Techrate1 Techrate

TechRate

AUDIT COMPANY

# Smart Contract Security Audit

TechRate

January, 2022

# Audit Details

Audited project

Lemon Swap

Deployer address

0x161a61bc66f625277da70a38bb7307c89fc92836

Client contacts:

Lemon Swap team

Blockchain

Binance Smart Chain

Project website:

[https://lemonswap.net/](https://lemonswap.net/)

# 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 Lemon Swap to perform an audit of smart contracts:

https://bscscan.com/address/0x86A611fa791C22f91f38E49dEa494A85ae2dCbc0#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.

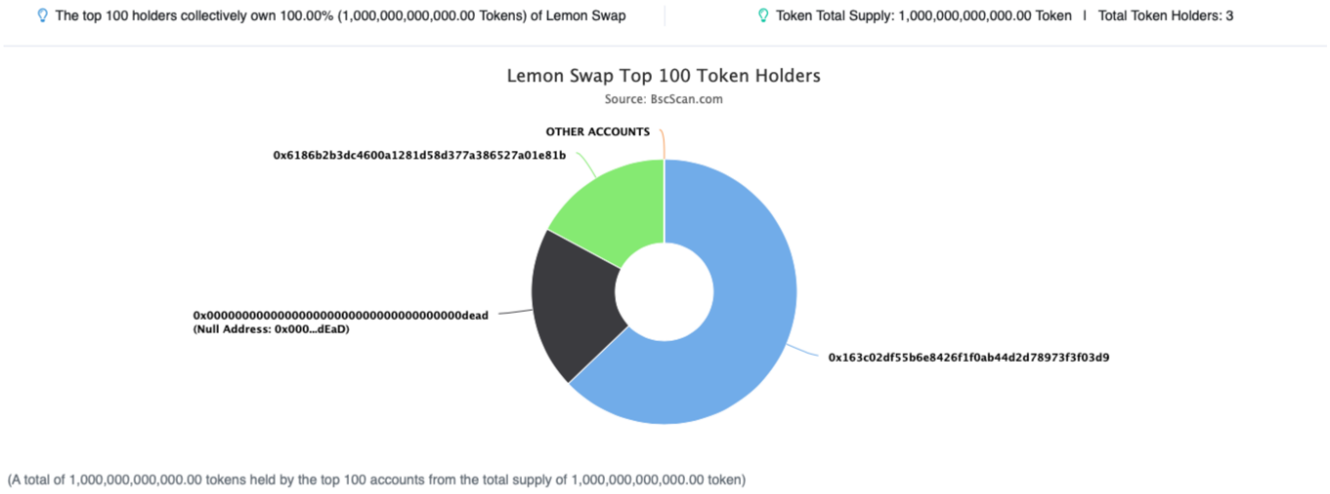
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

# Contracts Details

## Token contract details for 20.01.2022

| | |
|---|---|
| Contract name | Lemon Swap |
| Contract address | 0x86A611fa791C22f91f38E49dEa494A85ae2dCbc0 |
| Total supply | 1,000,000,000,000 |
| Token ticker | Lemon |
| Decimals | 18 |
| Token holders | 3 |
| Transactions count | 3 |
| Top 100 holders dominance | 100.00% |
| Max wallet rate | 300 |
| Marketing wallet | 0x4de20e96ce7690f72517c3ae299cb371f1e06b8b |
| Dev wallet | 0xcebbc397b444015c90c14359b4e4183dff6ac83a |
| Max transfer amount rate | 500 |
| Dividend tracker | 0x0f98643cbb2889af4e0f1081aa3a642dd7ef4340 |
| Uniswap V2 pair | 0x083994340c0f6192c62d968450acc3565797fa59 |
| Contract deployer address | 0x161a61bc66f625277da70a38bb7307c89fc92836 |
| Contract's current owner address | 0x6186b2b3dc4600a1281d58d377a386527a01e81b |

# Lemon Swap Token Distribution



The top 100 holders collectively own 100.00% (1,000,000,000,000.00 Tokens) of Lemon Swap

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

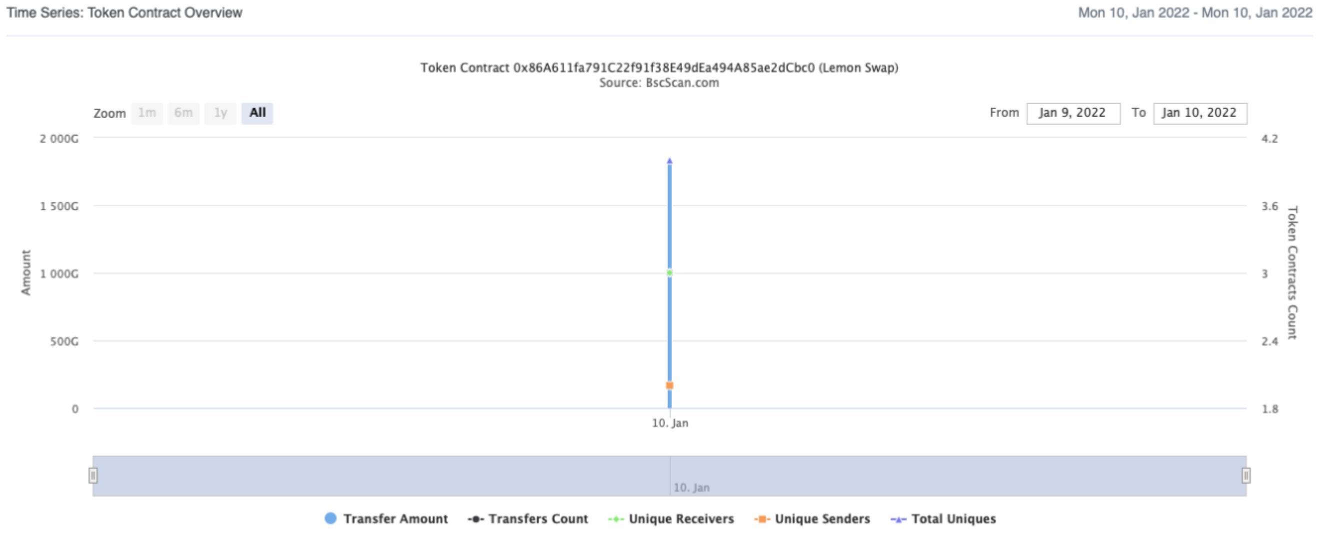
Lemon Swap Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0x6186b2b3dc4600a1281d58d377a386527a01e81b
0x000000000000000000000000000000000000dead
(Null Address: 0x000...dEaD)
0x163c02df55b6e8426f1f0ab44d2d78973f3f03d9

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

# Lemon Swap Contract Interaction Details



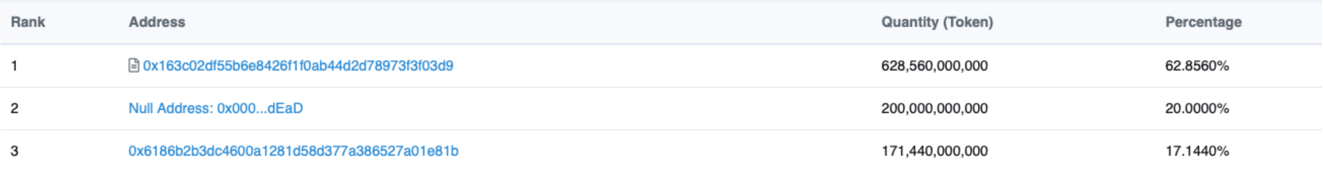
Time Series: Token Contract Overview

Mon 10, Jan 2022 - Mon 10, Jan 2022

Token Contract 0x86A611fa791C22f91f38E49dEa494A85ae2dCbc0 (Lemon Swap)

Source: BscScan.com

# Lemon Swap Top 10 Token Holders



| Rank | Address | Quantity (Token) | Percentage |
|---|---|---|---|
| 1 | 0x163c02df55b6e8426f1f0ab44d2d78973f3f03d9 | 628,560,000,000 | 62.8560% |
| 2 | Null Address: 0x000...dEaD | 200,000,000,000 | 20.0000% |
| 3 | 0x6186b2b3dc4600a1281d58d377a386527a01e81b | 171,440,000,000 | 17.1440% |

# Contract functions details

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

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

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

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

 +  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] SafeMath
   - [Int] add
   - [Int] sub
   - [Int] sub
   - [Int] mul
```

```
    - [Int] div
    - [Int] div
    - [Int] mod
    - [Int] mod

 + [Lib] SafeMathInt
    - [Int] mul
    - [Int] div
    - [Int] sub
    - [Int] add
    - [Int] abs
    - [Int] toUint256Safe

 + [Lib] SafeMathUint
    - [Int] toInt256Safe

 + [Int] DividendPayingTokenInterface
    - [Ext] dividendOf
    - [Ext] distributeDividends ($)
    - [Ext] withdrawDividend #

 + [Int] DividendPayingTokenOptionalInterface
    - [Ext] withdrawableDividendOf
    - [Ext] withdrawnDividendOf
    - [Ext] accumulativeDividendOf

 +  DividendPayingToken (ERC20, DividendPayingTokenInterface,
DividendPayingTokenOptionalInterface)
    - [Pub] <Constructor> #
       - modifiers: ERC20
    - [Ext] <Fallback> ($)
    - [Pub] distributeDividends ($)
    - [Pub] withdrawDividend #
    - [Int] _withdrawDividendOfUser #
    - [Pub] dividendOf
    - [Pub] withdrawableDividendOf
    - [Pub] withdrawnDividendOf
    - [Pub] accumulativeDividendOf
    - [Int] _transfer #
    - [Int] _mint #
    - [Int] _burn #
    - [Int] _setBalance #

 + [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 #

```
+ [Lib] IterableMapping
  - [Int] get
  - [Int] getIndexOfKey
  - [Int] getKeyAtIndex
  - [Int] size
  - [Int] set #
  - [Int] remove #

+  LemonSwapDividendTracker (DividendPayingToken, Ownable)
  - [Pub] <Constructor> #
    - modifiers: DividendPayingToken
  - [Pub] decimals
  - [Int] _transfer
  - [Pub] getAllowCustomTokens
  - [Ext] setAllowCustomTokens #
    - modifiers: onlyOwner
  - [Ext] excludeFromDividends #
    - modifiers: onlyOwner
  - [Pub] isExcludedFromDividends
  - [Ext] updateClaimWait #
    - modifiers: onlyOwner
  - [Ext] updateMinimumTokenBalanceForDividends #
    - modifiers: onlyOwner
  - [Ext] getLastProcessedIndex
  - [Ext] getNumberOfTokenHolders
  - [Pub] getAccount
  - [Pub] getAccountAtIndex
  - [Prv] canAutoClaim
  - [Ext] setBalance #
    - modifiers: onlyOwner
  - [Pub] process #
  - [Pub] processAccount #
    - modifiers: onlyOwner
  - [Pub] updateUniswapV2Router #
    - modifiers: onlyOwner
  - [Pub] updatePayoutToken #
    - modifiers: onlyOwner
  - [Pub] getPayoutToken
  - [Pub] updateAllowTokens #
    - modifiers: onlyOwner
  - [Pub] getAllowTokens
  - [Int] _withdrawDividendOfUser #

+  LemonSwap (ERC20, Ownable)
  - [Pub] <Constructor> #
    - modifiers: ERC20
  - [Pub] decimals
  - [Pub] setMaxWalletRate #
    - modifiers: onlyOwner
  - [Ext] <Fallback> ($)
  - [Ext] setSwapTokensAtAmount #
    - modifiers: onlyOwner
  - [Pub] updateDividendTracker #
    - modifiers: onlyOwner
  - [Pub] updateUniswapV2Router #
```

  - modifiers: onlyOwner
- [Pub] excludeFromFees #
  - modifiers: onlyOwner
- [Pub] excludeMultipleAccountsFromFees #
  - modifiers: onlyOwner
- [Ext] updateMarketingWallet #
  - modifiers: onlyOwner
- [Ext] updateDevWallet #
  - modifiers: onlyOwner
- [Int] isFeeAcceptable
- [Ext] setMarketingSellFee #
  - modifiers: onlyOwner
- [Ext] setMarketingBuyFee #
  - modifiers: onlyOwner
- [Ext] setDevSellFee #
  - modifiers: onlyOwner
- [Ext] setDevBuyFee #
  - modifiers: onlyOwner
- [Ext] setLiquiditySellFee #
  - modifiers: onlyOwner
- [Ext] setLiquidityBuyFee #
  - modifiers: onlyOwner
- [Ext] setReflectionSellFee #
  - modifiers: onlyOwner
- [Ext] setReflectionBuyFee #
  - modifiers: onlyOwner
- [Pub] setAutomatedMarketMakerPair #
  - modifiers: onlyOwner
- [Prv] _setAutomatedMarketMakerPair #
- [Pub] updateGasForProcessing #
  - modifiers: onlyOwner
- [Ext] updateClaimWait #
  - modifiers: onlyOwner
- [Ext] getClaimWait
- [Ext] updateMinimumTokenBalanceForDividends #
  - modifiers: onlyOwner
- [Ext] getMinimumTokenBalanceForDividends
- [Ext] getTotalDividendsDistributed
- [Pub] isExcludedFromFees
- [Pub] withdrawableDividendOf
- [Pub] dividendTokenBalanceOf
- [Ext] excludeFromDividends #
  - modifiers: onlyOwner
- [Pub] isExcludedFromDividends
- [Ext] getAccountDividendsInfo
- [Ext] getAccountDividendsInfoAtIndex
- [Ext] processDividendTracker #
- [Ext] claim #
- [Ext] claimFor #
- [Ext] getLastProcessedIndex
- [Ext] getNumberOfDividendTokenHolders
- [Int] _transfer #
  - modifiers: antiWhale
- [Prv] swapAndLiquify #
- [Prv] swapAndSendDividendsMarketingDev #

- [Prv] swapTokensForEth #
- [Prv] addLiquidity #
- [Pub] setAntiBotSystemEnable #
  - modifiers: onlyOwner
- [Pub] setBotSettingTime #
  - modifiers: onlyOwner
- [Pub] setBotFeeMultiplicator #
  - modifiers: onlyOwner
- [Pub] excludeAntibot #
  - modifiers: onlyOwner
- [Pub] isBot
- [Pub] setEnableAntiwhale #
  - modifiers: onlyOwner
- [Pub] maxTransferAmount
- [Pub] setMaxTransferAmountRate #
  - modifiers: onlyOwner
- [Pub] updatePayoutToken #
- [Pub] getPayoutToken
- [Pub] updateAllowTokens #
  - modifiers: onlyOwner
- [Pub] getAllowTokens
- [Pub] enableSwapAndLiquify #
  - modifiers: onlyOwner
- [Pub] setSwapTokensAmountMax #
  - modifiers: onlyOwner
- [Ext] getNativeBalance
- [Ext] getCountOfFeesToSwap
- [Ext] transferERC20Token #
  - modifiers: onlyOwner
- [Pub] setExcludeAntiwhale #
  - modifiers: onlyOwner
- [Pub] setExcludeMaxWallet #
  - 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. | Low issues |
| 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 excludeMultipleAccountsFromFees() uses the loop to exclude multiple accounts from fees. Function will be aborted with OUT_OF_GAS exception if there will be a long addresses list.

Recommendation:

Be careful about accounts array length.

### 2. swapAndLiquify issue

Issue:

- The function swapAndLiquify() do not returns after emitting zero event on “*(tokens > balanceOf(address(this)))”*.

Recommendation:

Return will restrict further code running.

## Notes:

- Dividend tracker may be changed. So that logic of setBalance and other functions could be another and not audited.

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

- Owner can change _maxWalletSize.
- Owner can change swapTokensAtAmount.
- Owner can change dividend tracker.
- Owner can change Uniswap router address.
- Owner can exclude from the fees.
- Owner can change marketing and dev wallet addresses.
- Owner can change fees.
- Owner can exclude and include addresses in automatedMarketMakerPairs array.
- Owner can change gas for processing.
- Owner can change claim wait value.
- Owner can change minimum tokens for dividends.
- Owner can exclude addresses from dividends.
- Owner can enable/disable antibotSystemEnable.
- Owner can change bot settings time.
- Owner can change _botIncreaseFee.
- Owner can exclude from antiBot.
- Owner can enable/disable antiWahle.
- Owner can change maxTransferAmountRate.
- Owner can change allow tokens.
- Owner can enable/disable swap and liquify.
- Owner can change swapTokensAtAmountMax.
- Owner can withdraw contract ERC20 tokens.
- Owner can exclude from antiWahle and maxWallet.

# 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 are provided by the team:
https://www.pinksale.finance/#/launchpad/0x163C02dF55b6e8426f1f0AB44d2D78973f3f03D9?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.*