Cannon U16 Security Review

Coinbase Protocol Security

May 30, 2025

Contents

Audit Scope

Executive Summary

This report presents the outcomes of our engagement with the Optimism team, focusing on the evaluation of the updates made to the MIPS64 smart contracts. The applicable MIPS64 smart contracts were reviewed from May 27, 2025 to May 30, 2025.

Project Overview/Summary of Changes

The Cannon VM has been updated to support the Go 1.23 runtime and the fault proof program Kona when compiled to MIPS64. These changes require new state transition rules to the onchain MIPS64 smart contracts. Additionally, there is a new STATE_VERSION variable to determine which set of state transition rules apply. This report focuses on version 7.

The following are new additions due to version 7:

- mprotect syscall, implemented as a no-op
- eventfd2 syscall, implemented as a no-op
- dclz opcode
- dclo opcode

Invariants of the Protocol

- The smart contract logic must match with the offchain Cannon VM's logic.

Conclusions

No issues were found with the changes due to the following reasons:

- mprotect: There is no memory protection by the VM. Only the PROT_NONE flag is used, meaning no memory protections are applied. The syscall number was also verified.
- eventfd2: This syscall would return a file descriptor, however the VM only tracks specific file descriptor values associated with PreimageOracle reads / writes and ignores all other values. The syscall number was also verified.
- dclz/dclo: These opcodes are similar to the clz and clo opcodes, but instead operate on 64-bit words. Correct execution of these opcodes was verified.