HackSafe

Smart Contract Security Audit Report

BITTO

December 2022

Security Status

★★★★½

www.hacksafe.io

Audit Details

Audited project
BITTO

Deployer address
0x1508f607522911cb6afa9e6b0ca28496e69d0cac

Client contacts
BITTO Team

Blockchain
Ethereum

Website
http://www.bittoexchange.com/

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 BITTO to perform an audit of smart contracts:

- https://etherscan.io/token/0x55a290f08Bb4CAe8DcF1Ea5635A3FCfd4Da60456#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 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	: Exchange
Contract name	: BITTO
Contract address	: 0x55a290f08Bb4CAe8DcF1Ea5635A3FCfd4Da60456
Total supply	: 17,709,627
Token ticker	: BITTO
Decimals	: 18
Token Holders	: 2,328
Transactions count	: 5,480
Compiler version	: v0.7.1+commit.f4a555be
Contract deployer address	: 0x1508f607522911cb6afa9e6b0ca28496e69d0cac
Owner address	: 0x1508f607522911Cb6AFa9E6B0Ca28496e69d0cAc

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.

Insecure	Poor secured	Secure	Well-secured

You are here 

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.

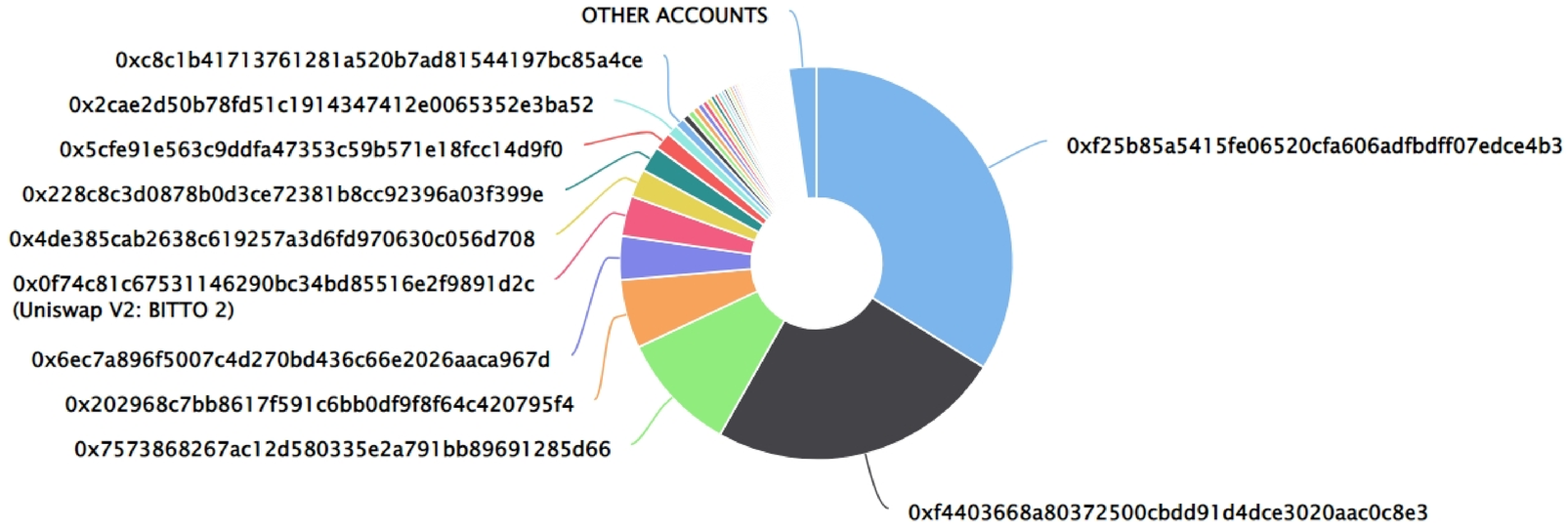
BITTO Token Distribution

The top 100 holders collectively own 97.74% (17,309,487.39 Tokens) of BITTO

Token Total Supply: 17,709,627.00 Token | Total Token Holders: 2,328

BITTO Top 100 Token Holders

Source: Etherscan.io



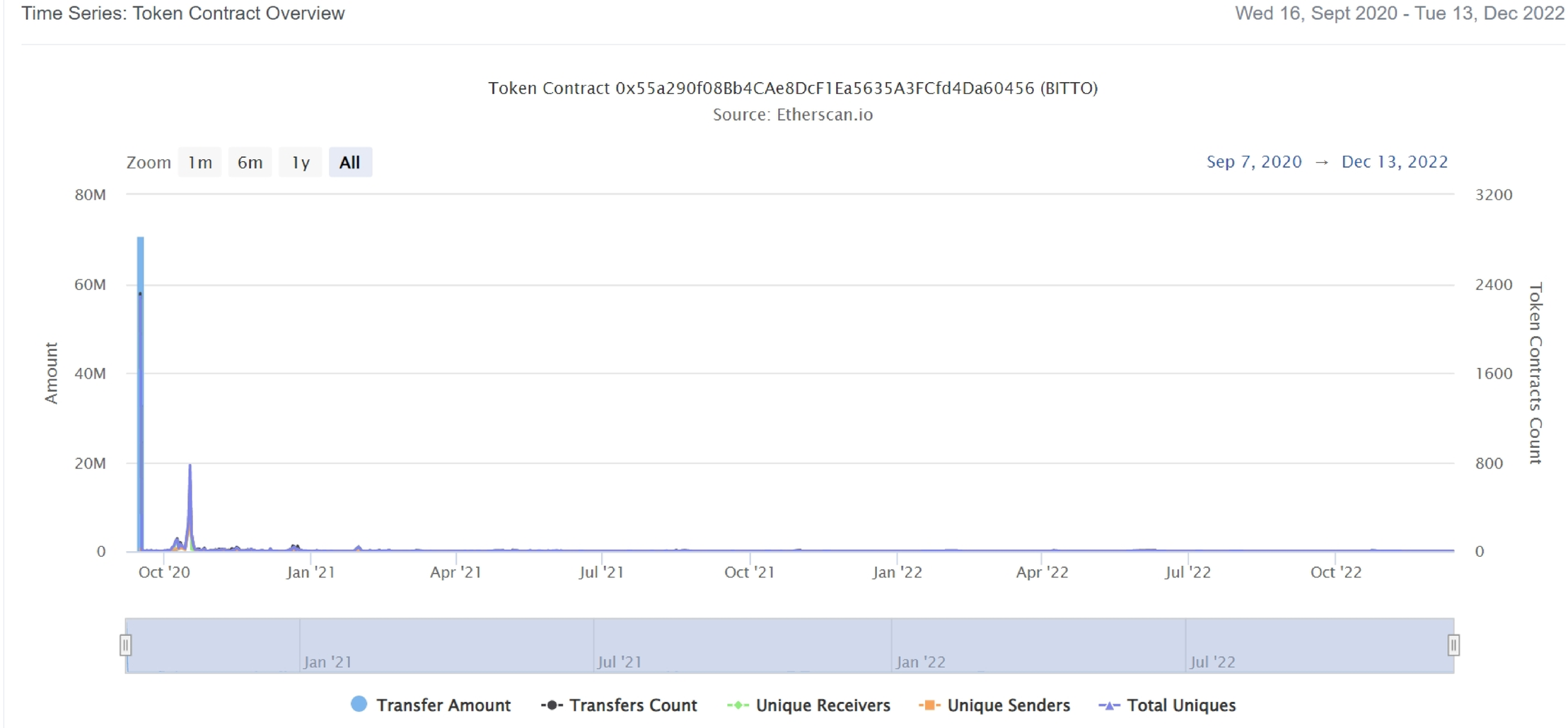
BITTO Top 20 Token Holders

(A total of 17,309,487.39 tokens held by the top 100 accounts from the total supply of 17,709,627.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xf25b85a5415fe06520cfa606adfbdff07edce4b3	6,000,000	33.8799%
2	0xf4403668a80372500cbdd91d4dce3020aac0c8e3	4,300,000	24.2806%
3	0x7573868267ac12d580335e2a791bb89691285d66	1,740,000	9.8252%
4	0x202968c7bb8617f591c6bb0df9f8f64c420795f4	1,000,000	5.6466%
5	0x6ec7a896f5007c4d270bd436c66e2026aaca967d	639,042	3.6084%
6	Uniswap V2: BITTO 2	586,534.892149922194500397	3.3120%
7	0x4de385cab2638c619257a3d6fd970630c056d708	411,236	2.3221%
8	0x228c8c3d0878b0d3ce72381b8cc92396a03f399e	370,274	2.0908%
9	0x5cfe91e563c9ddfa47353c59b571e18fcc14d9f0	258,055	1.4571%
10	0x2cae2d50b78fd51c1914347412e0065352e3ba52	166,843.308988073161129976	0.9421%
11	0xc8c1b41713761281a520b7ad81544197bc85a4ce	133,916.798102570189649717	0.7562%
12	0x905d1e30f530dcd62f03761c1a948b4369c7006a	97,831.1	0.5524%
13	0x7cf9edc4805f3e377979b8cf1e02ab2334606243	92,319.201641528105862613	0.5213%
14	0xc9bc5e2c3562f30b2b69582b8f2c950fec8259c9	82,900.606830368585051341	0.4681%
15	0xae48d3d37796140e425ea2429b26c8778ef000af	79,767	0.4504%
16	0x8a933162046b3203da27c775076728612786430a	75,794	0.4280%
17	0xfce2ddbbe54363b321eb10486e7c19ebb173a63a	66,391.868657	0.3749%
18	0xf50cf048114a24c791d7cfbe93b3d3fa5fe4f68f	62,974	0.3556%
19	0x1e735a9ed8378e3962610d48287466d0b319a851	57,500	0.3247%
20	0x652e7b4ffdba18fa172cf43a29a37deea91ba687	55,383.8	0.3127%

BITTO Token Distribution

BITTO Contract Overview



Contract functions details

+[Lib] SafeMath
    -[Int] add
    -[Int] sub
    -[Int] mul
    -[Int] div

+[Int] ERC20Interface
    -[Ext] totalSupply
    -[Ext] balanceOf
    -[Ext] transfer
    -[Ext] allowance
    -[Ext] approve
    -[Ext] transferFrom

+ApproveAndCallFallBack
    -[Pub] receiveApproval

+Owned
    -[Pub] <constructor>
    -[Pub] transferOwnership #
      -modifiers: onlyOwner
    -[Pub] acceptOwnership #

+BITTO (ERC20Interface, Owned)
    -[Pub]< constructor>
    -[Pub] totalSupply
    -[Pub] balanceOf
    -[Pub] transfer
    -[Pub] approve
    -[Pub] transferFrom
    -[Pub] allowance
    -[Pub] approveAndCall
    -[Ext] <fallback>
    -[Pub] transferAnyERC20Token #
      -modifiers: onlyOwner

($) = 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 :

- BITTO Contract:
    - Owner can transfer ownership.
    - Owner can transfer any ERC20 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
- transferAnyERC20Token

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.