Improving Trust in the FPGA Supply Chain using Blockchain and Keyless-Signature Technology

G. Richard Newell
Microsemi Corp.
System-on-Chip Products Group

Abstract

Blockchain and Keyless Signature Infrastructure (KSI) technologies that only rely on secure message digests and need no secret keys can be used to provide additional assurances that non-volatile FPGA components and systems moving up the supply chain hierarchy from wafer test through to completed systems are trustworthy. This is done by providing cryptographic evidence of the FPGA's provenance using a verifiable time-stamped audit trail of key events in the FPGA lifecycle using blockchain and KSI technology, complementing existing traditional measures. System manufacturers using those FPGAs can keep appending to the extensible information container that represents the entire history of the FPGA (and eventually the system), strengthening trust in the system, preventing counterfeiting at all levels (component and system), and providing a strong verifiable identity for use in the final run-time application.