TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

September, 2021

Audit Details

Audited project

Crypto Classic

Deployer address

0x1e1226d0a8d1e511b8dcbafceed978b02d21e0c1

Client contacts:

Crypto Classic team

Blockchain

Binance Smart Chain

Project website:

Not provided by Crypto Classic team

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 Crypto Classic to perform an audit of smart contracts:
https://bscscan.com/address/0x8a6cfd647abdafb80cfcf941bf96011a67f35e9a#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 30.09.2021

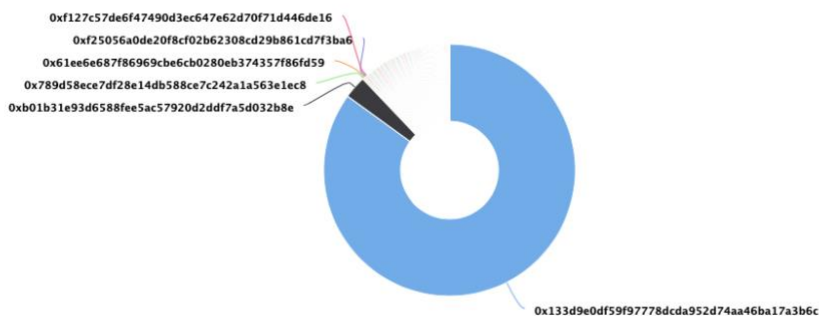|	
Contract name	Crypto Classic
Contract address	0x8A6cFd647Abdafb80CFcF941bF96011a67f35E9a
Total supply	100,000,000
Token ticker	CRC
Decimals	18
Token holders	102
Transactions count	111
Top 100 holders dominance	100.00%
Tax fee	1
Burn fee	0
Contract deployer address	0x1e1226d0a8d1e511b8dcbafceed978b02d21e0c1
Contract's current owner address	0x133d9e0df59f97778dcda952d74aa46ba17a3b6c

Crypto Classic Token Distribution

The top 100 holders collectively own 100.00% (99,999,750.00 Tokens) of Crypto Classic

Token Total Supply: 100,000,000.00 Token | Total Token Holders: 102

Crypto Classic Top 100 Token Holders
Source: BscScan.com

0xf127c57de6f47490d3ec647e62d70f71d446de16
0xf25056a0de20f8cf02b62308cd29b861cd7f3ba6
0x61ee6e687f86969cbe6cb0280eb374357f86fd59
0x789d58ece7df28e14db588ce7c242a1a563e1ec8
0xb01b31e93d6588fee5ac57920d2ddf7a5d032b8e

0x133d9e0df59f97778dcda952d74aa46ba17a3b6c

(A total of 99,999,750.00 tokens held by the top 100 accounts from the total supply of 100,000,000.00 token)

Crypto Classic Contract Interaction Details

Time Series: Token Contract Overview

Fri 24, Sept 2021 - Tue 28, Sept 2021

Token Contract 0x8a6cfd647abdafb80cfcf941bf96011a67f35e9a (Crypto Classic)
Source: BscScan.com

Zoom 1m 6m 1y All

From Sep 23, 2021 To Sep 28, 2021

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

Crypto Classic Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0x133d9e0df59f97778dcda952d74aa46ba17a3b6c	84,993,334	84.9933%
2	0xb01b31e93d6588fee5ac57920d2ddf7a5d032b8e	2,909,052.903936321403	2.9091%
3	0x789d58ece7df28e14db588ce7c242a1a563e1ec8	184,708.1205064927	0.1847%
4	0x61ee6e687f86969cbe6cb0280eb374357f86fd59	179,523.5165	0.1795%
5	0xf25056a0de20f8cf02b62308cd29b861cd7f3ba6	179,523.3165	0.1795%
6	0xf127c57de6f47490d3ec647e62d70f71d446de16	178,871.1247	0.1789%
7	0xc101e21055058741c960c9a9b29935323c346336	177,871.1247	0.1779%
8	0x2b9d325dfede2859122d214f0cc3bd635a94a7ec	176,871.124725916	0.1769%
9	0xef0093707a40f143e9b35a1dd45e952a8038acb6	176,865.1838	0.1769%
10	0x7c099e24e4efe1c11f6ecb03f8f050bbab7ce965	176,745.5224	0.1767%

Contract functions details

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

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

+ Pausable (Ownable)
- **[Pub]** pause **#**
  - modifiers: onlyOwner,whenNotPaused
- **[Pub]** unpause **#**
  - modifiers: onlyOwner,whenPaused

+ ERC20Basic
- **[Pub]** balanceOf
- **[Pub]** transfer **#**

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

+ StandardToken (ERC20)
- **[Pub]** transfer **#**
- **[Pub]** balanceOf
- **[Pub]** transferFrom **#**
- **[Pub]** approve **#**
- **[Pub]** allowance
- **[Pub]** increaseApproval **#**
- **[Pub]** decreaseApproval **#**
- [Int] _blackList **#**

+ PausableToken (StandardToken, Pausable)
- **[Pub]** transfer **#**
  - modifiers: whenNotPaused
- **[Pub]** transferFrom **#**
  - modifiers: whenNotPaused
- **[Pub]** approve **#**
  - modifiers: whenNotPaused
- **[Pub]** increaseApproval **#**
  - modifiers: whenNotPaused
- **[Pub]** decreaseApproval **#**
  - modifiers: whenNotPaused
- **[Pub]** blackListAddress **#**
  - modifiers: whenNotPaused,onlyOwner

+ CoinToken (PausableToken)
- **[Pub]** <Constructor> **#**

- **[Pub]** burn **#**
 - **[Pub]** updateFee **#**
    - modifiers: onlyOwner
 - **[Int]** _burn **#**
 - **[Pub]** mint **#**
    - 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.	Passed
10. Methods execution permissions.	Passed
11. Economy model of the contract.	High issues
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

1. Wrong allowance calculations

Issue:

- In transferFrom(address _from,...) function allowance decreases with taxes included recalculated value, but should be decreased by initial function argument value.

Recommendation:
Decrease allowance before taking from transfer amount or keep transfer value in another variable to decrease allowance with proper transfer amount.

⊘ Medium Severity Issues

No medium severity issues found.

⊘ Low Severity Issues

No low severity issues found.

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

- Owner can change the tax and burn fee and fee address.

```
function updateFee(uint256 _txFee,uint256 _burnFee,address _FeeAddress) onlyOwner public{
    txFee = _txFee;
    burnFee = _burnFee;
    FeeAddress = _FeeAddress;
}
```

- Owner can blacklist addresses.

```
function blackListAddress(address listAddress,  bool isBlackListed) public whenNotPaused onlyOwner  returns (bool success) {
  return super._blackList(listAddress, isBlackListed);
}
```

- Owner can mint any amount of tokens.

```
function mint(address account, uint256 amount) onlyOwner public {

    totalSupply = totalSupply.add(amount);
    balances[account] = balances[account].add(amount);
    emit Mint(address(0), account, amount);
    emit Transfer(address(0), account, amount);
}
```

- Owner can pause/unpause contract.

```
ftrace | funcSig
function pause() onlyOwner whenNotPaused public {
  paused = true;
  emit Pause();
}

/**
 * @dev called by the owner to unpause, returns to normal state
 */
ftrace | funcSig
function unpause() onlyOwner whenPaused public {
  paused = false;
  emit Unpause();
}
```

Conclusion

Smart contracts contain high 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.