

# KISHIELD

Security Audit

**DDCToken Token**

May 16, 2022



# Table of Contents

## **\*AUDIT NOT PASSED**

### **1 Audit Summary**

### **2 Project Overview**

#### 2.1 Token Summary

#### 2.2 Main Contract Assessed

### **3 Smart Contract Vulnerability Checks**

### **4 Contract Ownership**

#### 4.1 Privileged Functions

### **5 Important Notes To The Users**

### **6 Findings Summary**

#### 6.1 Classification of Issues

#### 6.1 Findings Table

##### 01 Tax too high

##### 02 Blacklist users wallets

##### 03 Variables could be declared as constant

##### 04 Public function that could be declared external

##### 05 Missing events arithmetic

### **7 Statistics**

#### 7.1 Liquidity

#### 7.2 Token Holders

#### 7.3 Liquidity Holders

### **8 Liquidity Ownership**

### **9 Disclaimer**



# Audit Summary

This report has been prepared for DDCToken Token on the Binance Chain network. KISHIELD provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk.
- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Thorough line-by-line manual review of the entire codebase by industry experts.

# Project Overview

## Token Summary

Parameter	Result
Address	0xc33cF11C0f804eAaf08115d86cA4446beaDd75e3
Name	DDCToken
Token Tracker	DDCToken (DDC)
Decimals	18
Supply	100,000,000
Platform	Binance Chain
compiler	v0.8.10+commit.fc410830
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	<a href="https://bscscan.com/address/0x892e8B77f5C2D1Fd3A9e76ba6f51eBDE4E837a58">https://bscscan.com/ address/0x892e8B77f5C2D1Fd3A9e76ba6f51eBDE4E837a58</a>
Url	<a href="https://digdogcrypto.com">digdogcrypto.com</a>

## Main Contract Assessed

Name	Contract	Live
DDCToken	0xc33cF11C0f804eAaf08115d86cA4446beaDd75e3	Yes

# Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	✓ Low / No Risk
Code With No Effects	Complete	Complete	✓ Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	✓ Low / No Risk
Hash Collisions With Multiple Variable Length Arguments	Complete	Complete	✓ Low / No Risk
Unexpected Ether balance	Complete	Complete	✓ Low / No Risk
Presence of unused variables	Complete	Complete	✓ Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	✓ Low / No Risk
Typographical Error	Complete	Complete	✓ Low / No Risk
DoS With Block Gas Limit	Complete	Complete	✓ Low / No Risk
Arbitrary Jump with Function Type Variable	Complete	Complete	✓ Low / No Risk
Insufficient Gas Griefing	Complete	Complete	✓ Low / No Risk
Incorrect Inheritance Order	Complete	Complete	✓ Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	✓ Low / No Risk
Requirement Violation	Complete	Complete	✓ Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	✓ Low / No Risk
Weak Sources of Randomness from Chain Attributes	Complete	Complete	✓ Low / No Risk

Vulnerability	Automatic Scan	Manual Scan	Result
Authorization through tx.origin	Complete	Complete	✓ Low / No Risk
Delegatecall to Untrusted Callee	Complete	Complete	✓ Low / No Risk
Use of Deprecated Solidity Functions	Complete	Complete	✓ Low / No Risk
Assert Violation	Complete	Complete	✓ Low / No Risk
Reentrancy	Complete	Complete	✓ Low / No Risk
Unprotected SELFDESTRUCT Instruction	Complete	Complete	✓ Low / No Risk
Unprotected Ether Withdrawal	Complete	Complete	✓ Low / No Risk
Unchecked Call Return Value	Complete	Complete	✓ Low / No Risk
Outdated Compiler Version	Complete	Complete	✓ Low / No Risk
Integer Overflow and Underflow	Complete	Complete	✓ Low / No Risk
Function Default Visibility	Complete	Complete	✓ Low / No Risk

## Contract Ownership

The contract ownership of DDCToken is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address 0x6d2F4e54600CaC538D2EBade7cdb18A464C98cad which can be viewed from:  
[HERE](#)

The owner wallet has the power to call the functions displayed on the privileged functions chart below, if the owner wallet is compromised this privileges could be exploited.

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.



## Important Notes To The Users:

- The owner cannot mint tokens after initial deployment.
- The owner cannot change the min tx amount.
- Once the owner renounces ownership of the contract, none of the following are applicable.
- The owner CAN enable/disable trading using the function `changeTradingState`.
- The owner can change tax fee amounts with no restrictions (up to 100%).
- The owner can include/exclude addresses from fees.
- The owner can include/exclude addresses from paused trading (excluded addresses can buy and sell with trading paused).
- The owner can add/remove WALLETS and contracts addresses to the bot blacklist using the `blacklisted` function (stops users from trading).
- The owner can withdraw BNB and ERC20, ERC721 and ERC1155 from the contract.
- No high-risk Exploits/Vulnerabilities Were Found in token Source Code other than Owner Privileges.

**Audit Not Passed**

# Technical Findings Summary

## Classification of Issues

Severity	Description
● High	Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency
● Medium	Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible.
● Low	Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.
● Info	Consistency, syntax or style best practices. Generally pose a negligible level of risk, if any.

## Findings

Severity	Found
● High	2
● Medium	0
● Low	0
● Info	3
Total	5



# Findings

## Tax too high

ID	Severity	Contract	Function
01	● High	DDCToken	Functions setRewardsFee, setTeamFee, setEcoFee, setMarketingFee

### Description

The owner can change the fees to 100% with no restrictions at any time. This only applies to non-tax-exempt users.

### Recommendation

We recommend adding a require statement to limit the max fee amount.

## Blacklist users wallets

ID	Severity	Contract	Function
02	● High	DDCToken	Function blacklisted()

### Description

The owner can add/remove WALLETS and contracts addresses to the bot blacklist which prevents users from trading.

### Recommendation

We recommend adding a require statement so only contract addresses can be added to the blacklist, not user wallets.

## Variables could be declared as constant

ID	Severity	Contract	Function
03	Informational	DDCToken	Variables burnAddress, maxSellAmount, totalSellFee

### Description

Gas Optimization. Variables that are never changed could be declared as constant.

### Recommendation

We recommend declaring those variables as constant.

## Public function that could be declared external

ID	Severity	Contract	Function
04	Informational	DDCToken	Functions withdraw setAutomatedMarketMakerPair, blacklisted, setRewardsFee, setTeamFee, setEcosystemFee, setMarketingFee

### Description

Gas Optimization. Public function that could be declared external

### Recommendation

Public functions that are never called by the contract should be declared external to save gas.

## Missing events arithmetic

ID	Severity	Contract	Function
05	Informational	DDCToken	Missing events for setBurnFee, setReserveFee, setRewardsFee, setTeamFee, setEcosystemFee, setMarketingFee

### Description

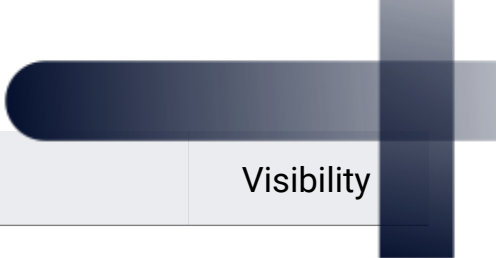
Functions that change critical arithmetic parameters should emit an event.

### Recommendation

Emit corresponding events for critical parameter changes.

## Privileged Functions (onlyOwner)

Function Name	Parameters	Visibility
renounceOwnership	none	public
transferOwnership	address newOwner	public
withdraw	uint256 amount	public
withdraw	none	public
withdrawERC20	none	external
withdrawERC20	none	external
withdrawERC721	address tokenAddress, calldata tokenIds	external
withdrawERC721	none	external
withdrawERC1155	address tokenAddress, uint256 id, uint256 amount	external
withdrawERC1155	none	external
setAutomatedMarketMakerPair	address pair, bool value	public
_setAutomatedMarketMakerPair	address pair, bool value	private
excludeFromFees	address account, bool excluded	public
excludeFromPause	address account, bool excluded	public
blacklisted	address account, bool excluded	public
_transfer	none	internal



Function Name	Parameters	Visibility
setReserveWallet	address _newWallet	external
setRewardsWallet	address _newWallet	external
setTeamWallet	address _newWallet	external
setEcoassWallet	address _newWallet	external
setMarketingWallet	address _newWallet	external
setBurnFee	uint256 _newFee	public
setReserveFee	uint256 _newFee	public
setRewardsFee	uint256 _newFee	public
setTeamFee	uint256 _newFee	public
setEcoassFee	uint256 _newFee	public
setMarketingFee	uint256 _newFee	public
changeTradingState	bool _state	external



# Statistics

## Liquidity Info

Parameter	Result
Pair Address	0xA60DDbe7c4db21e6ECaDB13a72C49d7D262b7d5A
DDC Reserves	0.00 DDC
BNB Reserves	0.00 BNB
Liquidity Value	\$0 USD

## Token (DDC) Holders Info

Parameter	Result
DDC Percentage Burnt	0.00%
DDC Amount Burnt	0 DDC
Top 10 Percentage Own	96.00%
Top 10 Amount Owned	96,000,000 DDC
Top 10 Aprox Value	\$NaN USD

## LP (DDC/BNB) Holders Info

Parameter	Result
DDC/BNB % Burnt	0.00%
DDC/BNB Amount Burnt	0 DDC
Top 10 Percentage Owned	0.00%
Top 10 Amount Owned	0 DDC
Locked Tokens Percentage	0.00%
Locked Tokens Amount	0 DDC

\* All the data displayed above was taken on-chain at block 17862476

\* The tokens on industry-standard burn wallets are not included on the top 10 wallets calculations

## Liquidity Ownership

The token does not have liquidity at the moment of the audit, block 17862476

# KISHIELD



## Disclaimer

KISHIELD has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocacy for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and KISHIELD is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will KISHIELD or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

The assessment services provided by KISHIELD is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.