

The background is a dark navy blue. It features several abstract geometric elements: a green horizontal bar at the top left with white wavy lines; a blue vertical bar on the left; a blue circle in the upper right; a green vertical bar on the right; a purple vertical bar on the left; a teal horizontal bar at the bottom; and a green circular arc on the right. White wavy lines also appear at the bottom right.

# KISHIELD

Security Audit

## **Tres Leches Cake Token**

January 27, 2022



# Table of Contents

- 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 (onlyOwner)
- 5 Important Notes To The Users**
- 6 Statistics**
  - 6.1 Liquidity
  - 6.2 Token Holders
  - 6.3 Liquidity Holders
- 7 Liquidity Ownership**
- 8 Disclaimer**



# Audit Summary

This report has been prepared for Tres Leches Cake Token on the Binance Smart 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	0x106feff621a395043b21a602d4b6a2039e16bbec
Name	Tres Leches Cake
Token Tracker	Tres Leches Cake (3LechesCake)
Decimals	9
Supply	1,000,000,000,000
Platform	Binance Smart Chain
compiler	v0.8.7+commit.e28d00a7
Optimization	Yes with 200 runs
LicenseType	
Language	Solidity
Codebase	<a href="https://bscscan.com/address/0x106feff621a395043b21a602d4b6a2039e16bbec#code">https://bscscan.com/address/0x106feff621a395043b21a602d4b6a2039e16bbec#code</a>
Url	<a href="https://tresleches.finance">https://tresleches.finance</a>

## Main Contract Assessed

Name	Contract	Live
Tres Leches Cake	0x106feff621a395043b21a602d4b6a2039e16bbec	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 Tres Leches Cake 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 0x063f608bD5eF234F937BAb2B78218A939589CA3E 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.

## Privileged Functions (onlyOwner)

Function Name	Parameters	Visibility
clearStuckBalance	uint256 amountPercentage	external
updateBuyFees	uint256 busdReward, uint256 marketing, uint256 liquidity, uint256 scholarship	public
updateSellFees	uint256 busdReward, uint256 marketing, uint256 liquidity, uint256 scholarship	public
tradingStatus	bool _status	public
whitelistPreSale	address _preSale	public
swapBackInBnb	none	internal
setIsDividendExemptBusd	address holder, bool exempt	external
setIsFeeExempt	address holder, bool exempt	external
setFeeReceivers	address _marketingFeeReceiver, address _devFeeReceiver, address _scholarshipFeeReceiver	external
setSwapBackSettings	bool _enabled, uint256 _amount	external
setDistributionCriteriaBusd	uint256 _minPeriod, uint256 _minDistribution	external
setDistributorSettings	uint256 gas	external

## Important Notes To The Users:

- The owner can change the busdReward, liquidity, marketing and scholarship fees realated to buy and sell
- The owner can send a percentage of the BNB of the contract to himself.
- The owner can change the Trading Status.
- The owner can change the distribution setting and criteria.
- The owner can include/exclude addresses from fees and dividents.
- No high-risk Exploits Were Found in the Source Code.





# Statistics

## Liquidity Info

Parameter	Result
Pair Address	0x84f2eba9F77A3ac7d5A2E8256186E1e3C108F2f7
3LechesCake Reserves	364807763002.98 3LechesCake
BNB Reserves	13.23 BNB
Liquidity Value	\$4,814.397 USD

## Token (3LechesCake) Holders Info

Parameter	Result
3LechesCake Percentage Burnt	10.00%
3LechesCake Amount Burnt	100,000,000,000 3LechesCake
Top 10 Percentage Own	79.60%
Top 10 Amount Owned	795,983,678,812.213 3LechesCake
Top 10 Aprox Value	\$10,504.660 USD

## LP (3LechesCake/BNB) Holders Info

Parameter	Result
3LechesCake/BNB % Burnt	0.00%
3LechesCake/BNB Amount Burnt	0 3LechesCake
Top 10 Percentage Owned	100.00%
Top 10 Amount Owned	69.376 3LechesCake
Locked Tokens Percentage	99.94%
Locked Tokens Amount	69.336 3LechesCake

\* All the data displayed above was taken on-chain at block 14722506

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

## Liquidity Ownership

Most of the liquidity is currently locked, the lock can be seen here:

[https://bscscan.com/  
token/0x84f2eba9F77A3ac7d5A2E8256186E1e3C108F2f7?  
a=0x7ee058420e5937496f5a2096f04caa7721cf70cc](https://bscscan.com/token/0x84f2eba9F77A3ac7d5A2E8256186E1e3C108F2f7?a=0x7ee058420e5937496f5a2096f04caa7721cf70cc)

# 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.