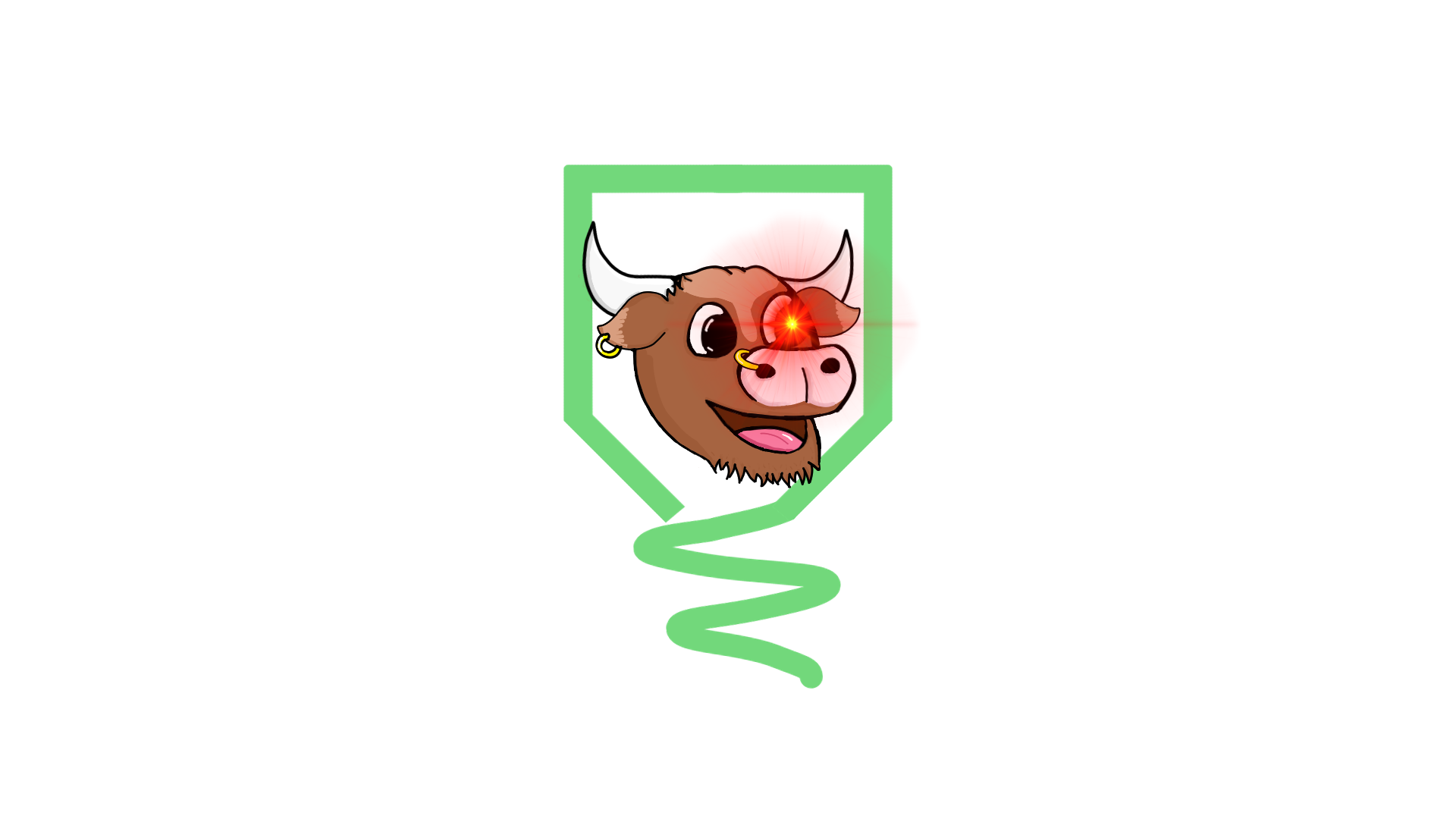
## 



**Rodeo Solutions**

**Develop - Audit - Coach**

## 

## 

## **Doge Coin Collection Smart Contract Audit**

[**Doge Coin Collection Smart Contract Audit**](#_4i7ojhp)

[Commision](#_2et92p0)

[Disclaimer](#_3dy6vkm)

[$DCC Properties](#_2xcytpi)

Holders distribution

[Contract Functions](#_2s8eyo1)

[Public](#_17dp8vu)

[View](#_3rdcrjn)

[Virtual](#_26in1rg)

[Executables](#_lnxbz9)

[Owner Executables](#_35nkun2)

[Checklist](#_1ci93xb)

[Potential Issues](#_44sinio)

Token logic doesn’t reflect website

[Owner privileges](#_z337ya)

[Conclusion](#_1y810tw)

### 

### Commision

|  |  |
| --- | --- |
| Audited Project | Doge Coin Collection |
| Project website | <https://www.dogecoincollection.info/> |
| Contract Owner | [0xdbde0b5d766e16f981c4372717403627f2a9b27d](https://bscscan.com/address/0xdbde0b5d766e16f981c4372717403627f2a9b27d) |
| SmartContract Address | [0x29e7FC61bd30Bc6797e3c502dD822a7022F9083b](https://bscscan.com/address/0x29e7FC61bd30Bc6797e3c502dD822a7022F9083b) |
| Blockchain | Binance Main Smart Chain |

Rodeo Solutions was commissioned by Doge Coin Collection owners to perform an audit of their main smart contract.

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.

### 

### 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 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 Rodeo Solutions and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Rodeo Solutions) owe no duty of care towards you or any other person, nor does Rodeo Solutions 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 Rodeo Solutions 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, Rodeo Solutions hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Rodeo Solutions, 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.

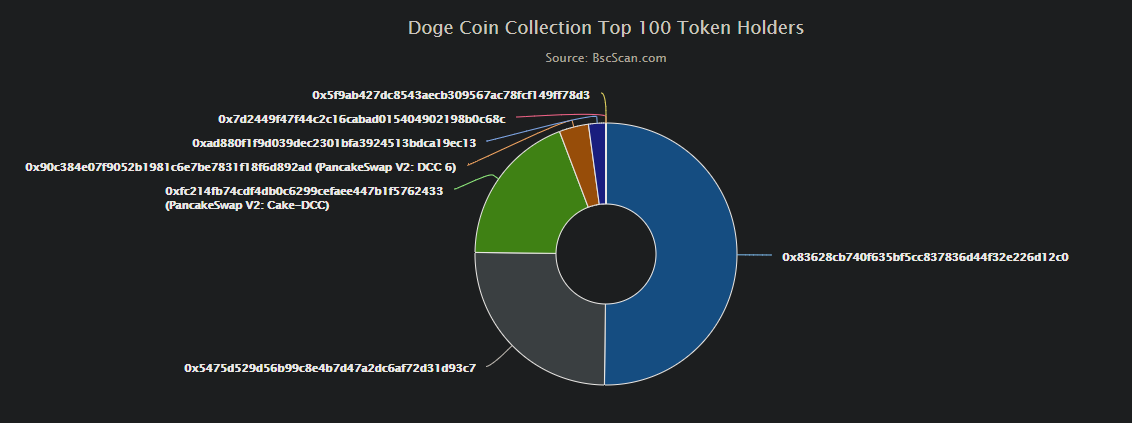
### $DCC Properties

|  |  |
| --- | --- |
| Contract name | Doge Coin Collection |
| Contract address | [0x29e7FC61bd30Bc6797e3c502dD822a7022F9083b](https://bscscan.com/address/0x29e7FC61bd30Bc6797e3c502dD822a7022F9083b) |
| Total supply | 100B |
| Token ticker | DCC |
| Decimals | 18 |
| Token holders | 12 |
| Transactions count | 36 |
| Top 100 holders dominance | 100.00% |
| Liquidity fee | No |
| Tax fee | No |
| Total fees | 0% |
| Mintable | Yes |
| Burnable | No |
| Uniswap V2 pair | No pair available |
| Contract deployer address | [0xdbde0b5d766e16f981c4372717403627f2a9b27d](https://bscscan.com/address/0xdbde0b5d766e16f981c4372717403627f2a9b27d) |
| Contract’s current owner address | [0xdbde0b5d766e16f981c4372717403627f2a9b27d](https://bscscan.com/address/0xdbde0b5d766e16f981c4372717403627f2a9b27d) |

As of 21/06/2021

### 

### [Holders distribution](#4d34og8)



### Contract Functions

#### Public

##### View

totalSupply()

balanceOf(address \_owner)

allowance(address \_owner, address \_spender)

##### Virtual

##### Executables

transfer(address \_to, uint256 \_value)

mint(address \_to, uint256 \_amount ) hasMintPermission canMint

transferFrom(address \_from, address \_to, uint256 \_value)

approve(address \_spender, uint256 \_value)

increaseApproval(address \_spender, uint256 \_addedValue)

decreaseApproval(address \_spender, uint256 \_subtractedValue)

#### Owner Executables

finishMinting() canMint

### Libraries

Ownable.sol

SafeMath.sol

### Checklist

|  |  |
| --- | --- |
| Compiler errors. | Passed |
| Possible delays in data delivery. | Passed |
| Timestamp dependence. | Passed |
| Integer Overflow and Underflow. | Passed |
| DoS with Revert. | Passed |
| DoS with block gas limit. | Passed |
| Methods execution permissions. | Passed |
| Economy model of the contract. | Passed |
| Private user data leaks. | Passed |
| Malicious Event log. | Passed |
| Scoping and Declarations. | Passed |
| Uninitialized storage pointers. | Passed |
| Arithmetic accuracy. | Passed |
| Design Logic. | Passed |
| Cross-function race conditions. | Passed |
| Fallback function security. | Passed |
| Safe Open Zeppelin contracts implementation and usage. | Passed |
| Website-Code syncronicities. | Low severity issues |

### Potential Issues

#### Token logic doesn’t reflect website

Given the Whitepaper present on the website the following features are stated:

# **Deflationary Burns**

Reducing the supply of DCC increases the price through deflation. Unlike many yield farming or staking projects that are burning tokens from what they mint on day one, we have implemented a 90-day burn, of 25% of the Total Supply. This being followed by a percentage to be burned from transactions after 90 days.

On-going deflation will push the price higher by making all of the tokens more scarce with every transaction. Over time the burn wallet will continue to grow. The burn cap for DCC at this time is set at 75% of the Total Supply. If the total burned supply reached 75% the remaining 25% will no longer continue to be burned.

# **Community Reward Tokens**

Community Rewards is a way to reward and say thank you to DCC Token supporters that help spread the word about our Token. The decision was made to set 25% of the Total supply to the side for this.

To be eligible to receive award Tokens we must receive an email to include your Receiving Wallet address. The leadership team will decide, upon discussion to whom to send reward tokens and the amount of the tokens.

The rewards tokens will be limited per 90 days with a cap of no more than 1% of the total reward budget. Rewards tokens are still eligible to be burned based upon community input.

The token reward distribution will not start until 90 days after launch but will be accepting emails for rewards during that period.

# **Operational Reward Tokens**

After the first 10 million dollar market cap 5% of the total Operational Wallet balance will be donated to a charity wallet for every 1 million dollar market cap increase.

After the first 25 million dollar market cap 5% of the total Operational Wallet balance will be donated to a charity wallet for every 5 million dollar market cap increase.

After the first 50 million dollar market cap 5% of the total Operational Wallet balance will be donated to a charity wallet for every 10 million dollar market cap increase.

After the first 500 million dollar market cap 5% of the total Operational Wallet balance will be donated to a charity wallet for every 50 million dollar market cap increase.

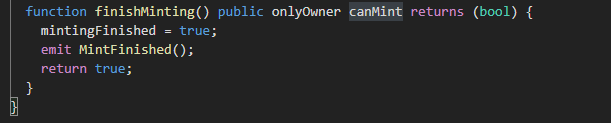
Said features are not present on the code to be performed automatically, nontheless they can be perfomed manually:

* Deflationary burns can be made transfering the given amount of tokens to a non existing address, such as 0x000000000000000000000000000000000000dEaD
* The Community rewards program can be performed with manual transfers

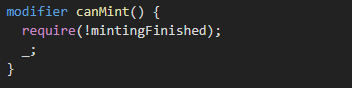
Both of the presented solutions rely on trusting the DCC team to perform them in time and form. This also render the Smart Contract not trustless.

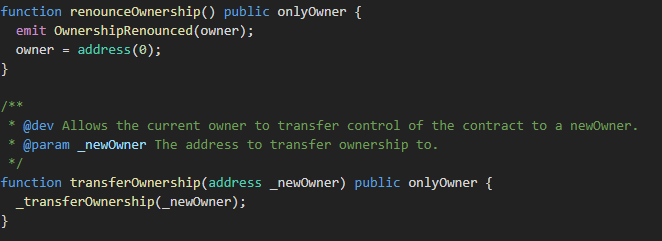
### Owner privileges

* The owner is the only one allowed to finish the minting period.



* The owner is the only one allowed to mint new tokens

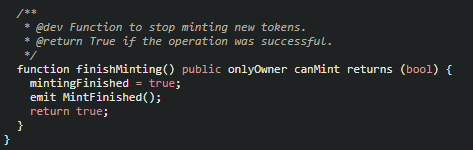
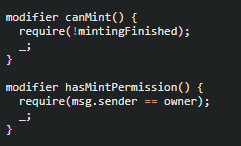


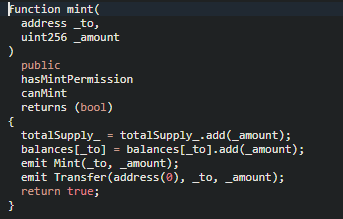
* The remaining functions only allowed by the owner are only those corresponding to the Ownable library

### Conclusion

The Smart Contract presents a straight forward and ERC20 standard compliant logic. Most of the code is equal to those present in the OpenZeppelin standards as well as the Owner and SafeMath libraries.

It doesn’t present further modifications apart from the modifiers present in the minting section:





They can be seen more in depth in the “Owner priviliges” section.

As it can be seen in the Checklist section, the only warning raised is that the deflationary burns, as well as the rewards program, can only be executed manually by the DCC, rendering the Smart Contract non-trustless.

As of 21st of June, 2021 the Token has passed the audit with a warning.