



TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

August, 2021

Audit Details



Audited project

CAKE BANK



Deployer address

0x51a19a45a6a714af580ef083e2c1486b097ddbaa



Client contacts:

CAKE BANK team



Blockchain

Binance Smart Chain



Project website:

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

TechRate was commissioned by CAKE BANK to perform an audit of smart contracts:

<https://bscscan.com/address/0x5f1b95784a033cd6842cf26eb9a9687f91ad9e78#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.

Contracts Details

Token contract details for 27.08.2021

Contract name	CAKE BANK
Contract address	0x5F1b95784a033CD6842cf26eb9A9687F91Ad9e78
Total supply	100,000,000,000
Token ticker	CAKEBANK
Decimals	18
Token holders	5,151
Transactions count	23,211
Top 100 holders dominance	94.17%
Liquidity fee	1
Cake reward fee	8
Marketing fee	4
Total dividends distributes	12084419278370012468132
Dividend tracker	0x71c177672e876f3302d6370771e65c40681ea4e0
Uniswap V2 pair	0x2f308f3c6994fc1ed690a318f07d67564dcc5aab
Contract deployer address	0x51a19a45a6a714af580ef083e2c1486b097ddbaa
Contract's current owner address	0x51a19a45a6a714af580ef083e2c1486b097ddbaa

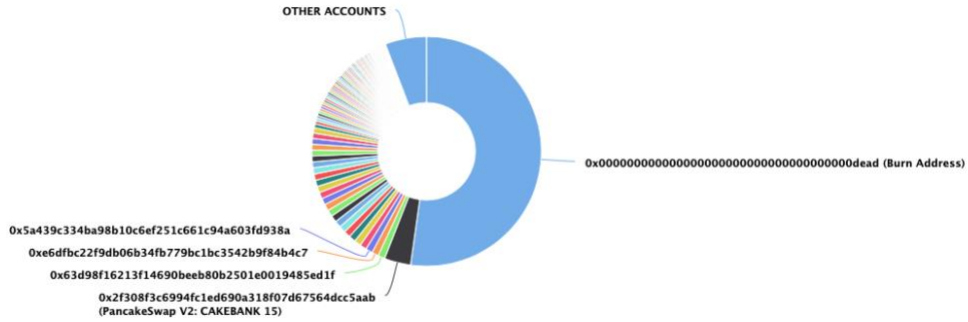
CAKE BANK Token Distribution

The top 100 holders collectively own 94.17% (94,172,830,017.46 Tokens) of CAKE BANK

Token Total Supply: 100,000,000,000.00 Token | Total Token Holders: 5,151

CAKE BANK Top 100 Token Holders

Source: BscScan.com



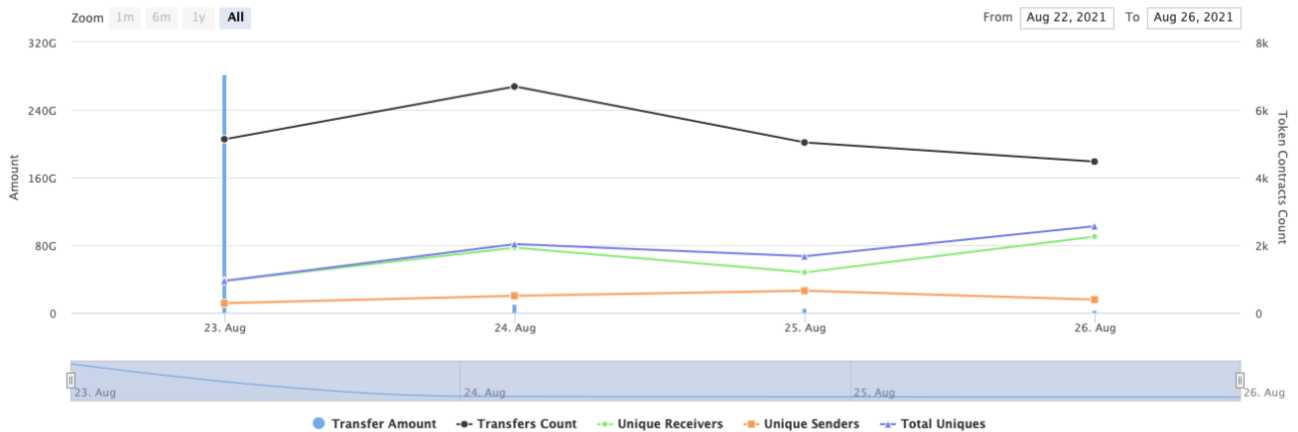
(A total of 94,172,830,017.46 tokens held by the top 100 accounts from the total supply of 100,000,000,000.00 token)

CAKE BANK Contract Interaction Details


Time Series: Token Contract Overview

Mon 23, Aug 2021 - Thu 26, Aug 2021



Token Contract 0x5f1b95784a033cd6842cf26eb9a9687f91ad9e78 (CAKE BANK)
Source: BscScan.com



CAKE BANK Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Burn Address	52,227,719,003.744985218466167791	52.2277%
2	 PancakeSwap V2: CAKEBANK 15	3,723,545,769.162376792632945063	3.7235%
3	0x63d98f16213f14690beeb80b2501e0019485ed1f	969,108,416.454466268895649062	0.9691%
4	0xe6dfbc22f9db06b34fb779bc1bc3542b9f84c7	965,483,428.446546180084772305	0.9655%
5	0x5a439c334ba98b10c6ef251c661c94a603fd938a	960,096,437.223748222043093051	0.9601%
6	0xa9c0178f0acd9ce72cb03443975f2ada6e19ab03	958,922,970.784164565958092822	0.9589%
7	0xeea4d15eef11fb11600e5e445b0fe8bc7292d3f8	957,214,778.908034753295436731	0.9572%
8	0x1d0cac1f0828097b763dfd6c134ddc7cefbd06	953,101,529.651857282753745105	0.9531%
9	0xdb82abe5ce8aef545fb7d22fe88e0edf8801afd	948,091,874.875680883394547211	0.9481%
10	0x81826c989b78e55f29c69c0f31de1206eff6a6d0	947,610,623.790213638040545464	0.9476%

CAKE BANK Top 10 LP Token Holders

Rank	Address	Quantity	Percentage
1	 0x0c89c0407775dd89b12918b9c0aa42b96518820	1,183,215.956619923208512465	79.6408%
2	 0x00	294,965.966050648281587068	19.8538%
3	0x8cc7bc33f5188b1fb683bedc4dbffa77b136833b	7,279.797467820202002333	0.4900%
4	0xffec5e719fd3d126ddd40a569d1d0237a405acc	98.590661920710084164	0.0066%
5	0x960d1fb94a7ed974e9eb380782953f106dbf9c17	67.46316009077644926	0.0045%
6	0xe77398de43513fe789cdb645b9219fa093e5660c	36.825295666880701127	0.0025%
7	0x0753cfb0dad1b51235c31d10187dd7b577bcf9c	19.108337172584108823	0.0013%
8	0x6f2dc8e02a1b3a086f54f8d791ad71b39c9547d6	7.794391457465680418	0.0005%



Contract functions details

- + [Lib] SafeMathUint
 - [Int] toInt256Safe
- + [Lib] SafeMathInt
 - [Int] mul
 - [Int] div
 - [Int] sub
 - [Int] add
 - [Int] abs
 - [Int] toUint256Safe
- + [Lib] SafeMath
 - [Int] add
 - [Int] sub
 - [Int] sub
 - [Int] mul
 - [Int] div
 - [Int] div
 - [Int] mod
 - [Int] mod
- + Ownable (Context)
 - [Pub] <Constructor> #
 - [Pub] owner
 - [Pub] renounceOwnership #
 - modifiers: onlyOwner
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
- + [Int] IUniswapV2Router01
 - [Ext] factory
 - [Ext] WETH
 - [Ext] addLiquidity #
 - [Ext] addLiquidityETH (\$)
 - [Ext] removeLiquidity #
 - [Ext] removeLiquidityETH #
 - [Ext] removeLiquidityWithPermit #
 - [Ext] removeLiquidityETHWithPermit #
 - [Ext] swapExactTokensForTokens #
 - [Ext] swapTokensForExactTokens #
 - [Ext] swapExactETHForTokens (\$)
 - [Ext] swapTokensForExactETH #
 - [Ext] swapExactTokensForETH #
 - [Ext] swapETHForExactTokens (\$)
 - [Ext] quote
 - [Ext] getAmountOut
 - [Ext] getAmountIn
 - [Ext] getAmountsOut
 - [Ext] getAmountsIn
- + [Int] IUniswapV2Router02 (IUniswapV2Router01)

- [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
 - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
 - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
 - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens (\$)
 - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
- + [Int] IUniswapV2Pair
- [Ext] name
 - [Ext] symbol
 - [Ext] decimals
 - [Ext] totalSupply
 - [Ext] balanceOf
 - [Ext] allowance
 - [Ext] approve #
 - [Ext] transfer #
 - [Ext] transferFrom #
 - [Ext] DOMAIN_SEPARATOR
 - [Ext] PERMIT_TYPEHASH
 - [Ext] nonces
 - [Ext] permit #
 - [Ext] MINIMUM_LIQUIDITY
 - [Ext] factory
 - [Ext] token0
 - [Ext] token1
 - [Ext] getReserves
 - [Ext] price0CumulativeLast
 - [Ext] price1CumulativeLast
 - [Ext] kLast
 - [Ext] mint #
 - [Ext] burn #
 - [Ext] swap #
 - [Ext] skim #
 - [Ext] sync #
 - [Ext] initialize #
- + [Int] IUniswapV2Factory
- [Ext] feeTo
 - [Ext] feeToSetter
 - [Ext] getPair
 - [Ext] allPairs
 - [Ext] allPairsLength
 - [Ext] createPair #
 - [Ext] setFeeTo #
 - [Ext] setFeeToSetter #
- + [Lib] IterableMapping
- [Pub] get
 - [Pub] getIndexOfKey
 - [Pub] getKeyAtIndex
 - [Pub] size
 - [Pub] set #
 - [Pub] remove #
- + [Int] IERC20Metadata (IERC20)
- [Ext] name

- [Ext] symbol
- [Ext] decimals
- + [Int] IERC20
 - [Ext] totalSupply
 - [Ext] balanceOf
 - [Ext] transfer #
 - [Ext] allowance
 - [Ext] approve #
 - [Ext] transferFrom #
- + ERC20 (Context, IERC20, IERC20Metadata)
 - [Pub] <Constructor> #
 - [Pub] name
 - [Pub] symbol
 - [Pub] decimals
 - [Pub] totalSupply
 - [Pub] balanceOf
 - [Pub] transfer #
 - [Pub] allowance
 - [Pub] approve #
 - [Pub] transferFrom #
 - [Pub] increaseAllowance #
 - [Pub] decreaseAllowance #
 - [Int] _transfer #
 - [Int] _mint #
 - [Int] _burn #
 - [Int] _approve #
 - [Int] _beforeTokenTransfer #
- + [Int] DividendPayingTokenOptionalInterface
 - [Ext] withdrawableDividendOf
 - [Ext] withdrawnDividendOf
 - [Ext] accumulativeDividendOf
- + [Int] DividendPayingTokenInterface
 - [Ext] dividendOf
 - [Ext] withdrawDividend #
- + DividendPayingToken (ERC20, Ownable, DividendPayingTokenInterface, DividendPayingTokenOptionalInterface)
 - [Pub] <Constructor> #
 - modifiers: ERC20
 - [Pub] distributeCAKEDividends #
 - modifiers: onlyOwner
 - [Pub] withdrawDividend #
 - [Int] _withdrawDividendOfUser #
 - [Pub] dividendOf
 - [Pub] withdrawableDividendOf
 - [Pub] withdrawnDividendOf
 - [Pub] accumulativeDividendOf
 - [Int] _transfer #
 - [Int] _mint #
 - [Int] _burn #
 - [Int] _setBalance #

- + Context
 - [Int] _msgSender
 - [Int] _msgData
- + CAKEBANK (ERC20, Ownable)
 - [Pub] <Constructor> #
 - modifiers: ERC20
 - [Ext] <Fallback> (\$)
 - [Pub] updateDividendTracker #
 - modifiers: onlyOwner
 - [Pub] updateUniswapV2Router #
 - modifiers: onlyOwner
 - [Pub] excludeFromFees #
 - modifiers: onlyOwner
 - [Pub] excludeMultipleAccountsFromFees #
 - modifiers: onlyOwner
 - [Ext] setMarketingWallet #
 - modifiers: onlyOwner
 - [Ext] setCAKERewardsFee #
 - modifiers: onlyOwner
 - [Ext] setLiquiditFee #
 - modifiers: onlyOwner
 - [Ext] setMarketingFee #
 - modifiers: onlyOwner
 - [Pub] setAutomatedMarketMakerPair #
 - modifiers: onlyOwner
 - [Ext] blacklistAddress #
 - modifiers: onlyOwner
 - [Prv] _setAutomatedMarketMakerPair #
 - [Pub] updateGasForProcessing #
 - modifiers: onlyOwner
 - [Ext] updateClaimWait #
 - modifiers: onlyOwner
 - [Ext] getClaimWait
 - [Ext] getTotalDividendsDistributed
 - [Pub] isExcludedFromFees
 - [Pub] withdrawableDividendOf
 - [Pub] dividendTokenBalanceOf
 - [Ext] excludeFromDividends #
 - modifiers: onlyOwner
 - [Ext] getAccountDividendsInfo
 - [Ext] getAccountDividendsInfoAtIndex
 - [Ext] processDividendTracker #
 - [Ext] claim #
 - [Ext] getLastProcessedIndex
 - [Ext] getNumberOfDividendTokenHolders
 - [Int] _transfer #
 - [Prv] swapAndSendToFee #
 - [Prv] swapAndLiquify #
 - [Prv] swapTokensForEth #
 - [Prv] swapTokensForCake #
 - [Prv] addLiquidity #
 - [Prv] swapAndSendDividends #

- + CAKEBANKDividendTracker (Ownable, DividendPayingToken)
 - [Pub] <Constructor> #
 - modifiers: DividendPayingToken
 - [Int] _transfer #
 - [Pub] withdrawDividend #
 - [Ext] excludeFromDividends #
 - modifiers: onlyOwner
 - [Ext] updateClaimWait #
 - modifiers: onlyOwner
 - [Ext] getLastProcessedIndex
 - [Ext] getNumberOfTokenHolders
 - [Pub] getAccount
 - [Pub] getAccountAtIndex
 - [Prv] canAutoClaim
 - [Ext] setBalance #
 - modifiers: onlyOwner
 - [Pub] process #
 - [Pub] processAccount #
 - modifiers: onlyOwner

(\$) = payable function

= non-constant function

Issues Checking Status

Issue description	Checking status
1. Compiler errors.	Passed
2. Race conditions and Reentrancy. Cross-function race conditions.	Passed
3. Possible delays in data delivery.	Passed
4. Oracle calls.	Passed
5. Front running.	Passed
6. Timestamp dependence.	Passed
7. Integer Overflow and Underflow.	Passed
8. DoS with Revert.	Passed
9. DoS with block gas limit.	Low issues
10. Methods execution permissions.	Passed
11. Economy model of the contract.	Passed
12. The impact of the exchange rate on the logic.	Passed
13. Private user data leaks.	Passed
14. Malicious Event log.	Passed
15. Scoping and Declarations.	Passed
16. Uninitialized storage pointers.	Passed
17. Arithmetic accuracy.	Passed
18. Design Logic.	Passed
19. Cross-function race conditions.	Passed
20. Safe Open Zeppelin contracts implementation and usage.	Passed
21. Fallback function security.	Passed

Security Issues

✓ High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No medium severity issues found.

✓ Low Severity Issues

1. Out of gas

Issue:

- The function `excludeMultipleAccountsFromFees()` uses the loop to exclude multiple accounts from fees. Function will be aborted with `OUT_OF_GAS` exception if there will be a long addresses list.

Recommendation:

Be careful about accounts array length.

Notes:

- Dividend tracker may be changed. So that logic of `setBalance` and other functions could be another and not audited.

Owner privileges (In the period when the owner is not renounced)

- Owner can change dividend tracker.
- Owner can change Uniswap router address.
- Owner can exclude from the fees.
- Owner can blacklist addresses.
- Owner can change liquidity, marketing and CAKE reward fees.
- Owner can exclude and include addresses in `automatedMarketMakerPairs` array.
- Owner can exclude from dividends.
- Owner can change marketing wallet.
- Owner can change gas for processing.
- Owner can update `claimWait` value.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details are provided by the team:

<https://team.finance/view-coin/0x5F1b95784a033CD6842cf26eb9A9687F91Ad9e78?name=CAKE%20BANK&symbol=CAKEBANK>

TechRate 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.