



**TechRate**  
AUDIT COMPANY

# Smart Contract Security Audit

TechRate

July, 2021

# Audit Details



Audited project

**Cardence**



Deployer address

**0xD8eC219Ce7Bd7FF8D8c974EC28B3d5e02C5d96cF**



Client contacts:

**Cardence team**



Blockchain

**Binance Smart Chain**



Project website:

**[www.cardence.io](http://www.cardence.io)**

# 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 Cardence to perform an audit of smart contracts:

<https://bscscan.com/address/0xfa17b330bcc4e7f3e2456996d89a5a54ab044831#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 05.07.2021

Contract name	Cardence
Contract address	0xFa17b330bCC4e7F3E2456996d89A5a54AB044831
Total supply	50,000,000
Token ticker	\$CRDN
Decimals	18
Token holders	37,498
Transactions count	42,620
Top 100 holders dominance	98.95%
Contract deployer address	0xD8eC219Ce7Bd7FF8D8c974EC28B3d5e02C5d96cF
Contract's current owner address	0x00

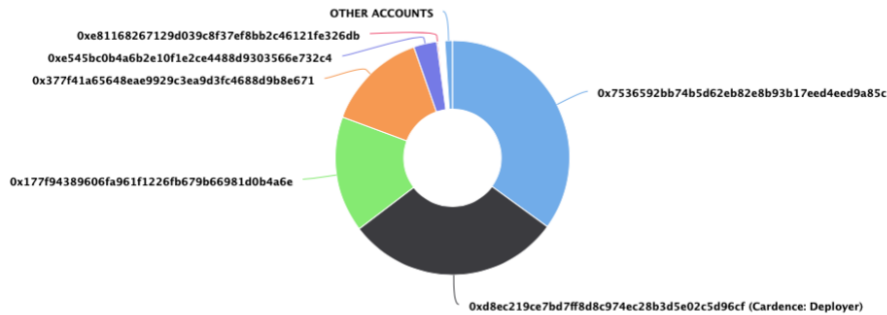
# Cardence Token Distribution

The top 100 holders collectively own 98.95% (49,476,238.10 Tokens) of Cardence

Token Total Supply: 50,000,000.00 Token | Total Token Holders: 37,497

Cardence Top 100 Token Holders

Source: BscScan.com



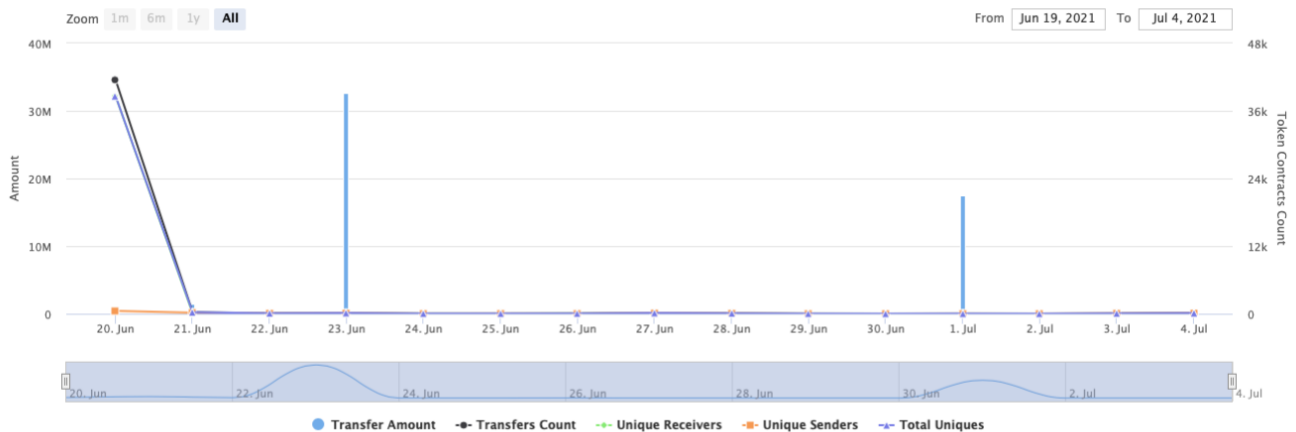
(A total of 49,476,238.10 tokens held by the top 100 accounts from the total supply of 50,000,000.00 token)

# Cardence Contract Interaction Details

Time Series: Token Contract Overview




Sun 20, Jun 2021 - Sun 4, Jul 2021

Token Contract 0xfa17b330bcc4e7f3e2456996d89a5a54ab044831 (Cardence)  
Source: BscScan.com





# Cardence Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	 0x7536592bb74b5d62eb82e8b93b17eed4eed9a85c	17,500,000	35.0000%
2	Cardence: Deployer	14,831,564	29.6631%
3	0x177f94389606fa961f1226fb679b66981d0b4a6e	8,000,000	16.0000%
4	0x377f41a65648eae9929c3ea9d3fc4688d9b8e671	7,000,000	14.0000%
5	 0xe545bc0b4a6b2e10f1e2ce4488d9303566e732c4	1,598,295.2	3.1966%
6	 0xe81168267129d039c8f37ef8bb2c46121fe326db	101,889.75	0.2038%
7	0xd380d2ad5c7f895c034a83f5ff9ae43982844122	26,199.2	0.0524%
8	0xb9b2355417d03f3716b6427e6407864f0b634744	20,013	0.0400%
9	0x9d78ff98313aa38a64e0d4f44ad5ddfa905da305	19,668	0.0393%
10	0x841c6d53ca98fb4609d4af0475429f61c8671daa	17,886	0.0358%



# Contract functions details

- + [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #
- + Ownable
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] geUnlockTime
  - [Pub] lock #
    - modifiers: onlyOwner
  - [Pub] unlock #
    - modifiers: onlyOwner
- + Token (IBEP20, Ownable)
  - [Pub] balanceOf
  - [Pub] allowance
  - [Pub] transfer #
    - modifiers: whenNotFrozen
  - [Pub] transferFrom #
    - modifiers: whenNotFrozen
  - [Pub] approve #
    - modifiers: whenNotFrozen
- + Cardence (Token)
  - [Pub] <Constructor> #
  - [Ext] \_mint #
    - modifiers: onlyOwner
  - [Pub] FreezeAcc #
    - modifiers: onlyOwner,whenNotFrozen
  - [Pub] UnfreezeAcc #
    - modifiers: onlyOwner,whenFrozen
  - [Pub] burn #
    - modifiers: whenNotFrozen
- + [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] \_functionCallWithValue #



+ [Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div
- [Int] mod
- [Int] mod

(\$) = 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.	Low issue
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.	Low 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

No high severity issues found.

## ✓ Medium Severity Issues

No medium severity issues found.

## ✓ Low Severity Issues

### 1. Wrong minting

Issue:

- The function `_mint()` do not increase total supply when minting tokens and do not set total cap to prevent unlimited minting.  
(In the period when the owner is not renounced)

```
function _mint(address _user↑, uint256 _amount↑) external onlyOwner{
    require(_user↑ != address(0), "BEP20: address can not be zero");

    balances[_user↑] = balances[_user↑].add(_amount↑);
    emit Transfer(address(0), _user↑, _amount↑);
}
```

Recommendation:

Do not forget to increase total supply and set max value.

### 2. Wrong owner unlock

Issue:

- Owner can lock ownership. But the unlock function is allowed to call only by the owner, since the owner is zero address, nobody could call this function.

```
ftrace | funcSig
function lock(uint256 time↑) public virtual onlyOwner {
    _previousOwner = _owner;
    _owner = address(0);
    _lockTime = block.timestamp + time↑;
    emit OwnershipTransferred(_owner, address(0));
}

//Unlocks the contract for owner when _lockTime is exceeds
ftrace | funcSig
function unlock() public virtual onlyOwner{
    require(_previousOwner == msg.sender, "You don't have permission to unlock");
    require(block.timestamp > _lockTime, "Contract is locked until 7 days");
    emit OwnershipTransferred(_owner, _previousOwner);
    _owner = _previousOwner;
}
```

Recommendation:

Change unlock's function access modifier.

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

- Owner can freeze and unfreeze accounts.

```
function FreezeAcc(address target↑) onlyOwner public whenNotFrozen(target) returns (bool) {
    frozen[target↑]=true;
    emit Freeze(target↑, true);
    return true;
}

ftrace | funcSig
function UnfreezeAcc(address target↑) onlyOwner public whenFrozen(target) returns (bool) {
    frozen[target↑]=false;
    emit Unfreeze(target↑, false);
    return true;
}
```

# Conclusion

Smart contracts contain low severity issues!

Liquidity locking details provided by the team:

“We have locked all tokens belonging to these categories.

1. Team Tokens
2. Advisors
3. Partnership
4. Marketing.

Locking was done on team.finance and can be seen here :

[https://team.finance/view-coin/0xFa17b330bCC4e7F3E2456996d89A5a54AB044831?name=Cardence&symbol=\\$CRDN](https://team.finance/view-coin/0xFa17b330bCC4e7F3E2456996d89A5a54AB044831?name=Cardence&symbol=$CRDN)

Details of the lock has been updated here. You can have a look.

<https://docs.google.com/spreadsheets/d/1j6gBmbPFoBo9mEzGhcuATaVNZekIHBAFjYPq7f-bBOY/edit?usp=sharing>

Tokens belonging to these categories are still unlocked as they will be utilized in listing and staking.

1. Liquidity : To be used in listing of token on DEX and CEX
2. Liquidity Mining : To be used in our staking rewards. These tokens will be sent to a smart contract which will govern it.”

Ownership renounce details provided by the team:

<https://bscscan.com/tx/0xc6850c36905f409f49fee89faa21bce48bc9e6db5101fc781edbbac0d08852d0>

---

***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.***



[Techrate1](#)



[Techrate](#)



[Techrate\\_audits](#)