Graduate School of Science and Technology Master's Thesis Abstract

Laboratory name (Supervisor)	Computing Architecture (Yasuhiko Nakashima (Professor))		
Student ID	2011412	Submission date	2022 / 1 / 14
Name	LE VU TRUNG DUONG		
Thesis title	MRSA: A High-Efficiency Multi ROMix Scrypt Accelerator for Cryptocurrency Mining and Data Security		

Abstract

Nowadays, industrial revolution 4.0 is at the forefront of socio-economic development in many countries. As one of the most developed countries, Japan has proposed new criteria for socio-economic called Super Smart Society 5.0 as a future society for aspiring to. Many state-of-the-art technologies such as Data Science, Big Data, Artificial Intelligence (AI), Robotics, the Internet of Things (IoT), Blockchain, and so on are the backbone of Society 5.0.

The data for IoT, robotics, Big Data, or even AI are transferred through cyberspace. The cybersecurity requirements are more and more paid attention to preventing malicious attackers' data. One of the most reasons is that many current networks are centralized in which the cloud servers keep and control their whole systems. It will be dangered if the centralized servers are attacked, which appears some famous criteria in cybersecurity such as data threat, server crash attack, data loss, etc. A new technology called blockchain was invented to avoid these concerns and has become popular. Blockchain is distributed database recording digital events, important data, or digital currency transactions that have been executed and shared among participating nodes in the network. Accordingly, blockchain is a decentralized network that stores data in blocks, and these blocks are chained together through cryptographic hash functions. This helps the network easily verify that all data in the chain of blocks are kept intact from the beginning. One of the most famous blockchain applications is cryptocurrencies, widely known as Bitcoin, Litecoin, Ethereum, etc. They use Proof-of-Work (PoW) as the consensus mechanism for adding new blocks to the blockchain through the mining process. This process requires miners to perform hash computations until a valid nonce is found to add a new block to the blockchain.

The development of low-energy, high-performance hardware for blockchain mining is gaining widespread attention. The mining process for proof-of-work (PoW) in conventional cryptocurrencies' blockchains is increasingly being replaced by Application-Specific Integrated Circuits (ASICs). This leads to many security threats for the blockchain network because it decreases security and increases power consumption for mining. Therefore, Scrypt, the most representative ASIC-resistant algorithm, was developed to solve this problem. However, there are still some problems and challenges with the current Scrypt hardware. This thesis presents a new hardware architecture for the Scrypt algorithm intended for a PoW-based cryptocurrency mining system. The proposed Multi ROMix Scrypt Accelerator (MRSA) hardware architecture applies several optimization techniques: configuration, local-memory computing with high-performance pipelined Multi ROMix, and rescheduling resources to significantly increase processing speed, flexibility, and energy efficiency. For evaluation, the MRSA is implemented on Field-Programmable Gate Arrays (FPGAs) to examine its actual performance, consumption, and correctness. Evaluation results on a Xilinx system-on-chip (SoC) with the ALVEO U280 Data Center Accelerator Card FPGA show that the MRSA is much more power-efficient than some of the most powerful commercial CPUs, GPUs, and other FPGA implementations. On the ALVEO U280, the MRSA achieves a maximum hash rate of 296.76 kHash/s, a throughput of 304.9 Mbps when reaching a maximum frequency of 259.94 MHz, and power consumption of 18.12 W. The energy efficiency of the MRSA on the ALVEO U280 SoC is 52.83 and 867.88 times higher than those on an RTX 3090 GPU and an i9-10940X CPU, respectively.