Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

November, 2021

Audit Details

Audited project

DEEPMAZE

Deployer address

0x25c576144e75f86db15fc8420c09bda1e3ac4d99

Client contacts:

DEEPMAZE team

Blockchain

Binance Smart Chain

Project website:

deepmaze.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 DEEPMAZE to perform an audit of smart contracts:

https://bscscan.com/address/0xdC0118B27276065C573386aa44e7a6E5e2AF07C1#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

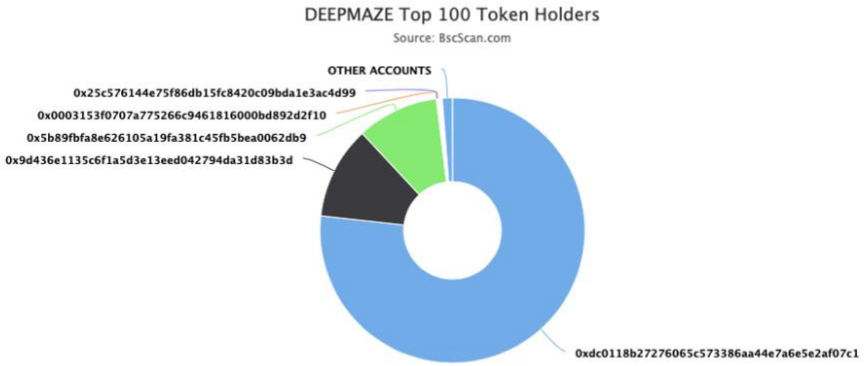
Token contract details for 19.11.2021

Contract name	DEEPMAZE
Contract address	0xdC0118B27276065C573386aa44e7a6E5e2AF07C1
Total supply	1,000,000,000
Token ticker	DPZ
Decimals	18
Token holders	3,459
Transactions count	5,210
Top 100 holders dominance	98.76% (76.6432% is on the contract balance)
Presale tokens	267589216235500000000000000
Hard cap	1000000000000000000000000
Price	101540992961188
Uniswap V2 pair	0xade8078986e1128702f2bfc038ccc78397d4849e
Contract deployer address	0x25c576144e75f86db15fc8420c09bda1e3ac4d99
Contract's current owner address	0x25c576144e75f86db15fc8420c09bda1e3ac4d99

DEEPMAZE Token Distribution

The top 100 holders collectively own 98.76% (987,620,400.01 Tokens) of DEEPMAZE

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 3,459

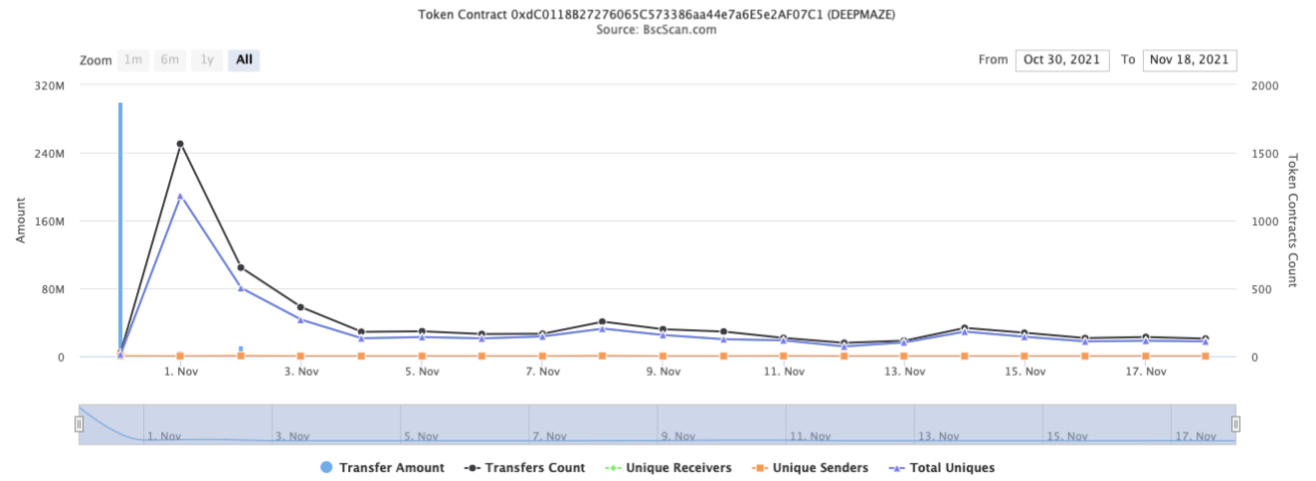


(A total of 987,620,400.01 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

DEEPMAZE Contract Interaction Details

Time Series: Token Contract Overview

Sun 31, Oct 2021 - Thu 18, Nov 2021



DEEPMAZE Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0xdc0118b27276065c573386aa44e7a6e5e2af07c1	767,587,716.2355	76.7588%
2	0x9d436e1135c6f1a5d3e13eed042794da31d83b3d	113,103,000	11.3103%
3	0x5b89fbfa8e626105a19fa381c45fb5bea0062db9	100,000,000	10.0000%
4	0x0003153f0707a775266c9461816000bd892d2f10	1,148,000	0.1148%
5	0x25c576144e75f86db15fc8420c09bda1e3ac4d99	347,183.778	0.0347%
6	0xd383052d93f1bbf6fd2a6d39fc98d875ddc43b8f	256,499.9998	0.0256%
7	0xdb23ce2a9371b0ebd23d6e09c39f82a2d5670056	253,500	0.0254%
8	0x984d2ed78eec7d39ef263fbd18f8693f31ef0f2f	200,000	0.0200%
9	0xde9bd4057eeab8c6d48a236e23c1137da69414af	185,500	0.0186%
10	0xb3ed87d96e6d06d18cf44eeec63f73675d5c573b	150,000	0.0150%

Contract functions details

+ [Int] IERC20
  - [Ext] totalSupply
  - [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

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

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

+ Ownable (Context)
  - [Int] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] getUnlockTime
  - [Pub] lock #
    - modifiers: onlyOwner
  - [Pub] unlock #

+ [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 #

+ DeepMaze (Context, IERC20, Ownable)
- [Pub] <Constructor> #
- [Pub] setStarted #
  - modifiers: onlyOwner
- [Pub] setPause #
  - modifiers: onlyOwner
- [Pub] setPrice #
  - modifiers: onlyOwner
- [Pub] setMinimum #
  - modifiers: onlyOwner
- [Pub] setEnds #
  - modifiers: onlyOwner
- [Pub] setTransferOk #
  - modifiers: onlyOwner
- [Pub] startPresale #
  - modifiers: onlyOwner
- [Pub] calculateAmountPurchased
- [Pub] burnReflection #
  - modifiers: onlyOwner
- [Pub] buy_presale ($)
- [Pub] setLiquidityThreshold #
  - modifiers: onlyOwner
- [Pub] endPresale #
  - modifiers: onlyOwner
- [Pub] name
- [Pub] symbol
- [Pub] getPresaleTokensR
- [Pub] getPresaleTokens
- [Pub] decimals
- [Pub] totalSupply
- [Pub] totalCrowdPool
- [Pub] getRtotal
- [Pub] getTotalDistributed
- [Pub] getCrowdingPool
- [Pub] getRemainingCrowdingPool
- [Pub] getPendingPool
- [Pub] getAccumulatedLiquidtyPool
- [Pub] getPoolDecay
- [Pub] getRate
- [Pub] getLiquidityThreshold
- [Pub] getMaxTxThreshold
- [Pub] getLiquidityProvided
- [Pub] getTokensSwapped
- [Pub] getBnbProvided
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #

- [Pub] getTokenFromReflection
- [Ext] setLiquidityFeePercent #
  - modifiers: onlyOwner
- [Ext] setCrowdRatePercent #
  - modifiers: onlyOwner
- [Ext] setMaxTxThreshold #
  - modifiers: onlyOwner
- [Pub] setLiquidityProvisionEnabled #
  - modifiers: onlyGateKeeper
- [Ext] <Fallback> ($)
- [Prv] _approve #
- [Prv] _transfer #
- [Pub] getBNBBalance
- [Ext] checkBNB ($)
  - modifiers: onlyGateKeeper
- [Prv] LiquidityProvision #
  - modifiers: lockTheLiquidityProvision
- [Prv] swapTokensForBnb #
- [Prv] addLiquidity #
- [Pub] setRouterAddress #
  - modifiers: onlyGateKeeper
- [Prv] _tokenTransfer #
- [Prv] _get_tokens_to_distribute #
- [Prv] _transferStandard #

($) = 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

No low severity issues found.

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

- Gatekeeper address can enable/disable LiquidityProvisionEnabled.
- Gatekeeper address can withdraw contract BNBs.
- Gatekeeper address can change router address.
- Owner can enable/disable started and paused.
- Owner can change price, minimum and ends value.
- Owner can enable/disable transferok.
- Owner can start and end presale.
- Owner can burn tokens.
- Owner can change liquidityThreshold.
- Owner can change _liquidityFee and _crowdingRate.
- Owner can change the maximum transaction amount.

Conclusion

Smart contracts contain owner privileges! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details are NOT provided by the team.

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.