Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

September, 2021

Audit Details

Audited project

Double Bubble

Deployer address

0xcdf698f5f3175b47c480fbef352e4e1566316ab4

Client contacts:

Double Bubble team

Blockchain

Binance Smart Chain

Project website:

https://doublebubble.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 Double Bubble to perform an audit of smart contracts:

https://bscscan.com/address/0xda81440dd054aeafdaea1c12bccba3cc3b4470d9#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.

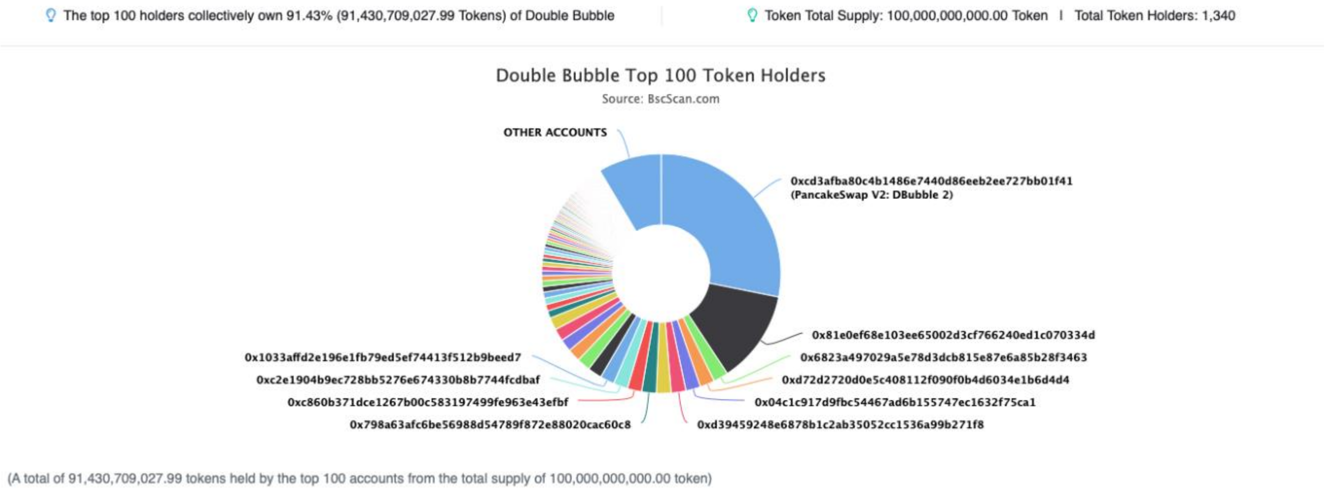
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 05.09.2021

Contract name	Double Bubble
Contract address	0xda81440Dd054AeafDAEA1C12bcCbA3CC3B4470d9
Total supply	100,000,000,000
Token ticker	DBubble
Decimals	9
Token holders	1,340
Transactions count	16,064
Top 100 holders dominance	91.43%
Trading enabled	true
Total fee	990
Total reflected	25036337628591209790 6
lp Pair	0xcd3afba80c4b1486e7440d86eeb2ee727bb01f41
Contract deployer address	0xcdf698f5f3175b47c480fbef352e4e1566316ab4
Contract’s current owner address	0xcdf698f5f3175b47c480fbef352e4e1566316ab4

Double Bubble Token Distribution



The top 100 holders collectively own 91.43% (91,430,709,027.99 Tokens) of Double Bubble

Token Total Supply: 100,000,000,000.00 Token | Total Token Holders: 1,340

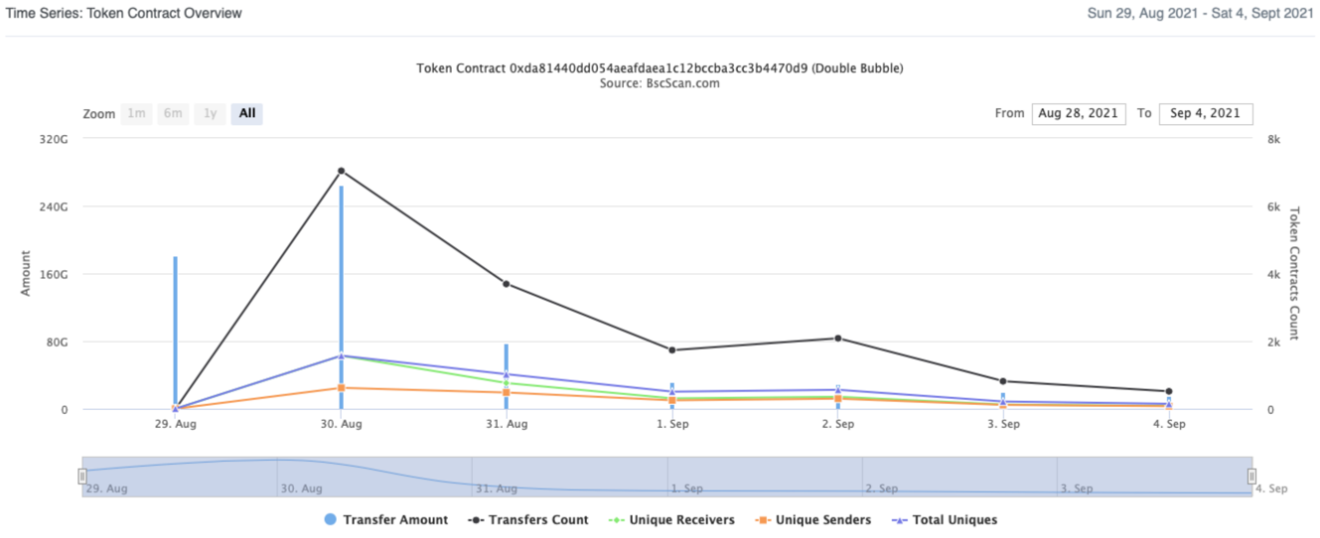
Double Bubble Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0xcd3afba80c4b1486e7440d86eeb2ee727bb01f41 (PancakeSwap V2: DBubble 2)
0x81e0ef68e103ee65002d3cf766240ed1c070334d
0x6823a497029a5e78d3dcb815e87e6a85b28f3463
0xd72d2720d0e5c408112f090f0b4d6034e1b6d4d4
0x04c1c917d9fbc54467ad6b155747ec1632f75ca1
0xd39459248e6878b1c2ab35052cc1536a99b271f8
0x1033affd2e196e1fb79ed5ef74413f512b9beed7
0xc2e1904b9ec728bb5276e674330b8b7744fcdbaf
0xc860b371dce1267b00c583197499fe963e43efbf
0x798a63afc6be56988d54789f872e88020cac60c8

(A total of 91,430,709,027.99 tokens held by the top 100 accounts from the total supply of 100,000,000,000.00 token)

Double Bubble Contract Interaction Details



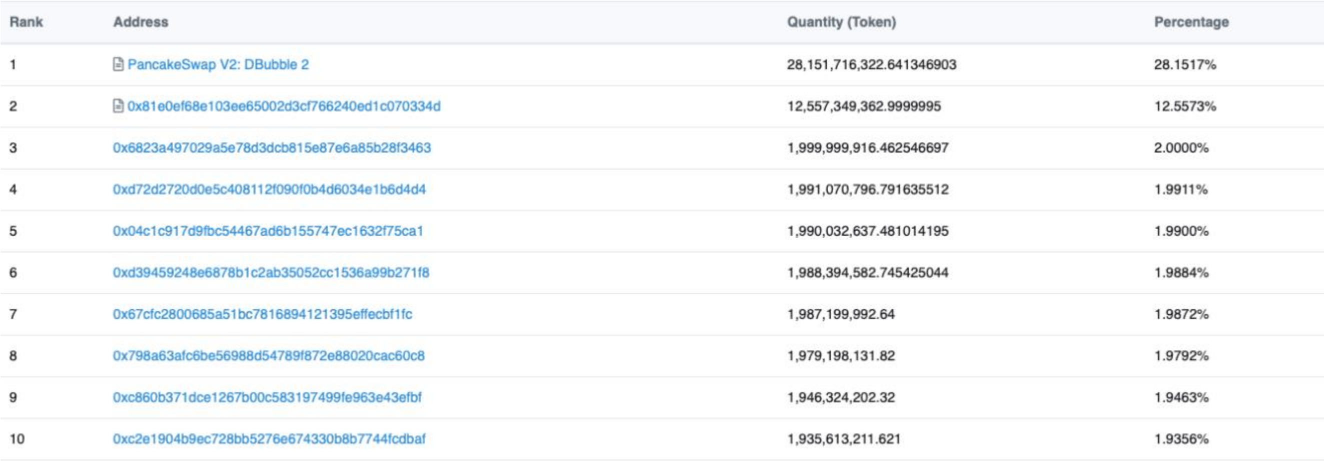
Time Series: Token Contract Overview

Sun 29, Aug 2021 - Sat 4, Sept 2021

Token Contract 0xda81440dd054aeafdaea1c12bccba3cc3b4470d9 (Double Bubble)

Source: BscScan.com

Double Bubble Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	🗎 PancakeSwap V2: DBubble 2	28,151,716,322.641346903	28.1517%
2	🗎 0x81e0ef68e103ee65002d3cf766240ed1c070334d	12,557,349,362.9999995	12.5573%
3	0x6823a497029a5e78d3dcb815e87e6a85b28f3463	1,999,999,916.462546697	2.0000%
4	0xd72d2720d0e5c408112f090f0b4d6034e1b6d4d4	1,991,070,796.791635512	1.9911%
5	0x04c1c917d9fbc54467ad6b155747ec1632f75ca1	1,990,032,637.481014195	1.9900%
6	0xd39459248e6878b1c2ab35052cc1536a99b271f8	1,988,394,582.745425044	1.9884%
7	0x67cfc2800685a51bc7816894121395effecbf1fc	1,987,199,992.64	1.9872%
8	0x798a63afc6be56988d54789f872e88020cac60c8	1,979,198,131.82	1.9792%
9	0xc860b371dce1267b00c583197499fe963e43efbf	1,946,324,202.32	1.9463%
10	0xc2e1904b9ec728bb5276e674330b8b7744fcdbaf	1,935,613,211.621	1.9356%

Contract functions details

+ Context
  - [Int] _msgSender
  - [Int] _msgData

+ [Int] IERC20
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] _functionCallWithValue #

+ [Int] IUniswapV2Factory
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #
  - [Ext] setFeeToSetter #

+ [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] 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] Cashier
  - [Ext] whomst
  - [Ext] setReflectionCriteria #
  - [Ext] tally #

```
  - [Ext] load ($)
  - [Ext] cashout #
  - [Ext] giveMeWelfarePlease #
  - [Ext] getTotalDistributed
  - [Ext] getShareholderInfo
  - [Ext] getShareholderRealized
  - [Ext] updateRewardsTokens #
  - [Ext] getCurrentTokens

+ DoubleBubble (IERC20)
  - [Pub] <Constructor> ($)
  - [Pub] owner
  - [Ext] transferOwner #
    - modifiers: onlyOwner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Ext] <Fallback> ($)
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Pub] balanceOf
  - [Ext] allowance
  - [Pub] approve #
  - [Pub] approveMax #
  - [Prv] _approve #
  - [Ext] transfer #
  - [Ext] transferFrom #
  - [Pub] isSniper
  - [Pub] isFeeExcluded
  - [Pub] isDividendExcluded
  - [Ext] setProtectionSettings #
    - modifiers: onlyOwner
  - [Ext] setGasPriceLimit #
    - modifiers: onlyOwner
  - [Pub] setDividendExcluded #
    - modifiers: onlyOwner
  - [Pub] setExcludeFromFees #
    - modifiers: onlyOwner
  - [Ext] setTaxesBuy #
    - modifiers: onlyOwner
  - [Ext] setTaxesSell #
    - modifiers: onlyOwner
  - [Ext] setTaxesTransfer #
    - modifiers: onlyOwner
  - [Ext] setMarketingWallet #
    - modifiers: onlyOwner
  - [Ext] setDevWallet #
    - modifiers: onlyOwner
  - [Ext] setSwapBackSettings #
    - modifiers: onlyOwner
  - [Ext] setSwapThreshold #
    - modifiers: onlyOwner
  - [Ext] setSwapAmount #
```

  - modifiers: onlyOwner
- [Ext] setTargetLiquidity #
  - modifiers: onlyOwner
- [Ext] setReflectionCriteria #
  - modifiers: onlyOwner
- [Ext] setReflectorSettings #
  - modifiers: onlyOwner
- [Ext] setInitialSubEnabled #
  - modifiers: onlyOwner
- [Pub] getCirculatingSupply
- [Pub] getLiquidityBacking
- [Pub] isOverLiquified
- [Ext] giveMeWelfarePlease #
- [Ext] getTotalReflected
- [Ext] getShareholderRealizedGains
- [Ext] getUserInfo
- [Ext] getCurrentTokens
- [Pub] setNewRouter #
  - modifiers: onlyOwner
- [Ext] setMaxTxPercent #
  - modifiers: onlyOwner
- [Ext] setMaxWalletSize #
  - modifiers: onlyOwner
- [Ext] updateRewardsTokens #
  - modifiers: onlyOwner
- [Ext] excludePresaleAddresses #
  - modifiers: onlyOwner
- [Prv] _hasLimits
- [Ext] enableTrading #
  - modifiers: onlyOwner
- [Int] _transfer #
- [Int] _finalizeTransfer #
- [Int] processTokenReflect #
- [Int] _basicTransfer #
- [Pub] getTotalFee
- [Int] takeTaxes #
- [Int] adjustTaxes #
- [Int] swapBack #
  - modifiers: swapping
- [Int] transferBNB #
- [Ext] manualDepost #
  - modifiers: onlyOwner
- [Prv] _checkLiquidityAdd #

($) = 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.	Passed
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. **Safe math** (Not the issue for current deployed contract due to *Compiler Version: v0.8.4+commit.c7e474f2*)

   Issue:

   - Solidity version acceptable for the contract is “>=0.6.0 <0.9.0”, if Solidity version would be lower than 0.8.0, then code blocks without safe math could fail (if there will be inappropriate values).

   Recommendation:

   Fix solidity version from actual value, not the old one.

Notes:

- swapBack function distributes reflection and marketing fee and adds liquidity.
- If dynamic liquidity fee will equal to zero, liquidity fee part goes to reflection.
- reflector(Cashier) provided only as interface, so actual working of its functions is not audited.

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

- Owner can change protection settings.
- Owner can change gasPriceLimit.
- Owner can exclude and include in dividends.
- Owner can exclude from the fees.
- Owner can change the fees.
- Owner can change marketing and dev wallet.
- Owner can change swap back settings.
- Owner can change swapThreshold.
- Owner can change swapAmount.
- Owner can change target liquidity.
- Owner can change reflection criteria.
- Owner can change reflector GAS amount.
- Owner can enable/disable initialSubEnabled.
- Owner can change router address.
- Owner can change the maximum transaction amount.
- Owner can change max wallet size.
- Owner can update rewards token.
- Owner can enable trading.
- Owner can add addresses in multiple exclusions.
- Owner can manually deposit contract balance to Cashier.

Conclusion

Smart contracts do not contain high 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/v3/dxlplocksearch?id=0&add=0xda81440Dd054AeafDAEA1C12bcCbA3CC3B4470d9&type=lpdefi&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.