HackSafe

Smart Contract Security Audit Report

0chain

November 2022

Security Status

★★★★½

www.hacksafe.io

Audit Details

Audited project
0chain

Deployer address
0xf0d85b3858764e9540c3fdade38a7e3c410c4b16

Client contacts
0chain Team

Blockchain
Ethereum

Website
https://0chain.net/

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 0chain to perform an audit of smart contracts:

- https://etherscan.io/token/0xb9EF770B6A5e12E45983C5D80545258aA38F3B78#code

The purpose of the audit was to achieve the following:

- Ensutre 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 01.11.2022

Token Type	: ERC20
Contract name	: ZerochainToken
Contract address	: 0xb9EF770B6A5e12E45983C5D80545258aA38F3B78
Total supply	: 400,000,000
Token ticker	: ZCN
Decimals	: 10
Token holders	: 24,662
Transactions count	: 125,089
Compiler version	: v0.4.21+commit.dfe3193c
Contract deployer address	: 0xf0d85b3858764e9540c3fdade38a7e3c410c4b16
Owner address	: 0x2d5e4272Df07E27DBB84d7f4a2208939b837A35E

Social profiles

Telegram profile	: https://t.me/Ochain
Facebook profile	: https://www.facebook.com/0chain
Coinmarketcap profile	: https://coinmarketcap.com/currencies/0chain/
Coingecko profile	: https://coinmarketcap.com/currencies/0chain/

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 as owner does have control over smart contract.

Insecure	Poor secured	Secure	Well-secured

You are here 

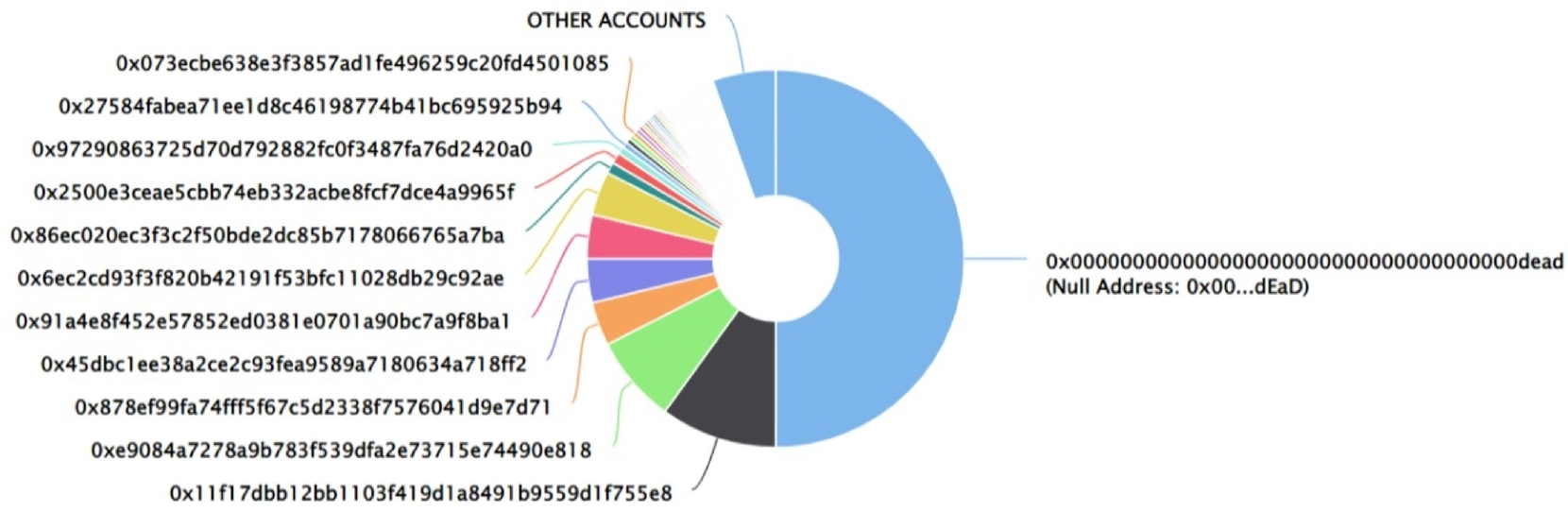
We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

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

0chain Token Distribution

The top 100 holders collectively own 94.60% (378,412,394.88 Tokens) of 0chain

Token Total Supply: 400,000,000.00 Token | Total Token Holders: 24,662



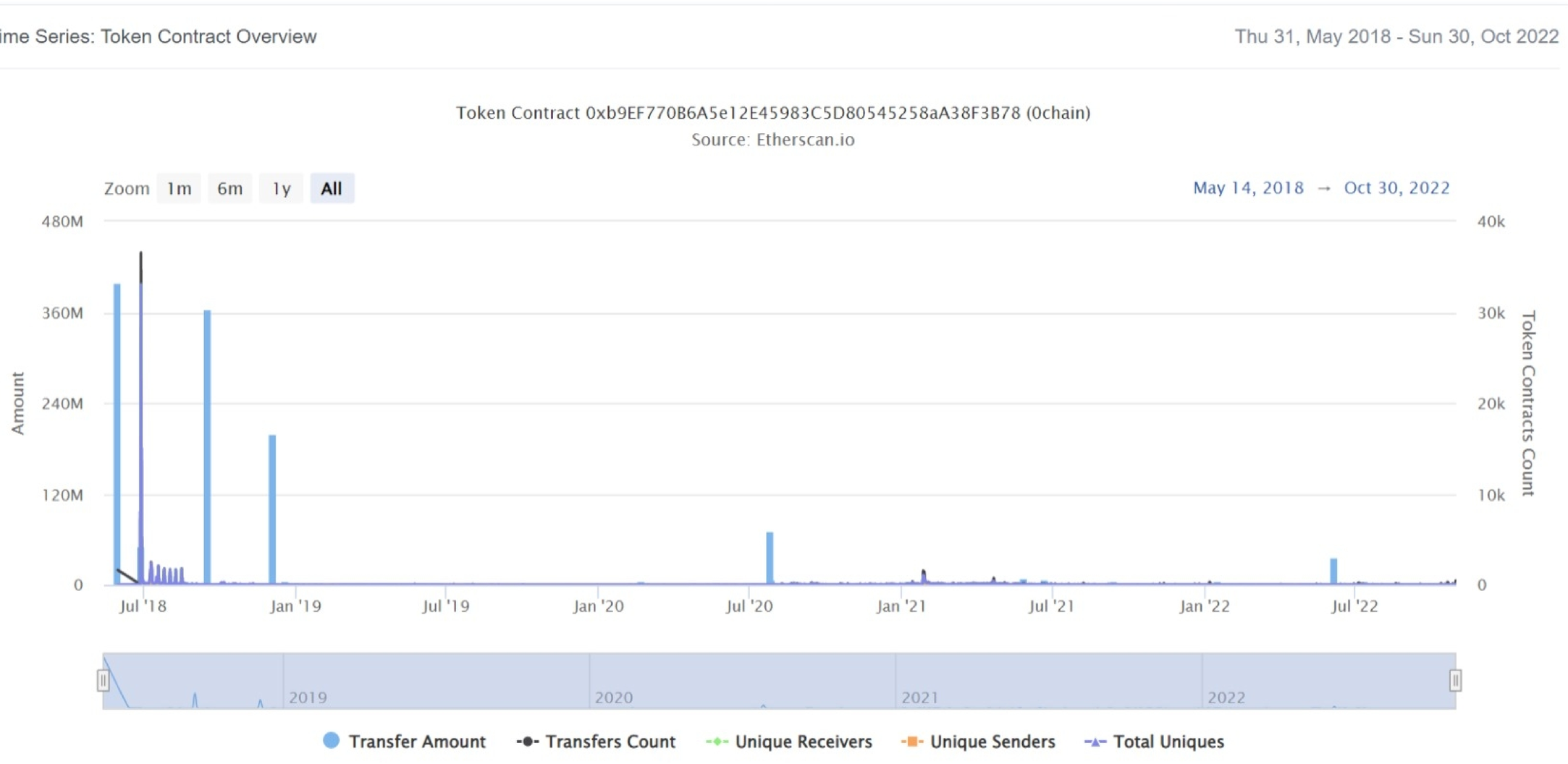
0chain Token Top 20 Token Holders

(A total of 378,412,394.88 tokens held by the top 100 accounts from the total supply of 400,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x00...dEaD	200,000,000	50.0000%
2	0x11f17dbb12bb1103f419d1a8491b9559d1f755e8	40,000,000	10.0000%
3	0xe9084a7278a9b783f539dfa2e73715e74490e818	30,000,100	7.5000%
4	0x878ef99fa74fff5f67c5d2338f7576041d9e7d71	15,000,100	3.7500%
5	0x45dbc1ee38a2ce2c93fea9589a7180634a718ff2	15,000,100	3.7500%
6	0x91a4e8f452e57852ed0381e0701a90bc7a9f8ba1	15,000,100	3.7500%
7	0x6ec2cd93f3f820b42191f53bfc11028db29c92ae	15,000,100	3.7500%
8	0x86ec020ec3f3c2f50bde2dc85b7178066765a7ba	3,831,880.3141042652	0.9580%
9	0x2500e3ceae5cbb74eb332acbe8fcf7dce4a9965f	3,762,251.0537784265	0.9406%
10	0x97290863725d70d792882fc0f3487fa76d2420a0	2,577,369.6791167108	0.6443%
11	0x27584fabea71ee1d8c46198774b41bc695925b94	1,924,369.7617325279	0.4811%
12	0xcdee00396de617edcae0ef1a42eee6cf1dad4846	1,614,826	0.4037%
13	0xc4daf0861daacf5a317aa932fcc9b367d2a2dc13	1,614,826	0.4037%
14	0x073ecbe638e3f3857ad1fe496259c20fd4501085	1,614,826	0.4037%
15	0x8aac6438dbc12107576152f1c3ee9d545ba73296	1,327,911.0000076068	0.3320%
16	0xf92e4ae9853948bde09f7a0e513e89cdd97f5aef	1,327,911	0.3320%
17	0xae287e76409678282e49f08fab52814a6ea51394	1,123,654.975	0.2809%
18	0x9c8bf378496ee310bc9e89aa193bac5a6142b7d9	1,025,758	0.2564%
19	0xc68083a0d9efc61d1212fbe08bc8e624b46968be	1,006,201.3291364584	0.2516%
20	0x16886d89daffd4a9e2b9da7308bfe0d52087d24d	1,002,700.16822	0.2507%

0chain Token Distribution

0chain Token Contract Overview



Contract functions details

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

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

+ERC20Basic
  - -[Pub] totalSupply
  - -[Pub] balanceOf
  - -[Pub] transfer

+BasicToken (ERC20Basic)
  - -[Pub] totalSupply
  - -[Pub] transfer
  - -[Pub] balanceOf

+ERC20 (ERC20Basic)
  - -[Pub] allowance
  - -[Pub] transferFrom
  - -[Pub] approve

+StandardToken (ERC20, BasicToken)
  - -[Pub] transferFrom #
  - -[Pub] approve #
  - -[Pub] allowance
  - -[Pub] increaseApproval #
  - -[Pub] decreaseApproval #

+MintableToken (StandardToken, Ownable)
  - -[Pub] mint #
    - -modifiers: onlyOwner, canMint
  - -[Pub] finishMinting #
    - -modifiers: onlyOwner, canMint

+ZerochainToken (MintableToken)

Contract functions details

($) = 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.	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 issues found.
- **Medium Severity Issues**
  No medium severity issues found
- **Low Severity Issues**
  One low severity issue founds.

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:

- Owner can transfer ownership.
- Owner can mint new tokens.
- Owner can finish minting.

Centralization 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. Following are Admin functions:

- Renounceownership
- Mint
- Finishminting

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.