



# Smart Contract Security Audit Report

---

## **AnimalTycoon**

December 2022

Security Status



[www.hacksafe.io](https://www.hacksafe.io)



# Audit Details



## Audited project

AnimalTycoon



## Deployer address

0x2ff6F5D62c86fA901D288dF03C3549Dcd26B8d1A



## Client contacts

AnimalTycoon 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 AnimalTycoon to perform an audit of smart contracts:

- <https://bscscan.com/token/0xE86752f7655B61161d6B71987EbC9e4f4F5EEAD7#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

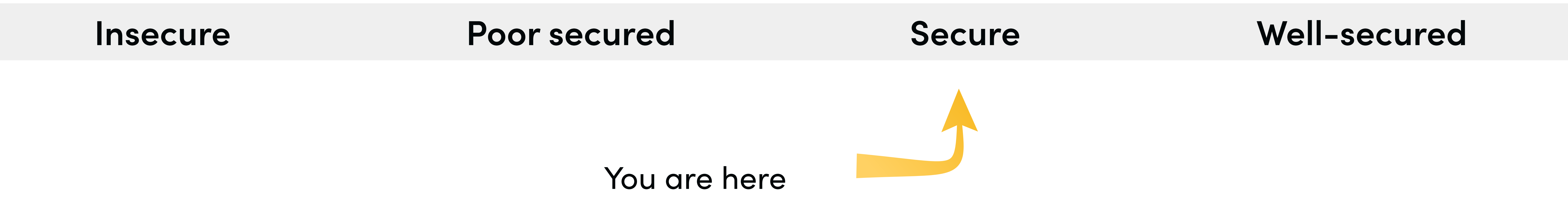
## Token contract details for 22.12.2022

Token Type	: MEME
Contract name	: BEP20AnimalTycoon
Contract address	: 0xE86752f7655B61161d6B71987EbC9e4f4F5EEAD7
Total supply	: 20,314,249,321.820541
Token ticker	: AMT
Decimals	: 18
Token Holders	: 2,174
Transactions count	: 22,504
Compiler version	: v0.7.6+commit.7338295f
Contract deployer address	: 0x2ff6F5D62c86fA901D288dF03C3549Dcd26B8d1A
Owner address	: 0xacb826a38df4d82948c3f6cadfbb84d5ee2073ab



# 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 1 low.

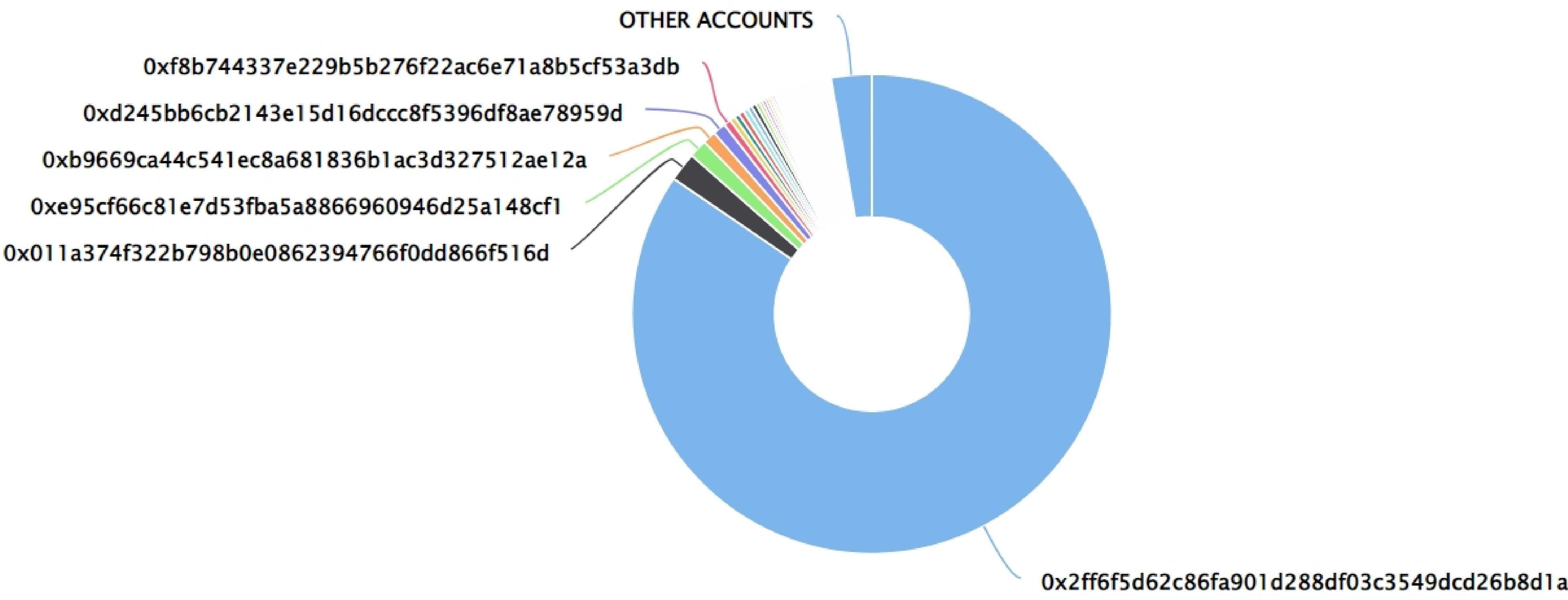
# AnimalTycoon Token Distribution

💡 The top 100 holders collectively own 97.27% (19,760,215,447.66 Tokens) of AnimalTycoon

💡 Token Total Supply: 20,314,249,321.82 Token | Total Token Holders: 2,174




AnimalTycoon Top 100 Token Holders

Source: BscScan.com



## AnimalTycoon Top 20 Token Holders

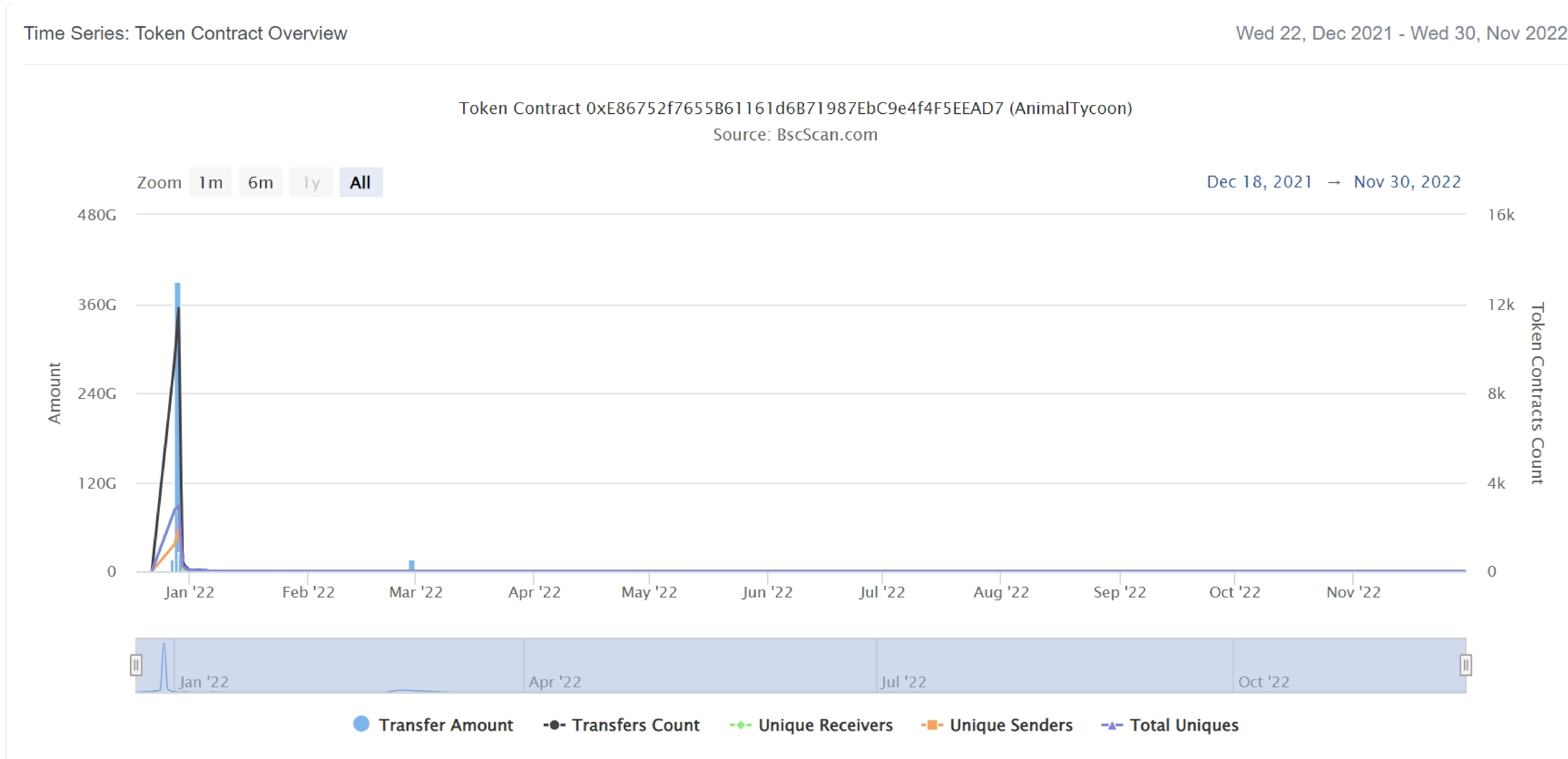
(A total of 19,760,215,447.66 tokens held by the top 100 accounts from the total supply of 20,314,249,321.82 token)

Rank	Address	Quantity (Token)	Percentage
1	0x2ff6f5d62c86fa901d288df03c3549dcd26b8d1a	17,173,942,505.041682728044032832	84.5414%
2	0x011a374f322b798b0e0862394766f0dd866f516d	398,387,412.990640860017154104	1.9611%
3	0xe95cf66c81e7d53fba5a8866960946d25a148cf1	246,503,817.834964363814150566	1.2135%
4	0xb9669ca44c541ec8a681836b1ac3d327512ae12a	180,963,677.619596564168475478	0.8908%
5	0xd245bb6cb2143e15d16dccc8f5396df8ae78959d	175,258,405.291577456701274627	0.8627%
6	0xf8b744337e229b5b276f22ac6e71a8b5cf53a3db	101,201,014.9419277335086524	0.4982%
7	0x5c7579006876b1f219213f24965de1c621979fde	73,496,502.08974051329883306	0.3618%
8	0xb5b7d379ab62187dbcb683f0b615acaa0269ca0a	70,209,382.992530596598628607	0.3456%
9	0x864072a079340d5c94b362f25af1da3bf38c9e84	70,000,000	0.3446%
10	0x4990f0751b2201843fba0d15872b015661df6298	70,000,000	0.3446%
11	 0x0ed943ce24baebf257488771759f9bf482c39706	63,431,967.721485728630846014	0.3123%
12	 PancakeSwap V2: AMT 45	58,706,909.39313153696431178	0.2890%
13	 PancakeSwap V2: AMT-BUSD 3	52,530,346.8707774592688629	0.2586%
14	0xa4bc4ab6c3c9d199b9c608448fbb110077172ec6	42,626,327.497217404196399781	0.2098%
15	0x634f98e19b101dc375217ca0b107f3c702e8613e	41,609,419.863122318279620368	0.2048%
16	0xe3d2ccadaf0e527da870c245fb10902b2266ee2	39,397,935.791575782900850955	0.1939%
17	0x2f5c687593447a12ec2727a3f9bda43fc89ea5d0	37,125,268.321878701332125188	0.1828%
18	0xb3c59184ccdfff40903963cb4cdd160d383e6921	34,209,488.439710052548780944	0.1684%
19	0x58177269672cef634819f8ec07e245ccf691304e	33,401,730.754465492458238714	0.1644%
20	0x966285f3901698c4c839a45a808272d5f2f9cdfaf	28,534,191.241045835366317779	0.1405%



# AnimalTycoon Token Distribution

## AnimalTycoon Contract Overview



# Contract functions details

## **+[Int]** IBEP20

- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Ext] balanceOf
- [Ext] transfer
- [Ext] allowance
- [Ext] approve
- [Ext] transferFrom

## **+[Int]** IBEP20Mint20 (IBEP20)

- [Ext] mint

## **+Context**

- <constructor>
- [Int] \_msgSender
- [Int] \_msgData

## **+[Lib]** SafeMath

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

## **+Ownable (Context)**

- <constructor>
- [Pub] owner
- [Pub] renounceOwnership #
  - modifiers: onlyOwner
- [Pub] transferOwnership #
  - modifiers: onlyOwner
- [Int] \_transferOwnership #



# Contract functions details

+BEP20AnimalTycoon (Context, IBEPMint20, Ownable)

-<constructor>

-[Pub] setNFTCenter #

-[Ext] getOwner

-[Ext] decimals

-[Ext] symbol

-[Ext] name

-[Ext] totalSupply

-[Ext] balanceOf

-[Ext] transfer #

-[Ext] allowance

-[Ext] approve #

-[Ext] transferFrom #

-[Pub] increaseAllowance #

-[Pub] decreaseAllowance #

-[Pub] mint #

-modifiers: onlyOwner

-[Pub] burn #

-[Pub] burnFrom #

-[Pub] setBot #

-[Int] \_transfer #

-[Int] \_mint #

-[Int] \_burn #

-[Int] \_approve #

-[Int] \_burnFrom #

(\$) = 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	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

No medium severity issue found.

## ✔ 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.



# Centralization

## Owner privileges :

- AnimalTycoon Contract:
  - Owner Can Transfer/ Renounce Ownership.
  - Owner Can Mint 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.

- transferOwnership
- renounceOwnership
- mint

# Conclusion

Smart contract contains low 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.