Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

January, 2022

Audit Details

Audited project

ICEBERG

Deployer address

0x6b75c7d0411d4670cc520a94e603a6ea6986aaa2

Client contacts:

ICEBERG team

Blockchain

Binance Smart Chain

Project website:

https://icebergprotocol.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 ICEBERG to perform an audit of smart contracts:
https://bscscan.com/address/0xc22e223c332e51340cc80ffbeeac088fd026ad2e#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 04.01.2022

Contract name	ICEBERG
Contract address	0xc22E223C332E51340cc80FFBEeAC088fD026AD2E
Total supply	100,000,000
Token ticker	ICEBERG
Decimals	18
Token holders	3,566
Transactions count	48,789
Top 100 holders dominance	86.43%
Marketing wallet	0x88eca0a7bd82530243cc8883ba8ec5c9d6c47119
Buyback wallet	0xf2fe6749a67a624265fd9c19ddeeb52954f9adbe
Sell / Buy Total fees	20 / 5
Uniswap V2 pair	0x98cdfe14d56e0ed45f69c8f6399b53fc61cf9be6
Contract deployer address	0x6b75c7d0411d4670cc520a94e603a6ea6986aaa2
Contract's current owner address	0x6b75c7d0411d4670cc520a94e603a6ea6986aaa2

ICEBERG Token Distribution

The top 100 holders collectively own 86.43% (86,427,500.87 Tokens) of ICEBERG

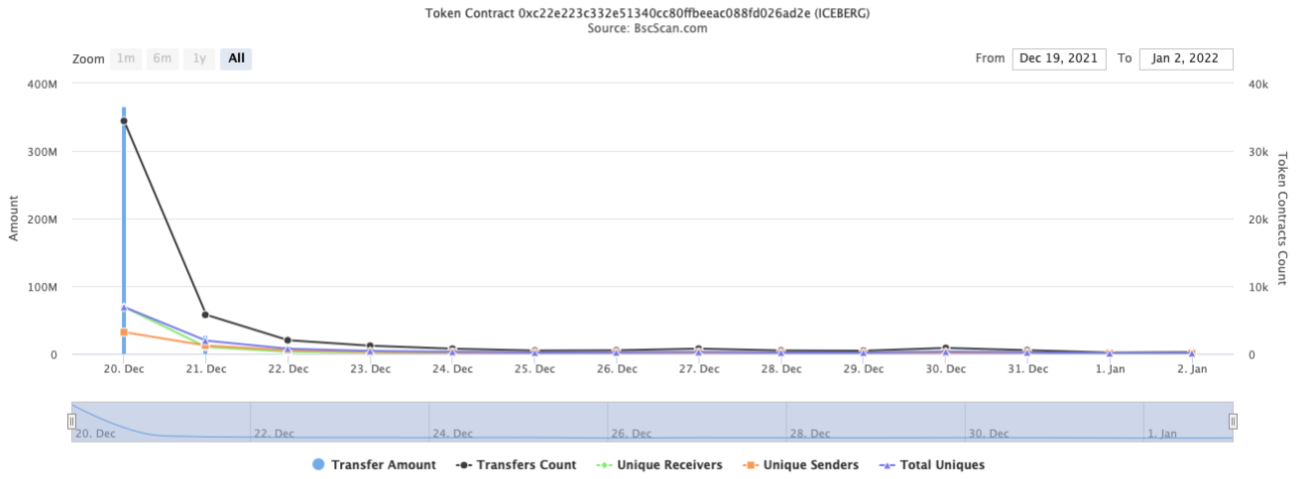
Token Total Supply: 100,000,000.00 Token | Total Token Holders: 3,566

(A total of 86,427,500.87 tokens held by the top 100 accounts from the total supply of 100,000,000.00 token)

ICEBERG Contract Interaction Details

Time Series: Token Contract Overview

Mon 20, Dec 2021 - Sun 2, Jan 2022



ICEBERG Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0xeef334715828a7e558ed1b6e5d0705057bdb6e71	33,000,000	33.0000%
2	Null Address: 0x000...dEaD	20,200,001.266105253756861729	20.2000%
3	PancakeSwap V2: ICEBERG 46	8,645,997.47277689248562539	8.6460%
4	0xc10fad9a976b50fda5353a8000d1b01c2452375b	2,000,000	2.0000%
5	0xba892e09887227f6c01915f42021cc5bed16b65a	1,979,220.226178653040724108	1.9792%
6	0xfe665723d420bb3909748e83881b415af2d66cf5	1,547,828.841808503486694115	1.5478%
7	0x03840d7e98007a0d694b2a7035531e6920e20057	1,514,004.230035619793737328	1.5140%
8	0xf2fe6749a67a624265fd9c19ddeeb52954f9adbe	1,287,421.906481330980553258	1.2874%
9	0x58b9f3bff7b52e63eec7e3de4d1b67ac56dca396	1,095,244.992503	1.0952%
10	0xb71b13b85d2c094b0fdec64ab891b5bf5f110a8e	995,099.999999999957092273	0.9951%

Contract functions details

+ [Int] IERC20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ [Int] IERC20Metadata (IERC20)
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals

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

+ 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] _afterTokenTransfer #

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Int] functionStaticCall
  - [Int] functionStaticCall
  - [Int] functionDelegateCall #
  - [Int] functionDelegateCall #
  - [Int] verifyCallResult

+ [Lib] SafeERC20

  - [Int] safeTransfer #
  - [Int] safeTransferFrom #
  - [Int] safeApprove #
  - [Int] safeIncreaseAllowance #
  - [Int] safeDecreaseAllowance #
  - [Prv] _callOptionalReturn #

+ Ownable (Context)
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Prv] _setOwner #

+ [Lib] SafeMath
  - [Int] tryAdd
  - [Int] trySub
  - [Int] tryMul
  - [Int] tryDiv
  - [Int] tryMod
  - [Int] add
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] mod
  - [Int] sub
  - [Int] div
  - [Int] mod

+ [Lib] Counters
  - [Int] current
  - [Int] increment #
  - [Int] decrement #
  - [Int] reset #

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

+ [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 #

+ ICEBERG (ERC20, Ownable)
- [Pub] <Constructor> #
  - modifiers: ERC20
- [Ext] <Fallback> ($)
- [Ext] decreaseTax #
  - modifiers: onlyOwner
- [Ext] disableDecreasingTax #
  - modifiers: onlyOwner
- [Ext] enableContractAddressTrading #
  - modifiers: onlyOwner
- [Ext] disableContractAddressTrading #
  - modifiers: onlyOwner
- [Ext] enableTrading #
  - modifiers: onlyOwner
- [Ext] disableTrading #
  - modifiers: onlyOwner
- [Ext] disableTransferDelay #
  - modifiers: onlyOwner
- [Ext] enableTransferDelay #
  - modifiers: onlyOwner
- [Ext] blackListAddress #
  - modifiers: onlyOwner
- [Ext] blackListAddresses #
  - modifiers: onlyOwner
- [Ext] unblackListAddress #
  - modifiers: onlyOwner
- [Ext] unblackListAddresses #
  - modifiers: onlyOwner
- [Ext] setBlackListFee #
  - modifiers: onlyOwner
- [Ext] updateLimitsInEffect #
  - modifiers: onlyOwner
- [Ext] setSwapTokensAtAmount #
  - modifiers: onlyOwner
- [Ext] setMaxTransactionAmount #

    - modifiers: onlyOwner
  - [Ext] setMaxWalletAmount #
    - modifiers: onlyOwner
  - [Pub] excludeFromMaxTransaction #
    - modifiers: onlyOwner
  - [Ext] updateSwapEnabled #
    - modifiers: onlyOwner
  - [Ext] setBuyFees #
    - modifiers: onlyOwner
  - [Ext] setSellFees #
    - modifiers: onlyOwner
  - [Pub] excludeFromFees #
    - modifiers: onlyOwner
  - [Pub] setAutomatedMarketMakerPair #
    - modifiers: onlyOwner
  - [Prv] _setAutomatedMarketMakerPair #
  - [Ext] setMarketingWallet #
    - modifiers: onlyOwner
  - [Ext] setBuyBackWallet #
    - modifiers: onlyOwner
  - [Ext] clearStuckBNBBalance #
    - modifiers: onlyOwner
  - [Ext] clearStuckTokenBalance #
    - modifiers: onlyOwner
  - [Pub] isExcludedFromFees
  - [Int] _transfer #
    - modifiers: onlyNonContract
  - [Prv] swapTokensForETH #
  - [Prv] swapTokensForUSDC #
  - [Prv] addLiquidity #
  - [Prv] swapBack #
  - [Ext] buyBackTokens #
    - 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 `blackListAddresses() and unblackListAddresses()` uses the loop to blacklist addresses from the list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long addresses list.

Recommendation:
Check that the excluded array length is not too big.

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

- Owner can enable/disable decreasing taxes.
- Owner can include/exclude addresses in _isExcludedFromContractBuyingLimit array.
- Owner can enable/disable trading.
- Owner can enable/disable transfer delay.
- Owner can blacklist addresses.
- Owner can change blacklist fee.
- Owner can enable/disable limitsInEffect.
- Owner can change swapTokensAtAmount value.
- Owner can change maximum transaction amount.
- Owner can change maximum wallet amount.
- Owner can exclude from maximum transaction amount.
- Owner can enable / disable swap.
- Owner can change buy/sell fees.
- Owner can include in and exclude from fees.
- Owner can include in and exclude from addresses in automatedMarketMakerPairs array.
- Owner can change marketing and buyback wallets.
- Owner can withdraw contract BNBs and ERC20 tokens.
- Owner can manually buyback wallet.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope. Blacklist fee is 99%.

Liquidity locking details provided by the team:
https://dxsale.app/app/v3/dxlockview?id=0&add=0x6b75c7d0411d4670Cc520A94e603A6EA6986AAA2&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.