



TechRate
AUDIT COMPANY

Smart Contract Security Audit

Audit Details



Audited project

MoonBet



Deployer address

0xE043d6327d900D733b3186CF77002f72778cc90c



Client contacts:

MoonBet team



Blockchain

Binance Smart Chain



Project website:

www.moonbet.org

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 MoonBet to perform an audit of smart contracts:

<https://bscscan.com/address/0x44220eeb754ade4aa72b83d587c2c959d34560cf#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 05.08.2021

Contract name	MoonBet
Contract address	0x44220eeB754aDe4aa72b83d587C2c959d34560Cf
Total supply	1,000,000,000,000
Token ticker	MBET
Decimals	18
Token holders	3,086
Transactions count	4,523
Top 100 holders dominance	99.55%
Contract deployer address	0xE043d6327d900D733b3186CF77002f72778cc90c
Contract's current owner address	0x96a3c2f2b439973e58431c5313c57de4a59e1594

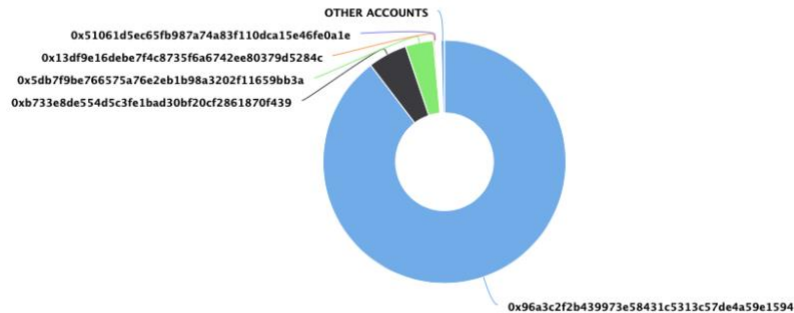
MoonBet Token Distribution

The top 100 holders collectively own 99.55% (995,511,780,968.85 Tokens) of MoonBet

Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 3,087

MoonBet Top 100 Token Holders

Source: BscScan.com



(A total of 995,511,780,968.85 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

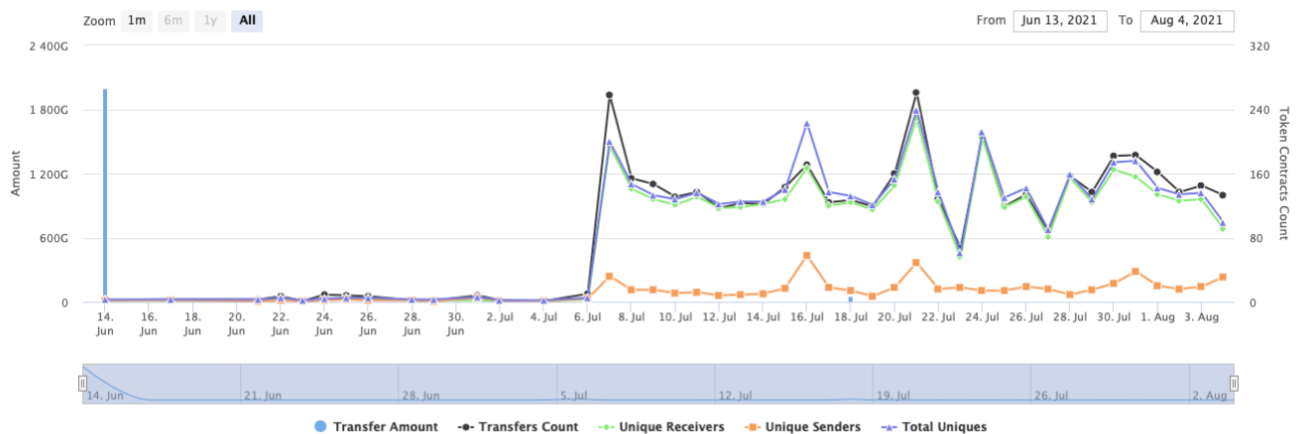
MoonBet Contract Interaction Details

Time Series: Token Contract Overview

Mon 14, Jun 2021 - Wed 4, Aug 2021

Token Contract 0x44220eeb754ade4aa72b83d587c2c959d34560cf (MoonBet)

Source: BscScan.com



MoonBet Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0x96a3c2f2b439973e58431c5313c57de4a59e1594	896,043,508,749.999999999999999	89.6044%
2	0xb733e8de554d5c3fe1bad30bf20cf2861870f439	52,212,755,200	5.2213%
3	0x5db7f9be766575a76e2eb1b98a3202f11659bb3a	37,350,639,745.79999999978699	3.7351%
4	0x13df9e16debe7f4c8735f6a6742ee80379d5284c	2,000,000,000	0.2000%
5	0x51061d5ec65fb987a74a83f110dca15e46fe0a1e	625,000,000	0.0625%
6	0x422b6868cb18e3b23b607402de8699a4a6d2023c	500,000,001	0.0500%
7	0x5aa978d4e44e2ee7486c59f11bf31a670d76c7e4	400,000,000	0.0400%
8	0xf9f18fce3225d67191b0f2b6f5930f8cdef91645	390,194,412.9	0.0390%
9	0x39fdbec9f3f1163baf22836b1dbc834354be1950	272,589,604	0.0273%
10	0x0b4ec4532e79901fbc0cbf8a9f971c8c9bc1dd2	207,306,637	0.0207%



Contract functions details

- + [Int] IBEP20
 - [Ext] totalSupply
 - [Ext] balanceOf
 - [Ext] transfer #
 - [Ext] allowance
 - [Ext] approve #
 - [Ext] transferFrom #
- + BEP20Detailed (IBEP20)
 - [Pub] <Constructor> #
 - [Pub] name
 - [Pub] symbol
 - [Pub] decimals
- + [Lib] SafeMath
 - [Int] add
 - [Int] sub
 - [Int] sub
- + Context
 - [Int] <Constructor> #
 - [Int] _msgSender
 - [Int] _msgData
- + BEP20 (Context, IBEP20)
 - [Pub] totalSupply
 - [Pub] balanceOf
 - [Pub] transfer #
 - [Pub] allowance
 - [Pub] approve #
 - [Pub] transferFrom #
 - [Int] _transfer #
 - [Int] _mint #
 - [Int] _approve #
- + Ownable (Context, BEP20)
 - [Pub] <Constructor> #
 - [Pub] owner
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
- + MoonBet (BEP20, BEP20Detailed, Ownable)
 - [Pub] <Constructor> #
 - modifiers: BEP20Detailed

(\$)= 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.

Conclusion

Smart contracts do not contain high severity issues!

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.