



SMART CONTRACT SECURITY AUDIT for



Staking Contract

Token Overview

0xSafe received the application for a smart contract security audit of **QI DEX's Staking** smart contract on December 24, 2022.

Details

Client: QI DEX

Blockchain: QIE Blockchain

Contract: N/D

Compiler: N/D

Optimization: N/D

Website: <https://www.qidex.site>

KEY

N/D - Not Deployed Yet

Table of Contents

| | |
|----------------------------|-----------|
| Token Overview | 1 |
| Details | 1 |
| KEY | 1 |
| Table of Contents | 2 |
| Methodology | 3 |
| Audit Details | 3 |
| Code Quality | 3 |
| Scope of work | 3 |
| Tools | 3 |
| Risk Classification | 4 |
| Audit Findings | 4 |
| Critical Issues | 4 |
| Medium Issues | 4 |
| Minor Issues | 4 |
| SWC Attacks | 5 |
| Important Notes | 8 |
| Good Practices | 8 |
| Inheritance Tree | 9 |
| Contract Inspection | 9 |
| Legend | 9 |
| Table | 9 |
| Audit Results | 12 |
| Disclaimer | 13 |

Methodology

Audit Details

This comprehensive audit report provides an overview of the **QI DEX Staking** smart contract. 0xSafe utilizes a combination of static, automated, and manual analysis tools to check for any potential vulnerabilities or hacks in the system.

Code Quality

This includes a full review of the smart contract code. The prime areas of focus are:

- Accuracy
- Exploits
- Functionality
- Readability
- Security
- Vulnerabilities

Scope of work

QI DEX's team provided us with the files that need to be tested (BSCscan, Etherscan, Github, etc.). The focus of the security audit is the main token smart contract.

Tools

Ganache, Mithril, MythX, Open Zeppelin Code Analyzer, Proprietary tests, Remix IDE, Solidity Compiler, SWC Registry.

Risk Classification

| | |
|-----------------------|---|
| !Critical | This signifies vulnerabilities with the smart contract's functionality or performance. Issues should be resolved immediately. |
| !Medium | This signifies vulnerabilities that can potentially cause problems and should eventually be fixed. |
| !Minor | Minor vulnerabilities may or may not impact smart contract functionality. |
| !Informational | This is there to offer suggestions for improvement |

Audit Findings

Critical Issues

-no critical issues found-

Medium Issues

| Issue | Type | Line #(s) | Description |
|-------|--|-----------|---|
| #1 | Multiple calls are executed in the same transaction. | 543, 696 | This call is executed following another call within the same transaction. |

Minor Issues

| Issue | Type | Line #(s) | Description |
|-------|------|-----------|-------------|
|-------|------|-----------|-------------|

| | | | |
|----|--|---|--|
| #1 | A floating pragma is set. | 7, 231, 259, | Current pragma directive is: ">=0.6.6 <0.8.0" |
| #2 | Read of persistent state following external call. | 338, 427, 550-552, 505, 512-514, 516, 520, 534, 535, 537, 540, 555, 575-579, 598-599, 602, 605, 615, 659-562, 696, 733, 833, 834, 836 | The contract account state is accessed after an external call. |
| #3 | Potential use of "block.number" as source of randomness. | 476, 729-730, 823, 826, 830, 836 | The environment variable "block.number" looks like it might be used as a source of randomness. |
| #4 | Requirement violation. | 763 | A requirement was violated in a nested call and the call was reverted as a result. |

SWC Attacks

| SWC ID | Description | Status |
|---------|--------------------------------------|--------|
| SWC-100 | Function Default Visibility | PASSED |
| SWC-101 | Integer Overflow and Underflow | PASSED |
| SWC-102 | Outdated Compiler Version | PASSED |
| SWC-103 | Floating Pragma | MINOR |
| SWC-104 | Unchecked Call Return Value | PASSED |
| SWC-105 | Unprotected Ether Withdrawal | PASSED |
| SWC-106 | Unprotected SELFDESTRUCT Instruction | PASSED |
| SWC-107 | Reentrancy | MINOR |
| SWC-108 | State Variable Default Visibility | PASSED |

| | | |
|----------------|---|--------|
| SWC-109 | Uninitialized Storage Pointer | PASSED |
| SWC-110 | Assert Violation | PASSED |
| SWC-111 | Use of Deprecated Solidity Functions | PASSED |
| SWC-112 | Delegatecall to Untrusted Callee | PASSED |
| SWC-113 | DoS with Failed Call | MEDIUM |
| SWC-114 | Transaction Order Dependence | PASSED |
| SWC-115 | Authorization through tx.origin | PASSED |
| SWC-116 | Block values as a proxy for time | PASSED |
| SWC-117 | Signature Malleability | PASSED |
| SWC-118 | Incorrect Constructor Name | PASSED |
| SWC-119 | Shadowing State Variables | PASSED |
| SWC-120 | Weak Sources of Randomness from Chain Attributes | MINOR |
| SWC-121 | Missing Protection against Signature Replay Attacks | PASSED |
| SWC-122 | Lack of Proper Signature Verification | PASSED |
| SWC-123 | Requirement Violation | MINOR |
| SWC-124 | Write to Arbitrary Storage Location | PASSED |
| SWC-125 | Incorrect Inheritance Order | PASSED |
| SWC-126 | Insufficient Gas Griefing | PASSED |
| SWC-127 | Arbitrary Jump with Function Type Variable | PASSED |
| SWC-128 | DoS With Block Gas Limit | PASSED |
| SWC-129 | Typographical Error | PASSED |
| SWC-130 | Right-To-Left-Override control character (U+202E) | PASSED |
| SWC-131 | Presence of unused variables | PASSED |
| SWC-132 | Unexpected Ether balance | PASSED |
| SWC-133 | Hash Collisions With Multiple Variable Length Arguments | PASSED |

| | | |
|----------------|--|--------|
| SWC-134 | Message call with hardcoded gas amount | PASSED |
| SWC-135 | Code With No Effects | PASSED |
| SWC-136 | Unencrypted Private Data On-Chain | PASSED |

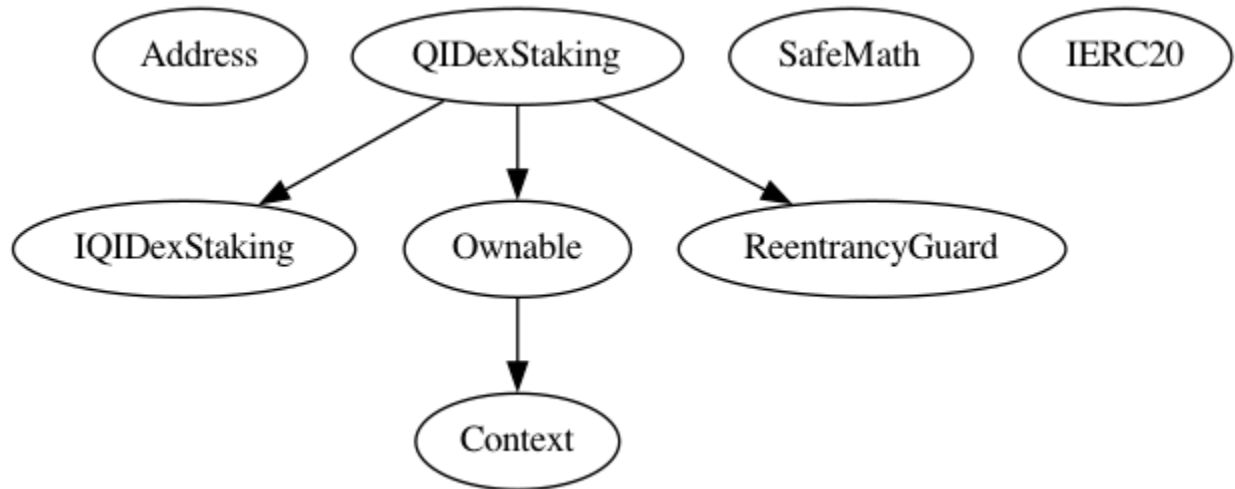
Important Notes

- Owner can recover tokens
- Owner can update reward token
- Owner can update pool limit per user
- Owner can update pool duration
- Owner can update fee without limits
- Owner can update the pool reward per block

Good Practices

- The smart contract utilizes “SafeMath” to prevent overflows




Inheritance Tree










Contract Inspection

Below is a visual description report comprising of information about the system's files, contracts, and their functions.

Legend

| Symbol | Meaning |
|---|---------------------------|
| :-----: -----: | |
|  | Function can modify state |
|  | Function is payable |
|  | Internal function |
| NO ! | Function has no modifier |

Table

| Contract | Type | Bases | | | |
|---|-------------------|--|---|---------------|--|
| :-----: :-----: :-----: :-----: :-----: | | | | | |
| L | **Function Name** | **Visibility** | **Mutability** | **Modifiers** | |
| | | | | | |
| **Address** | Library | | | | |
| L | isContract | Internal  | | | |
| L | sendValue | Internal  |  | | |
| L | functionCall | Internal  |  | | |
| L | functionCall | Internal  |  | | |

```

|  | functionCallWithValue | Internal | 🔒 | 🔴 | |
|  | functionCallWithValue | Internal | 🔒 | 🔴 | |
|  | functionStaticCall | Internal | 🔒 | | |
|  | functionStaticCall | Internal | 🔒 | | |
|  | functionDelegateCall | Internal | 🔒 | 🔴 | |
|  | functionDelegateCall | Internal | 🔒 | 🔴 | |
|  | _verifyCallResult | Private | 🔒 | | |
|||||
| **IQIDexStaking** | Interface | |||
|  | deposit | External | ! | 💰 | NO ! |
|  | withdraw | External | ! | 🔴 | NO ! |
|  | claimReward | External | ! | 🔴 | NO ! |
|  | userInfo | External | ! | | NO ! |
|||||
| **SafeMath** | Library | |||
|  | add | Internal | 🔒 | | |
|  | sub | Internal | 🔒 | | |
|  | mul | Internal | 🔒 | | |
|  | div | Internal | 🔒 | | |
|||||
| **IERC20** | Interface | |||
|  | name | External | ! | | NO ! |
|  | symbol | External | ! | | NO ! |
|  | decimals | External | ! | | NO ! |
|  | totalSupply | External | ! | | NO ! |
|  | balanceOf | External | ! | | NO ! |
|  | allowance | External | ! | | NO ! |
|  | mint | External | ! | 🔴 | NO ! |
|  | approve | External | ! | 🔴 | NO ! |
|  | transfer | External | ! | 🔴 | NO ! |
|  | transferFrom | External | ! | 🔴 | NO ! |
|||||
| **Context** | Implementation | |||
|  | _msgSender | Internal | 🔒 | | |
|  | _msgData | Internal | 🔒 | | |
|||||
| **Ownable** | Implementation | Context |||
|  | <Constructor> | Internal | 🔒 | 🔴 | |
|  | owner | Public | ! | | NO ! |
|  | renounceOwnership | Public | ! | 🔴 | onlyOwner |

```

```

|  | transferOwnership | Public ! |  | onlyOwner |
|||||
| **ReentrancyGuard** | Implementation | |||
|  | <Constructor> | Public ! |  | NO ! |
|||||
| **QIDexStaking** | Implementation | Ownable, ReentrancyGuard, IQIDexStaking |||
|  | <Constructor> | Public ! |  | NO ! |
|  | deposit | External ! |  | nonReentrant |
|  | _addStake | Internal  |  | |
|  | withdraw | External ! |  | nonReentrant |
|  | claimReward | External ! |  | nonReentrant |
|  | safeTokenTransfer | Internal  |  | |
|  | availableRewardTokens | Public ! |  | NO ! |
|  | userInfo | Public ! |  | NO ! |
|  | pendingReward | External ! |  | NO ! |
|  | recoverWrongTokens | External ! |  | onlyOwner |
|  | updateRewardToken | External ! |  | onlyOwner |
|  | updatePoolLimitPerUser | External ! |  | onlyOwner |
|  | updateDuration | External ! |  | onlyOwner |
|  | updateFee | External ! |  | onlyOwner |
|  | updateRewardPerBlock | External ! |  | onlyOwner |
|  | _updatePool | Internal  |  | |
|  | <Receive Ether> | External ! |  | NO ! |

```

Audit Results

QI DEX's Staking smart contract does not contain any severe issues or risks. The security of the smart contract was tested by 0xSafe using static, automated, and manual analysis. The



AUDIT PASSED

Note:

Please check the disclaimer below and note the audit makes no statements or warranties on the business model, investment attractiveness, or code sustainability of this project. The security audit report is provided for the only contract mentioned in this report.

Disclaimer

0xSafe.io provides contract auditing, KYC, development, and launch services for blockchain projects. The purpose of the security audit is to analyze the on-chain smart contract source code and to provide an easy-to-understand assessment of the crypto project and the smart contract. **0xSafe.io provides information as is.**

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 0xSafe.io and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers, and other representatives) (0xSafe.io) owes no duty of care towards you or any other person, nor does 0xSafe.io 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 0xSafe.io 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, 0xSafe.io hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against 0xSafe.io, 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 the use of this report, and any reliance on this report.

This report should not be considered as an endorsement or disapproval of any project or team. The information provided in this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. Conduct your own due diligence and consult your financial advisor before making any investment decisions.



<https://0xsafe.io>