Smart Contract Security Audit

Audit details:

Audited project:	Rarechain
Deployer address	0x1e620b603216b10ba157eb2b87a4ce0dca0570de
Blockchain:	Ethereum
Project website:	https://www.qao.io

May, 2021
TechRate

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 Rarechain to perform an audit of smart contracts:

- *https://etherscan.io/address/0x3402E15b3EA0f1aEC2679c4Be4c6d051ceF93953#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

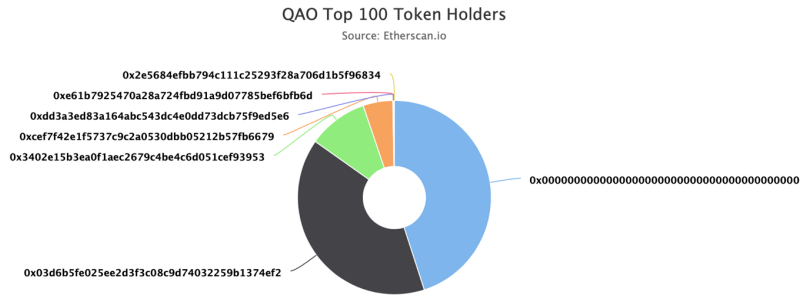
Token contract details for 10.05.2021.

Contract name:	QAO
Compiler version:	v0.8.1+commit.df193b15
Contract address:	0x3402E15b3EA0f1aEC2679c4Be4c6d051ceF93953
Total supply:	100000000000000000000000000000000
Token ticker:	🌐
Decimals:	18
Token holders:	9
Transactions count:	27
Top 100 dominance:	100 %
Contract deployer address:	0x1e620b603216b10ba157eb2b87a4ce0dca0570de
Contract’s current owner address:	0x1e620b603216b10ba157eb2b87a4ce0dca0570de

Rarechain token distribution

The top 100 holders collectively own 100.00% (9,999,999,999,999.99 Tokens) of QAO

Token Total Supply: 10,000,000,000,000.00 Token | Total Token Holders: 9



(A total of 9,999,999,999,999.99 tokens held by the top 100 accounts from the total supply of 10,000,000,000,000.00 token)

Rarechain top 10 token holders

Rank	Address	Quantity (Token)	Percentage
1	0x0000000000000000000000000000000000000000	4,500,000,000,000	45.0000%
2	0x03d6b5fe025ee2d3f3c08c9d74032259b1374ef2	3,978,840,565,051.766769554225015222	39.7884%
3	0x3402e15b3ea0f1aec2679c4be4c6d051cef93953	1,000,000,000,000	10.0000%
4	0xcef7f42e1f5737c9c2a0530dbb05212b57fb6679	496,975,381,697.314153857907283849	4.9698%
5	0xdd3a3ed83a164abc543dc4e0dd73dcb75f9ed5e6	12,000,000,000.000000630060093155	0.1200%
6	0xe61b7925470a28a724fbd91a9d07785bef6bfb6d	9,707,623,309.213200124616608652	0.0971%
7	0x2e5684efbb794c111c25293f28a706d1b5f96834	1,476,429,941.705875833171879057	0.0148%
8	0x85c5ebaa91b5c71ab294d15490450cfcedbc9f1f	1,000,000,000	0.0100%
9	0x2d75e425789af735081f6db184f0148349abac0b	0.000000000019120065	0.0000%

Functions outline

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

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

+ ERC20 (Context, IERC20)
  - [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 #

+ ERC20Burnable (Context, ERC20)
  - [Pub] burn #
  - [Pub] burnFrom #

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

+ QAOToken (ERC20Burnable, Ownable)

- [Pub] <Constructor> #
  - modifiers: ERC20
- [Pub] transfer #
- [Pub] activateMinting #
  - modifiers: onlyOwner
- [Prv] _applyMintSchedule #
- [Prv] _mintToPools #
- [Prv] _getPassedDays
- [Prv] _annualTreasuryMint #
- [Pub] unlockTreasuryByGuard #
- [Pub] unlockTreasuryByOwner #
  - modifiers: onlyOwner
- [Pub] withdrawFromTreasury #
  - modifiers: onlyOwner
- [Pub] setVotingEngine #
  - modifiers: onlyOwner
- [Pub] votingEngine
- [Pub] mintVoteStakeReward #
- [Pub] mintMultiplier
- [Pub] setMintMultiplier #
  - modifiers: onlyOwner
- [Pub] airdropPool
- [Pub] setAirdropPool #
  - modifiers: onlyOwner
- [Pub] liquidityPool
- [Pub] setLiquidityPool #
  - modifiers: onlyOwner
- [Pub] apiRewardPool
- [Pub] setApiRewardPool #
  - modifiers: onlyOwner
- [Pub] mintAirdropShare
- [Pub] setMintAirdropShare #
  - modifiers: onlyOwner
- [Pub] mintLiqPoolShare
- [Pub] setMintLiqPoolShare #
  - modifiers: onlyOwner
- [Pub] mintApiRewardShare
- [Pub] setMintApiRewardShare #
  - 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. Wrong burning

Issue:

There is sending tokens to the zero address instead of real burning (decreasing the balance of the burner's account and total supply) in function burn.

Recommendation:

Please recheck that the burn is used correctly or change it!

Update: team members claimed that the burn function is designed this way by the project logic.

2. Known vulnerabilities of ERC-20 token

Issue:

Lack of transaction handling mechanism issue. WARNING! This is a very common issue and it already caused millions of dollars losses for lots of token users! More details here.

Recommendation:

Add the following code to the _transfer(address sender, ...) function:

```
require( _to != address(this) );
```

Owner privileges

- ❏ Owner can change the reward by week.
- ❏ Owner can withdraw from the treasury.

- ❏ Owner can change the voting engine address to any not audited contract.
- ❏ Owner can change the minting multiplier.
- ❏ Owner can change the liquidity, airdrop and api reward pools.
- ❏ Owner can change the airdrop, liquidity and api reward minting shares.

Conclusion

Smart contracts contain low severity issues and owner privileges.

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.