



AUDIT REPORT

SecureWise

SMART CONTRACT AUDIT



Table of Contents

03

Disclaimer

04

Overview

05

Quick Result

06

Auditing
Approach and
Methodologies

07

Automated
Analysis

13

Inheritance
Graph

14

Contract
Summary

15

Manual Review

Disclaimer

SecureWise provides the smart contract audit of solidity. Audit and report are for informational purposes only and not, nor should be considered, as an endorsement to engage with, invest in, participate, provide an incentive, or disapprove, criticise, discourage, or purport to provide an opinion on any particular project or team.

This audit report doesn't provide any warranty or guarantee regarding the nature of the technology analysed. These reports, in no way, provide investment advice, nor should be used as investment advice of any sort. Investors must always do their own research and manage their risk.

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 SecureWise and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) SecureWise owe no duty of care towards you or any other person, nor does SecureWise 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 SecureWise 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, SecureWise hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SecureWise, 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.

Overview

Token Name: QATAR INU (**QTRINU**)

Methodology: Automated Analysis, Manual Code Review

Language: Solidity

Contract Address: 0x9B33c8a57FBFaa764C5A0FE4189cDad70710d1F5

ContractLink: <https://bscscan.com/address/0x9B33c8a57FBFaa764C5A0FE4189cDad70710d1F5>

Network: Binance Smart Chain (BSC)

Decimals: 9

Supply: 100.000.000.000

Website: <https://qatarinu.com/>

Twitter: <https://twitter.com/Qatarinu>

Telegram: <https://t.me/QatarInu>

Report Date: September 2, 2022

Quick Result

SecureWise has applied the automated and manual analysis of Smart Contract and were reviewed for common contract vulnerabilities and centralized exploits

Owner Privileges

-  The owner can set the max tx amount "0"
-  The owner can set fees up to 100%
-  Auto liquidity is going to an externally owned account
-  The owner can exclude accounts from rewards
-  The owner can change transaction lock-time without limit
-  The owner can exclude accounts from fees
-  The owner can change swap settings

QATAR INU (QTRINU) has successfully **PASSED** the smart contract audit with **HIGH MEDIUM and LOW** severity issue

Auditing Approach and Methodologies

SecureWise has performed starting with analyzing the code, issues, code quality, and libraries. Reviewed line-by-line by our team. Finding any potential issue like race conditions, transaction-ordering dependence, timestamp dependence, and denial of service attacks.

Methodology

- Understanding the size, scope and functionality of your project's source code
- Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Testing and automated analysis of the Smart Contract to determine proper logic has been followed throughout the whole process
- Deploying the code on testnet using multiple live test
- Analyzing a program to determine the specific input that causes different parts of a program to execute its functions.
- Checking whether all the libraries used in the code are on the latest version.

Goals

Smart Contract System is secure, resilient and working according to the specifications and without any vulnerabilities.

Risk Classification

High: Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, of the contract and its functions. Must be fixed as soon as possible.

Medium: Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Must be fixed as soon as possible.

Low: Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.

Automated Analysis

| Symbol | Meaning |
|--------|---------------------------|
| | Function can modify state |
| | Function is payable |

| Context | Implementation | | | |
|-----------------|----------------|----------|--|----|
| L | _msgSender | Internal | | |
| L | _msgData | Internal | | |
| | | | | |
| IERC20 | Interface | | | |
| L | totalSupply | External | | NO |
| L | balanceOf | External | | NO |
| L | transfer | External | | NO |
| L | allowance | External | | NO |
| L | approve | External | | NO |
| L | transferFrom | External | | NO |
| | | | | |
| SafeMath | Library | | | |
| L | add | Internal | | |
| L | sub | Internal | | |
| L | sub | Internal | | |
| L | mul | Internal | | |
| L | div | Internal | | |
| L | div | Internal | | |
| L | mod | Internal | | |
| L | mod | Internal | | |

| Address | Implementation | | | |
|---------|------------------------|----------|--|--|
| L | isContract | Internal | | |
| L | sendValue | Internal | | |
| L | functionCall | Internal | | |
| L | functionCall | Internal | | |
| L | functionCallWithValue | Internal | | |
| L | functionCallWithValue | Internal | | |
| L | _functionCallWithValue | Private | | |

Automated Analysis

| Ownable | Implementation | Context | | |
|-------------------|----------------------|----------|---|-----------|
| L | | Public | ● | NO |
| L | owner | Public | | NO |
| L | renounceOwnership | Public | ● | onlyOwner |
| L | transferOwnership | Public | ● | onlyOwner |
| L | getUnlockTime | Public | | NO |
| L | getTime | Public | | NO |
| L | lock | Public | ● | onlyOwner |
| L | unlock | Public | ● | NO |
| IUniswapV2Factory | Interface | | | |
| L | feeTo | External | | NO |
| L | feeToSetter | External | | NO |
| L | getPair | External | | NO |
| L | allPairs | External | | NO |
| L | allPairsLength | External | | NO |
| L | createPair | External | ● | NO |
| L | setFeeTo | External | ● | NO |
| L | setFeeToSetter | External | ● | NO |
| IUniswapV2Pair | Interface | | | |
| L | name | External | | NO |
| L | symbol | External | | NO |
| L | decimals | External | | NO |
| L | totalSupply | External | | NO |
| L | balanceOf | External | | NO |
| L | allowance | External | | NO |
| L | approve | External | ● | NO |
| L | transfer | External | ● | NO |
| L | transferFrom | External | ● | NO |
| L | DOMAIN_SEPARATOR | External | | NO |
| L | PERMIT_TYPEHASH | External | | NO |
| L | nonces | External | | NO |
| L | permit | External | ● | NO |
| L | MINIMUM_LIQUIDITY | External | | NO |
| L | factory | External | | NO |
| L | token0 | External | | NO |
| L | token1 | External | | NO |
| L | getReserves | External | | NO |
| L | price0CumulativeLast | External | | NO |
| L | price1CumulativeLast | External | | NO |
| L | kLast | External | | NO |
| L | burn | External | ● | NO |
| L | swap | External | ● | NO |
| L | skim | External | ● | NO |
| L | sync | External | ● | NO |
| L | initialize | External | ● | NO |

Automated Analysis

| IUniswapV2Router01 | Interface | | | |
|--------------------|------------------------------|----------|---|----|
| L | factory | External | | NO |
| L | WETH | External | | NO |
| L | addLiquidity | External | ● | NO |
| L | addLiquidityETH | External | ■ | NO |
| L | removeLiquidity | External | ● | NO |
| L | removeLiquidityETH | External | ● | NO |
| L | removeLiquidityWithPermit | External | ● | NO |
| L | removeLiquidityETHWithPermit | External | ● | NO |
| L | swapExactTokensForTokens | External | ● | NO |
| L | swapTokensForExactTokens | External | ● | NO |
| L | swapExactETHForTokens | External | ■ | NO |
| L | swapTokensForExactETH | External | ● | NO |
| L | swapExactTokensForETH | External | ● | NO |
| L | swapETHForExactTokens | External | ■ | NO |
| L | quote | External | | NO |
| L | getAmountOut | External | | NO |
| L | getAmountIn | External | | NO |
| L | getAmountsOut | External | | NO |
| L | getAmountsIn | External | | NO |

| IUniswapV2Router02 | Interface | IUniswapV2Router01 | | |
|--------------------|---|--------------------|---|----|
| L | removeLiquidityETHSupportingFeeOnTransferTokens | External | ● | NO |
| L | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External | ● | NO |
| L | swapExactTokensForTokensSupportingFeeOnTransferTokens | External | ● | NO |
| L | swapExactETHForTokensSupportingFeeOnTransferTokens | External | ■ | NO |
| L | swapExactTokensForETHSupportingFeeOnTransferTokens | External | ● | NO |

Automated Analysis

| QTRINU | Implementation | Context, IERC20, Ownable | | |
|--------|-------------------------------|--------------------------|---|-------------|
| L | | Public | ● | NO |
| L | name | Public | | NO |
| L | symbol | Public | | NO |
| L | decimals | Public | | NO |
| L | totalSupply | Public | | NO |
| L | balanceOf | Public | | NO |
| L | transfer | Public | ● | NO |
| L | allowance | Public | | NO |
| L | approve | Public | ● | NO |
| L | transferFrom | Public | ● | NO |
| L | increaseAllowance | Public | ● | NO |
| L | decreaseAllowance | Public | ● | NO |
| L | isExcludedFromReward | Public | | NO |
| L | totalFees | Public | | NO |
| L | minimumTokensBeforeSwapAmount | Public | | NO |
| L | buyBackSellLimitAmount | Public | | NO |
| L | deliver | Public | ● | NO |
| L | reflectionFromToken | Public | | NO |
| L | tokenFromReflection | Public | | NO |
| L | excludeFromReward | Public | ● | onlyOwner |
| L | includeInReward | External | ● | onlyOwner |
| L | _approve | Private | ● | |
| L | _transfer | Private | ● | |
| L | swapTokens | Private | ● | lockTheSwap |
| L | buyBackTokens | Private | ● | lockTheSwap |

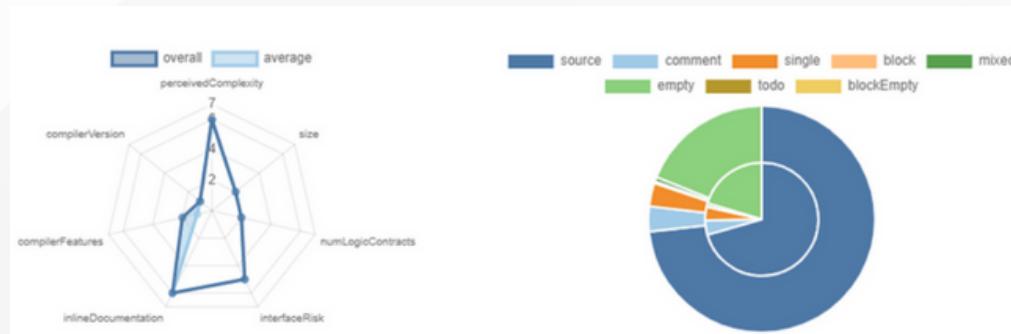
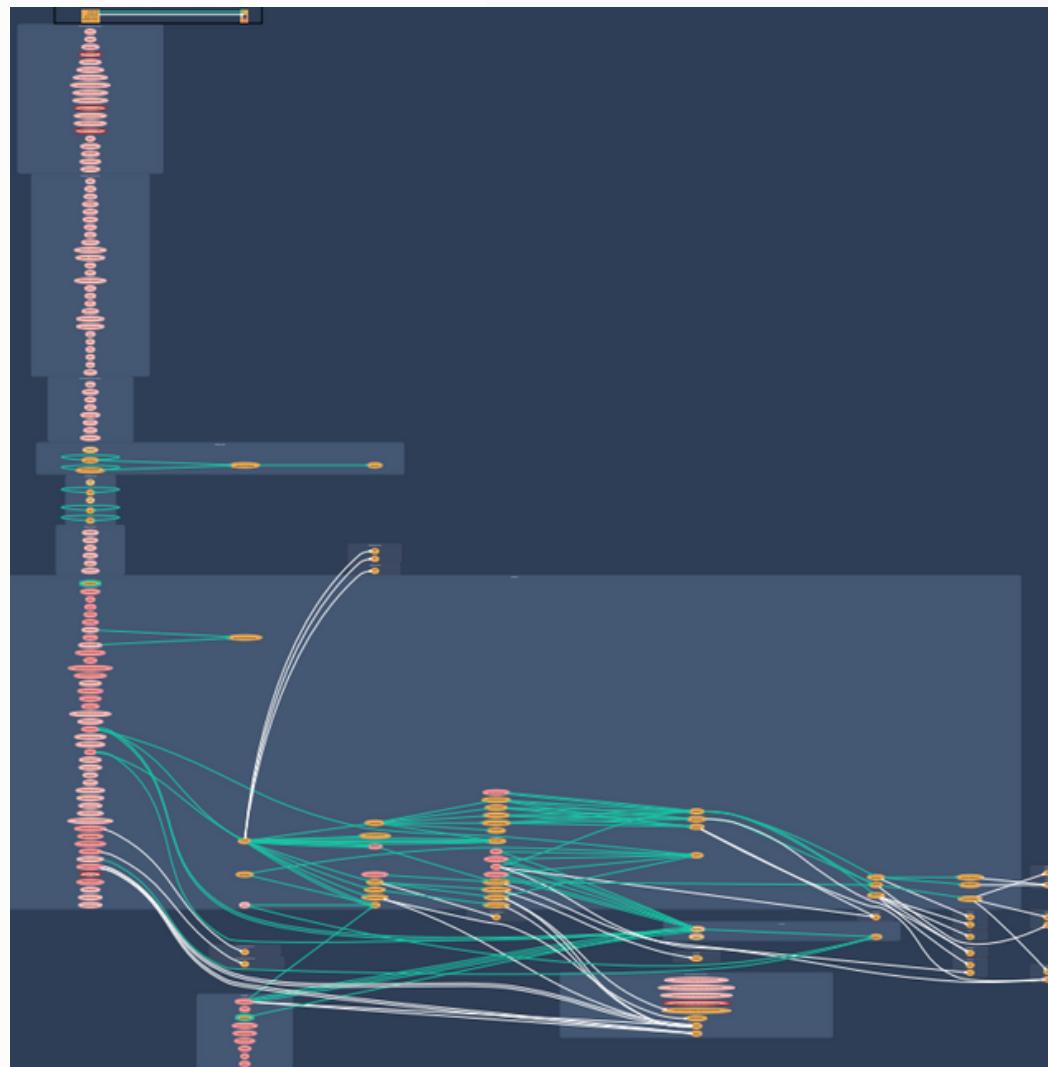
Automated Analysis

| | | | | |
|---|-------------------------------|------------|---|-----------|
| L | swapTokensForEth | Private 🚫 | ● | |
| L | swapETHForTokens | Private 🚫 | ● | |
| L | addLiquidity | Private 🚫 | ● | |
| L | _tokenTransfer | Private 🚫 | ● | |
| L | _transferStandard | Private 🚫 | ● | |
| L | _transferToExcluded | Private 🚫 | ● | |
| L | _transferFromExcluded | Private 🚫 | ● | |
| L | _transferBothExcluded | Private 🚫 | ● | |
| L | _reflectFee | Private 🚫 | ● | |
| L | _getValues | Private 🚫 | | |
| L | _getTValues | Private 🚫 | | |
| L | _getRValues | Private 🚫 | | |
| L | _getRate | Private 🚫 | | |
| L | _getCurrentSupply | Private 🚫 | | |
| L | _takeLiquidity | Private 🚫 | ● | |
| L | calculateTaxFee | Private 🚫 | | |
| L | calculateLiquidityFee | Private 🚫 | | |
| L | removeAllFee | Private 🚫 | ● | |
| L | restoreAllFee | Private 🚫 | ● | |
| L | isExcludedFromFee | Public 🚩 | | NO 🚩 |
| L | excludeFromFee | Public 🚩 | ● | onlyOwner |
| L | includeInFee | Public 🚩 | ● | onlyOwner |
| L | _getSellBnBAmount | Private 🚫 | | |
| L | _removeOldSellHistories | Private 🚫 | ● | |
| L | SetBuyBackMaxTimeForHistories | External 🚩 | ● | onlyOwner |
| L | SetBuyBackDivisor | External 🚩 | ● | onlyOwner |

Automated Analysis

| | | | | |
|---|--------------------------------|----------|---|-----------|
| L | GetBuyBackTimeInterval | Public | | NO |
| L | SetBuyBackTimeInterval | External | ● | onlyOwner |
| L | SetBuyBackRangeRate | External | ● | onlyOwner |
| L | GetSwapMinutes | Public | | NO |
| L | SetSwapMinutes | External | ● | onlyOwner |
| L | setTaxFeePercent | External | ● | onlyOwner |
| L | setBuyFee | External | ● | onlyOwner |
| L | setSellFee | External | ● | onlyOwner |
| L | setLiquidityFeePercent | External | ● | onlyOwner |
| L | setBuyBackSellLimit | External | ● | onlyOwner |
| L | setMaxTxAmount | External | ● | onlyOwner |
| L | setMarketingDivisor | External | ● | onlyOwner |
| L | setNumTokensSellToAddToBuyBack | External | ● | onlyOwner |
| L | setMarketingAddress | External | ● | onlyOwner |
| L | setSwapAndLiquifyEnabled | Public | ● | onlyOwner |
| L | setBuyBackEnabled | Public | ● | onlyOwner |
| L | setAutoBuyBackEnabled | Public | ● | onlyOwner |
| L | prepareForPreSale | External | ● | onlyOwner |
| L | afterPreSale | External | ● | onlyOwner |
| L | transferToAddressETH | Private | ● | |
| L | changeRouterVersion | Public | ● | onlyOwner |
| L | | External | ● | NO |
| L | transferForeignToken | Public | ● | onlyOwner |
| L | Sweep | External | ● | onlyOwner |
| L | setAddressFee | External | ● | onlyOwner |
| L | setBuyAddressFee | External | ● | onlyOwner |
| L | setSellAddressFee | External | ● | onlyOwner |

Inheritance Graph



Contract Summary

| Logic Contracts | Interfaces | Lines | nLines | nSLOC | Comment Lines | Complex. Score | Capabilities |
|-----------------|------------|-------|--------|-------|---------------|----------------|--------------|
| 5 | 5 | 1191 | 957 | 716 | 45 | 729 | |
| 5 | 5 | 1191 | 957 | 716 | 45 | 729 | |

Components

| Contracts | Libraries | Interfaces | Abstract |
|-----------|-----------|------------|----------|
| 2 | 2 | 5 | 1 |

Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

| Public | Payable |
|--------|---------|
| 122 | 5 |

| External | Internal | Private | Pure | View |
|----------|----------|---------|------|------|
| 86 | 109 | 27 | 19 | 50 |

StateVariables

| Total | Public |
|-------|--------|
| 45 | 25 |

Capabilities

| Solidity Versions observed | Experimental Features | Can Receive Funds | Uses Assembly | Has Destroyable Contracts |
|----------------------------|-----------------------|-------------------|-----------------------|---------------------------|
| ^0.8.4 | | yes | yes (2 asm blocks) | |
| Transfers ETH | Low-Level Calls | DelegateCall | Uses Hash Functions | ECRecover |
| yes | | | yes | |
| TryCatch | Unchecked | | | |

Manual Review

The owner can set the max tx amount "0"

```
1094     function setMaxTxAmount(uint256 maxTxAmount) external onlyOwner {  
1095         _maxTxAmount = maxTxAmount;  
1096     }
```

Recommendation

These functions should be provided arbitrary limits, e.g., put a **require** check that allows maximum limit etc. if **set 0** these cause pause the trading.

The owner can set fees up to 100%

```
1076     function setBuyFee(uint256 buyTaxFee, uint256 buyLiquidityFee) external onlyOwner {  
1077         _buyTaxFee = buyTaxFee;  
1078         _buyLiquidityFee = buyLiquidityFee;  
1079     }  
1080  
1081     function setSellFee(uint256 sellTaxFee, uint256 sellLiquidityFee) external onlyOwner {  
1082         _sellTaxFee = sellTaxFee;  
1083         _sellLiquidityFee = sellLiquidityFee;  
1084     }
```

Recommendation

These functions should be provided arbitrary limits, e.g., put a **require** check that allows maximum limit etc.

Auto liquidity is going to an externally owned account

```
844     function addLiquidity(uint256 tokenAmount, uint256 ethAmount) private {  
845         // Approve token transfer to cover all possible scenarios  
846         _approve(address(this), address(uniswapV2Router), tokenAmount);  
847  
848         // Add the liquidity  
849         uniswapV2Router.addLiquidityETH{value: ethAmount}(  
850             address(this),  
851             tokenAmount,  
852             0, // Slippage is unavoidable  
853             0, // Slippage is unavoidable  
854             owner(),  
855             block.timestamp  
856         );  
857     }
```

Recommendation

Authorizing privileged roles to externally-owned-account (EOA) is dangerous.
Send LP tokens to dead address or unreachable address.

Manual Review

The owner can exclude accounts from rewards

```
639     function excludeFromReward(address account) public onlyOwner() {
640
641         require(!_isExcluded[account], "Account is already excluded");
642         if(_rOwned[account] > 0) {
643             _tOwned[account] = tokenFromReflection(_rOwned[account]);
644         }
645         _isExcluded[account] = true;
646         _excluded.push(account);
647     }
648
649     function includeInReward(address account) external onlyOwner() {
650         require(_isExcluded[account], "Account is not excluded");
651         for (uint256 i = 0; i < _excluded.length; i++) {
652             if (_excluded[i] == account) {
653                 _excluded[i] = _excluded[_excluded.length - 1];
654                 _tOwned[account] = 0;
655                 _isExcluded[account] = false;
656                 _excluded.pop();
657                 break;
658             }
659         }
660     }
```

Recommendation

Authorizing privileged roles to exclude accounts from rewards. These cause affect decentralization

The owner can change transaction lock-time without limit

```
1068     function SetSwapMinutes(uint256 newMinutes) external onlyOwner {
1069         _intervalMinutesForSwap = newMinutes * 1 minutes;
1070     }
```

Recommendation

Authorizing privileged roles to change transaction lock-time without limit. these cause lock trade x minutes means pause. remove lock time or reasonable max limit.

Manual Review

The owner can exclude accounts from fees

```
999     function excludeFromFee(address account) public onlyOwner {
1000         _isExcludedFromFee[account] = true;
1001     }
1002
1003     function includeInFee(address account) public onlyOwner {
1004         _isExcludedFromFee[account] = false;
1005     }
```

Recommendation

Authorizing privileged roles to exclude accounts from fees. These cause affect decentralization

The owner can change swap settings

```
1102     function setNumTokensSellToAddToBuyBack(uint256 _minimumTokensBeforeSwap) external onlyOwner
1103         minimumTokensBeforeSwap = _minimumTokensBeforeSwap;
1104     }
```

Recommendation

Authorizing privileged roles to enable or disable the swap. These cause affect decentralization

AUDIT REPORT

SecureWise

SMART CONTRACT AUDIT

-  <https://github.com/securewise>
-  <https://t.me/securewise>
-  <https://securewise.info/>

