



Cyberscope

# Audit Report

## **DAKHUND**

March 2023

Network    BSC

Address    0xa23173b053fe3faab4c1d86e3bdb307d27ebb46d

Audited by    © cyberscope

# Table of Contents

|                                                  |           |
|--------------------------------------------------|-----------|
| <b>Table of Contents</b>                         | <b>1</b>  |
| <b>Review</b>                                    | <b>2</b>  |
| Audit Updates                                    | 2         |
| Source Files                                     | 2         |
| <b>Findings Breakdown</b>                        | <b>3</b>  |
| <b>Analysis</b>                                  | <b>4</b>  |
| <b>Diagnostics</b>                               | <b>5</b>  |
| PVC - Price Volatility Concern                   | 6         |
| Description                                      | 6         |
| Recommendation                                   | 6         |
| RSML - Redundant SafeMath Library                | 7         |
| Description                                      | 7         |
| Recommendation                                   | 7         |
| IDI - Immutable Declaration Improvement          | 8         |
| Description                                      | 8         |
| Recommendation                                   | 8         |
| L04 - Conformance to Solidity Naming Conventions | 9         |
| Description                                      | 9         |
| Recommendation                                   | 10        |
| L07 - Missing Events Arithmetic                  | 11        |
| Description                                      | 11        |
| Recommendation                                   | 11        |
| L09 - Dead Code Elimination                      | 12        |
| Description                                      | 12        |
| Recommendation                                   | 13        |
| L16 - Validate Variable Setters                  | 14        |
| Description                                      | 14        |
| Recommendation                                   | 14        |
| L17 - Usage of Solidity Assembly                 | 15        |
| Description                                      | 15        |
| Recommendation                                   | 15        |
| <b>Functions Analysis</b>                        | <b>16</b> |
| <b>Inheritance Graph</b>                         | <b>23</b> |
| <b>Flow Graph</b>                                | <b>24</b> |
| <b>Summary</b>                                   | <b>25</b> |
| <b>Disclaimer</b>                                | <b>26</b> |
| <b>About Cyberscope</b>                          | <b>27</b> |

## Review

|                  |                                                                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Contract Name    | LiquidityGeneratorToken                                                                                                                                     |
| Compiler Version | v0.8.4+commit.c7e474f2                                                                                                                                      |
| Optimization     | 200 runs                                                                                                                                                    |
| Explorer         | <a href="https://bscscan.com/address/0xa23173b053fe3faab4c1d86e3bdb307d27ebb46d">https://bscscan.com/address/0xa23173b053fe3faab4c1d86e3bdb307d27ebb46d</a> |
| Address          | 0xa23173b053fe3faab4c1d86e3bdb307d27ebb46d                                                                                                                  |
| Network          | BSC                                                                                                                                                         |
| Symbol           | DAKHUND                                                                                                                                                     |
| Decimals         | 9                                                                                                                                                           |
| Total Supply     | 1,000,000,000                                                                                                                                               |

## Audit Updates

|               |             |
|---------------|-------------|
| Initial Audit | 03 Apr 2023 |
|---------------|-------------|

## Source Files

|                             |                                                                      |
|-----------------------------|----------------------------------------------------------------------|
| Filename                    | SHA256                                                               |
| LiquidityGeneratorToken.sol | 1724eac36d3892bd38b0d2906dcc95930<br>443e7f66b307b3295bc1cad040ceac7 |

## Findings Breakdown



|                       |   |
|-----------------------|---|
| ● Critical            | 0 |
| ● Medium              | 0 |
| ● Minor / Informative | 8 |

| Severity              | Unresolved | Acknowledged | Resolved | Other |
|-----------------------|------------|--------------|----------|-------|
| ● Critical            | 0          | 0            | 0        | 0     |
| ● Medium              | 0          | 0            | 0        | 0     |
| ● Minor / Informative | 8          | 0            | 0        | 0     |

# Analysis

● Critical ● Medium ● Minor / Informative ● Pass

| Severity | Code | Description                        | Status |
|----------|------|------------------------------------|--------|
| ●        | ST   | Stops Transactions                 | Passed |
| ●        | OCTD | Transfers Contract's Tokens        | Passed |
| ●        | OTUT | Transfers User's Tokens            | Passed |
| ●        | ELFM | Exceeds Fees Limit                 | Passed |
| ●        | ULTW | Transfers Liquidity to Team Wallet | Passed |
| ●        | MT   | Mints Tokens                       | Passed |
| ●        | BT   | Burns Tokens                       | Passed |
| ●        | BC   | Blacklists Addresses               | Passed |

# Diagnostics

● Critical ● Medium ● Minor / Informative

| Severity | Code | Description                                | Status     |
|----------|------|--------------------------------------------|------------|
| ●        | PVC  | Price Volatility Concern                   | Unresolved |
| ●        | RSML | Redundant SafeMath Library                 | Unresolved |
| ●        | IDI  | Immutable Declaration Improvement          | Unresolved |
| ●        | L04  | Conformance to Solidity Naming Conventions | Unresolved |
| ●        | L07  | Missing Events Arithmetic                  | Unresolved |
| ●        | L09  | Dead Code Elimination                      | Unresolved |
| ●        | L16  | Validate Variable Setters                  | Unresolved |
| ●        | L17  | Usage of Solidity Assembly                 | Unresolved |

## PVC - Price Volatility Concern

|             |                                   |
|-------------|-----------------------------------|
| Criticality | Minor / Informative               |
| Location    | LiquidityGeneratorToken.sol#L1264 |
| Status      | Unresolved                        |

### Description

The contract accumulates tokens from the taxes to swap them for ETH. The variable `numTokensSellToAddToLiquidity` sets a threshold where the contract will trigger the swap functionality. If the variable is set to a big number, then the contract will swap a huge amount of tokens for ETH.

It is important to note that the price of the token representing it, can be highly volatile. This means that the value of a price volatility swap involving Ether could fluctuate significantly at the triggered point, potentially leading to significant price volatility for the parties involved.

```
function setSwapBackSettings(uint256 _amount) external onlyOwner {
    require(
        _amount >= totalSupply().mul(5).div(10**4),
        "Swapback amount should be at least 0.05% of total supply"
    );
    numTokensSellToAddToLiquidity = _amount;
    emit SwapAndLiquifyAmountUpdated(_amount);
}
```

### Recommendation

The contract could ensure that it will not sell more than a reasonable amount of tokens in a single transaction. A suggested implementation could check that the maximum amount should be less than a fixed percentage of the total supply. Hence, the contract will guarantee that it cannot accumulate a huge amount of tokens in order to sell them.

## RSML - Redundant SafeMath Library

|             |                             |
|-------------|-----------------------------|
| Criticality | Minor / Informative         |
| Location    | LiquidityGeneratorToken.sol |
| Status      | Unresolved                  |

### Description

SafeMath is a popular Solidity library that provides a set of functions for performing common arithmetic operations in a way that is resistant to integer overflows and underflows.

Starting with Solidity versions that are greater than or equal to 0.8.0, the arithmetic operations revert to underflow and overflow. As a result, the native functionality of the Solidity operations replaces the SafeMath library. Hence, the usage of the SafeMath library adds complexity, and overhead and increases gas consumption unnecessarily.

```
library SafeMath {...}
```

### Recommendation

The team is advised to remove the SafeMath library. Since the version of the contract is greater than `0.8.0` then the pure Solidity arithmetic operations produce the same result.

If the previous functionality is required, then the contract could exploit the `unchecked { ... }` statement.

Read more about the breaking change at

<https://docs.soliditylang.org/en/v0.8.16/080-breaking-changes.html#solidity-v0-8-0-breaking-changes>.

## IDI - Immutable Declaration Improvement

|                    |                                                                   |
|--------------------|-------------------------------------------------------------------|
| <b>Criticality</b> | Minor / Informative                                               |
| <b>Location</b>    | LiquidityGeneratorToken.sol#L997,998,999,1001,1010,1016,1022,1026 |
| <b>Status</b>      | Unresolved                                                        |

### Description

The contract is using variables that initialize them only in the constructor. The other functions are not mutating the variables. These variables are not defined as `immutable`.

```
_name  
_symbol  
_decimals  
_tTotal  
_charityAddress  
swapAndLiquifyEnabled  
uniswapV2Pair  
uniswapV2Router
```

### Recommendation

By declaring a variable as immutable, the Solidity compiler is able to make certain optimizations. This can reduce the amount of storage and computation required by the contract, and make it more gas-efficient.

## L04 - Conformance to Solidity Naming Conventions

|                    |                                                                      |
|--------------------|----------------------------------------------------------------------|
| <b>Criticality</b> | Minor / Informative                                                  |
| <b>Location</b>    | LiquidityGeneratorToken.sol#L641,942,945,948,953,1264,1403,1407,1415 |
| <b>Status</b>      | Unresolved                                                           |

### Description

The Solidity style guide is a set of guidelines for writing clean and consistent Solidity code. Adhering to a style guide can help improve the readability and maintainability of the Solidity code, making it easier for others to understand and work with.

The followings are a few key points from the Solidity style guide:

1. Use camelCase for function and variable names, with the first letter in lowercase (e.g., myVariable, updateCounter).
2. Use PascalCase for contract, struct, and enum names, with the first letter in uppercase (e.g., MyContract, UserStruct, ErrorEnum).
3. Use uppercase for constant variables and enums (e.g., MAX\_VALUE, ERROR\_CODE).
4. Use indentation to improve readability and structure.
5. Use spaces between operators and after commas.
6. Use comments to explain the purpose and behavior of the code.
7. Keep lines short (around 120 characters) to improve readability.

```
function WETH() external pure returns (address);
uint256 public _taxFee
uint256 public _liquidityFee
uint256 public _charityFee
address public _charityAddress
uint256 _amount
```

## Recommendation

By following the Solidity naming convention guidelines, the codebase increased the readability, maintainability, and makes it easier to work with.

Find more information on the Solidity documentation

<https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-convention>.

## L07 - Missing Events Arithmetic

|                    |                                             |
|--------------------|---------------------------------------------|
| <b>Criticality</b> | Minor / Informative                         |
| <b>Location</b>    | LiquidityGeneratorToken.sol#L1238,1249,1257 |
| <b>Status</b>      | Unresolved                                  |

### Description

Events are a way to record and log information about changes or actions that occur within a contract. They are often used to notify external parties or clients about events that have occurred within the contract, such as the transfer of tokens or the completion of a task.

It's important to carefully design and implement the events in a contract, and to ensure that all required events are included. It's also a good idea to test the contract to ensure that all events are being properly triggered and logged.

```
_taxFee = taxFeeBps  
_liquidityFee = liquidityFeeBps  
_charityFee = charityFeeBps
```

### Recommendation

By including all required events in the contract and thoroughly testing the contract's functionality, the contract ensures that it performs as intended and does not have any missing events that could cause issues with its arithmetic.

## L09 - Dead Code Elimination

|             |                                                                          |
|-------------|--------------------------------------------------------------------------|
| Criticality | Minor / Informative                                                      |
| Location    | LiquidityGeneratorToken.sol#L441,469,494,504,523,537,556,566,583,593,610 |
| Status      | Unresolved                                                               |

### Description

In Solidity, dead code is code that is written in the contract, but is never executed or reached during normal contract execution. Dead code can occur for a variety of reasons, such as:

- Conditional statements that are always false.
- Functions that are never called.
- Unreachable code (e.g., code that follows a return statement).

Dead code can make a contract more difficult to understand and maintain, and can also increase the size of the contract and the cost of deploying and interacting with it.

```
function isContract(address account) internal view returns (bool) {
    // This method relies on extcodesize, which returns 0 for
    contracts in
    // construction, since the code is only stored at the end of the
    // constructor execution.

    uint256 size;
    assembly {
        size := extcodesize(account)
    }
    return size > 0;
}

...
```

## Recommendation

To avoid creating dead code, it's important to carefully consider the logic and flow of the contract and to remove any code that is not needed or that is never executed. This can help improve the clarity and efficiency of the contract.

## L16 - Validate Variable Setters

|                    |                                   |
|--------------------|-----------------------------------|
| <b>Criticality</b> | Minor / Informative               |
| <b>Location</b>    | LiquidityGeneratorToken.sol#L1041 |
| <b>Status</b>      | Unresolved                        |

### Description

The contract performs operations on variables that have been configured on user-supplied input. These variables are missing of proper check for the case where a value is zero. This can lead to problems when the contract is executed, as certain actions may not be properly handled when the value is zero.

```
payable(serviceFeeReceiver_).transfer(serviceFee_)
```

### Recommendation

By adding the proper check, the contract will not allow the variables to be configured with zero value. This will ensure that the contract can handle all possible input values and avoid unexpected behavior or errors. Hence, it can help to prevent the contract from being exploited or operating unexpectedly.

## L17 - Usage of Solidity Assembly

|                    |                                      |
|--------------------|--------------------------------------|
| <b>Criticality</b> | Minor / Informative                  |
| <b>Location</b>    | LiquidityGeneratorToken.sol#L447,622 |
| <b>Status</b>      | Unresolved                           |

### Description

Using assembly can be useful for optimizing code, but it can also be error-prone. It's important to carefully test and debug assembly code to ensure that it is correct and does not contain any errors.

Some common types of errors that can occur when using assembly in Solidity include Syntax, Type, Out-of-bounds, Stack, and Revert.

```
assembly {  
    size := extcodesize(account)  
}  
  
assembly {  
    let returndata_size := mload(returndata)  
    revert(add(32, returndata), returndata_size)  
}
```

### Recommendation

It is recommended to use assembly sparingly and only when necessary, as it can be difficult to read and understand compared to Solidity code.

## Functions Analysis

| Contract       | Type              | Bases      |            |           |
|----------------|-------------------|------------|------------|-----------|
|                | Function Name     | Visibility | Mutability | Modifiers |
|                |                   |            |            |           |
| <b>IERC20</b>  | Interface         |            |            |           |
|                | totalSupply       | External   |            | -         |
|                | balanceOf         | External   |            | -         |
|                | transfer          | External   | ✓          | -         |
|                | allowance         | External   |            | -         |
|                | approve           | External   | ✓          | -         |
|                | transferFrom      | External   | ✓          | -         |
|                |                   |            |            |           |
| <b>Context</b> | Implementation    |            |            |           |
|                | _msgSender        | Internal   |            |           |
|                | _msgData          | Internal   |            |           |
|                |                   |            |            |           |
| <b>Ownable</b> | Implementation    | Context    |            |           |
|                |                   | Public     | ✓          | -         |
|                | owner             | Public     |            | -         |
|                | renounceOwnership | Public     | ✓          | onlyOwner |
|                | transferOwnership | Public     | ✓          | onlyOwner |
|                | _setOwner         | Private    | ✓          |           |

|                 |                       |          |   |  |
|-----------------|-----------------------|----------|---|--|
|                 |                       |          |   |  |
| <b>SafeMath</b> | Library               |          |   |  |
|                 | tryAdd                | Internal |   |  |
|                 | trySub                | Internal |   |  |
|                 | tryMul                | Internal |   |  |
|                 | tryDiv                | Internal |   |  |
|                 | tryMod                | Internal |   |  |
|                 | add                   | Internal |   |  |
|                 | sub                   | Internal |   |  |
|                 | mul                   | Internal |   |  |
|                 | div                   | Internal |   |  |
|                 | mod                   | Internal |   |  |
|                 | sub                   | Internal |   |  |
|                 | div                   | Internal |   |  |
|                 | mod                   | Internal |   |  |
|                 |                       |          |   |  |
| <b>Address</b>  | Library               |          |   |  |
|                 | isContract            | Internal |   |  |
|                 | sendValue             | Internal | ✓ |  |
|                 | functionCall          | Internal | ✓ |  |
|                 | functionCall          | Internal | ✓ |  |
|                 | functionCallWithValue | Internal | ✓ |  |
|                 | functionCallWithValue | Internal | ✓ |  |

|                           |                              |          |         |   |
|---------------------------|------------------------------|----------|---------|---|
|                           | functionStaticCall           | Internal |         |   |
|                           | functionStaticCall           | Internal |         |   |
|                           | functionDelegateCall         | Internal | ✓       |   |
|                           | functionDelegateCall         | Internal | ✓       |   |
|                           | verifyCallResult             | Internal |         |   |
|                           |                              |          |         |   |
| <b>IUniswapV2Router01</b> | Interface                    |          |         |   |
|                           | factory                      | External |         | - |
|                           | WETH                         | External |         | - |
|                           | addLiquidity                 | External | ✓       | - |
|                           | addLiquidityETH              | External | Payable | - |
|                           | removeLiquidity              | External | ✓       | - |
|                           | removeLiquidityETH           | External | ✓       | - |
|                           | removeLiquidityWithPermit    | External | ✓       | - |
|                           | removeLiquidityETHWithPermit | External | ✓       | - |
|                           | swapExactTokensForTokens     | External | ✓       | - |
|                           | swapTokensForExactTokens     | External | ✓       | - |
|                           | swapExactETHForTokens        | External | Payable | - |
|                           | swapTokensForExactETH        | External | ✓       | - |
|                           | swapExactTokensForETH        | External | ✓       | - |
|                           | swapETHForExactTokens        | External | Payable | - |
|                           | quote                        | External |         | - |
|                           | getAmountOut                 | External |         | - |

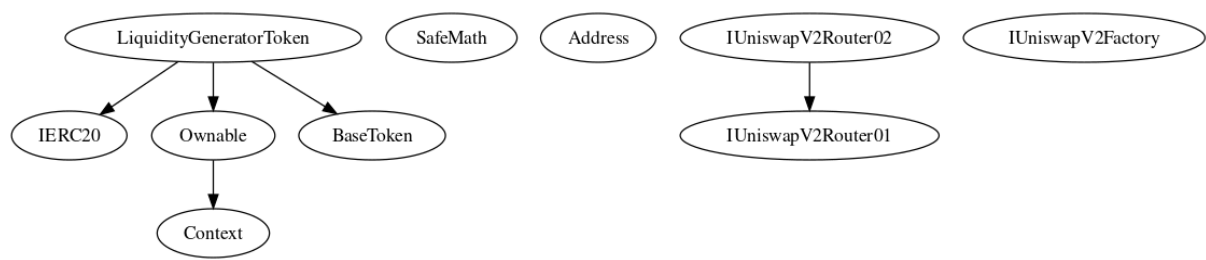
|                           |                                                           |                    |         |   |
|---------------------------|-----------------------------------------------------------|--------------------|---------|---|
|                           | getAmountIn                                               | External           |         | - |
|                           | getAmountsOut                                             | External           |         | - |
|                           | getAmountsIn                                              | External           |         | - |
|                           |                                                           |                    |         |   |
| <b>IUniswapV2Router02</b> | Interface                                                 | IUniswapV2Router01 |         |   |
|                           | removeLiquidityETHSupportingFeeOnTransferTokens           | External           | ✓       | - |
|                           | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External           | ✓       | - |
|                           | swapExactTokensForTokensSupportingFeeOnTransferTokens     | External           | ✓       | - |
|                           | swapExactETHForTokensSupportingFeeOnTransferTokens        | External           | Payable | - |
|                           | swapExactTokensForETHSupportingFeeOnTransferTokens        | External           | ✓       | - |
|                           |                                                           |                    |         |   |
| <b>IUniswapV2Factory</b>  | Interface                                                 |                    |         |   |
|                           | feeTo                                                     | External           |         | - |
|                           | feeToSetter                                               | External           |         | - |
|                           | getPair                                                   | External           |         | - |
|                           | allPairs                                                  | External           |         | - |
|                           | allPairsLength                                            | External           |         | - |
|                           | createPair                                                | External           | ✓       | - |
|                           | setFeeTo                                                  | External           | ✓       | - |
|                           | setFeeToSetter                                            | External           | ✓       | - |
|                           |                                                           |                    |         |   |
| <b>BaseToken</b>          | Implementation                                            |                    |         |   |

|                                |                       |                            |         |           |
|--------------------------------|-----------------------|----------------------------|---------|-----------|
|                                |                       |                            |         |           |
| <b>LiquidityGeneratorToken</b> | Implementation        | IERC20, Ownable, BaseToken |         |           |
|                                |                       | Public                     | Payable | -         |
|                                | name                  | Public                     |         | -         |
|                                | symbol                | Public                     |         | -         |
|                                | decimals              | Public                     |         | -         |
|                                | totalSupply           | Public                     |         | -         |
|                                | balanceOf             | Public                     |         | -         |
|                                | transfer              | Public                     | ✓       | -         |
|                                | allowance             | Public                     |         | -         |
|                                | approve               | Public                     | ✓       | -         |
|                                | transferFrom          | Public                     | ✓       | -         |
|                                | increaseAllowance     | Public                     | ✓       | -         |
|                                | decreaseAllowance     | Public                     | ✓       | -         |
|                                | isExcludedFromReward  | Public                     |         | -         |
|                                | totalFees             | Public                     |         | -         |
|                                | deliver               | Public                     | ✓       | -         |
|                                | reflectionFromToken   | Public                     |         | -         |
|                                | tokenFromReflection   | Public                     |         | -         |
|                                | excludeFromReward     | Public                     | ✓       | onlyOwner |
|                                | includeInReward       | External                   | ✓       | onlyOwner |
|                                | _transferBothExcluded | Private                    | ✓       |           |
|                                | excludeFromFee        | Public                     | ✓       | onlyOwner |

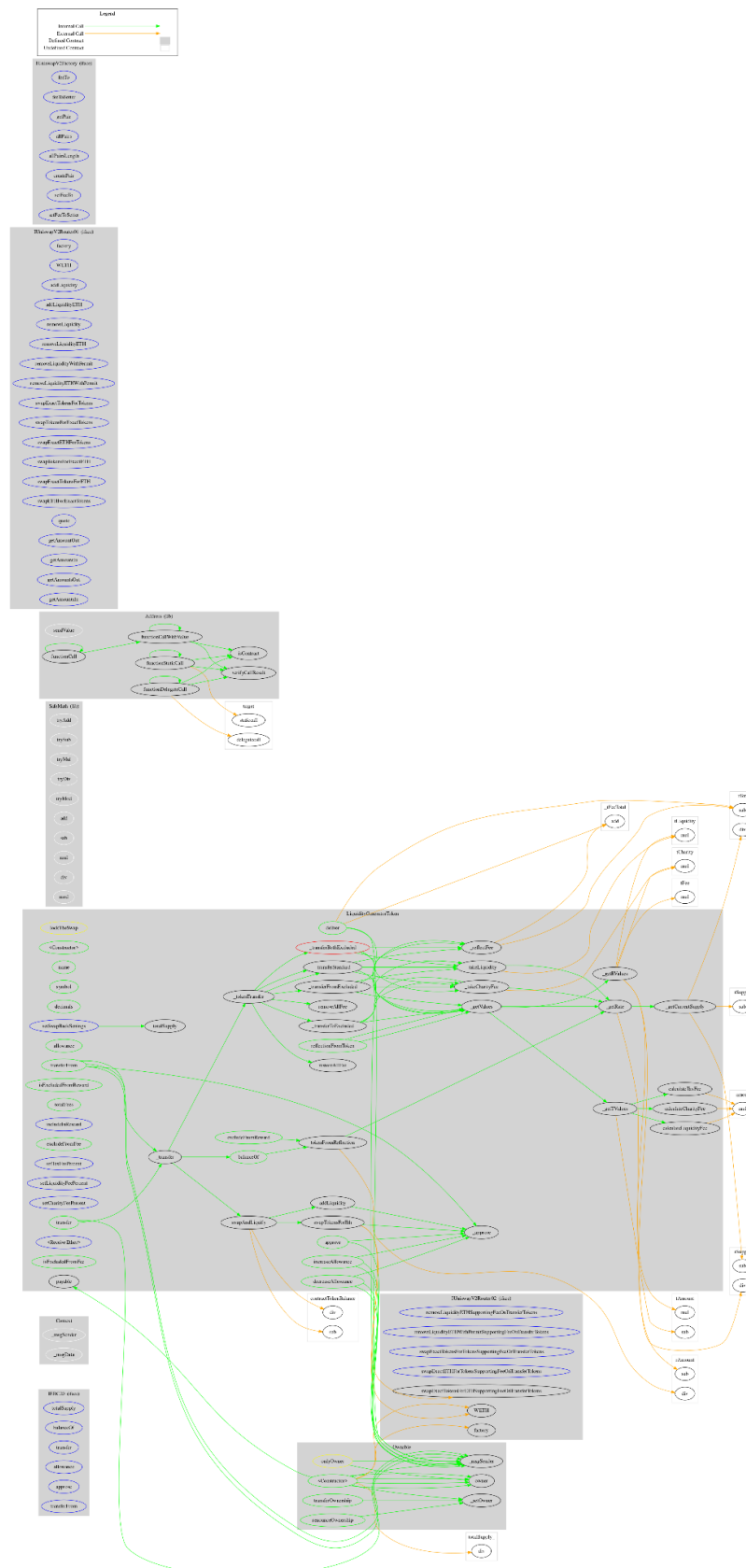
|  |                        |          |         |             |
|--|------------------------|----------|---------|-------------|
|  | setTaxFeePercent       | External | ✓       | onlyOwner   |
|  | setLiquidityFeePercent | External | ✓       | onlyOwner   |
|  | setCharityFeePercent   | External | ✓       | onlyOwner   |
|  | setSwapBackSettings    | External | ✓       | onlyOwner   |
|  |                        | External | Payable | -           |
|  | _reflectFee            | Private  | ✓       |             |
|  | _getValues             | Private  |         |             |
|  | _getTVValues           | Private  |         |             |
|  | _getRValues            | Private  |         |             |
|  | _getRate               | Private  |         |             |
|  | _getCurrentSupply      | Private  |         |             |
|  | _takeLiquidity         | Private  | ✓       |             |
|  | _takeCharityFee        | Private  | ✓       |             |
|  | calculateTaxFee        | Private  |         |             |
|  | calculateLiquidityFee  | Private  |         |             |
|  | calculateCharityFee    | Private  |         |             |
|  | removeAllFee           | Private  | ✓       |             |
|  | restoreAllFee          | Private  | ✓       |             |
|  | isExcludedFromFee      | Public   |         | -           |
|  | _approve               | Private  | ✓       |             |
|  | _transfer              | Private  | ✓       |             |
|  | swapAndLiquify         | Private  | ✓       | lockTheSwap |
|  | swapTokensForEth       | Private  | ✓       |             |

|  |                       |         |   |  |
|--|-----------------------|---------|---|--|
|  | addLiquidity          | Private | ✓ |  |
|  | _tokenTransfer        | Private | ✓ |  |
|  | _transferStandard     | Private | ✓ |  |
|  | _transferToExcluded   | Private | ✓ |  |
|  | _transferFromExcluded | Private | ✓ |  |

## Inheritance Graph



# Flow Graph



## Summary

DAKHUND Token contract implements a token mechanism. This audit investigates security issues, business logic concerns, and potential improvements. DAKHUND Token is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. There is also a limit of max 25% fees.

## Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security. Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

## About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.



**The Cyberscope team**

<https://www.cyberscope.io>