



**TechRate**  
AUDIT COMPANY

# Smart Contract Security Audit

# Audit Details



Audited project

**Kevlar**



Deployer address

**0x351F1A4A417184E487B0CF10f9989642F0130080**



Client contacts:

**Kevlar team**



Blockchain

**Binance Smart Chain**



Project website:

**<https://kevlarfinance.com>**

# 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 Kevlar to perform an audit of smart contracts:

<https://bscscan.com/address/0xa7b6874fc2a3602bc351fa3ece9ad10631f05fef#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 29.07.2021

Contract name	Kevlar
Contract address	0xA7B6874FC2a3602bC351fA3eCe9AD10631F05FeF
Total supply	888,888,888,888,888
Token ticker	KVLR
Decimals	9
Token holders	274
Transactions count	1,506
Top 100 holders dominance	97.91%
Liquidity fee	80
Buy/Sell/Transfer fee	10/20/20
Total payots	2911176443616876612
Team wallet	0x444ea52b99be919ab39740f17cecafc58902c61c
Contract deployer address	0x351F1A4A417184E487B0CF10f9989642F0130080
Contract's current owner address	0x351f1a4a417184e487b0cf10f9989642f0130080

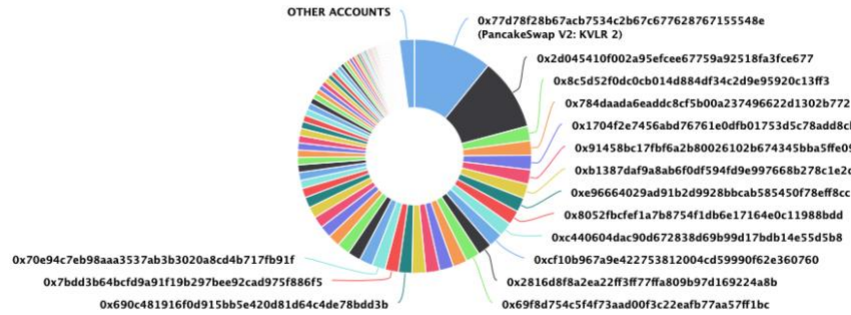
# Kevlar Token Distribution

The top 100 holders collectively own 97.91% (870,281,417,330.172.00 Tokens) of Kevlar Finance

Token Total Supply: 888,888,888,888.00 Token | Total Token Holders: 274

Kevlar Finance Top 100 Token Holders

Source: BscScan.com



(A total of 870,281,417,330.172.00 tokens held by the top 100 accounts from the total supply of 888,888,888,888.00 token)

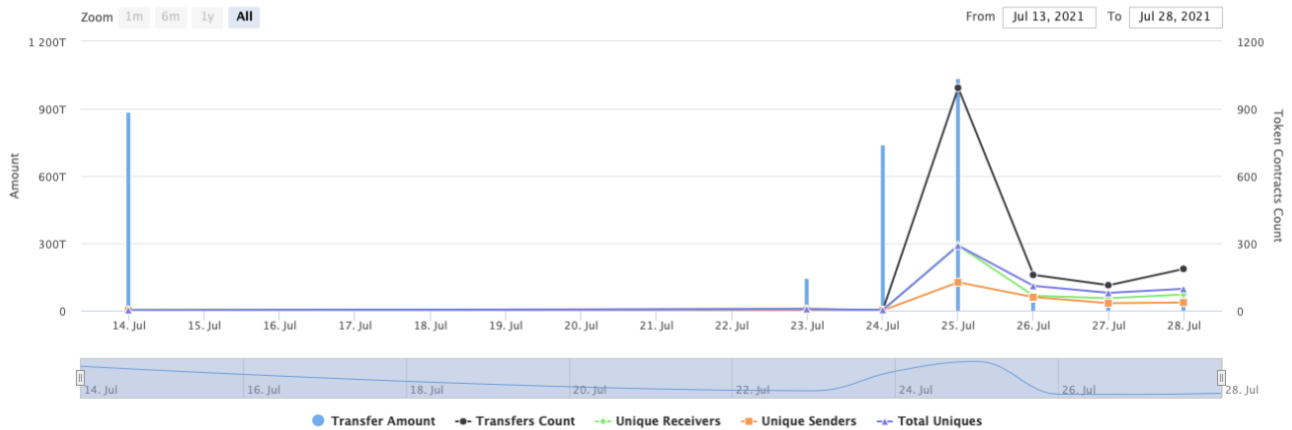
## Kevlar Contract Interaction Details

Time Series: Token Contract Overview

Wed 14, Jul 2021 - Wed 28, Jul 2021



Token Contract 0xa7b6874fc2a3602bc351fa3ece9ad10631f05fef (Kevlar Finance)

Source: BscScan.com





# Kevlar Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	 PancakeSwap V2: KVLR 2	96,586,340,878,025.910307209	10.8660%
2	 0x2d045410f002a95efcee67759a92518fa3fce677	88,888,888,888,888.79	10.0000%
3	0x8c5d52f0dc0cb014d884df34c2d9e95920c13ff3	17,777,777,777,777	2.0000%
4	0x784daada6eaddc8cf5b00a237496622d1302b772	17,777,777,743,738.210594158	2.0000%
5	0x1704f2e7456abd76761e0dfb01753d5c78add8cb	17,777,521,499,811.792993319	2.0000%
6	0x91458bc17bf6a2b80026102b674345bba5ffe09	17,776,349,079,999.3	1.9998%
7	0xb1387daf9a8ab6f0df594fd9e997668b278c1e2d	17,775,061,988,940.470964881	1.9997%
8	0xe96664029ad91b2d9928bbcab585450f78eff8cc	17,598,530,107,269.48930486	1.9798%
9	0x8052fbcfef1a7b8754f1db6e17164e0c11988bdd	17,525,410,345,507.148476139	1.9716%
10	0xc440604dac90d672838d69b99d17bdb14e55d5b8	17,448,736,965,522.989182676	1.9630%



# Contract functions details

## + [Int] IBEP20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner

## + [Int] IPancakeERC20

- [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 #

## + [Int] IPancakeFactory

- [Ext] feeTo
- [Ext] feeToSetter
- [Ext] getPair
- [Ext] allPairs
- [Ext] allPairsLength
- [Ext] createPair #
- [Ext] setFeeTo #
- [Ext] setFeeToSetter #

## + [Int] IPancakeRouter01

- [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] IPancakeRouter02 (IPancakeRouter01)
- [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens (\$)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
- + Ownable
- [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] geUnlockTime
  - [Pub] lock #
    - modifiers: onlyOwner
  - [Pub] unlock #
- + [Lib] Address
- [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Int] functionStaticCall
  - [Int] functionStaticCall
  - [Int] functionDelegateCall #
  - [Int] functionDelegateCall #
  - [Prv] \_verifyCallResult
- + [Lib] EnumerableSet
- [Prv] \_add #
  - [Prv] \_remove #
  - [Prv] \_contains
  - [Prv] \_length
  - [Prv] \_at
  - [Int] add #
  - [Int] remove #
  - [Int] contains
  - [Int] length
  - [Int] at
  - [Int] add #
  - [Int] remove #
  - [Int] contains
  - [Int] length
  - [Int] at

- [Int] add #
- [Int] remove #
- [Int] contains
- [Int] length
- [Int] at

#### + Kevlar (IBEP20, Ownable)

- [Prv] \_isTeam
- [Pub] <Constructor> #
- [Prv] \_transfer #
- [Prv] \_whiteListTransfer #
- [Prv] \_taxedTransfer #
- [Prv] \_feelessTransfer #
- [Prv] \_calculateFee
- [Pub] isExcludedFromStaking
- [Pub] \_getTotalShares
- [Prv] \_addToken #
- [Prv] \_removeToken #
- [Prv] \_newDividendsOf
- [Prv] \_distributeStake #
- [Prv] Claim #
- [Prv] \_swapContractToken #
  - modifiers: lockTheSwap
- [Prv] \_swapTokenForBNB #
- [Prv] \_addLiquidity #
- [Pub] getLiquidityReleaseTimeInSeconds
- [Pub] getBurnedTokens
- [Pub] getLimits
- [Pub] getTaxes
- [Pub] getWhitelistedStatus
- [Pub] getAddressSellLockTimeInSeconds
- [Pub] getSellLockTimeInSeconds
- [Pub] AddressResetSellLock #
- [Pub] AAAWithdraw #
- [Pub] getDividends
- [Pub] TeamBuyBack #
  - modifiers: onlyTeam
- [Pub] TeamBuyBack #
  - modifiers: onlyTeam
- [Pub] TeamExcludeFromStaking #
  - modifiers: onlyTeam
- [Pub] TeamIncludeToStaking #
  - modifiers: onlyTeam
- [Pub] TeamWithdrawMarketingBNB #
  - modifiers: onlyTeam
- [Pub] TeamWithdrawMarketingBNB #
  - modifiers: onlyTeam
- [Pub] TeamSwitchManualBNBConversion #
  - modifiers: onlyTeam
- [Pub] TeamDisableSellLock #
  - modifiers: onlyTeam
- [Pub] TeamSetSellLockTime #
  - modifiers: onlyTeam
- [Pub] TeamSetTaxes #
  - modifiers: onlyTeam

- [Pub] TeamChangeMarketingShare #
  - modifiers: onlyTeam
- [Pub] TeamCreateLPandBNB #
  - modifiers: onlyTeam
- [Pub] TeamExcludeAccountFromFees #
  - modifiers: onlyTeam
- [Pub] TeamIncludeAccountToFees #
  - modifiers: onlyTeam
- [Pub] TeamExcludeAccountFromSellLock #
  - modifiers: onlyTeam
- [Pub] TeamIncludeAccountToSellLock #
  - modifiers: onlyTeam
- [Pub] TeamUpdateLimits #
  - modifiers: onlyTeam
- [Pub] SetupEnableTrading #
  - modifiers: onlyTeam
- [Pub] SetupLiquidityTokenAddress #
  - modifiers: onlyTeam
- [Pub] TeamlimitLiquidityReleaseTo20Percent #
  - modifiers: onlyTeam
- [Pub] TeamUnlockLiquidityInSeconds #
  - modifiers: onlyOwner
- [Prv] \_prolongLiquidityLock #
- [Pub] TeamReleaseLiquidity #
  - modifiers: onlyTeam
- [Pub] TeamRemoveLiquidity #
  - modifiers: onlyTeam
- [Pub] TeamRemoveRemainingBNB #
  - modifiers: onlyTeam
- [Ext] <Fallback> (\$)
- [Ext] <Fallback> (\$)
- [Ext] getOwner
- [Ext] name
- [Ext] symbol
- [Ext] decimals
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Prv] \_approve #
- [Ext] transferFrom #
- [Ext] increaseAllowance #
- [Ext] decreaseAllowance #

(\$ ) = 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 `_getTotalShares()` uses the loop to find and decrease shares from the `_excludedFromStaking` list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function _getTotalShares() public view returns (uint256){
    uint256 shares=_circulatingSupply;
    //subtracts all excluded from shares, excluded list is limited to 30
    // to avoid creating a Honeypot through OutOfGas exeption
    for(uint i=0; i<_excludedFromStaking.length(); i++){
        shares-=_balances[_excludedFromStaking.at(i)];
    }
    return shares;
}
```

Recommendation:

Check that the excluded array length is not too big.

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

- Team can manually buyback BNB to dead address.
- Team can exclude and include in staking.
- Team can withdraw marketing balance.
- Team can disable auto call of `_swapContractToken` function.
- Team can disable sell lock.
- Team can change sell lock time.
- Team can change taxes.
- Team can change marketing share (percentage of BNB that goes to marketing).
- Team can manually call `_swapContractToken` function.
- Team can exclude from fees and sell lock.
- Team can change target balance and sell limits.
- Team can enable trading.
- Team can change liquidity token address.
- Team can call `TeamLimitLiquidityReleaseTo20Percent()` to set only 20% withdraw available.
- Owner can increase `_liquidityUnlockTime`.
- Team can withdraw liquidity to team wallet if it is not locked.
- Team can remove liquidity.
- Team can withdraw contract BNBs if it is not locked.
- Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.



# Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details provided by the team:

[https://dxsale.app/app/v2\\_9/dxlockview?id=0&add=0x351F1A4A417184E487B0CF10f9989642F0130080&type=lplock&chain=BSC](https://dxsale.app/app/v2_9/dxlockview?id=0&add=0x351F1A4A417184E487B0CF10f9989642F0130080&type=lplock&chain=BSC)

---

***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.***