



# SMART CONTRACT SECURITY AUDIT



QRT

NUMBER AUDIT PTA - 2109700003

**POLICE TECH AUDIT** received the application for a smart contract security audit of QRKITA TOKEN on Sept 18, 2021. The following are the details and results of this smart contract security audit:

Token Name	QRT
address	0x921d3a6ed8223AFb6358410F717e2FB13cbae700
Website	<a href="https://qrkita.exchange/">https://qrkita.exchange/</a>
Link Address	<a href="https://bscscan.com/token/0x921d3a6ed8223AFb6358410F717e2FB13cbae700">https://bscscan.com/token/0x921d3a6ed8223AFb6358410F717e2FB13cbae700</a>
Audit Number	PTA-2109700003
Audit Date	September 18, 2021

The audit items and results: (Other unknown security vulnerabilities are not included in the audit responsibility scope)

**Audit Team:** **POLICE TECH AUDIT** <https://POLICETECH.FINANCE/>



## Introduction

This Audit Report mainly focuses on the overall security of POLICE CRYPTO AUDIT Smart Contract. With this report, we have tried to ensure the reliability and correctness of their smart contract by complete and rigorous assessment of their system's architecture and the smart contract codebase.

## Auditing Approach and Methodologies applied

The POLICE TECH AUDIT team has performed rigorous testing of the project starting with analyzing the code Design patterns in which we reviewed the smart contract architecture to ensure it is structured and safe use of third-party smart contracts and libraries.

Our team then performed a formal line by line inspection of the Smart Contract to find any potential issue like race conditions, transaction-ordering dependence, timestamp dependence, and denial of service attacks.

In the Unit testing Phase, we coded/conducted custom unit tests written for each function in the contract to verify that each function works as expected. In Automated Testing, we tested the Smart Contract with our in-house developed tools to identify vulnerabilities and security flaws. The code was tested in collaboration of our multiple team members and this included -

- Testing the functionality of the Smart Contract to determine proper logic has been followed throughout the whole process.
- Analyzing the complexity of the code in depth and detailed, manual review of the code, line by line.
- Deploying the code on testnet using multiple clients to run live tests.
- Analyzing failure preparations to check how the Smart Contract performs in case of any bugs and vulnerabilities.
- Checking whether all the libraries used in the code are on the latest version.
- Analyzing the security of the on-chain data.

## Audit Goals

The focus of the audit was to verify that the Smart Contract System is secure, resilient and working according to the specifications. The audit activities can be grouped in the following three categories:



## Security

Identifying security related issues within each contract and the system of contract.

## Sound Architecture

Evaluation of the architecture of this system through the lens of established smart contract best practices and general software best practices.

## Code Correctness and Quality

A full review of the contract source code. The primary areas of focus include:

- Accuracy
- Readability
- Sections of code with high complexity
- Quantity and quality of test coverage

## Issue Categories

Every issue in this report was assigned a severity level from the following:

### High level severity issues

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

### Medium level severity issues

Issues on this level could potentially bring problems and should eventually be fixed.

### Low level severity issues

Issues on this level are minor details and warnings that can remain unfixed but would be better fixed at some point in the future.

### Number Of Issues Per Severity

Critical	High	Medium	Low	Note
0	0	0	1	0

### ISSUES CHECKING STATUS

No.	Issue Description	Checking Status
1	Compiler errors	Passed
2	Race conditions and Reentrancy	Passed
3	Delays in data delivery	Passed
4	Oracle calls.	Passed
5	Front running	Passed
6	Design Logic	Passed
7	DoS with Revert	Passed
8	Timestamp dependence	Passed
9	DoS with block gas limit	Passed
10	Methods execution permissions	Passed
11	Economy model.	Passed
12	Impact of the exchange rate.	Passed
13	Private user data leaks	Passed
14	Malicious Event log	Passed
15	Uninitialized storage pointers	Passed
16	Arithmetic accuracy.	Passed
17	Cross-function race conditions.	Passed
18	Scoping and Declarations	Passed
19	Safe Zeppelin module	Passed
20	Fallback function security	Passed

## Manual Audit:

For this section the code was tested/read line by line by our developers. We also used Remix IDE's JavaScript VM and Kovan networks to test the contract functionality.

### Critical Severity Issues

No critical severity issues found.

### High Severity Issues

No high severity issues found.

### Medium Severity Issues

No medium severity issues found.

### Low Severity Issues [1]

- Low
- Description: Other visibility settings are public and private, Visibility of state variables has not been fixed. This is a good way to organize state variable visibility explicitly. Default visibility for "inSwapAndLiquify" is internal.
- Variables can be interpreted as public, internal or private.

```
bool inSwapAndLiquify;  
bool public swapAndLiquifyEnabled = false;
```

NO.PTA-2109700003

## Automated Audit

### Remix Compiler Warnings

It throws warnings by Solidity's compiler. If it encounters any errors the contract cannot be compiled and deployed. No issues found.

### Summary Smart

contracts do not contain any high severity issues.

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





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