Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

July, 2021

Audit Details

Audited project

CrocoSwap

Deployer address

0x23CD5C32AfB00182231Ea1779eBAa972EaB4B34B

Client contacts:

CrocoSwap team

Blockchain

Binance Smart Chain

Project website:

https://www.crocoswap.com/tokens/

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 CrocoSwap to perform an audit of smart contracts:

- https://bscscan.com/address/0x3eeb7af2f42ec2b16bb56bad91d831a69212b569#readContract
- https://bscscan.com/address/0x219b199bb671a3ff387d9afa741ffabd13986719#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.

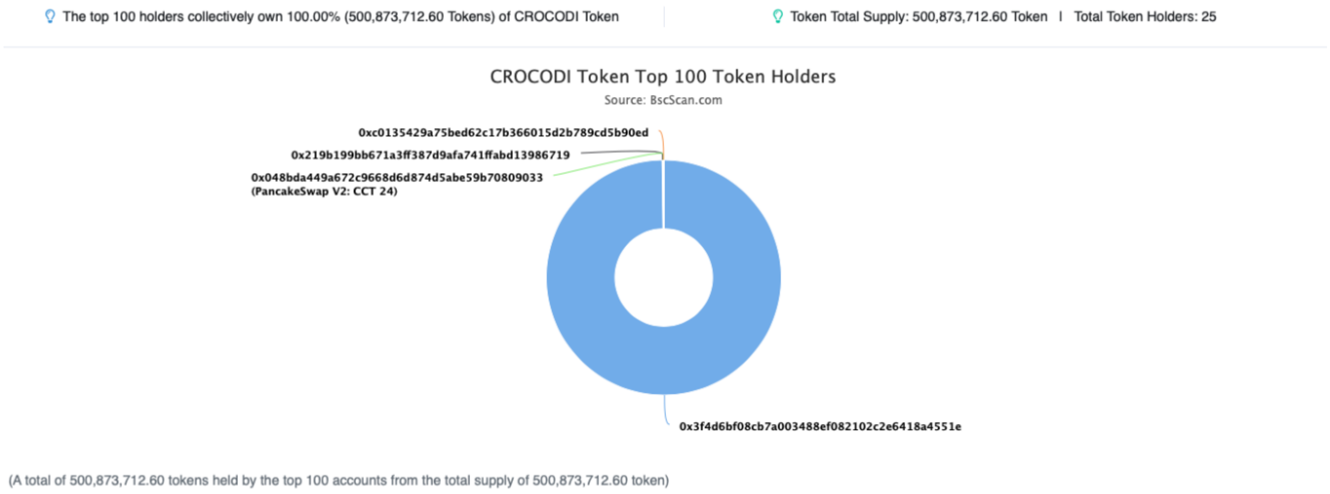
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 18.07.2021

Contract name	CrocoSwap
Contract address	0x3Eeb7AF2f42EC2b16Bb56BaD91d831a69212B569
Total supply	500,873,712.600873
Token ticker	CCT
Decimals	18
Token holders	25
Transactions count	739
Top 100 holders dominance	100.00%
Contract deployer address	0x23CD5C32AfB00182231Ea1779eBAa972EaB4B34B
Contract’s current owner address	0x219b199bb671a3ff387d9afa741ffabd13986719

CrocoSwap Token Distribution



The top 100 holders collectively own 100.00% (500,873,712.60 Tokens) of CROCODI Token

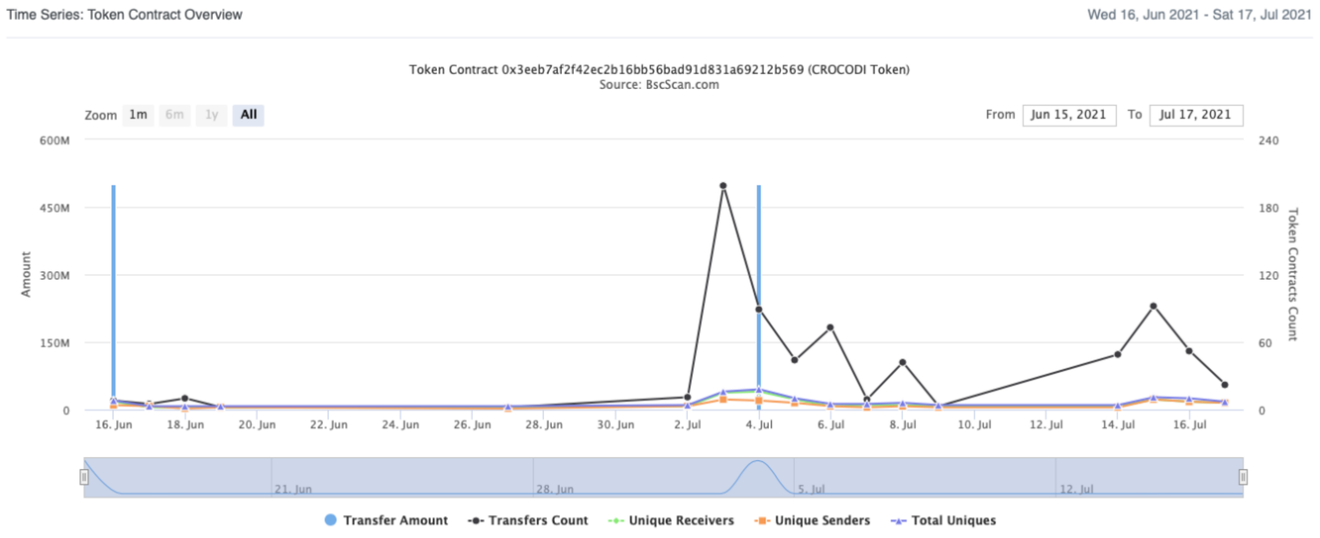
Token Total Supply: 500,873,712.60 Token | Total Token Holders: 25

CROCODI Token Top 100 Token Holders

Source: BscScan.com

(A total of 500,873,712.60 tokens held by the top 100 accounts from the total supply of 500,873,712.60 token)

CrocoSwap Contract Interaction Details



Time Series: Token Contract Overview

Wed 16, Jun 2021 - Sat 17, Jul 2021

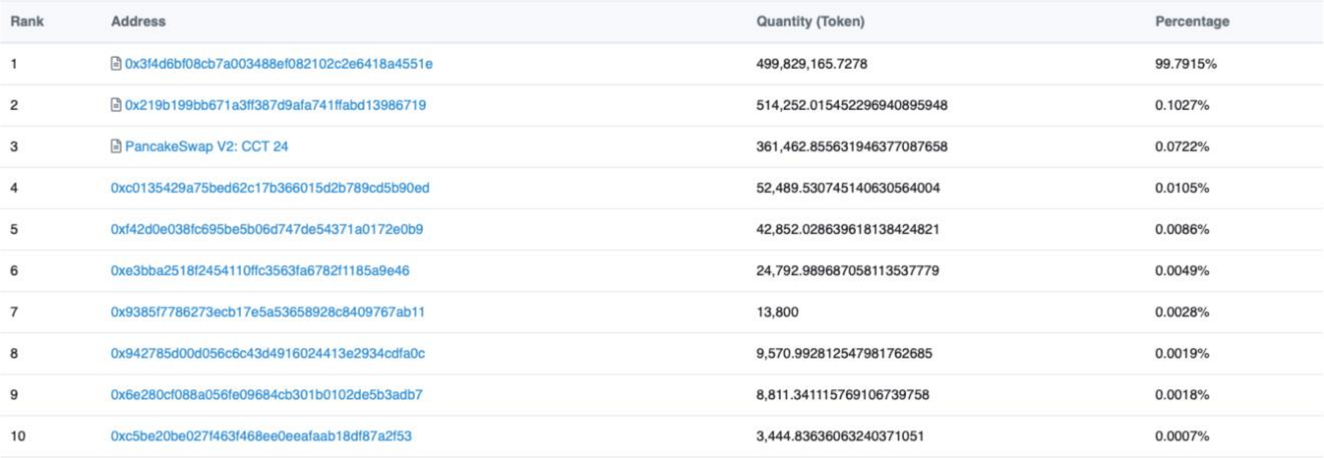
Token Contract 0x3eeb7af2f42ec2b16bb56bad91d831a69212b569 (CROCODI Token)

Source: BscScan.com

Zoom 1m 6m 1y All

From Jun 15, 2021 To Jul 17, 2021

CrocoSwap Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	🗎 0x3f4d6bf08cb7a003488ef082102c2e6418a4551e	499,829,165.7278	99.7915%
2	🗎 0x219b199bb671a3ff387d9afa741ffabd13986719	514,252.015452296940895948	0.1027%
3	🗎 PancakeSwap V2: CCT 24	361,462.855631946377087658	0.0722%
4	0xc0135429a75bed62c17b366015d2b789cd5b90ed	52,489.530745140630564004	0.0105%
5	0xf42d0e038fc695be5b06d747de54371a0172e0b9	42,852.028639618138424821	0.0086%
6	0xe3bba2518f2454110ffc3563fa6782f1185a9e46	24,792.989687058113537779	0.0049%
7	0x9385f7786273ecb17e5a53658928c8409767ab11	13,800	0.0028%
8	0x942785d00d056c6c43d4916024413e2934cdfa0c	9,570.992812547981762685	0.0019%
9	0x6e280cf088a056fe09684cb301b0102de5b3adb7	8,811.341115769106739758	0.0018%
10	0xc5be20be027f463f468ee0eeafaab18df87a2f53	3,444.83636063240371051	0.0007%

MasterChef functions details

+ ReentrancyGuard
  - [Int] <Constructor> #

+ Context
  - [Int] _msgSender
  - [Int] _msgData

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

+ [Int] IERC20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ ERC20 (Context, IERC20)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Int] _transfer #
  - [Int] _mint #
  - [Int] _burn #
  - [Int] _approve #
  - [Int] _setupDecimals #
  - [Int] _beforeTokenTransfer #

+ Ownable (Context)
  - [Int] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #

```
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner

+  CCTToken (ERC20, Ownable)
  - [Pub] mint #
    - modifiers: onlyOwner
  - [Int] _beforeTokenTransfer #

+  MasterChefV2 (Ownable, ReentrancyGuard)
  - [Pub] <Constructor> #
  - [Ext] poolLength
  - [Pub] add #
    - modifiers: onlyOwner,nonDuplicated
  - [Pub] set #
    - modifiers: onlyOwner
  - [Pub] getMultiplier
  - [Ext] pendingCct
  - [Pub] massUpdatePools #
  - [Pub] updatePool #
  - [Pub] deposit #
    - modifiers: nonReentrant
  - [Pub] withdraw #
    - modifiers: nonReentrant
  - [Pub] emergencyWithdraw #
    - modifiers: nonReentrant
  - [Int] safeCctTransfer #
  - [Pub] dev #
  - [Pub] setFeeAddress #
  - [Pub] updateEmissionRate #
    - modifiers: onlyOwner

($) = 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.	Low issues
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.	High issue
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

1. Limited minting

Issue:

Due to token owner is MasterChef, limited minting will cause deposit and withdraw function fail after reaching _maxTotalSupply minting restriction.

Recommendation:

Do not restrict minting tokens.

Medium Severity Issues

No high severity issues found.

Low Severity Issues

2. Block gas limit

Issue:

`add(uint256 _allocPoint, ...)`, `set(uint256 _pid, ...)` and `updateEmissionRate()` could invoke `massUpdatePools()` function, that can fail due to block gas limit if the pool size is too big.

Conclusion

Smart contracts contain high severity issues.
4% of rewards also adds to devAddress. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details provided by the team:
https://deeplock.io/lock/0xc14E17bBBd90DA1F23588757Bad588C771e1ADE3
https://deeplock.io/lock/0x6d3DAB508eCd71Bd2AE53fbcC2fB67A12B5d597D
https://deeplock.io/lock/0x3Eeb7AF2f42EC2b16Bb56BaD91d831a69212B569

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.