Hardware Accelerator for Blockchain-Based Applications in IoT Devices: A Review

CW Dissanayake#, RHNS Jayathissa

Department of Computer Engineering, Faculty of Computing, General Sir John Kotelawala Defence University, Sri Lanka

Abstract. A growing number of Internet of Things devices are contemplating the usage of blockchain technology mainly due to various privacy and security concerns. Blockchain can be used in the IoT sector for making data tamper-proof while sharing between devices, storing sensitive data in a decentralized manner, and using smart contracts in blockchain to trigger various events upon meeting certain conditions. There are also other use cases such as asset tracking, supply chain tracking, and integration with machine learning algorithms. Since participation in blockchain protocol is required for those use cases, it necessitates dedicated computational capabilities of the underlying devices. This is an inherent challenge in an application domain infamous for having many, often strict, resource limitations such as computational power and area. This study focuses on the SHA256 hash function, a major component of blockchain technology, as well as hardware accelerators for the SHA-256 hash function and critically reviews key literature in this research area. The results in this review demonstrate how hardware accelerators can be used to overcome various limitations in IoT devices, providing low-power devices with the computational power needed to complete demanding tasks such as participating in blockchain protocols. It also demonstrates a performance comparison of existing implementations regarding throughput, power consumption, and area, as well as the advantages and disadvantages of each approach.

Keywords: *SHA-256, Blockchain, IoT, Cryptography, Hash Function, Hardware Accelerator, FPGA*