TechRate

Blockchain solutions and consulting

Smart Contract Security Audit

Audit details:

Audited project:	**PlanetFinance**
Deployer address	**0xd0770397b59b1f6238e9c125c5ef4cb9007fe81f**
Blockchain:	**Binance Smart Chain**
Project website:	**Not provided**

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 PlanetFinance to perform an audit of smart contracts:

- *https://bscscan.com/address/0x72B7D61E8fC8cF971960DD9cfA59B8C829D91991#code*
- *https://bscscan.com/address/0x0ac58fd25f334975b1b61732cf79564b6200a933#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 04.05.2021.

Contract name:	**AQUA**
Compiler version:	**v0.6.12+commit.27d51765**
Contract address:	**0x72B7D61E8fC8cF971960DD9cfA59B8C829D91991**
Total supply:	**842_128_262_993_243_241_021**
Token ticker:	**AQUA**
Decimals:	**18**
Token holders:	**140**
Transactions count:	**12686**
Top 100 holders dominance:	**100 %**
Contract deployer address:	**0xd0770397b59b1f6238e9c125c5ef4cb9007fe81f**
Contract's current owner address:	**0x0ac58fd25f334975b1b61732cf79564b6200a933**

AQUA top 5 token holders

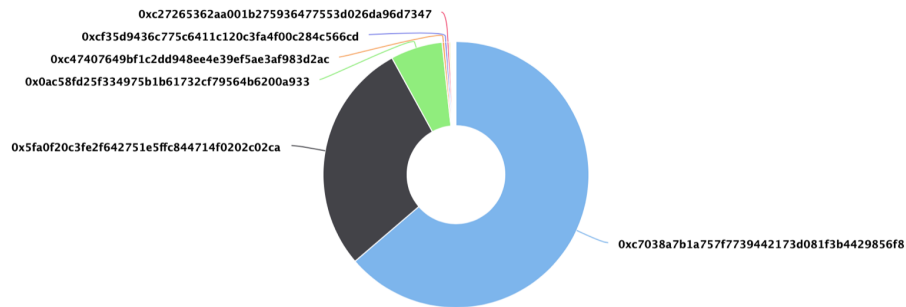| Rank	Address	Quantity	Percentage
1	0xc7038a7b1a757f7739442173d081f3b4429856f8	535.78216742975996293	64.0479%
2	0x5fa0f20c3fe2f642751e5ffc844714f0202c02ca	237.526060114751334091	28.3941%
3	0x0ac58fd25f334975b1b61732cf79564b6200a933	53.232156583575893215	6.3634%
4	0xc47407649bf1c2dd948ee4e39ef5ae3af983d2ac	2.577733835393850831	0.3081%
5	0xcf35d9436c775c6411c120c3fa4f00c284c566cd	2.329156552843255977	0.2784%

AQUA top 100 token distribution

Token Total Supply: 840.54 Token | Total Token Holders: 140

AQUA Top 100 Token Holders
Source: BscScan.com

0xc27265362aa001b275936477553d026da96d7347
0xcf35d9436c775c6411c120c3fa4f00c284c566cd
0xc47407649bf1c2dd948ee4e39ef5ae3af983d2ac
0x0ac58fd25f334975b1b61732cf79564b6200a933
0x5fa0f20c3fe2f642751e5ffc844714f0202c02ca
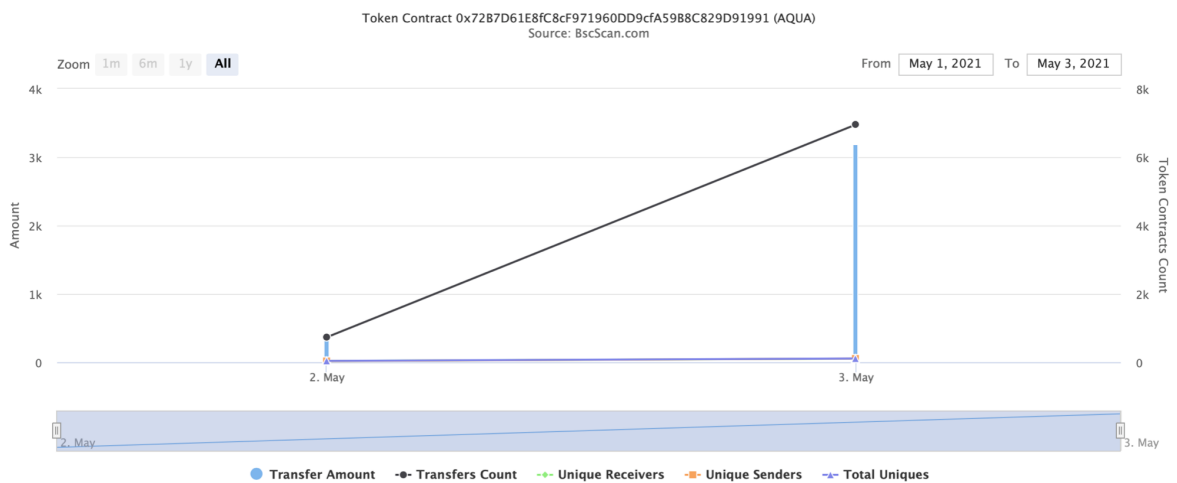
0xc7038a7b1a757f7739442173d081f3b4429856f8

(A total of 840.54 tokens held by the top 100 accounts from the total supply of 840.54 token)

AQUA contract interaction details

Time Series: Token Contract Overview   Sun 2, May 2021 - Mon 3, May 2021

Token Contract 0x72B7D61E8fC8cF971960DD9cfA59B8C829D91991 (AQUA)
Source: BscScan.com

Zoom 1m 6m 1y All   From May 1, 2021   To May 3, 2021

● Transfer Amount   -●- Transfers Count   -●- Unique Receivers   -■- Unique Senders   -▲- Total Uniques

PlanetFinance contract details for 04.05.2021.

Contract name:	PlanetFinance
Compiler version:	v0.6.12+commit.27d51765
Contract address:	0x0ac58fd25f334975b1b61732cf79564b6200a933
Burn address:	0x000000000000000000000000000000000000dead
AQUA contract address:	0x72b7d61e8fc8cf971960dd9cfa59b8c829d91991
AQUA per block:	17_361_100_000_000_000
Contract owner address:	0x084e9b6928888a1d372b87e3d7bb3f90700df137
Pool length:	6
Start block:	0
Total alloc point:	7400
Bonus multiplier:	1
AQUA max supply:	100_000_000_000_000_000_000_000

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.	Passed
19	Cross-function race conditions.	Passed
20	Safe Open Zeppelin contracts implementation and usage.	Passed
21	Fallback function security.	Passed

Planet Finance functions outline

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

+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod

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

+ 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] _setupDecimals #
  - [Int] _beforeTokenTransfer #

+ [Lib] Address
  - [Int] isContract

- [Int] sendValue #
- [Int] functionCall #
- [Int] functionCall #
- [Int] functionCallWithValue #
- [Int] functionCallWithValue #
- [Int] functionStaticCall
- [Int] functionStaticCall
- [Int] functionDelegateCall #
- [Int] functionDelegateCall #
- [Prv] _verifyCallResult

+ [Lib] SafeERC20
- [Int] safeTransfer #
- [Int] safeTransferFrom #
- [Int] safeApprove #
- [Int] safeIncreaseAllowance #
- [Int] safeDecreaseAllowance #
- [Prv] _callOptionalReturn #

+ [Lib] EnumerableSet
- [Prv] _add #
- [Prv] _remove #
- [Prv] _contains
- [Prv] _length
- [Prv] _at
- [Int] add #
- [Int] remove #
- [Int] contains
- [Int] length
- [Int] at
- [Int] add #
- [Int] remove #
- [Int] contains
- [Int] length
- [Int] at
- [Int] add #
- [Int] remove #
- [Int] contains
- [Int] length
- [Int] at

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

- modifiers: onlyOwner

+ ReentrancyGuard
- [Int] <Constructor> #

+ AquaToken (ERC20)
- [Pub] mint #

+ [Int] IStrategy
- [Ext] wantLockedTotal
- [Ext] sharesTotal
- [Ext] earn #
- [Ext] deposit #
- [Ext] withdraw #
- [Ext] inCaseTokensGetStuck #

+ PlanetFinance (Ownable, ReentrancyGuard)
- [Ext] poolLength
- [Pub] add #
  - modifiers: onlyOwner
- [Pub] set #
  - modifiers: onlyOwner
- [Pub] getMultiplier
- [Ext] pendingAQUA
- [Ext] stakedWantTokens
- [Pub] massUpdatePools #
- [Pub] updatePool #
- [Pub] deposit #
  - modifiers: nonReentrant
- [Pub] withdraw #
  - modifiers: nonReentrant
- [Pub] withdrawAll #
  - modifiers: nonReentrant
- [Pub] emergencyWithdraw #
  - modifiers: nonReentrant
- [Int] safeAQUATransfer #
- [Pub] inCaseTokensGetStuck #
  - modifiers: onlyOwner
- [Pub] changeAQUAaddress #
  - modifiers: onlyOwner

($) = payable function
 # = non-constant function

Security Issues

High Severity Issues

No high severity issues found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

1. Block gas limit

Issue:

The updateEmissionRate function can fail due to block gas limit if the pool size is too big.

2. add function issue

Issue:

If some LP token is added to the contract twice using function add, then the total amount of reward AQUAReward in function updatePool will be incorrect.

Recommendation:

Add the mapping from address to bool and check that same address will not be added twice.

Owner privileges

❏ Owner can change the AQUA token address in PlanetFinance contract to any not audited contract.
❏ Owner can withdraw tokens from the PlanetFinance contract using the function inCaseTokensGetStuck.

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.