ZKSync
Smart Contracts and Circuit. Audit

Mikhail Vladimirov and Dmitry Khovratovich

16th June 2020

This document describes the audit results of the ZKSync protocol implementation performed by ABDK Consulting.

1. Phase 1

We've been asked to review the ZKSync smart contracts given in two repos: one with zero knowledge proof verifier and the other with all other smart contracts and circuits. The former repo was supposed to verify a proof in the extended PLONK ZK proof system. The specification to this extension of PLONK was provided to us in a separate document. We have found a number of issues in the smart contracts, suggested a modification for the PLONK prover, and prepared a report.

2. Phase 2

We reviewed the fixes to the previous smart contracts in the main repo. All the significant issues from Phase 1 were fixed. We did not prepare a new report, but reported several new major issues. We also reviewed the protocol itself and reported some issues to the authors.

3. Phase 3

The protocol was modified, and then we reviewed the circuit generator. We prepared a circuit specification and reported several important issues to the authors. We reviewed the changes in the latest fix. We also reviewed the fixes to the contracts and found no issues in the latest version.

To summarize, we have reviewed smart contracts, the protocol, and the circuit generator in several iterations. To the best of our knowledge, there is no security issues left.