TechRate

AUDIT COMPANY

Smart Contract Security Audit

Audit Details

Audited project

Cryptonite

Deployer address

0x99f77454042fa23c2fff532de0f195dd81481a15

Client contacts:

Cryptonite team

Blockchain

Binance Smart Chain

Project website:

https://www.cryptoniterelief.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) (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 Cryptonite to perform an audit of smart contracts:

https://bscscan.com/address/0x6904b1c25c91fBD9431621fbE495d7c49FCD171F#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 26.09.2021

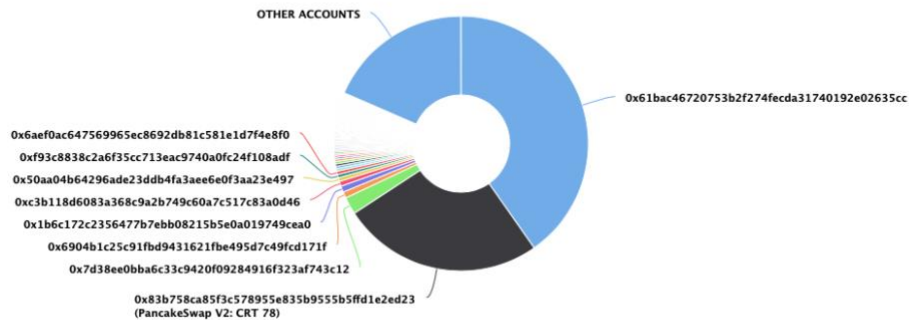|	
Contract name	Cryptonite
Contract address	0x6904b1c25c91fBD9431621fbE495d7c49FCD171F
Total supply	1,000,000,000,000,000
Token ticker	CRT
Decimals	9
Token holders	1,487
Transactions count	30,780
Top 100 holders dominance	81.51%
Total sell fee	1300
Total buy fee	700
Distributor	0x7d38ee0bba6c33c9420f09284916f323af743c12
Uniswap V2 pair	0x83b758ca85f3c578955e835b9555b5ffd1e2ed23
Contract deployer address	0x99f77454042fa23c2fff532de0f195dd81481a15
Contract's current owner address	0x6bec7e2d35fbc3c3fe5a7960bcf3004e4f1d0217

Cryptonite Token Distribution

Cryptonite Top 100 Token Holders
Source: BscScan.com

OTHER ACCOUNTS

0x61bac46720753b2f274fecda31740192e02635cc

0x6aef0ac647569965ec8692db81c581e1d7f4e8f0
0xf93c8838c2a6f35cc713eac9740a0fc24f108adf
0x50aa04b64296ade23ddb4fa3aee6e0f3aa23e497
0xc3b118d6083a368c9a2b749c60a7c517c83a0d46
0x1b6c172c2356477b7ebb08215b5e0a019749cea0
0x6904b1c25c91fbd9431621fbe495d7c49fcd171f
0x7d38ee0bba6c33c9420f09284916f323af743c12
0x83b758ca85f3c578955e835b9555b5ffd1e2ed23
(PancakeSwap V2: CRT 78)

(A total of 815,132,309,179,316.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000.00 token)
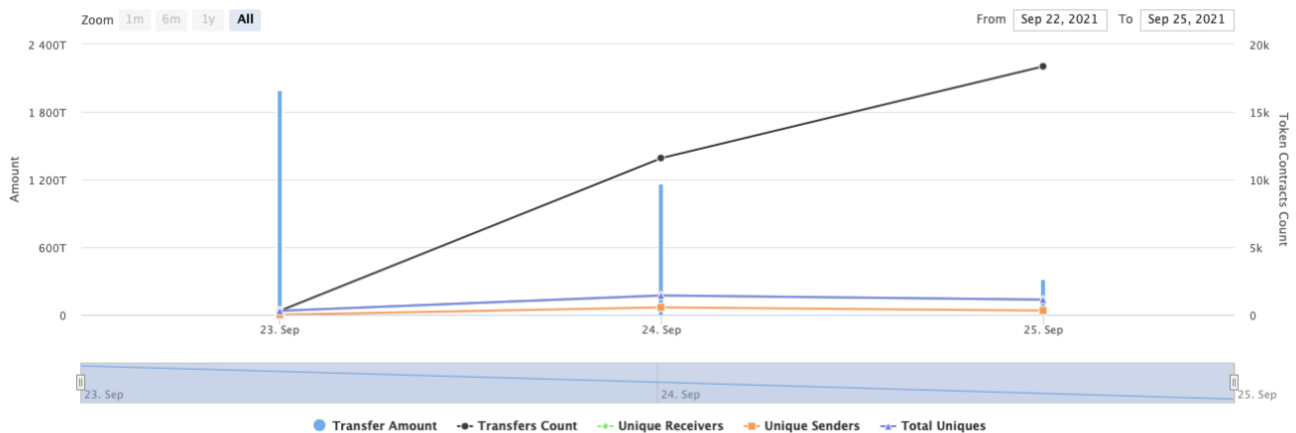
Cryptonite Contract Interaction Details

Time Series: Token Contract Overview   Thu 23, Sept 2021 - Sat 25, Sept 2021

Token Contract 0x6904b1c25c91fBD9431621fbE495d7c49FCD171F (Cryptonite)
Source: BscScan.com

Zoom 1m 6m 1y **All**   From Sep 22, 2021 To Sep 25, 2021

● Transfer Amount   -●- Transfers Count   -●- Unique Receivers   -■- Unique Senders   -▲- Total Uniques

Cryptonite Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0x61bac46720753b2f274fecda31740192e02635cc	402,585,250,004,292.21740153	40.2585%
2	PancakeSwap V2: CRT 78	255,494,271,933,076.96181083	25.5494%
3	0x7d38ee0bba6c33c9420f09284916f323af743c12	21,973,973,294,768.383042167	2.1974%
4	0x6904b1c25c91fbd9431621fbe495d7c49fcd171f	7,998,590,859,898.819212962	0.7999%
5	0x1b6c172c2356477b7ebb08215b5e0a019749cea0	7,765,103,585,769.027548688	0.7765%
6	0xc3b118d6083a368c9a2b749c60a7c517c83a0d46	6,163,468,581,640.272797109	0.6163%
7	0x50aa04b64296ade23ddb4fa3aee6e0f3aa23e497	4,724,223,917,006.918724529	0.4724%
8	0xf93c8838c2a6f35cc713eac9740a0fc24f108adf	4,205,919,995,513.795084247	0.4206%
9	0x6aef0ac647569965ec8692db81c581e1d7f4e8f0	4,200,950,953,279.199868414	0.4201%
10	0x8eccde53ae2a6cc579548b6d0b08197d5971e534	3,222,867,666,892.268605358	0.3223%

Contract functions details

+ [Lib] Address
- [Int] isContract
- [Int] sendValue **#**
- [Int] functionCall **#**
- [Int] functionCall **#**
- [Int] functionCallWithValue **#**
- [Int] functionCallWithValue **#**
- **[Prv]** _functionCallWithValue **#**

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

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

+ [Int] IDEXFactory
- **[Ext]** createPair **#**

+ [Int] IDEXRouter
- **[Ext]** factory
- **[Ext]** WETH
- **[Ext]** addLiquidity **#**
- **[Ext]** addLiquidityETH **($)**
- **[Ext]** swapExactTokensForTokensSupportingFeeOnTransferTokens **#**
- **[Ext]** swapExactETHForTokensSupportingFeeOnTransferTokens **($)**
- **[Ext]** swapExactTokensForETHSupportingFeeOnTransferTokens **#**

+ [Int] IDistributor
- **[Ext]** startDistribution **#**
- **[Ext]** setDistributionParameters **#**
- **[Ext]** setShares **#**
- **[Ext]** process **#**
- **[Ext]** deposit **#**
- **[Ext]** claim **#**
- **[Ext]** getUnpaidRewards
- **[Ext]** getPaidRewards
- **[Ext]** getClaimTime
- **[Ext]** countShareholders
- **[Ext]** getTotalRewards
- **[Ext]** getTotalRewarded
- **[Ext]** migrate **#**

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

- **[Pub]** renounceOwnership **#**
    - modifiers: onlyOwner
  - **[Pub]** transferOwnership **#**
    - modifiers: onlyOwner

  + **Cryptonite** **(IERC20, Ownable)**
  - **[Pub]** **<Constructor>** **#**
  - **[Ext]** **<Fallback>** **($)**
  - **[Ext]** totalSupply
  - **[Ext]** decimals
  - **[Ext]** symbol
  - **[Ext]** name
  - **[Ext]** getOwner
  - **[Ext]** maxBuyTxTokens
  - **[Ext]** maxSellTxTokens
  - **[Ext]** maxWalletTokens
  - **[Pub]** balanceOf
  - **[Ext]** allowance
  - **[Pub]** approve **#**
  - **[Ext]** approveMax **#**
  - **[Ext]** airdrop **#**
    - modifiers: onlyOwner
  - **[Ext]** openTrading **#**
    - modifiers: onlyOwner
  - **[Ext]** startDistribution **#**
    - modifiers: onlyOwner
  - **[Ext]** transfer **#**
  - **[Ext]** transferFrom **#**
  - [Int] _transferFrom **#**
  - [Int] launched
  - [Int] launch **#**
  - [Int] _basicTransfer **#**
  - [Int] checkWalletLimit
  - [Int] checkTxLimit
  - [Int] shouldTakeFee
  - **[Pub]** getTotalFee
  - [Int] takeFee **#**
  - [Int] shouldSwapBack
  - [Int] swapBack **#**
    - modifiers: swapping
  - **[Ext]** setup **#**
    - modifiers: onlyOwner
  - **[Ext]** updateDistributor **#**
    - modifiers: onlyOwner
  - **[Ext]** addLiquidityPool **#**
    - modifiers: onlyOwner
  - **[Ext]** switchRouter **#**
    - modifiers: onlyOwner
  - **[Ext]** excludePresaleAddresses **#**
    - modifiers: onlyOwner
  - **[Ext]** updateShares **#**
    - modifiers: onlyOwner
  - **[Ext]** setRateLimit **#**
    - modifiers: onlyOwner
  - **[Ext]** setTxLimit **#**

- modifiers: onlyOwner
- **[Ext]** setMaxWallet **#**
  - modifiers: onlyOwner
- **[Ext]** setIsDividendExempt **#**
  - modifiers: onlyOwner
- **[Ext]** setIsFeeExempt **#**
  - modifiers: onlyOwner
- **[Ext]** setIsTxLimitExempt **#**
  - modifiers: onlyOwner
- **[Ext]** setFees **#**
  - modifiers: onlyOwner
- **[Ext]** setFeeReceivers **#**
  - modifiers: onlyOwner
- **[Ext]** setSwapBackSettings **#**
  - modifiers: onlyOwner
- **[Ext]** setDistributionCriteria **#**
  - modifiers: onlyOwner
- **[Pub]** getCirculatingSupply
- **[Ext]** getPoolStatistics
- **[Ext]** getWalletStatistics
- **[Ext]** claimDividends **#**
- **[Int]** toString
- **[Int]** concatenate

($) = 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.	Passed
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

No high severity issues found.

⊘ Medium Severity Issues

No medium severity issues found.

✓ Low Severity Issues

1. Out of gas

Issue:

- The function **airdrop()** uses the loop to distribute amounts to multiple accounts. Function will be aborted with **OUT_OF_GAS** exception if there will be a long addresses list.

```
function airdrop(address[] memory addresses, uint256 amount) external onlyOwner {
    require(addresses.length > 0);
    address from = msg.sender;

    for (uint i = 0; i < addresses.length; i++) {
        if(!liquidityPools[addresses[i]] && !liquidityCreator[addresses[i]]) {
            _basicTransfer(from, addresses[i], amount * (10 ** _decimals));
            distributor.setShares(addresses[i], amount);
        }
    }
}
```

Recommendation:
Be careful about addresses array length.

Notes:

- Contract has interfaces that are not audited. Some functions may work another way.

Owner privileges (In the period when the owner is not renounced)

- Owner can airdrop.
- Owner can open trading.
- Owner can start distribution.
- Owner can change distributor.
- Owner can add liquidity pool.
- Owner can switch router.
- Owner can exclude addresses from multiple restrictions.
- Owner can reset shares.
- Owner can change rate limit.
- Owner can change max buy and sell tx amount.
- Owner can change max wallet size.
- Owner can include in and exclude from dividends.
- Owner can include in and exclude from fee and transaction amount.
- Owner can change fees.
- Owner can change fee receivers.
- Owner can change swapBack settings.
- Owner can change distribution criteria.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details NOT provided by the team.

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.