



# SAFEFAIRMOON

**Audit Report For:**

**Royal Protocol**



# Smart Contract Security Audit

## Audit details:

Audited project: Royal Protocol

Client address: 0xcbcB497D505469F34463BBd5490CC46aE43f81cA

Blockchain: Binance Smart Chain

Project website: <https://royalprotocal.com/>

# Disclaimer: Standard Token Audit

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.

Standard Token Audit Report – Our Standard Token audit reports are specifically tailored to standardized launches on IDO platforms such as DxSale. As standard token launches are defined code with no variation we perform and analysis of the underlying code for vulnerabilities. These tokens are managed by the IDO in the token deployment and presale phase and the token owner remains the IDO platform.

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

SafeFairMoon was commissioned by Royal Protocol to perform an audit of smart contracts:

- <https://bscscan.com/address/0xcbcB497D505469F34463BBd5490CC46aE43f81cA#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.

# Contract Details:

Token Contract details as of 05/03/21

Contract name:	Royal Protocol
Contract address:	0xcbcB497D505469F34463BBd5490CC46aE43f81cA
Total supply:	5,579,730,000,000.000
Liquidity Locked:	Yes
Liquidity Locked Until:	04/15/22
Proof of Liquidity Lock	<a href="https://dxsale.app/app/pages/dxlockview?id=124&amp;add=0&amp;type=lpdx&amp;chain=BSC">https://dxsale.app/app/pages/dxlockview?id=124&amp;add=0&amp;type=lpdx&amp;chain=BSC</a>
Token ticker:	ROY
Decimals:	18
Token holders:	454
Transactions count:	2092
Top 100 holders dominance:	97.28%
Pancake Swap Holding %	3.1573%
Tokens Locked	53.76%
Locked Until	Vesting Schedule see <a href="#">Appendix A</a>
Contract deployer address:	0x82B9F1dCBF5e62d79ae22775A7657568E1403782
Contract's current owner:	0x82B9F1dCBF5e62d79ae22775A7657568E1403782
Ownership Renounced Tx:	No - owner is DxSale as is standard for their standard token launch
PancakeSwap pair:	0x9b67167268476a443fd7e3cfa0fb2b260743e2a2
PancakeSwap router:	0x05ff2b0db69458a0750badebc4f9e13add608c7f
Deployed at transaction:	0xa27d4334a532abc87af270a07782b5d658864a5d9bba18951ae3a06325fe98d2

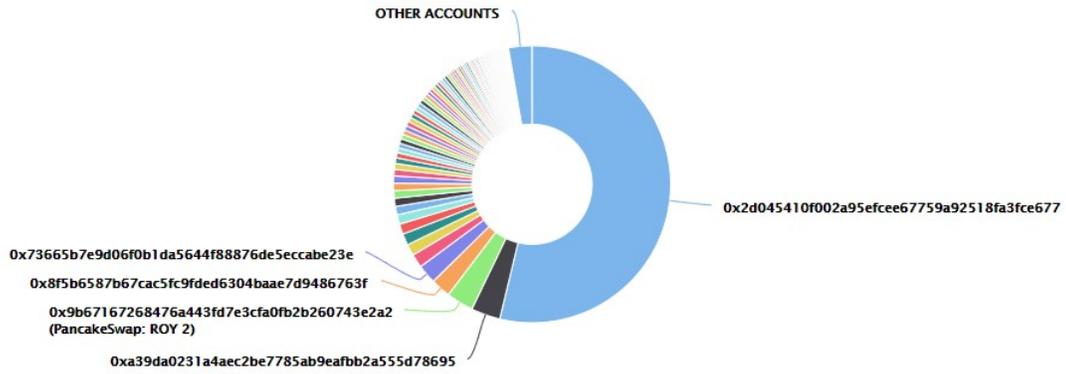
# Royal Protocol Token Distribution

The top 100 holders collectively own 97.28% (5,427,874,835,731.31 Tokens) of Royal

Token Total Supply: 5,579,730,000,000.00 Token | Total Token Holders: 454

## Royal Top 100 Token Holders

Source: BscScan.com



(A total of 5,427,874,835,731.31 tokens held by the top 100 accounts from the total supply of 5,579,730,000,000.00 token)

# Code Analysis: Standard Launch

The Royal Protocol is a standard launched token from DxSale BSC launchpad. This is a one-stop-solution where DxSale manages both the token deployment and presale. DxSale also keeps contract ownership after token is deployed.

The token itself is a standard ERC20 token with freeze and mint functions. These types of functions are usually characterized as being code associated with rug pull. Rug pulls are defined as when a contract owner or owner of liquidity pool pulls the liquidity from an exchange leaving investors unable to sell. Colloquially it can also mean the contract owner or dev minting new coins or freezing all trading leaving investors holding the bag. In the case of Royal Protocol, as it is a DxSale standard token launch, the token does not allow use of these functions after deployment. This is the result of DxSale retaining contract ownership and the functions being disabled after initial minting and finalization occurs.

Mint functions can be used to create new tokens and freeze functions can be used to freeze the balance for an address rendering the address owner to be unable to transfer the amount. For this token the freeze function is incorporated together with a mint function to mint new tokens to an address and freeze them for a specific amount of time.

To ensure investors' safety it is therefore important that these functions are not accessible to anyone, even the owner.

For a DxSale standard presale the minting function is only used during the presale where tokens corresponding to each contributors' amount is minted. When the presale is finalized the mintingFinished variable is set to true. Any instance of the minting function checks if this variable is false so new tokens cannot ever be minted. This variable can not be set back to true once set to false. The minting function is also blocked by the fact that DxSale retain ownership.

Regarding the freeze function, it would only be accessible through the mintAndFreeze call which will be blocked by the fact that mintingFinished is already set to true.

SafeFairMoon has gained reasonable assurance this contract itself does not contain any known bugs resulting in inherent risk for prospective investors. However investors should take caution and monitor the individual wallets with a significant amount of the supply. SafeFairMoon gives the Royal Protocol contract an Unqualified Opinion.

1. Unqualified opinion - clean report.
2. Qualified opinion - qualified report i.e. contract is fairly presented with exception of specified area.
3. Disclaimer of opinion - disclaimer report i.e. assessment was not able to be made due restrictions in scope or lack of information provided by client.
4. Adverse opinion - adverse audit report i.e. severe deficiencies that client's contract is misrepresented, misstated, and do not accurately reflect claims by client.

## **SafeFairMoon note:**

*Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness, team, 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.*

# Security Issues:

## Critical Issues:

No high severity issues found.

## High Severity Issues:

No high severity issues found.

## Medium Severity Issues:

No medium severity issues found.

## Low Severity Issues:

No Low severity issues found.

Note: As this was a pre-launch token ownership is not renounced, SafeFairMoon makes no claim of contract integrity if any changes are applied after the time the contract snapshot was taken.

# Conclusion:

As this is a DxSale Standard Launch analysis was conducted on the DxSale standard code for token launches. SafeFairMoon validated there were no apparent flaws in the DxSale standard token launch process with the minting and freezing functions disabled. In addition, as DxSale retains ownership there is no risk of the Devs of the token changing the code to re-enable the minting function or conduct any other changes.

SafeFairMoon reviewed the token holders list and found 53.78% of tokens locked within DxLocker amounting to 3trillion tokens. These tokens will be released to the developers are a vesting schedule with the first release scheduled for October 28th 2021 (See [Appendix A: Vesting Schedule](#) for details). Therefore we can assess there is not a significant risk to investors of developers 'dumping' the token on investors before that date.. Investors should take caution and these monitor the vesting schedule.

SafeFairMoon was able to validate that liquidity is locked via DxLocker until 04/15/2022. Therefore the risk of the owners of the LP tokens 'rugging' investors, characterized as pulling liquidity and leaving investors unable to sell is significantly reduced until that date.

SafeFairMoon in their analysis of the DxSale Standard Launch contract and the DxSale Standard Launch process found no issues with the contract itself. SafeFairMoon has gained reasonable assurance this contract itself is does not contain any known bugs resulting in inherent risk for prospective investors of Royal Protocol. Therefore SafeFairMoon gives the Royal Protocol contract an Unqualified Opinion.

1. Unqualified opinion - clean report.
2. Qualified opinion - qualified report i.e. contract is fairly presented with exception of specified area.
3. Disclaimer of opinion - disclaimer report i.e. assessment was not able to be made due restrictions in scope or lack of information provided by client.
4. Adverse opinion - adverse audit report i.e. sever deficiencies that client's contract is misrepresented, misstated, and do not accurately reflect claims by client.

## SafeFairMoon 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.*

# Appendix A: Vesting Schedule

<https://dxsale.app/app/pages/dxlockview?id=0&add=0xa3bc0836109f42170A70C68490187012cdA8a817&type=tokenlock&chain=BSC>

← **Token Locker** ↗

  
ROY  
**Royal**

ROY ADDRESS ↗

**DxLock Certified Token Locker**

  
**725:01:01:36**  
4 remaining payouts!

Total Supply	5579730000000
Tokens in Locker	3000000000000.0000
100% Unlock Date	28 Apr 2023 at 16:19
Number of Vests	4

## Vesting Schedule

Vesting Period	Estimated Release Date	Tokens Released
1	28 Oct 2021 at 04:40	750000000000.0000
2	28 Apr 2022 at 16:33	1500000000000.0000
3	28 Oct 2022 at 04:26	2250000000000.0000
4	28 Apr 2023 at 16:19	3000000000000.0000