RugFreeCoins Audit

Tres Leches Cake Audit

Smart Contract Security Audit

November 17, 2021

Contents

Audit details

Audited project

Tres Leches Cake Token

Contract Address

0x106FEFf621a395043b21a602D4b6a2039e16bBeC

Client contact

Tres Leches Cake Team

Blockchain

Binance smart chain

Project website

https://tresleches.finance/

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

Rugfreecoins was commissioned by Tres Leches Cake to perform an audit of the smart contract.

https://bscscan.com/token/0x106FEFf621a395043b21a602D4b6a2039e16bBeC

The focus of this audit is to verify that the smart contract is secure, resilient and working according to the specifications.

The information in this report should be used to understand the risk exposure of the smart contract, project feasibility, long term sustainability and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

About the project

Tres Leches Cake is a token built on the Binance Smart Chain. Each transaction, purchase and sale incur a 12% fee. The main goal of this token is to create a community effort to assist the feature students in having a fantastic education via scholarship donations. The token is driven by the community, and the options are endless.

Features

- The **automatic Cake rewards** will be distributed among every holder proportional to how many tokens each individual holds in values of 5% when buying and selling..

- The **sustainability fee of 3% when buying and selling for marketing and dev** is what allows Tres Leches Cake Token to hold the aforementioned promise. Tokens will be swapped into BNB and will be sent to a marketing wallet per transaction. This way, Tres Leches Cake Token will have enough funds to promote the coin and spend for future development without selling tokens as the traditional way.

- The additional component included under the sustainability section is a **liquidity fee of 2%**, which is a redistribution mechanism that ensures the trading pool always has sufficient liquidity. This is a key element for decentralized exchanges like Pancakeswap!

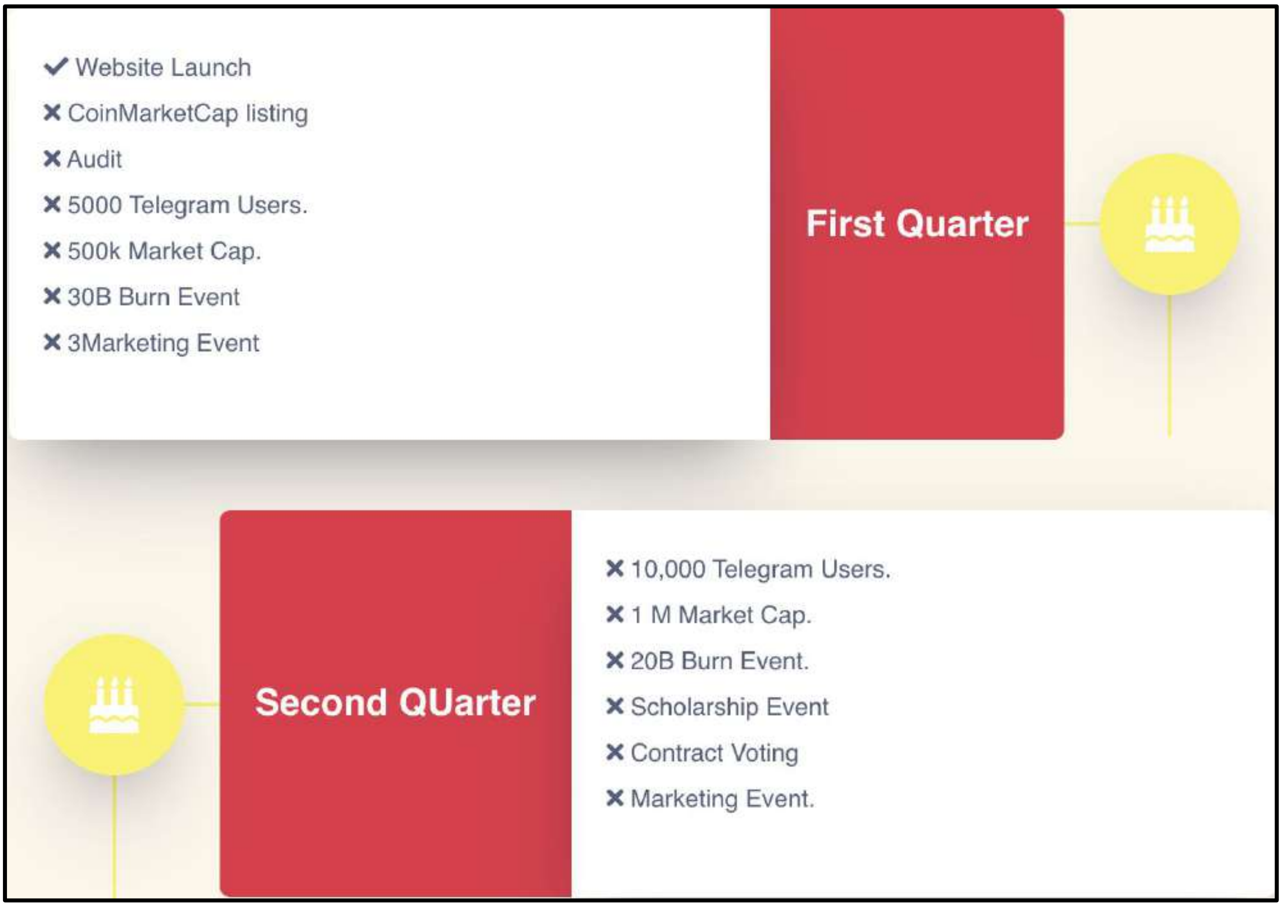
- The **scholarship fee of 2% when buying and selling for charity** is what allows Tres Leches Cake to allocate funds for the good cause. This will empower the Tres Leches Cake community in the long run, and motivate more people to join in

Tokenomics

12% fee when buying and selling

- 5% of trade goes to holders' pockets in Cake tokens.
- 3% of trade goes to Marketing & Dev wallets.
- 2% of every trade goes to the liquidity pool.
- 2% of trade goes to the scholarship wallet in tokens.

Roadmap

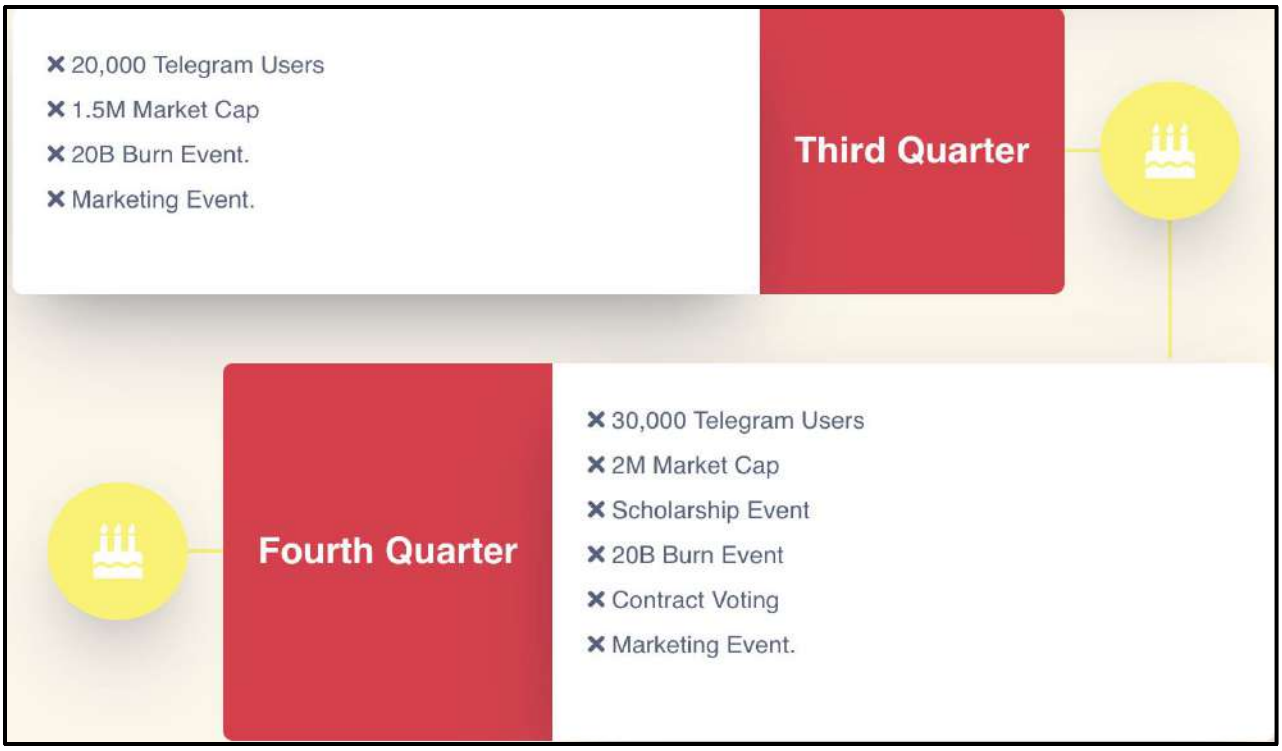


- ✓ Website Launch
- ✕ CoinMarketCap listing
- ✕ Audit
- ✕ 5000 Telegram Users.
- ✕ 500k Market Cap.
- ✕ 30B Burn Event
- ✕ 3Marketing Event

First Quarter

Second QUarter

- ✕ 10,000 Telegram Users.
- ✕ 1 M Market Cap.
- ✕ 20B Burn Event.
- ✕ Scholarship Event
- ✕ Contract Voting
- ✕ Marketing Event.



- ✕ 20,000 Telegram Users
- ✕ 1.5M Market Cap
- ✕ 20B Burn Event.
- ✕ Marketing Event.

Third Quarter

Fourth Quarter

- ✕ 30,000 Telegram Users
- ✕ 2M Market Cap
- ✕ Scholarship Event
- ✕ 20B Burn Event
- ✕ Contract Voting
- ✕ Marketing Event.

Target market and the concept

Target market

- ❖ Anyone who's interested in Crypto space with long term investment plans.
- ❖ Anyone who's ready to earn a passive income in Tres Leches Cake tokens by holding tokens.
- ❖ Anyone who's interested in trading tokens.
- ❖ Anyone who's interested in taking part with decision making of the project.
- ❖ Anyone who's interested in collecting NFTs or trading NFTs.
- ❖ Anyone who's interested in taking part with the future plans of the Tres Leches Cake token.
- ❖ Anyone who's interested in supporting a good cause. (Scholarship feature)
- ❖ Anyone who's interested in making financial transactions with any other party using Tres Leches Cake token as the currency.

Core concept

The token reward system

5% of each transaction when selling gets sent amongst all holders in cake rewards. The holders will be eligible to receive CAKE,in every one hour, and rewards are proportional to how many tokens each individual holds.

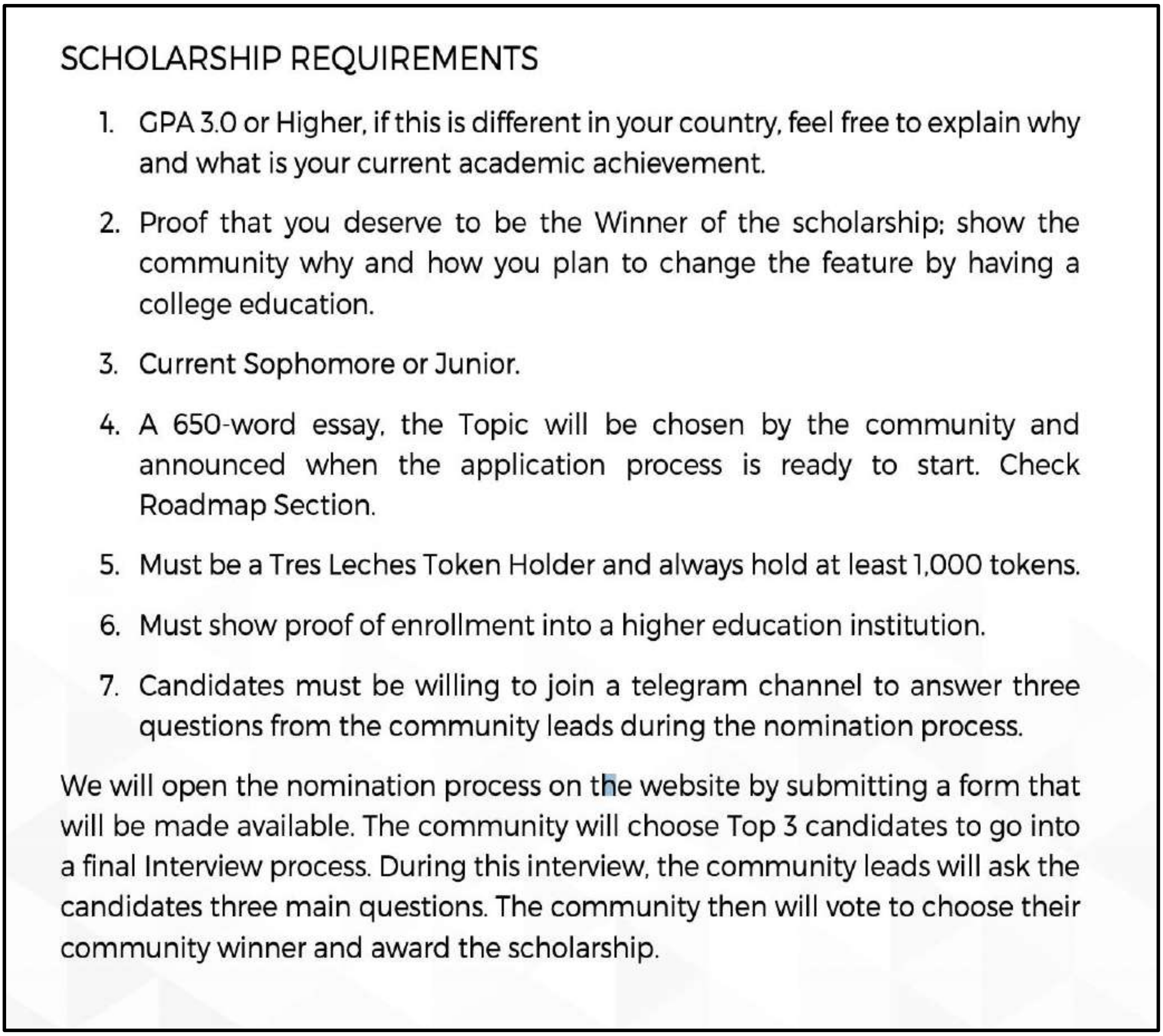
Sustainable mechanism

The **sustainability fee of 3% when buying and selling for marketing and Dev** is what allows Tres Leches Cake Token to promote the token and use funds to further development of the platform. Tokens will be swapped into BNB and will be sent to a marketing wallet per transaction. This way, Tres Leches Cake Token will have access to the funds without selling tokens as the traditional way, which will enable them to consume funds without hurting the project.

The liquidity fee of 2% when buying and selling, which is a redistribution mechanism that ensures the trading pool always has sufficient liquidity.

Good cause

2% Scholarship fee per transaction will be sent in tokens to a separate wallet.



SCHOLARSHIP REQUIREMENTS

1. GPA 3.0 or Higher, if this is different in your country, feel free to explain why and what is your current academic achievement.
2. Proof that you deserve to be the Winner of the scholarship; show the community why and how you plan to change the feature by having a college education.
3. Current Sophomore or Junior.
4. A 650-word essay, the Topic will be chosen by the community and announced when the application process is ready to start. Check Roadmap Section.
5. Must be a Tres Leches Token Holder and always hold at least 1,000 tokens.
6. Must show proof of enrollment into a higher education institution.
7. Candidates must be willing to join a telegram channel to answer three questions from the community leads during the nomination process.

We will open the nomination process on the website by submitting a form that will be made available. The community will choose Top 3 candidates to go into a final Interview process. During this interview, the community leads will ask the candidates three main questions. The community then will vote to choose their community winner and award the scholarship.

WINNER ANNOUNCEMENT

The Winner will be announced on our social media channels. After the Winner has been chosen, the Winner will have 30 days (about four and a half weeks) to present the evidence required for the award.

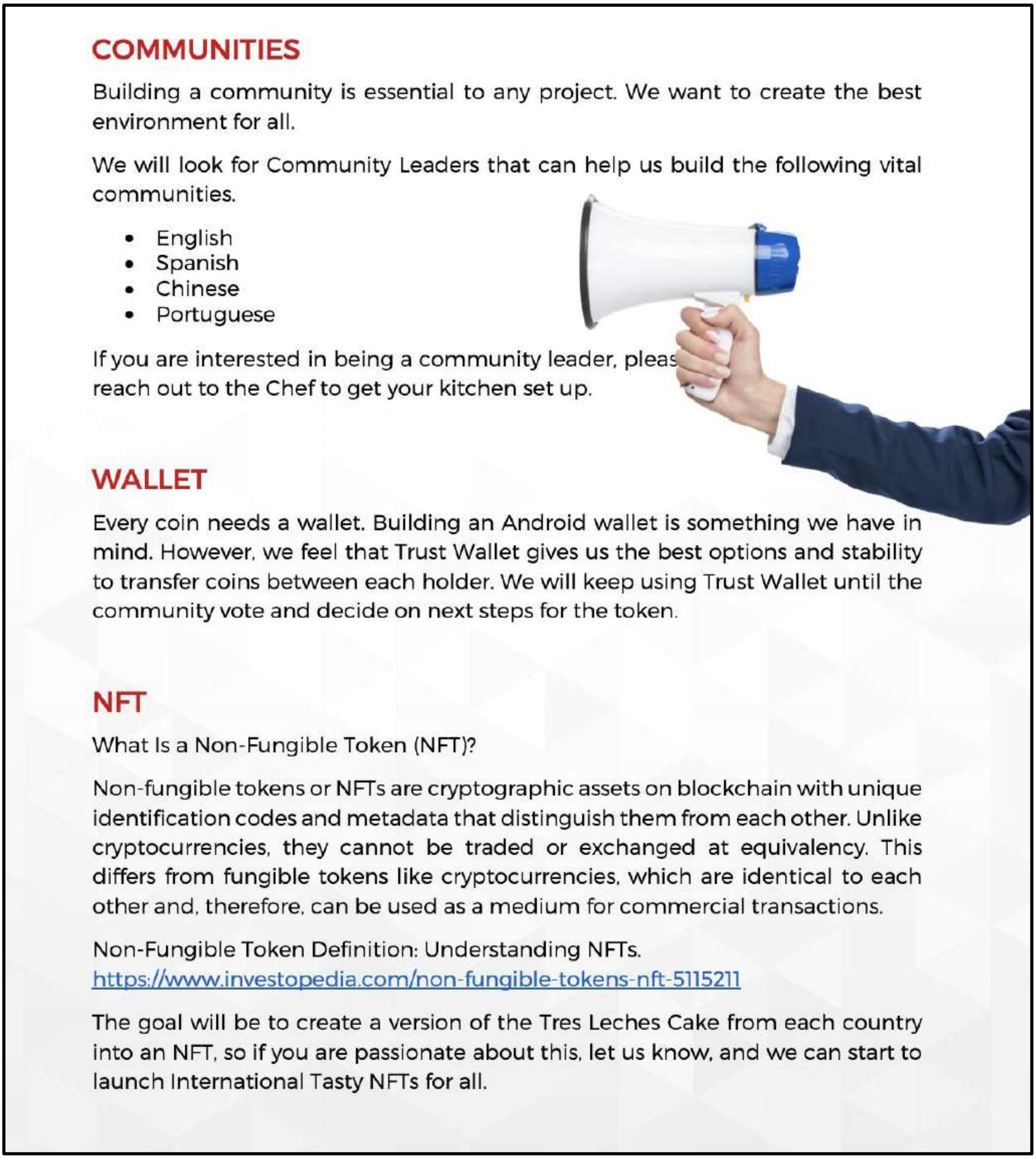
The award will be paid in BNB to the Winner, and the transaction will be made available. Why not an official check? This is the cryptocurrency world. We want to encourage all the nominees to use these methods to pay for their college education.

What is the maximum a winner can expect to win from the scholarship?

These will all depend on the cryptocurrency market and the token market cap. The money will be taken out of the scholarship wallet and converted into BNB. We should see at least 1,000 in the scholarship wallet or an equivalent to 10 Billon tokens, and if the value of 10 Billon tokens is more, then we will award that total value to the Winner.

What happens if the market cap is less than the desired amount? Then we as a community should contribute to make the first Winner of the scholarship a success. If everything fails, then the community leads will meet with the Chef and decide how to proceed. But rest assured that we will do our best to meet our goals.

Future plans



COMMUNITIES

Building a community is essential to any project. We want to create the best environment for all.

We will look for Community Leaders that can help us build the following vital communities.

- English
- Spanish
- Chinese
- Portuguese

If you are interested in being a community leader, pleas reach out to the Chef to get your kitchen set up.

WALLET

Every coin needs a wallet. Building an Android wallet is something we have in mind. However, we feel that Trust Wallet gives us the best options and stability to transfer coins between each holder. We will keep using Trust Wallet until the community vote and decide on next steps for the token.

NFT

What Is a Non-Fungible Token (NFT)?

Non-fungible tokens or NFTs are cryptographic assets on blockchain with unique identification codes and metadata that distinguish them from each other. Unlike cryptocurrencies, they cannot be traded or exchanged at equivalency. This differs from fungible tokens like cryptocurrencies, which are identical to each other and, therefore, can be used as a medium for commercial transactions.

Non-Fungible Token Definition: Understanding NFTs.
https://www.investopedia.com/non-fungible-tokens-nft-5115211

The goal will be to create a version of the Tres Leches Cake from each country into an NFT, so if you are passionate about this, let us know, and we can start to launch International Tasty NFTs for all.

Potential to grow with score points

1.	Project efficiency	9/10
2.	Project uniqueness	8/10
3	Information quality	10/10
4	Service quality	9/10
5	System quality	8/10
6	Impact on the community	10/10
7	Impact on the business	9/10
8	Preparing for the future	9/10
Total Points		**9/10**

Contract details

Token contract details for 17th November 2021

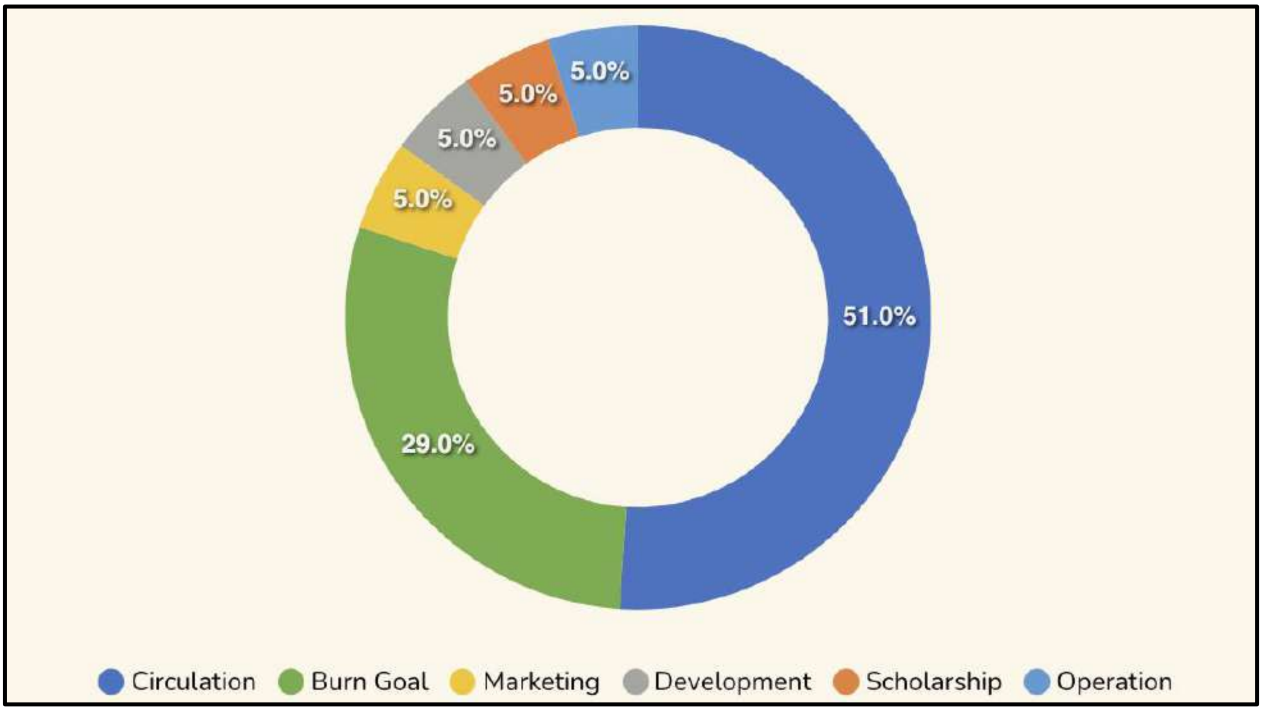
Contract name	Tres Leches Cake
Contract address	0x106FEFf621a395043b21a602D4b6a2039e16bBeC
Token supply	1,000,000,000,000
Token ticker	3LechesCake
Decimals	9
Token holders	1
Transaction count	1
Dev fee receiver	0xecc075cb2926564568f0b7c9a98ac0dc496817d1
Distributor	0xe0543d6797ea0f381bbd5dd787c33ea9540e7a08
Marketing wallet	0xacb48ee17ddfd41a3273837238d10c4680d40206
Scholarship wallet	0x558b624de1d61379e0a131c7a9c6f6d9dcc14abe
Contract deployer address	0xD9EA912E0169388dfAe2fADfEfaaca85dC505066
Contract’s current owner address	0x063f608bd5ef234f937bab2b78218a939589ca3e

Token distribution

Tokens are distributed as follows:

Total of 1 trillion tokens, with 51% of the tokens being in circulation, and the other 49% will be distributed as follows.

- ❖ Tres Leches Cake Team will add 200B to the Operations Wallet, and this will be divided into the following areas.
  - 50B for Marketing.
  - 50B for Operations.
  - 50B for Development.
  - 50B for the Scholarship Wallet.
- ❖ 290B of the remaining will be burned monthly.
  - 30B burned the first month of the token.
  - 20B will be burned every until ran out of tokens to burn.



Contract code function details

No	Category	Item	Result
1	Coding conventions	BRC20 Token standards	pass
		compile errors	pass
		Compiler version security	pass
		visibility specifiers	pass
		Gas consumption	pass
		SafeMath features	pass
		Fallback usage	pass
		tx.origin usage	pass
		deprecated items	pass
		Redundant code	pass
		Overriding variables	pass
2	Function call audit	Authorization of function call	pass
		Low level function (call/delegate call) security	pass
		Returned value security	pass
		Selfdestruct function security	pass
3	Business security	Access control of owners	pass
		Business logics	pass
		Business implementations	pass
4	Integer overflow/underflow		pass
5	Reentrancy		pass
6	Exceptional reachable state		pass
7	Transaction ordering dependence		pass
8	Block properties dependence		pass
9	Pseudo random number generator (PRNG)		pass
10	DoS (Denial of Service)		pass
11	Token vesting implementation		pass
12	Fake deposit		pass
13	Event security		pass

Contract description table

Below table represents the summary of the contracts and methods in the token contract. We scanned the whole contract and listed down all the Interfaces, functions and implementations with its visibility and mutability.

Contract	**Type**	**Bases**		
└	Function Name	Visibility	Mutability	Modifiers
Tresleches	**Implementation**	**IERC20, Ownable**		
└		Public ❗	🛑	NO❗
└		External ❗	💵	NO❗
└	totalSupply	External ❗		NO❗
└	name	Public ❗		NO❗
└	symbol	Public ❗		NO❗
└	decimals	Public ❗		NO❗
└	balanceOf	Public ❗		NO❗
└	getHolderDetailsBusd	Public ❗		NO❗
└	getLastProcessedIndexBusd	Public ❗		NO❗
└	getNumberOfTokenHoldersBusd	Public ❗		NO❗
└	totalDistributedRewardsBusd	Public ❗		NO❗
└	allowance	External ❗		NO❗

└	approve	Public ❗	🛑	NO❗
└	_approve	Internal 🔒	🛑	
└	approveMax	External ❗	🛑	NO❗
└	transfer	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
└	_transferFrom	Internal 🔒	🛑	
└	_basicTransfer	Internal 🔒	🛑	
└	shouldTakeFee	Internal 🔒		
└	takeFee	Internal 🔒	🛑	
└	shouldSwapBack	Internal 🔒		
└	clearStuckBalance	External ❗	🛑	onlyOwner
└	updateBuyFees	Public ❗	🛑	onlyOwner
└	updateSellFees	Public ❗	🛑	onlyOwner
└	tradingStatus	Public ❗	🛑	onlyOwner
└	whitelistPreSale	Public ❗	🛑	onlyOwner
└	___claimRewardsBusd	Public ❗	🛑	NO❗
└	claimProcessBusd	Public ❗	🛑	NO❗
└	swapBackInBnb	Internal 🔒	🛑	swapping

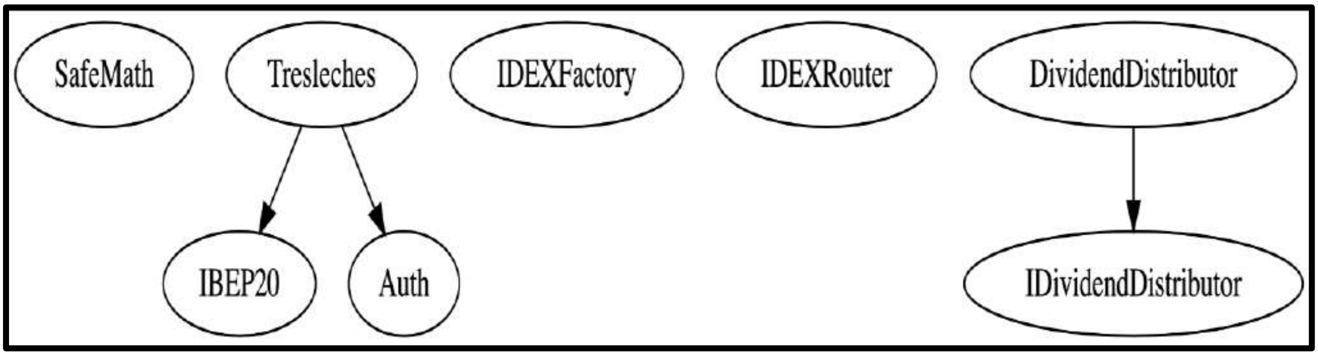
└	swapAndLiquify	Private 🔐	🛑	
└	swapTokensForEth	Private 🔐	🛑	
└	swapTokensForTokens	Private 🔐	🛑	
└	addLiquidity	Private 🔐	🛑	
└	setIsDividendExemptBusd	External ❗	🛑	onlyOwner
└	setIsFeeExempt	External ❗	🛑	onlyOwner
└	setFeeReceivers	External ❗	🛑	onlyOwner
└	setSwapBackSettings	External ❗	🛑	onlyOwner
└	setDistributionCriteriaBusd	External ❗	🛑	onlyOwner
└	setDistributorSettings	External ❗	🛑	onlyOwner
IUniswapV2Router01	**Interface**			
└	factory	External ❗		NO❗
└	WETH	External ❗		NO❗
└	addLiquidity	External ❗	🛑	NO❗
└	addLiquidityETH	External ❗	💵	NO❗
└	removeLiquidity	External ❗	🛑	NO❗
└	removeLiquidityETH	External ❗	🛑	NO❗

L	removeLiquidityWithPermit	External ❗	🛑	NO❗
L	removeLiquidityETHWithPermit	External ❗	🛑	NO❗
L	swapExactTokensForTokens	External ❗	🛑	NO❗
L	swapTokensForExactTokens	External ❗	🛑	NO❗
L	swapExactETHForTokens	External ❗	💵	NO❗
L	swapTokensForExactETH	External ❗	🛑	NO❗
L	swapExactTokensForETH	External ❗	🛑	NO❗
L	swapETHForExactTokens	External ❗	💵	NO❗
L	quote	External ❗		NO❗
L	getAmountOut	External ❗		NO❗
L	getAmountIn	External ❗		NO❗
L	getAmountsOut	External ❗		NO❗
L	getAmountsIn	External ❗		NO❗

Legend

Symbol	Meaning
🛑	**Function can modify state**
💵	**Function is payable**

Inheritance Hierarchy



Security issue checking status

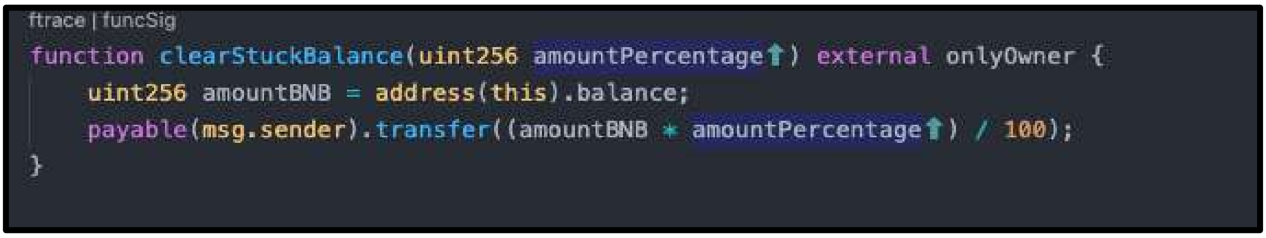
- **High severity issues**
  No high severity issues found.

- **Medium severity issues**
  No medium severity issues found.

- **Low severity issues**
  No low severity issues found

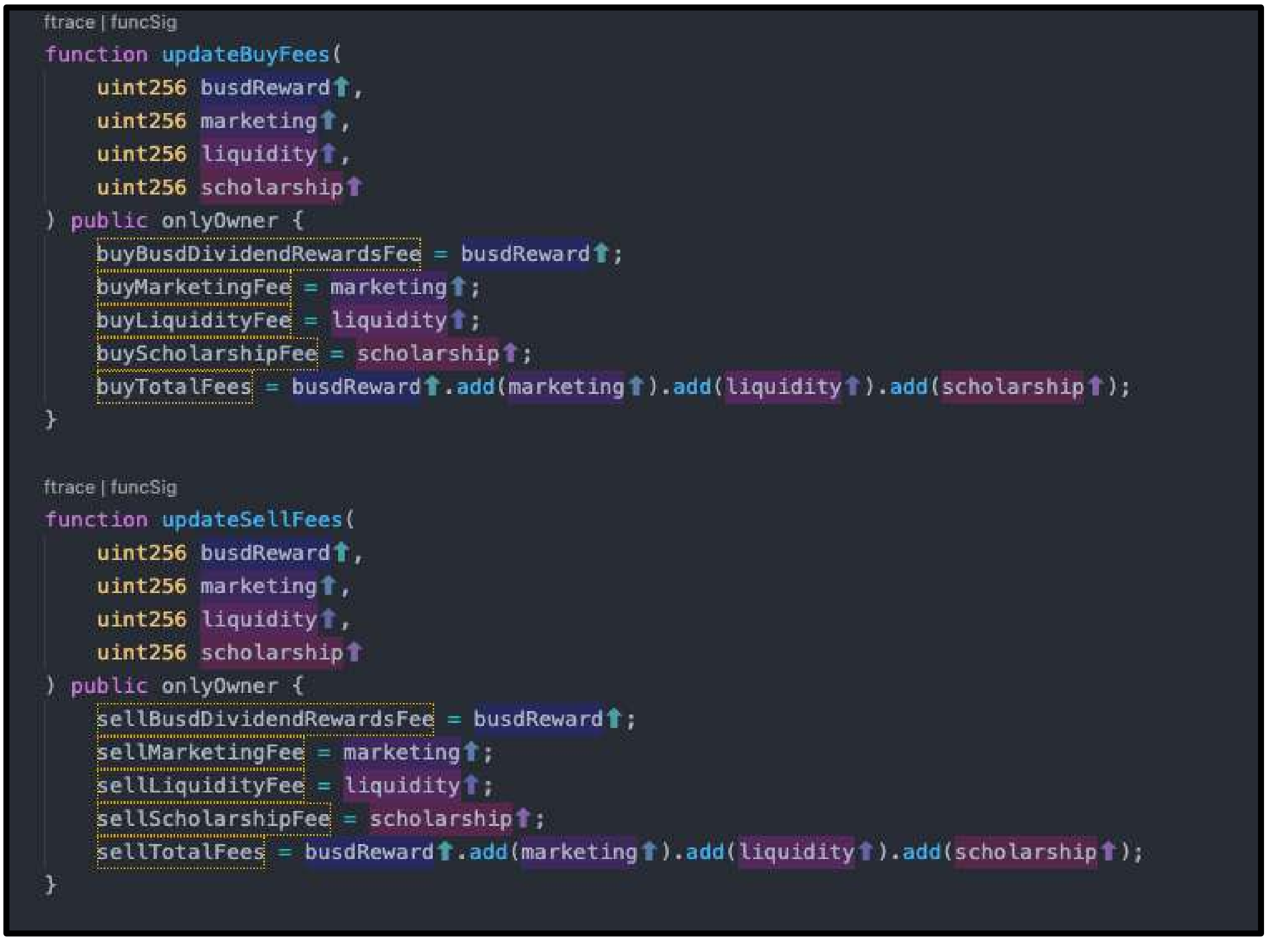
Owner privileges

- The owner can get contract stuck BNB balance to the owner wallet.



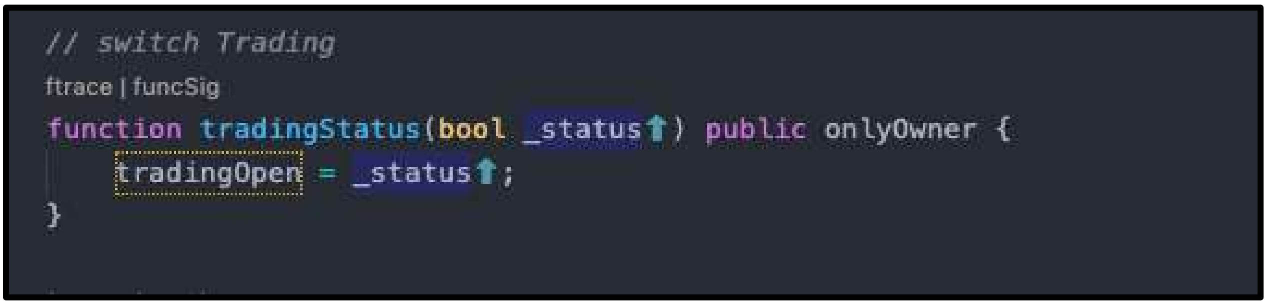
```
ftrace | funcSig
function clearStuckBalance(uint256 amountPercentage) external onlyOwner {
    uint256 amountBNB = address(this).balance;
    payable(msg.sender).transfer((amountBNB * amountPercentage) / 100);
}
```

- The owner can change all buy and sell fees.



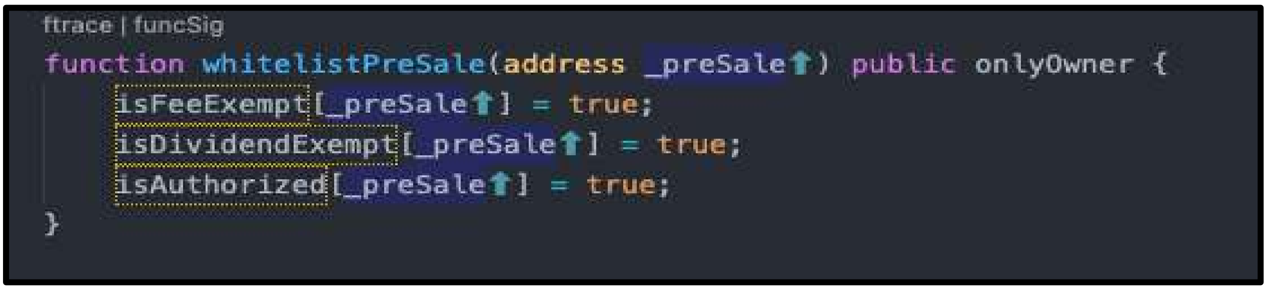
```
ftrace | funcSig
function updateBuyFees(
    uint256 busdReward,
    uint256 marketing,
    uint256 liquidity,
    uint256 scholarship
) public onlyOwner {
    buyBusdDividendRewardsFee = busdReward;
    buyMarketingFee = marketing;
    buyLiquidityFee = liquidity;
    buyScholarshipFee = scholarship;
    buyTotalFees = busdReward.add(marketing).add(liquidity).add(scholarship);
}

ftrace | funcSig
function updateSellFees(
    uint256 busdReward,
    uint256 marketing,
    uint256 liquidity,
    uint256 scholarship
) public onlyOwner {
    sellBusdDividendRewardsFee = busdReward;
    sellMarketingFee = marketing;
    sellLiquidityFee = liquidity;
    sellScholarshipFee = scholarship;
    sellTotalFees = busdReward.add(marketing).add(liquidity).add(scholarship);
}
```

- The owner can enable/disable trading.



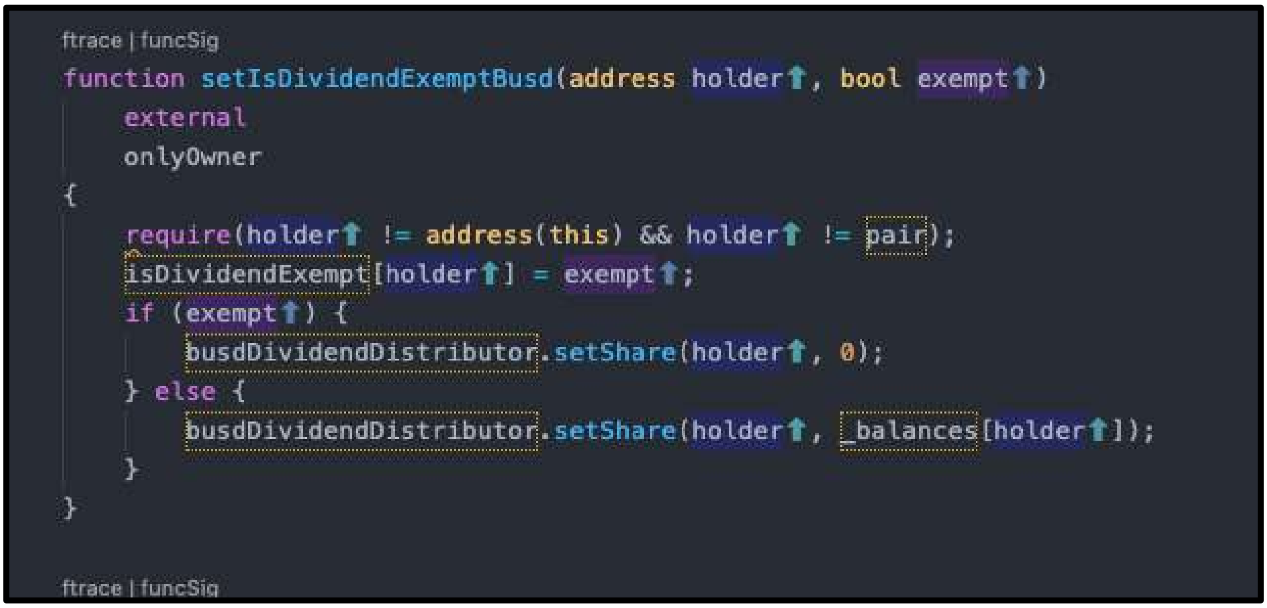
```
// switch Trading
ftrace | funcSig
function tradingStatus(bool _status) public onlyOwner {
    tradingOpen = _status;
}
```

- The owner can whitelist pre-sale.



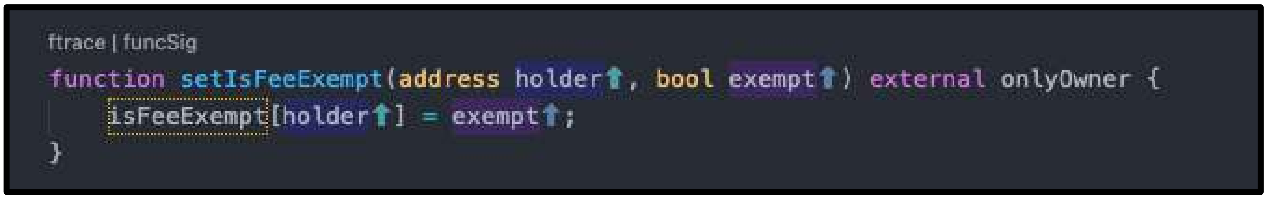
```
function whitelistPreSale(address _preSale) public onlyOwner {
    isFeeExempt[_preSale] = true;
    isDividendExempt[_preSale] = true;
    isAuthorized[_preSale] = true;
}
```

- The owner can exclude wallets from rewards.



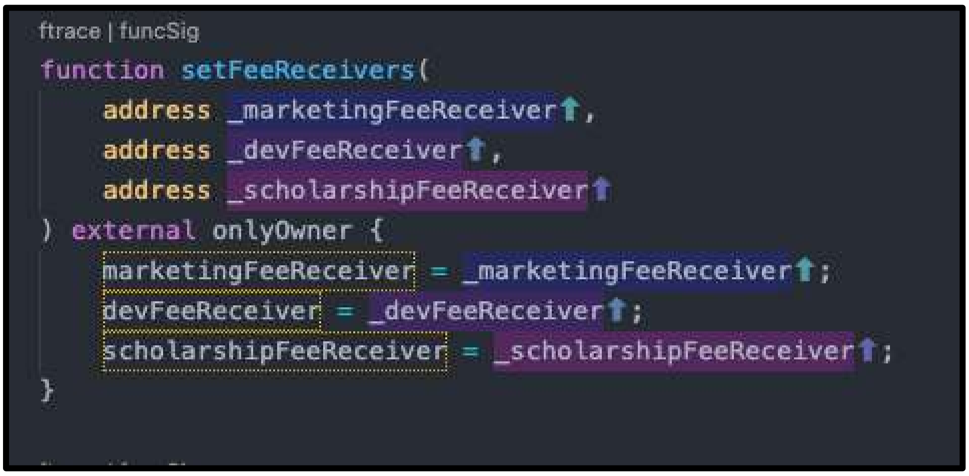
```
function setIsDividendExemptBusd(address holder, bool exempt)
    external
    onlyOwner
{
    require(holder != address(this) && holder != pair);
    isDividendExempt[holder] = exempt;
    if (exempt) {
        busdDividendDistributor.setShare(holder, 0);
    } else {
        busdDividendDistributor.setShare(holder, _balances[holder]);
    }
}
```

- The owner can exclude wallets from fees.



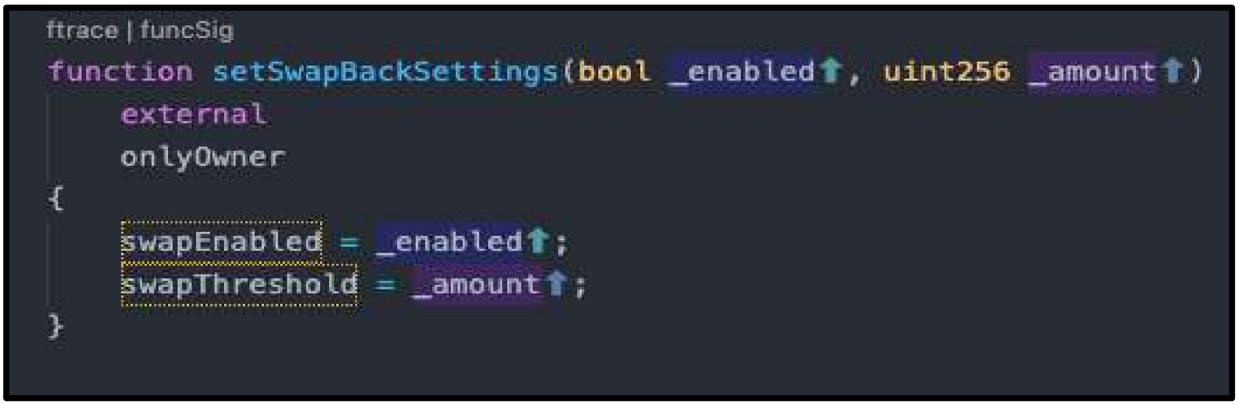
```
function setIsFeeExempt(address holder, bool exempt) external onlyOwner {
    isFeeExempt[holder] = exempt;
}
```

- The owner can change all fee receivers.



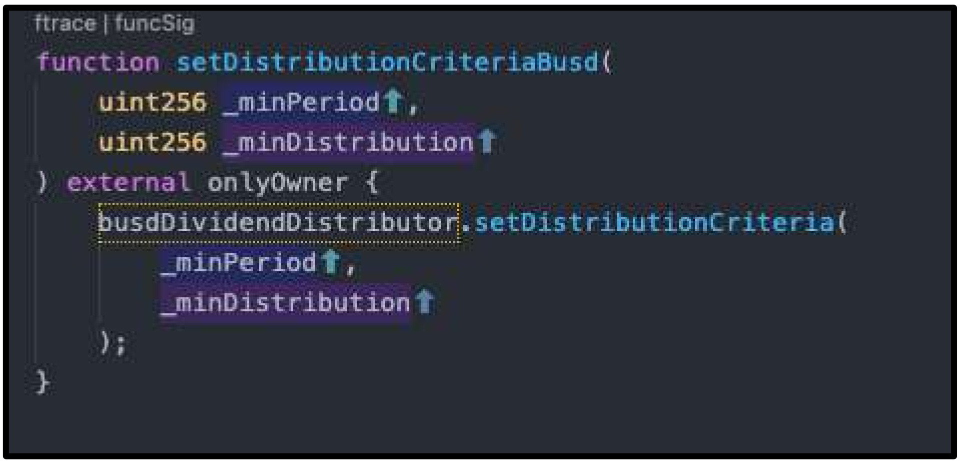
```
function setFeeReceivers(
    address _marketingFeeReceiver,
    address _devFeeReceiver,
    address _scholarshipFeeReceiver
) external onlyOwner {
    marketingFeeReceiver = _marketingFeeReceiver;
    devFeeReceiver = _devFeeReceiver;
    scholarshipFeeReceiver = _scholarshipFeeReceiver;
}
```

- The owner can enable/disable swapping and can change swap point.



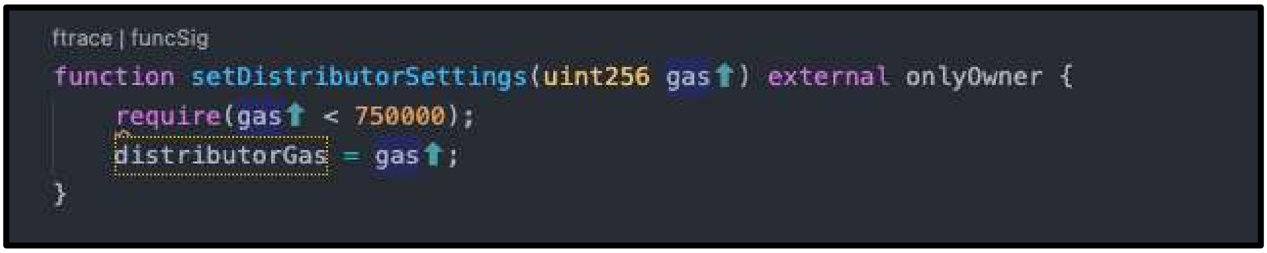
```
function setSwapBackSettings(bool _enabled, uint256 _amount)
    external
    onlyOwner
{
    swapEnabled = _enabled;
    swapThreshold = _amount;
}
```

- The owner can change minimum reward distribution time and minimum reward amount.



```
function setDistributionCriteriaBusd(
    uint256 _minPeriod,
    uint256 _minDistribution
) external onlyOwner {
    busdDividendDistributor.setDistributionCriteria(
        _minPeriod,
        _minDistribution
    );
}
```

- The owner can change max gas limit for reward distribution maximum up to 750000.



```
function setDistributorSettings(uint256 gas) external onlyOwner {
    require(gas < 750000);
    distributorGas = gas;
}
```

Audit conclusion

While conducting the audit of the Tres Leches Cake smart contract, it was observed that there is nothing alarming with the code.