Doge Gang

0xa14138FB151241f80e5F44f4829b84eFE9f6957A

SECURITY AUDIT

By auditplus.org
E-mail: business@auditplus.org

Audit Plus

Project information

- TOKEN Name: **Doge Gang**
- SYMBOL: **DogeGang**
- Contract Address: **0xa14138FB151241f80e5F44f4829b84eFE9f6957A**
- Website: https://www.dogegang.io
- Contract Type: **Deflationary Token**
- Audit Type: **Security Audit/ LP Check**
- The contract source code is verified on BSCSCAN
    - Contract name: **CoinToken**
    - Optimization: Yes with 200 runs
    - Compiler version: solidity 0.6.12
    - License: default evmVersion, Apache-2.0
- Contract owner: **0xf67efa43c88016d709c9037ed370ae9c048c3c91**
- Contract Deployer: **0xf103d2aba493749a402b7de11cf31f5844062b74**
- PancakeSwapV2 Address: **0x8Aa8f53175FEdA4add479154C7603B8912516128**
- E-mail: info@dogegang.io
- Telegram: https://t.me/dogegangtoken
- Twitter: https://twitter.com/dogegang_io
- Reddit: https://www.reddit.com/r/dogegang_io/

Function Report

+ **[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]** geUnlockTime
    - **[Pub]** lock # - modifiers: onlyOwner
    - **[Pub]** unlock #

Function Report

+ **[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 #

Function Report

+ **[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 #

+ CoinToken (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 #

Function Report

- [Pub] decreaseAllowance #
- [Pub] isExcludedFromReward
- [Pub] totalFees
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Pub] excludeFromReward # - modifiers: onlyOwner
- [Ext] includeInReward # - modifiers: onlyOwner
- [Prv] _transferBothExcluded #
- [Pub] excludeFromFee # - modifiers: onlyOwner
- [Pub] includeInFee # - modifiers: onlyOwner
- [Ext] setTaxFeePercent # - modifiers: onlyOwner
- [Ext] setLiquidityFeePercent # - modifiers: onlyOwner
- [Ext] setMaxTxPercent # - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled # - modifiers: onlyOwner
- [Ext] <Fallback> ($)
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] calculateTaxFee
- [Prv] calculateLiquidityFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] swapAndLiquify # - modifiers: lockTheSwap
- [Prv] swapTokensForEth #
- [Prv] addLiquidity #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #

($) = payable function
= non-constant function

Issues Status

Description	STATUS
1 Compiler errors.	Passed
2 Race conditions and Reentrancy.	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

1. High Severity Issues

No high severity issues found.

2. Medium Severity Issues

No medium severity issues found.

3. Low Severity Issues

3.1 Out of gas

Issue:

The function includeInReward() uses the loop to find and remove addresses from the _isExcluded 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];
            _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);
}
```

Conclusion

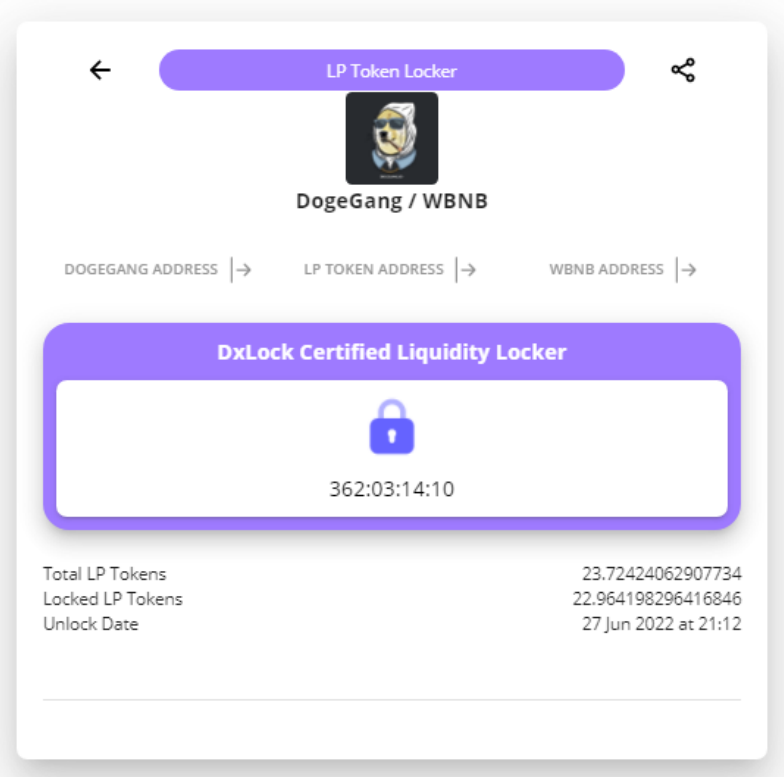
Smart-contract does not contain any high severity issues.

LP Check

LP includes 3 holders and 96.79% of the liquidity pool are in 0xeb3a9c56d963b971d320f889be2fb8b59853e449 contract address. The contract code is not verified but after researching we found out that the contract belongs to dxsale.app website.

Rank	Address	Quantity	Percentage
1	0xeb3a9c56d963b971d320f889be2fb8b59853e449	22.964198296416846809	96.7963%
2	0xf67efa43c88016d709c9037ed370ae9c048c3c91	0.705601331174294793	2.9742%
3	0x07d80ae6f36a5e08dca74ce884a24d39db9934ed	0.054441001486199513	0.2295%
4	0x0000000000000000000000000000000000000000	0.000000000000001	0.0000%

After browsing dxsale.app we found the token locker link. This link should be opened in DApp wallet browser or opened in chrome when Metamask is connected.
https://dxsale.app/app/pages/dxlockview?id=0&add=0xf67efa43C88016d709C9037Ed370ae9C048c3C91&type=lplock&chain=BSC



Disclaimer:
This report does not indicate the participation of AUDITPLUS in the project. The report only applies to the contract address mentioned and meant to be used only for the specified project. This audit makes no statements or warranties on the business model, investment attractiveness, or code sustainability.

Website: www.auditplus.org
Email: business@auditplus.org