HackSafe

Smart Contract Security Audit Report

FarmBit

May 2022

Security Status

★ ★ ★ ★ ★

www.hacksafe.io

Audit Details

Audited project
FarmBit

Deployer address
0x1b6e32242913fb82337679c844c802c3a9d112a4

Client contacts
FarmBit team

Blockchain
Binance Smart Chain

Website
Not provided by team

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 FamrBit to perform an audit of smart contract:

- https://bscscan.com/address/0x80473d3a473c9b63101dbb9359992b657a6b74fa#code

Contract Details

Token contract details for 30.05.2022

Contract name	: FarmBit
Contract address	: 0x80473d3a473C9b63101DBB9359992B657a6B74Fa
Compiler version	: v0.5.16+commit.9c3226ce
Total supply	: 200,000,000
Token Ticker	: FMB
Decimals	: 18
Token Holders	: 2,407
Transactions count	: 6,526
Contract deployer address	: 0x1b6e32242913fb82337679c844c802c3a9d112a4
owner address	: 0x1b6e32242913fb82337679c844c802c3a9d112a4

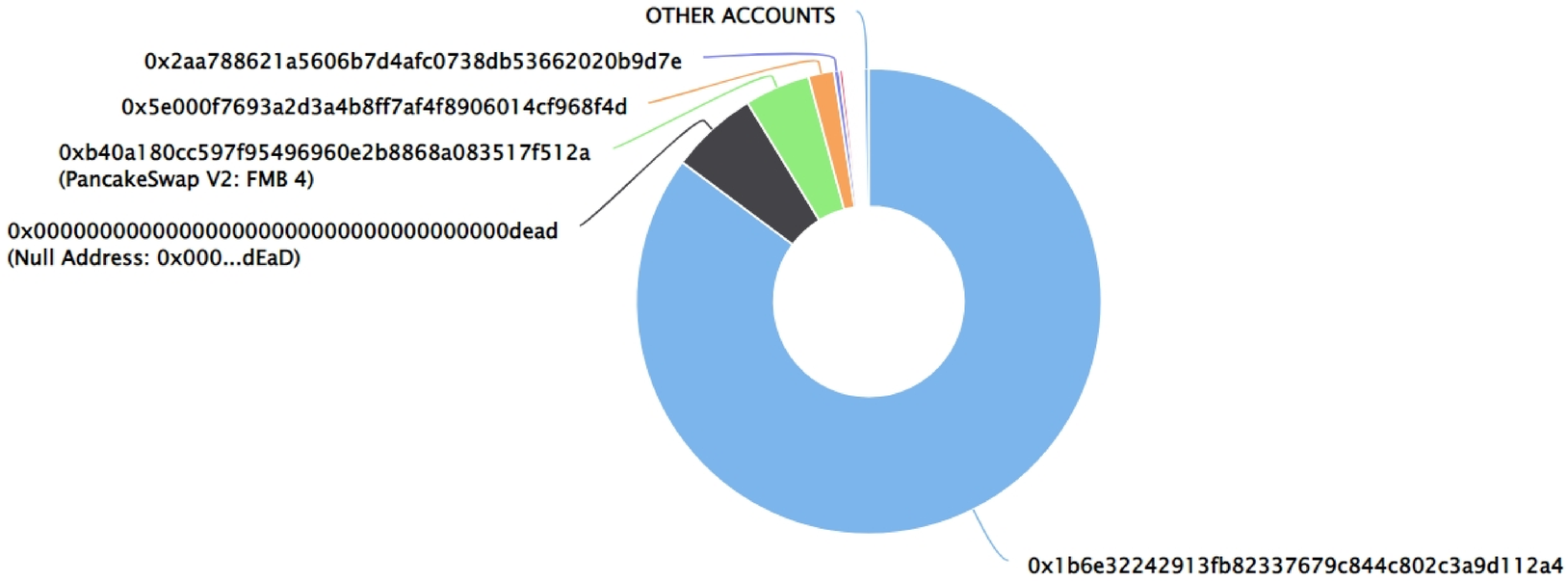
FarmBit Token Distribution

The top 100 holders collectively own 99.68% (199,356,529.83 Tokens) of FarmBit

Token Total Supply: 200,000,000.00 Token | Total Token Holders: 2,407

FarmBit Top 100 Token Holders

Source: BscScan.com



FarmBit Token Distribution

FarmBit Top 20 Token Holders

(A total of 199,356,529.83 tokens held by the top 100 accounts from the total supply of 200,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x1b6e32242913fb82337679c844c802c3a9d112a4	170,386,664.61772999997256	85.1933%
2	Null Address: 0x000...dEaD	12,144,023.741071964514237695	6.0720%
3	PancakeSwap V2: FMB 4	9,121,022.622844674280743139	4.5605%
4	0x5e000f7693a2d3a4b8ff7af4f8906014cf968f4d	3,545,704.767370007692234276	1.7729%
5	0x2aa788621a5606b7d4afc0738db53662020b9d7e	755,605.488938950247276165	0.3778%
6	0xcc4d2b17165cb473b4ba3af0c6dbea3322007cd9	511,027.242208371087055312	0.2555%
7	0x1247609bb652ab771fa1c7187f1f30928da307e3	256,043.1184	0.1280%
8	0x0a8852ab326a3454d4efabb2ba577654090dae12	195,172.914846	0.0976%
9	0x4901e7add42297e74ee255b12f89c42488e0ccd8	149,114	0.0746%
10	0x96df9c1fa0678c66fcec5dfc84ee79b8cd155225	146,806.47225	0.0734%
11	0xe8cbaaaa3100a4af84ed50bb7d4cb14d065f07f5	146,549.6039	0.0733%
12	0x47e9be9f12f2453eeb19abadf98ba556c4bd11a9	116,000	0.0580%
13	0x80473d3a473c9b63101dbb9359992b657a6b74fa	113,590	0.0568%
14	0x2f09d2d31a7305d6da01992af3a0fc05fcf0c2ed	111,074.3285	0.0555%
15	0x0db673a28bae84976a15caec50c688ba3c7d5862	85,119	0.0426%
16	0x6ed22c9a65b33b450f7d4c3f4ec75a7e053ad171	81,049	0.0405%
17	0x7efa58606085339dd6a778d5d7681d3f2fe87178	74,263	0.0371%
18	0xd2cee7c231e67414f95a7e8cd8a46991d9c856d5	67,233.45061399999944	0.0336%
19	0x622a52ed94abc304e2b4719f0594584a4dfa1bdd	66,218	0.0331%
20	0xca811aec04a5f8d2ae1a5b90f0c70f4d2800af09	62,962	0.0315%

FarmBit Token Distribution

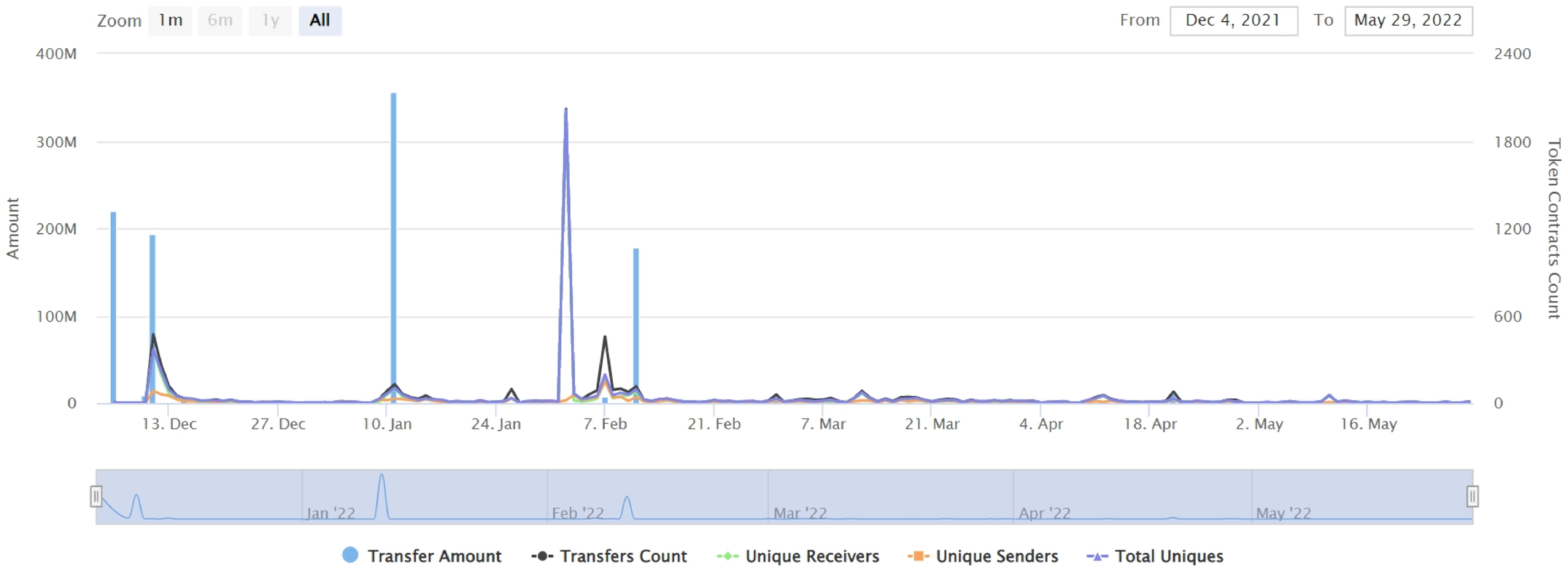
FarmBit Token Transfer Data

Time Series: Token Contract Overview

Mon 6, Dec 2021 - Sun 29, May 2022

Token Contract 0x80473d3a473c9b63101dbb9359992b657a6b74fa (FarmBit)

Source: BscScan.com



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 #

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

Contract functions details

+ FarmBit (Context, IBEP20, Ownable)
    - [Pub] <constructor>#
    - [Ext] getOwner
    - [Ext] decimals
    - [Ext] symbol
    - [Ext] name
    - [Ext] totalSupply
    - [Ext] balanceOf
    - [Ext] transfer #
    - [Ext] allowance
    - [Ext] approve #
    - [Ext] transferFrom #
    - [Pub] increaseAllowance #
    - [Pub] decreaseAllowance #
    - [Int] _transfer #
    - [Int] _mint #
    - [Int] _burn #
    - [Int] _approve #
    - [Int] _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.	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.	Low issue
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

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 issues found.

- **Low Severity Issues**
  One low severity issue found.

1. Scoping and Declarations.

Unused function.

- **Description**
  The _msgData function does nothing.

- **Recommendation**
  msgData function

- **Recommendation**
  We advise to remove unused code.

Owner Privileges

Owner Privileges (in the period when the owner is not renounced) :

- FarmBit CHAIN Contract:
    - Owner can renounce ownership.
    - owner can transfer ownership.

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.