Quantstamp Contract Security Certificate

November 6, 2019 — Quantstamp Verified

EMR Token Platform

This smart contract audit was prepared by Quantstamp, the protocol for securing smart contracts.

Executive Summary

Overall Assessment

The platform consists of two sets of smart contracts: contracts for private blockchain on Quorum operated by Emaar, and contracts for Ethereum mainnet. The core feature is an ERC20/ERC777 token on Quorum, with an Ethereum mainnet twin (Ethereum mainnet is treated as a side chain). The core utility of the Quorum token is redemption for services, which is realized through redeem gateways. The platform relies on a number of off-chain components. These components are not subject to this audit, but they are necessary to provide the functionality promised in the white paper. Additionally, the correctness of their implementation and availability is crucial from the security standpoint as they are supposed to guarantee some invariants as highlighted in this report. The platform is intentionally centralized, which provides the operator with the option of mitigating any arising issues by minting and burning tokens. The implementation itself is mostly clean, respects best practices, is extremely well tested, but does not contain in-code documentation.

Type	Loyalty Token Platform
Auditors	Martin Derka, Senior Research Engineer Sebastian Banescu, Senior Research Engineer Jan Gorzny, Blockchain Researcher
Timeline	2019-09-16 through 2019-11-06
EVM	Byzantium
Languages	Solidity, Javascript
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	EMR Token Lite Paper Miro Boards
Source Code	

Repository	Commit
Private Blockchain Contracts	acbb14d
Public Blockchain Contracts	35f5934

Severity Categories

High	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.
Medium	The issue puts a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.
Low	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low-impact in view of the client's business circumstances.
Informational	The issue does not pose an immediate threat to continued operation or usage, but is relevant for security best practices.
Undetermined	The impact of the issue is uncertain.

Total Issues	22	(22 Resolved)
High Risk Issues	2	(2 Resolved)
Medium Risk Issues	3	(3 Resolved)
Low Risk Issues	5	(5 Resolved)
Informational Risk Issues	11	(11 Resolved)
Undetermined Risk Issues	1	(1 Resolved)

Goals

- Assess security of the platform
- Assess adherence to the white paper
- Assess reliability and security of the cross-chain token transfers

Possible issues we looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Mishandled exceptions and call stack limits
- Unsafe external calls
- Integer overflow / underflow
- Number rounding errors
- Reentrancy and cross-function vulnerabilities
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting