



Smart Contract Security Audit Report

NextMoon

November 2022

Security Status



www.hacksafe.io



Audit Details



Audited project

NextMoon



Deployer address

0xe9740a88cc00095141dafdd2ea201906781c295c



Client contacts

NextMoon 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 NextMoon to perform an audit of smart contracts:

- <https://bscscan.com/token/0xE665d9abcFe78962385Aa5A8aa0A35E33B8F2C20#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.

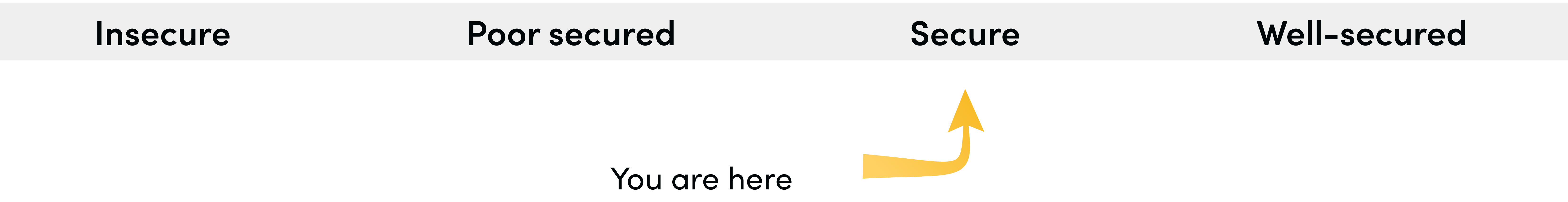
Contract Details

Token contract details for 29.11.2022

Token Type	: DEFI
Contract name	: NextMoonToken
Contract address	: 0xE665d9abcFe78962385Aa5A8aa0A35E33B8F2C20
Total supply	: 9,233,825,591,445
Token ticker	: NextMoon
Decimals	: 0
Token Holders	: 3,403
Transactions count	: 37,437
Compiler version	: v0.5.17+commit.d19bba13
Contract deployer address	: 0xe9740a88cc00095141dafdd2ea201906781c295c
Owner address	: 0xe9740a88cc00095141dafdd2ea201906781c295c

Audit Summary

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



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.

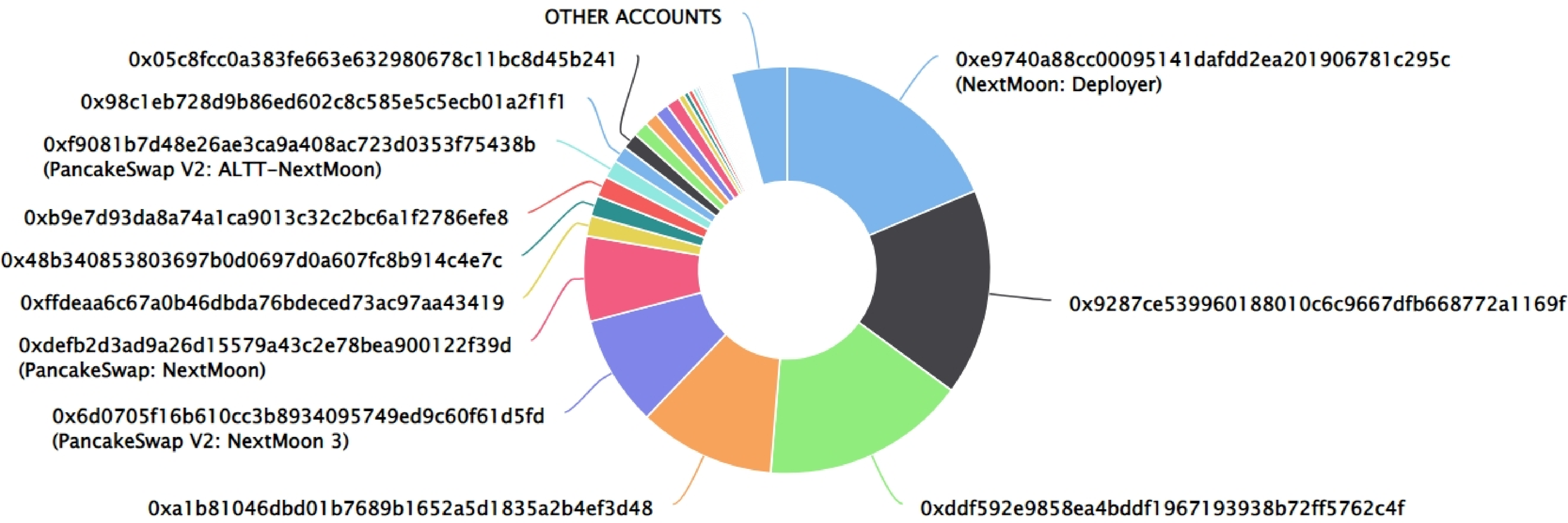
NextMoon Distribution

💡 The top 100 holders collectively own 95.56% (8,824,176,379,390.00 Tokens) of NextMoon

💡 Token Total Supply: 9,233,825,591,445.00 Token | Total Token Holders: 3,403




NextMoon Top 100 Token Holders

Source: BscScan.com



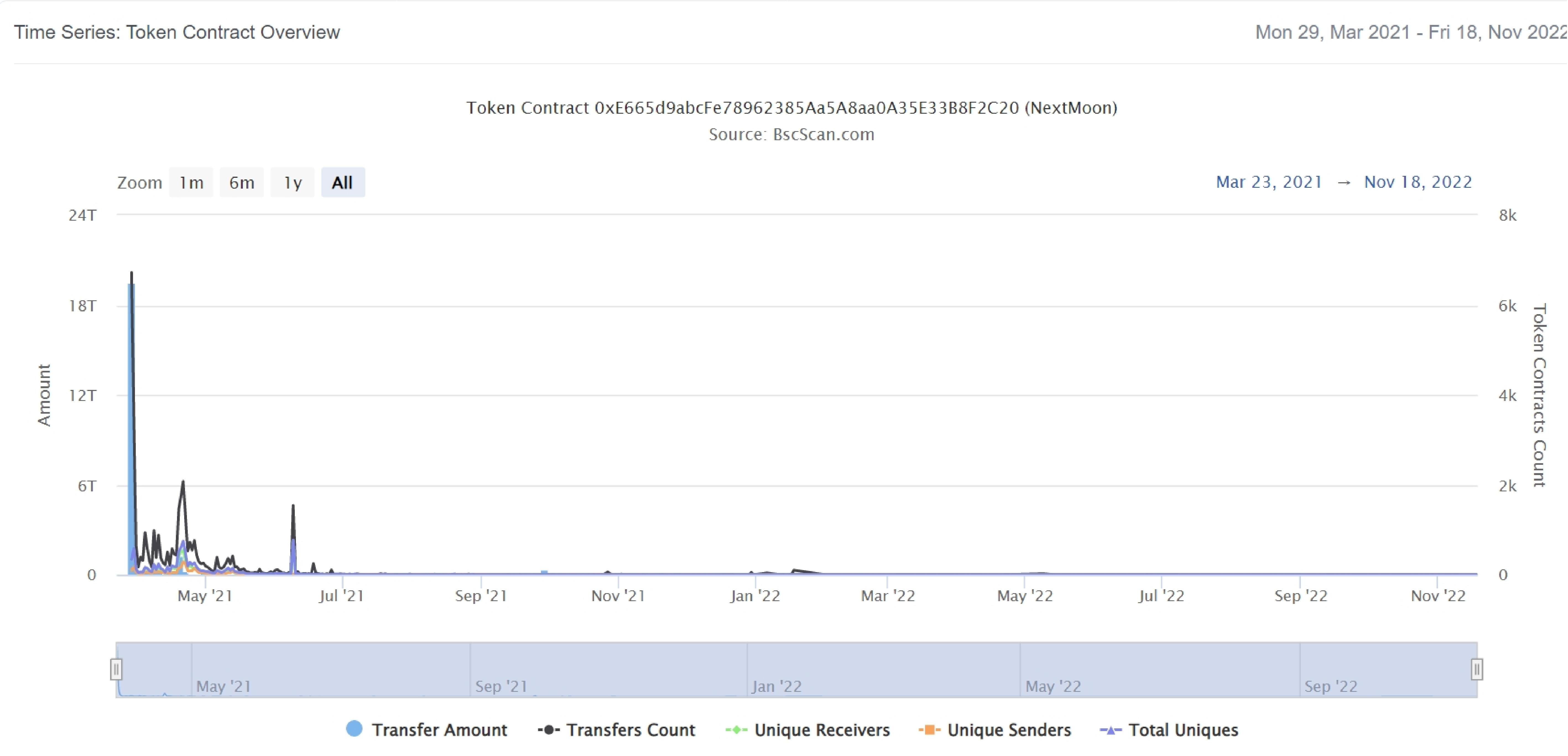
NextMoon Top 20 Token Holders

(A total of 8,824,176,379,390.00 tokens held by the top 100 accounts from the total supply of 9,233,825,591,445.00 token)

Rank	Address	Quantity (Token)	Percentage
1	NextMoon: Deployer	1,723,430,896,498	18.6643%
2	0x9287ce539960188010c6c9667dfb668772a1169f	1,514,669,056,608	16.4035%
3	0xddf592e9858ea4bddf1967193938b72ff5762c4f	1,500,000,000,000	16.2446%
4	0xa1b81046dbd01b7689b1652a5d1835a2b4ef3d48	1,000,000,000,000	10.8297%
5	 PancakeSwap V2: NextMoon 3	812,041,281,836	8.7942%
6	 PancakeSwap: NextMoon	622,591,327,138	6.7425%
7	0xffdeaa6c67a0b46dbda76bdeced73ac97aa43419	150,000,000,000	1.6245%
8	0x48b340853803697b0d0697d0a607fc8b914c4e7c	150,000,000,000	1.6245%
9	0xb9e7d93da8a74a1ca9013c32c2bc6a1f2786efe8	150,000,000,000	1.6245%
10	 PancakeSwap V2: ALTT-NextMoon	133,440,904,386	1.4451%
11	0x98c1eb728d9b86ed602c8c585e5c5ecb01a2f1f1	120,000,000,000	1.2996%
12	0x05c8fcc0a383fe663e632980678c11bc8d45b241	120,000,000,000	1.2996%
13	0xc72d9cd3130b08ca84daa43c61a8acdef393eb9b	110,000,000,000	1.1913%
14	0xdbb6a968a995f3af600b72b009eb287955112306	100,000,000,000	1.0830%
15	0xda25d4afb58ed8356c336bb236d5b242ba96965c	100,000,000,000	1.0830%
16	0x6af7fec41abc23a749f9f99b3b7f8e928f236f38	100,000,000,000	1.0830%
17	0x6e7e6c3e72a09228316f4bbc7b242c02ecaf5899	44,999,000,000	0.4873%
18	0x5c3331e790f048ddcdd63787524be4e13a06e6d7	36,100,000,000	0.3910%
19	0xb23dbdda06aac50b0285c7fa6d7c28d17ce104d4	34,845,093,290	0.3774%
20	0x447c1604043b88aab28be1479875ff499fcc4075	28,500,000,000	0.3086%

NextMoon Distribution

NextMoon Overview



Contract functions details

`+ [Int]` IERC20

- `- [Ext]` totalSupply
- `- [Ext]` balanceOf
- `- [Ext]` allowance
- `- [Ext]` transfer
- `- [Ext]` approve
- `- [Ext]` transferFrom

`+ [Lib]` SafeMath

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

`+ ERC20Detailed` (IERC20)

- `- [Pub]` <constructor>
- `- [Pub]` name
- `- [Pub]` symbol
- `- [Pub]` decimals

`+ NextMoonToken` (ERC20Detailed)

- `- [Pub]` <constructor> `$`
- `- [Pub]` totalSupply
- `- [Pub]` balanceOf
- `- [Pub]` allowance
- `- [Pub]` findOnePercent
- `- [Pub]` transfer `#`
- `- [Pub]` multiTransfer `#`
- `- [Pub]` approve `#`
- `- [Pub]` transferFrom `#`
- `- [Pub]` increaseAllowance `#`
- `- [Pub]` decreaseAllowance `#`
- `- [Int]` _mint `#`
- `- [Ext]` burn `#`
- `- [Int]` _burn `#`
- `- [Ext]` burnFrom `#`

`($)` = payable function

`#` = non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	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.	Medium issue
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

One medium severity issue found.

1. Out of gas limit

• Description

The function multiTransfer() uses the loop to transfer tokens. Function will be aborted with OUT_OF_GAS exception if there will be a long receivers addresses list.

• Recommendation

Use EnumerableSet instead of array or do not use long arrays.

✔ 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

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.