



**TechRate**  
AUDIT COMPANY

# Smart Contract Security Audit

TechRate

November, 2021

# Audit Details



Audited project

**Disco Burn Token**



Deployer address

**0x25945b405194d1311b4e2d9dad879a2bdd97e642**



Client contacts:

**Disco Burn Token team**



Blockchain

**Binance Smart Chain**



Project website:

**<https://discoburntoken.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 Disco Burn Token to perform an audit of smart contracts:

<https://bscscan.com/address/0x6bc736cc4a81ffc1ff67c89413913d418804ab43#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 14.11.2021

Contract name	Disco Burn Token
Contract address	0x6bC736Cc4a81FFc1FF67c89413913D418804ab43
Total supply	150,000,000
Token ticker	DBT
Decimals	9
Token holders	2,659
Transactions count	10,322
Top 100 holders dominance	85.63%
Liquidity fee	8
Tax fee	4
Total fees	6579270001021805
Uniswap V2 pair	0x3ce29a2bc916d726ab02d3007ae7842b763aa6e3
Contract deployer address	0x25945b405194d1311b4e2d9dad879a2bdd97e642
Contract's current owner address	0x29ada2cdba1bbebf05cf821405827c42d2929444

💡 The top 100 holders collectively own 85.63% (128,438,090.55 Tokens) of Disco Burn Token

Token Total Supply: 150,000,000.00 Token | Total Token Holders: 2,659

Source: BscScan.com



### Time Series: Token Contract Overview


Mon 25, Oct 2021 - Fri 12, Nov 2021

Source: BscScan.com





# Disco Burn Token Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	<a href="#">Burn Address</a>	52,396,186.32080572	34.9308%
2	 <a href="#">PancakeSwap V2: DBT 46</a>	10,807,030.165159028	7.2047%
3	<a href="#">0x281d13ee5476507d23d92bf2db4e44066a3a91cf</a>	2,263,351.91869866	1.5089%
4	<a href="#">0xb8559e102b995a98432ab89d0c4d24302565aad8</a>	1,856,835.480027294	1.2379%
5	<a href="#">0x49867adc3bed07281ecf9ce437a3eb8ddac91b47</a>	1,768,849.169109329	1.1792%
6	<a href="#">0xf7875570f40706d40f31ccdd3972dea4aeb47a3c</a>	1,697,574.261719067	1.1317%
7	<a href="#">0x0157a91cbdc493da602a89af4de4bc21730dc598</a>	1,448,281.932003414	0.9655%
8	<a href="#">0x158b533a5f1e80c74500ef4262dd4d78d2a51383</a>	1,390,681.179806291	0.9271%
9	<a href="#">0x8f9483df03572b46de31f6e2982d75327c12bd38</a>	1,331,988.311750606	0.8880%
10	<a href="#">0x50f0314dc203b38172c80808da3581f243e2f28d</a>	1,290,841.865789416	0.8606%



# Contract functions details

## + Context

- [Int] \_msgSender
- [Int] \_msgData

## + [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

## + [Lib] Address

- [Int] isContract
- [Int] sendValue #
- [Int] functionCall #
- [Int] functionCall #
- [Int] functionCallWithValue #
- [Int] functionCallWithValue #
- [Prv] \_functionCallWithValue #

## + Ownable (Context)

- [Int] <Constructor> #
- [Pub] owner
- [Pub] transferOwnership #
  - modifiers: onlyOwner
- [Pub] getUnlockTime
- [Pub] getTime
- [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] burn #
- [Ext] swap #
- [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 #
```

+ DiscoBurnToken (Context, IERC20, Ownable)

- [Pub] <Constructor> #
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] isExcludedFromReward
- [Pub] totalFees
- [Pub] minimumTokensBeforeSwapAmount
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Pub] excludeFromReward #
  - modifiers: onlyOwner
- [Ext] includeInReward #
  - modifiers: onlyOwner
- [Prv] \_approve #
- [Prv] \_transfer #
- [Int] swapAndLiquify #
  - modifiers: lockTheSwap
- [Int] swapTokensForEth #
- [Prv] addLiquidity #
- [Prv] \_tokenTransfer #
- [Prv] \_transferStandard #
- [Prv] \_transferToExcluded #
- [Prv] \_transferFromExcluded #
- [Prv] \_transferBothExcluded #
- [Prv] \_reflectFee #
- [Prv] \_getValues
- [Prv] \_getTValues
- [Prv] \_getRValues
- [Prv] \_getRate
- [Prv] \_getCurrentSupply
- [Prv] \_takeLiquidity #
- [Prv] calculateTaxFee
- [Prv] calculateLiquidityFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Pub] excludeFromFee #
  - modifiers: onlyOwner
- [Pub] isExcludedFromMaxTxAmount
- [Pub] excludeFromMaxTxAmount #
  - modifiers: onlyOwner
- [Pub] includeToMaxTxAmount #
  - modifiers: onlyOwner
- [Pub] includeInFee #

- modifiers: onlyOwner
- [Ext] setTaxFeePercent #
  - modifiers: onlyOwner
- [Ext] setLiquidityFeePercent #
  - modifiers: onlyOwner
- [Ext] setMaxTxAmount #
  - modifiers: onlyOwner
- [Ext] setNumTokensSellToAddToLiquidity #
  - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
  - modifiers: onlyOwner
- [Ext] setMarketingAddress #
  - modifiers: onlyOwner
- [Ext] setBurnPartyAddress #
  - modifiers: onlyOwner
- [Prv] setDevAddress #
  - modifiers: onlyOwner
- [Pub] transferContractBalance #
  - modifiers: onlyOwner
- [Prv] transferOutETH #
- [Ext] <Fallback> (\$)

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

```
function includeInReward(address account↑) external onlyOwner() {
    require(!_isExcluded[account↑], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account↑) {
            _excluded[i] = _excluded[_excluded.length - 1];
            uint256 currentRate = _getRate();
            _rOwned[account↑] = _tOwned[account↑].mul(currentRate);
            _tOwned[account↑] = 0;
            _isExcluded[account↑] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- The function `_getCurrentSupply` also uses the loop for evaluating total supply. It also could be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function _getCurrentSupply() private view returns (uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (
            _rOwned[_excluded[i]] > rSupply ||
            _tOwned[_excluded[i]] > tSupply
        ) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

Recommendation:

Check that the excluded array length is not too big.

## Notes:

- swapAndLiquify function do not fully distribute contractTokenBalance.
- \_maxTxAmount value is higher than total supply.

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

- Owner can change tax and liquidity fees.

```
ftrace | funcSig
function setTaxFeePercent(uint256 taxFee↑) external onlyOwner() {
    _taxFee = taxFee↑;
}

ftrace | funcSig
function setLiquidityFeePercent(uint256 liquidityFee↑) external onlyOwner() {
    _liquidityFee = liquidityFee↑;
}
```

- Owner can change maximum transaction amount.

```
ftrace | funcSig
function setMaxTxAmount(uint256 maxTxAmount↑) external onlyOwner() {
    _maxTxAmount = maxTxAmount↑;
}
```

- Owner can include/exclude from maximum transaction amount.

```
ftrace | funcSig
function excludeFromMaxTxAmount(address account↑) public onlyOwner {
    _isExcludedFromMaxTxAmount[account↑] = true;
}

ftrace | funcSig
function includeToMaxTxAmount(address account↑) public onlyOwner {
    _isExcludedFromMaxTxAmount[account↑] = false;
}
```

- Owner can exclude from the fee.

```
function excludeFromFee(address account↑) public onlyOwner {
    _isExcludedFromFee[account↑] = true;
}
```

- Owner can change minimum number of tokens to add to liquidity.

```
ftrace | funcSig
function setNumTokensSellToAddToLiquidity(uint256 _minimumTokensBeforeSwap↑) external onlyOwner() {
    minimumTokensBeforeSwap = _minimumTokensBeforeSwap↑;
}
```

- Owner can change charity, utility, development and donation address.

```
ftrace | funcSig
function setCharityAddress(address payable _charityAddress↑) external onlyOwner() {
    charityAddress = _charityAddress↑;
}

ftrace | funcSig
function setUtilityAddress(address payable _utilityAddress↑) external onlyOwner() {
    utilityAddress = _utilityAddress↑;
}

ftrace | funcSig
function setDevelopmentAddress(address payable _developmentAddress↑) external onlyOwner() {
    developmentAddress = _developmentAddress↑;
}

ftrace | funcSig
function setDonationAddress(address payable _donationAddress↑) external onlyOwner() {
    donationAddress = _donationAddress↑;
}
```

- Owner can withdraw contract BNBs.

```
ftrace | funcSig
function transferContractBalance(uint256 amount↑) public onlyOwner {
    require(amount↑ > 0, "Transfer amount must be greater than zero");
    payable(owner()).transfer(amount↑);
}
```

- Owner can change marketing, burnParty and dev addresses.

```
function setMarketingAddress(address payable _MarketingAddress↑) external onlyOwner() {
    MarketingAddress = _MarketingAddress↑;
}

ftrace | funcSig
function setBurnPartyAddress(address payable _BurnPartyAddress↑) external onlyOwner() {
    BurnPartyAddress = _BurnPartyAddress↑;
}

ftrace | funcSig
function setDevAddress(address payable _DevAddress↑) private onlyOwner() {
    DevAddress = _DevAddress↑;
}
```



- Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.

```
ftrace | funcSig
function lock(uint256 time↑) public virtual onlyOwner {
    _previousOwner = _owner;
    _owner = address(0);
    _lockTime = now + time↑;
    emit OwnershipTransferred(_owner, address(0));
}

ftrace | funcSig
function unlock() public virtual {
    require(_previousOwner == msg.sender, "You don't have permission to unlock");
    require(now > _lockTime, "Contract is locked until 7 days");
    emit OwnershipTransferred(_owner, _previousOwner);
    _owner = _previousOwner;
}
```

# 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 provided by the team:

<https://bscscan.com/tx/0x0a5b551a786e6a3112f4d6edfe26b2bec1c9e5fa3cc9d1ccf180db3215241b41>

---

## *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.*