Certik Post-Audit Report for Terra

Contents

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Verification Services Agreement between CertiK and Terra (the “Company”), or the scope of services/verification, and terms and conditions provided to the Company in connection with the verification (collectively, the “Agreement”). This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without CertiK’s prior written consent.

About CertiK

CertiK is a technology-led blockchain security company founded by Computer Science professors from Yale University and Columbia University built to prove the security and correctness of smart contracts and blockchain protocols.

CertiK, in partnership with grants from IBM and the Ethereum Foundation, has developed a proprietary Formal Verification technology to apply rigorous and complete mathematical reasoning against code. This process ensures algorithms, protocols, and business functionalities are secured and working as intended across all platforms.

CertiK differs from traditional testing approaches by employing Formal Verification to mathematically prove blockchain ecosystem and smart contracts are hacker-resistant and bug-free. CertiK uses this industry-leading technology together with standardized test suites, static analysis, and expert manual review to create a full-stack solution for our partners across the blockchain world to secure 6.2B in assets. For more information: https://certik.org

Executive Summary

This report is meant to act as verification that the Certik team has looked at the codebase of the project and confirmed that no code changes impacting the logic and functionality of KRT, the token of the Terra company, have been made. A comprehensive examination has been performed, utilizing Dynamic Analysis, Static Analysis, and Manual Review techniques.

Specifically, the “bank” module of Terra Core that governs the token transfers and account balances remains unchanged across the code updates that have been conducted since the original release of the Certik report. The logic for this module is inherited from the Cosmos SDK and maintains the same set of functionalities without material changes from Columbus-1, the landmark the last CertiK audit took place.

The code updates that have been done on the surrounding modules do not impact and are completely unrelated to the bank module, even more so to the KRT token underneath. As such, the behavior of the KRT token remains unchanged and would therefore achieve the same security level as it had in our original report.