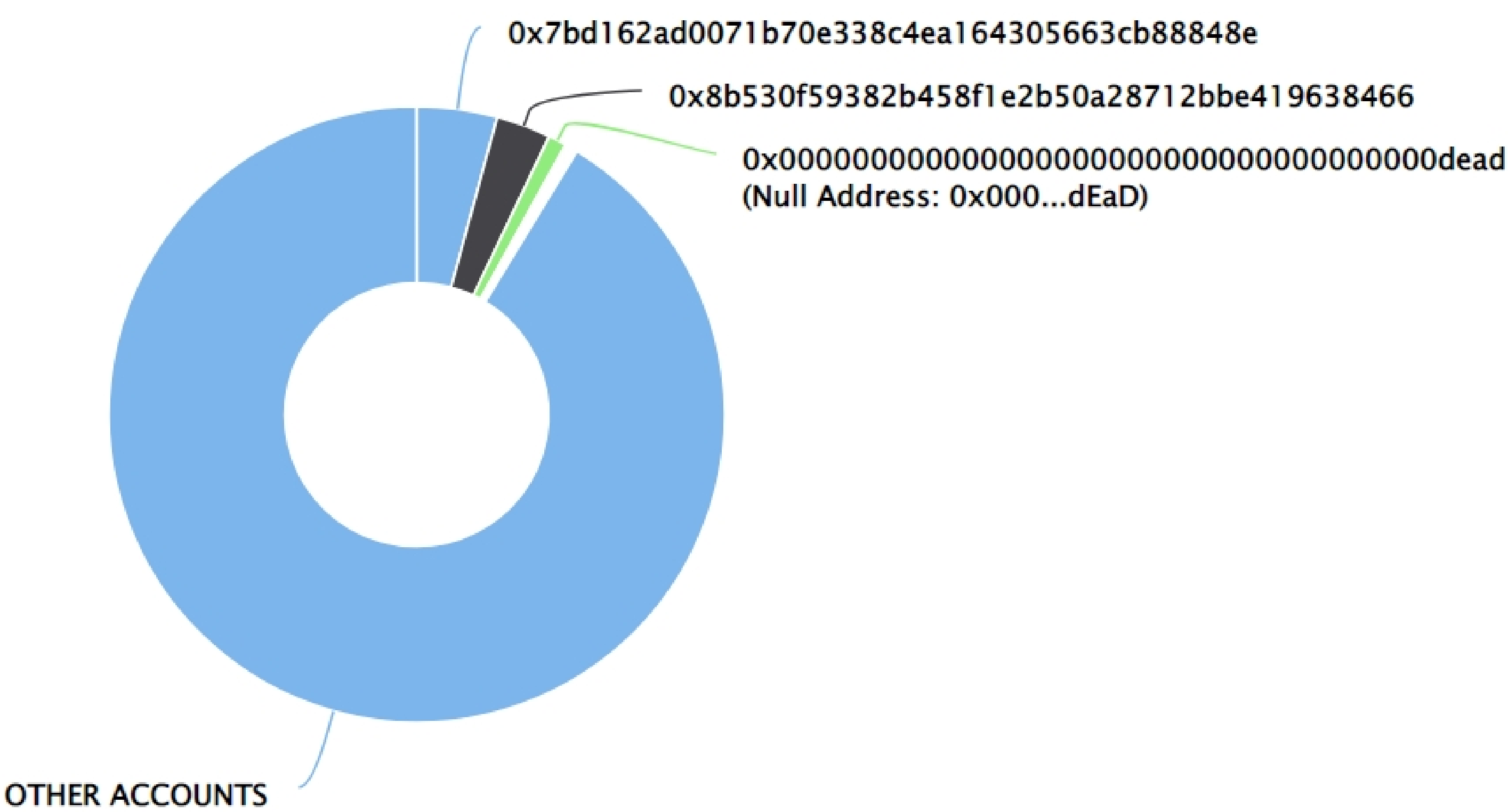
 Token Total Supply: 210,000,000,000.00 Token

|

Total Token Holders: 1,636,886


Terk Top 100 Token Holders

Source: BscScan.com



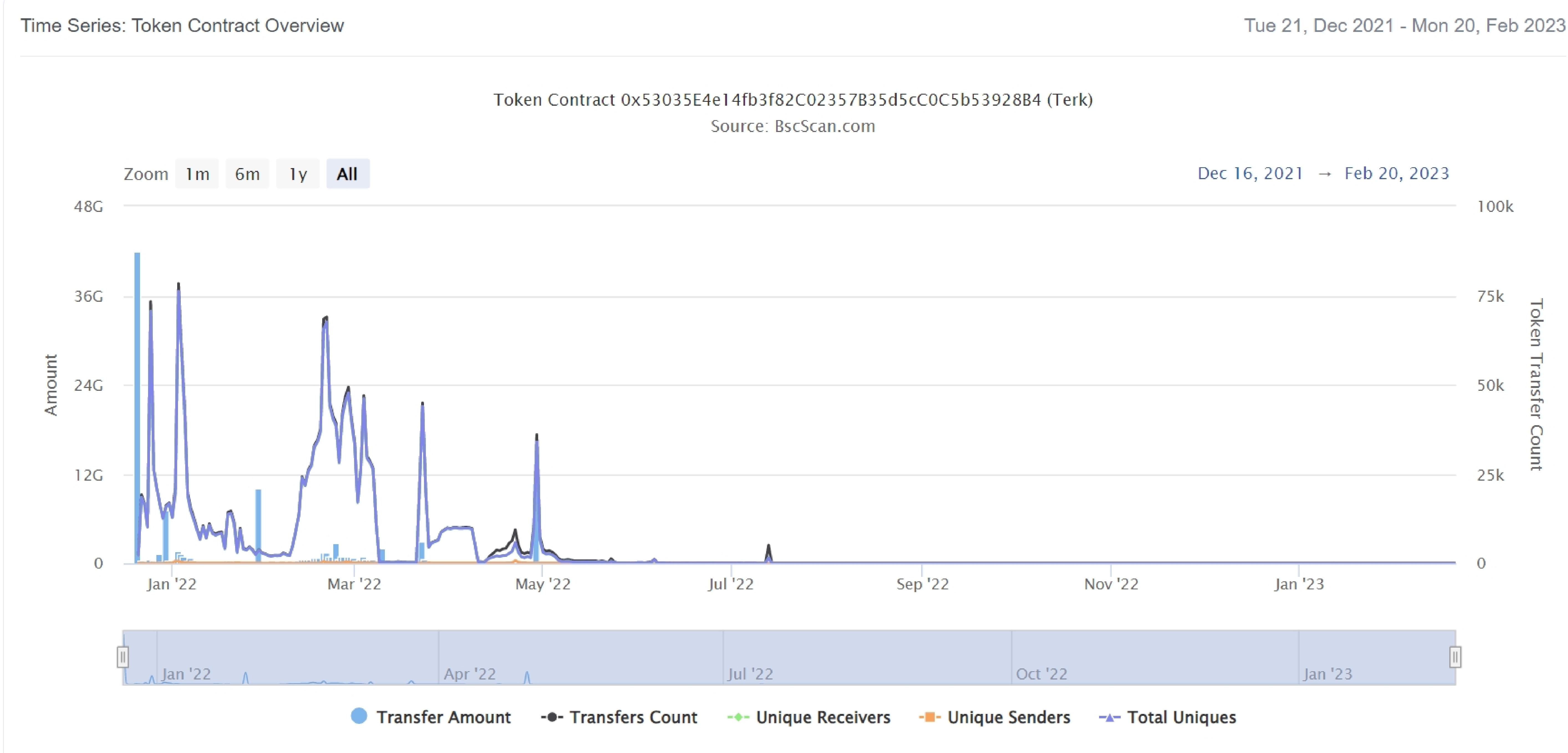
TERK Top 20 Token Holders

(A total of 19,340,555,278.48 tokens held by the top 500 accounts from the total supply of 210,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x7bd162ad0071b70e338c4ea164305663cb88848e	8,864,503,549.51255418650999982	4.2212%
2	0x8b530f59382b458f1e2b50a28712bbe419638466	6,000,133,882.550149270448423575	2.8572%
3	Null Address: 0x000...dEaD	2,000,002,010	0.9524%
4	 Terkeh: Terk Token	100,010,417.565305466074159091	0.0476%
5	0x12c235a92e5a3469c19ea2992a3674fcd92694d2	86,591,934.6	0.0412%
6	0x3e898fd0f10ed4b2cd9b2a10a3b24e2006cf7800	60,550,079.5	0.0288%
7	0x70d9a7c0176e00b913ceca3fc5f5ce82cca47d3e	54,499,926.2	0.0260%
8	0xb33a22012d4e47761b8849b327ebca0975686322	45,394,231.4	0.0216%
9	0xb1d93c7fc27aff52825ebc8fac0996ff3d3159a7	43,620,197.4	0.0208%
10	0x2079943391dc9261ca73364f12490548b7afc857	30,082,314.1	0.0143%
11	0x200254db32cabf393872f952c42ea8f8548394ef	25,162,330.418823429115698444	0.0120%
12	0xc3e8e0afbe45e216621f03345f87a2803117176a	24,257,062.4	0.0116%
13	0xba874e4ea8c0f70cc79b2903f31af63915ebb81c	24,083,723.1	0.0115%
14	0xf021276ac9a9a8e25d1d673b848a1cf56237df95	23,168,596.9	0.0110%
15	0xe258c72b6eb3afa0c24b9e53c385737f5ba96841	23,028,086.9	0.0110%
16	0x5a19610327b4428e12fe92bbe7b62c83e808b850	21,624,653.6	0.0103%
17	0x5d6cdf17263db88eb386744e09bc20240cfaa20	21,473,360.6	0.0102%
18	0x9b46fcbfce473f74de3c904a3d9e04dbac2d1469	20,327,468.5	0.0097%
19	0xd4cf599245a287149c23f6a1553c67329e85d21e	17,612,649.5	0.0084%
20	0x99127cfb74141081de2295b934641d0d4e51f3f9	15,504,231.5	0.0074%

TERK Token Distribution

TERK Contract overview



Contract functions details

+[Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] mul
- [Int] div
- [Int] sub
- [Int] div

+[Lib] RoundPool

- [Int] inc #
- [Int] getReflection
- [Int] settle #

+Terkehh

- [Pub] <Constructor >#
- [Ext] <Fallback >#
- [Ext] <Fallback >(\$)
- [Pub] name
- [Pub] owner
- [Pub] symbol
- [Int] _msgSender
- [Pub] decimals
- [Pub] cap
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] allowance
- [Pub] authNum #
- [Pub] transferOwnership #
- [Pub] Liquidity #
- [Pub] setAuth #
 - modifiers: onlyOwner
- [Pub] addLiquidity #
 - modifiers: onlyOwner
- [Pub] addAirdrop #
 - modifiers: onlyOwner
- [Int] _mint #
- [Pvt] incRoundBalances #
- [Pvt] spend #
- [Pvt] getRoundPrice #

Contract functions details

- [Pub] getRoundBalances
- [Pub] getRoundTotal
- [Int] _approve #
- [Pub] transferFrom #
- [Pub] approve #
- [Pub] clearETH #
 - modifiers: onlyOwner
- [Pub] black #
 - modifiers: onlyOwner
- [Int] _transfer #
- [Pub] update #
 - modifiers: onlyOwner
- [Pub] transfer #
- [Pub] getInfo
- [Pub] getTime
- [Pub] Airdrop (\$)

(\$) = 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.	Medium issue
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	Low issue

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

One medium severity issue found.

1. Economy model of the contract.

- **Issue:**

Owner can manually change balance of `_liquidity` address (kind of minting) but total supply is not affected in this operation. Sum of the all balance will not equal to total supply after that change.

- **Recommendation**

Change total supply on minting/burning tokens from liquidity address.

✓ Low Severity Issues

One low severity issue found.

1. Old compiler version

- **Description**

Contract has been deployed using too old solidity version.

- **Recommendation**

It is advisable to deploy contract using any of the latest version of solidity.

- **Notes:**

`balanceOf()` function do not show the actual balance that user can transfer

Centralization

Owner privileges :

- TERK Contract:
 - Owner can change auth addresses.
 - Owner can change liquidity and airdrop addresses.
 - Owner can withdraw contract BNBs.
 - Owner can blacklist addresses.
 - Owner can change contract settings (`_swSale`, `_roundRate`, `_roundCycle`, `_saleMin`, round settings).

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 low and 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.