HackSafe

Smart Contract Security Audit Report

OCoin

December 2022

Security Status

★★★★☆

www.hacksafe.io

Audit Details

Audited project
OCoin

Deployer address
0x85cbf5705cccc880411d6bd6d2fe5485621a968e

Client contacts
OCoin Team

Blockchain
Ethereum

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 OCoin to perform an audit of smart contracts:

- https://etherscan.io/token/0x4092678e4e78230f46a1534c0fbc8fa39780892b#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 30.12.2022

Token Type	: DEFI
Contract name	: OCoin
Contract address	: 0x4092678e4E78230F46A1534C0fbc8fA39780892B
Total supply	: 10,000,000,000
Token ticker	: OCN
Decimals	: 18
Token Holders	: 235,876
Transactions count	: 609,761
Compiler version	: v0.4.18+commit.9cf6e910
Contract deployer address	: 0x85cbf5705cccc880411d6bd6d2fe5485621a968e
Owner address	: 0x85CbF5705CCcc880411d6bD6D2fe5485621a968e

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.

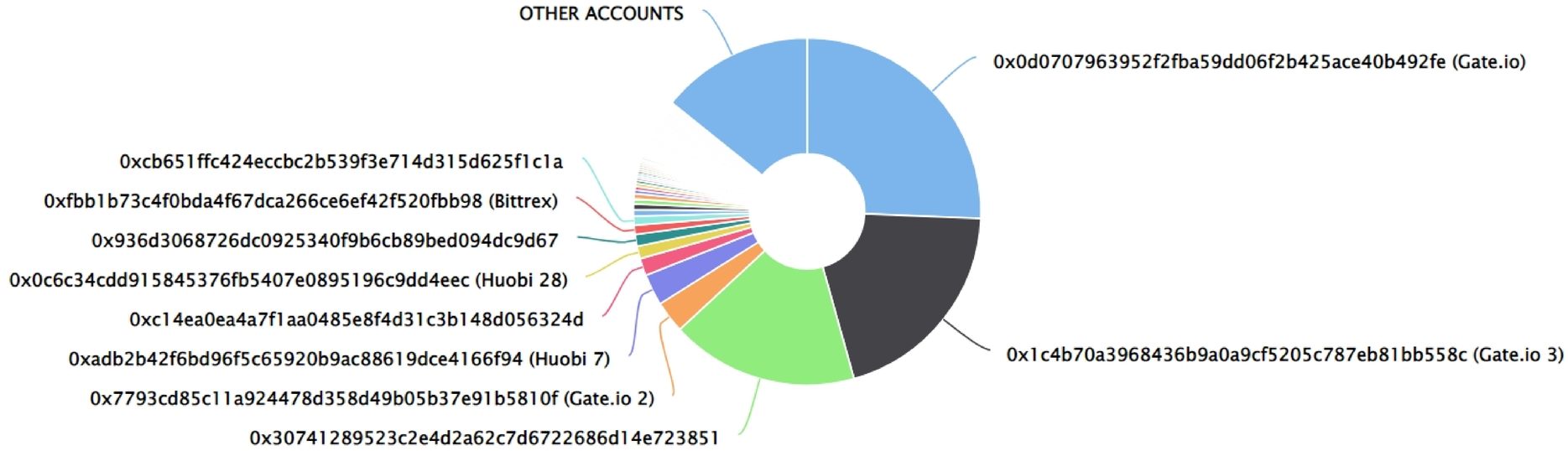
We found 0 critical, 0 high, 1 medium and 1 low.

OCoin Token Distribution

The top 100 holders collectively own 85.79% (8,578,653,597.52 Tokens) of OCoin | Token Total Supply: 10,000,000,000.00 Token | Total Token Holders: 235,87

OCoin Top 100 Token Holders

Source: Etherscan.io



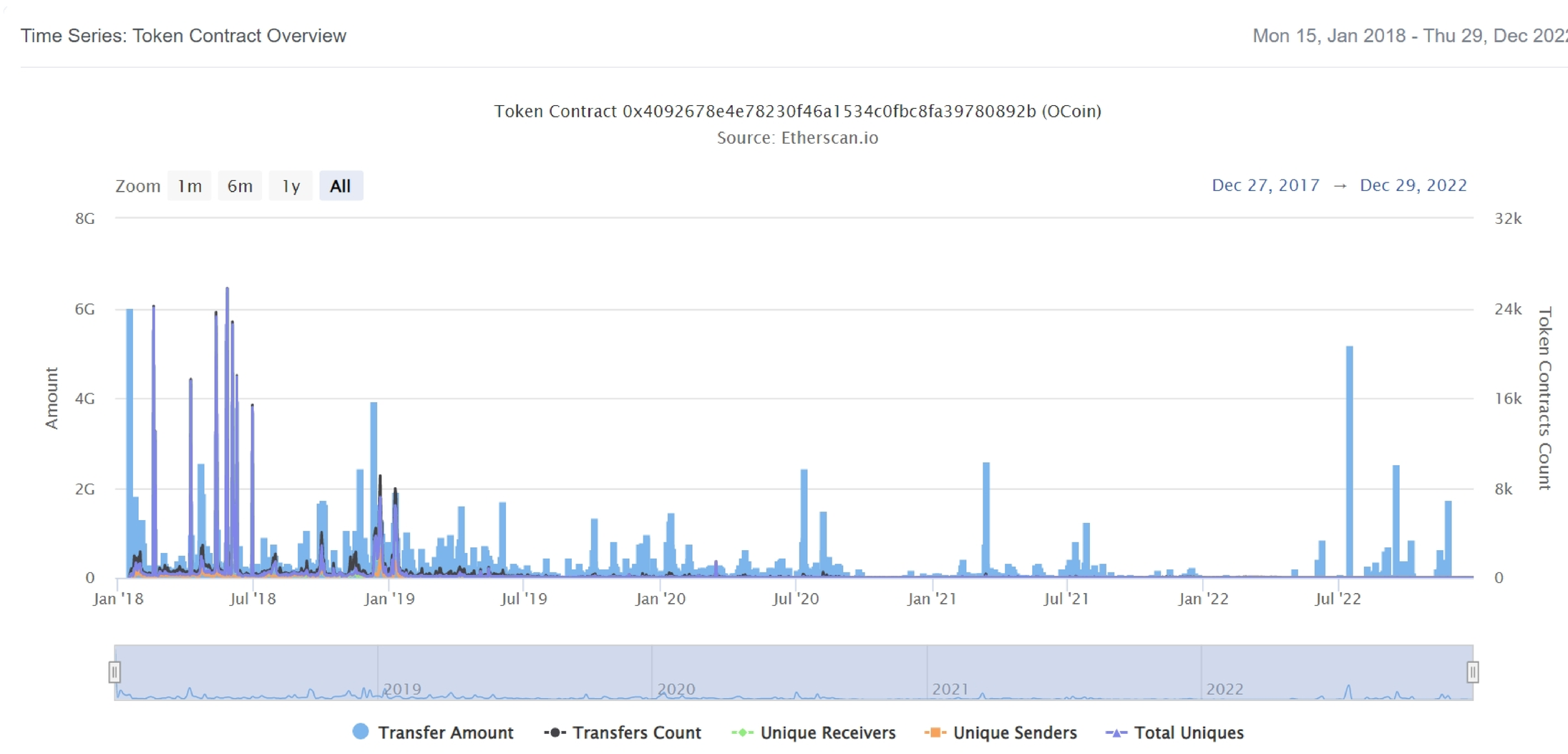
OCoin Top 20 Token Holders

(A total of 8,578,653,597.52 tokens held by the top 100 accounts from the total supply of 10,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Gate.io	2,565,956,595.455102969520381764	25.6596%
2	Gate.io 3	2,000,000,000.000000000000000753	20.0000%
3	0x30741289523c2e4d2a62c7d6722686d14e723851	1,746,219,630.769967848	17.4622%
4	Gate.io 2	296,834,092.982449595	2.9683%
5	Huobi 7	292,209,523.85325609	2.9221%
6	0xc14ea0ea4a7f1aa0485e8f4d31c3b148d056324d	159,626,718.96477248	1.5963%
7	Huobi 28	117,725,970.78176964	1.1773%
8	0x936d3068726dc0925340f9b6cb89bed094dc9d67	110,447,284.33774037	1.1045%
9	Bittrex	83,984,786.97909776	0.8398%
10	0xcb651ffc424eccbc2b539f3e714d315d625f1c1a	83,891,670.7	0.8389%
11	0x866291aa891671c02c550f4d795106a97272d69d	59,535,671.71103871	0.5954%
12	0xa5a893157e1251514f6a42362b93bc8f72540059	54,275,856.90348	0.5428%
13	0x3541f9dd7bddca6a328a0e550772e821dbcbf327	47,910,318.7006994	0.4791%
14	0x5adf08d358df450de88622f50ffbab3c2c1b71d7	47,154,955.78558863	0.4715%
15	0xd4a1e577351b2ce639d8463a67257d54ae4c797c	33,355,709.57513145	0.3336%
16	0x8066c4e664561e414b1771d313c37566cb20ec14	31,831,821.04140431	0.3183%
17	0x33a64dcdfa041befebc9161a3e0c6180cd94fa89	30,847,956.801075903850419206	0.3085%
18	0x172fd3c7a3796aefbe76be15a3db4e2065facfa8	28,393,672.6668128	0.2839%
19	0x3f68cad7c58feceabb8ef29b78389dcb208ca6bb	22,761,133.22872927	0.2276%
20	0xf8370ebbada466daed9dda9099d58c69d8fe5260	21,488,846.37400183	0.2149%

OCoin Token Distribution

Bezop Contract Overview



Contract functions details

+Ownable
  -[Pub] Ownable
  -[Pub] transferOwnership #
    -modifiers: onlyowner

+ Pausable (Ownable)
  - Ownable
  -[Pub] pause #
    -modifiers: onlyowner, whennotpaused
  -[Pub] unpause #
    -modifiers: onlyowner, whennotpaused

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

+ERC20
  -[Pub] balanceOf
  -[Pub] transfer #
  -[Pub] allowance
  -[Pub] transferFrom #
  -[Pub] approve #

+DetailedERC20 (ERC20)
  -[Pub] DetailedERC20 #

+OCoin (Pausable, DetailedERC20)
  -[Pub] OCoin #
  -[Pub] setCrowdsaleContract #
    -modifiers: onlyOwner
  -[Pub] transfer #
    -modifiers: timeLock, whenNotPaused
  -[Pub] transferToLockedBalance #
    -modifiers: whenNotPaused
  -[Pub] balanceOf
  -[Pub] transferFrom #
    -modifiers: timeLock, whenNotPaused
  -[Pub] approve #
    -modifiers: whenNotPaused

Contract functions details

-[Pub] allowance
-[Pub] increaseApproval #
  -modifiers: whenNotPaused
-[Pub] decreaseApproval #
  -modifiers: whenNotPaused

($) = 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.	Medium issue
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

One medium severity issue found.

1. Time stamp dependency

- **Issue:**

  This smart contract contain following modifier **timeLock** which uses now means functions or contract can be manipulated by miners if they have some incentive to do so as miners can adjust the timestamp.

- **Recommendation**

  It is advisable that Block timestamps should not be used for entropy or generating random numbers – i.e. they should not be the deciding factor (either directly or through some derivation) for changing an important state (if assumed to be random). This can be unnecessary if contracts aren't particularly concerned with miner manipulations of the block timestamp, but it is something to be aware of when developing contracts.

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 :

- OCoin Contract:
    - Owner can transfer Ownership.
    - Owner can pause/unpause transfers.
    - Owner can set Crowdsale Contract address.

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
- setcrowdsalecontract
- pause
- unpause

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.