Team members: **Team Leader:**

BlockChain Algorithms on ASIC chips

4th November 2019

OVERVIEW

Along with the development of the technology and internet, the concepts of the Internet of Things (IoT), system on chip and edge computing are becoming more popular as well. This implies that there is a high necessity in distributed computing, furthermore, such decentralization is also important or applicable for communication between devices within the grid. It can be noted that one of the vivid application of the highlighted notions is Blockchain technology, where the data is stored in the peer-to-peer network. Certainly, information security is a highly important requirement in all computation and communication. In the centralized system, where the majority of information is stored in a particular server, there is a considerable risk of data leakage. Therefore, due to the fact that in blockchain the data, secured in the specific block, cannot be altered without changing the data in all the related blocks, such a system lacks vulnerable points.

There are numerous ways of blockchain application including financial transactions, digital contracts, distributed smart grid with renewable energy sources and etc. As mentioned previously, the main advantage is owing to the experience that each block contains the cryptographic hash of the prior block. At this point, it is important to determine and implement the secure hash algorithm (SHA) which converts the data into the array of the bits with specific size, thus extremely minimizing the possibility of the corruption.

It is known that the next level of the elaboration of the bitcoin mining hardware after CPU and FPGA is the application-specific integrated circuit (ASIC). Therefore, in this project, the chip design for cryptocurrency mining including the data encryption will be proposed. It is planned to apply the SHA-256 algorithm for block hashing, in addition, the chip design is expected to be optimized to reduce the overall power consumption and latency.

GOALS

1. Design of the ASIC based cryptocurrency mining
2. Implement blockchain algorithm on ASIC based structure

SPECIFICATIONS

In this project, it is expected to propose the ASIC design for the implementation of the cryptocurrency mining and hashing algorithm applied in the blockchain. In addition, the suggested design should be advantageous in terms of power consumption.

MILESTONES

Front-End Design Process

Implement HDL based design of the chip, i.e. RTL coding, following synthesis to the physical hardware, in addition, functional verification of the structure.

Back-End Design Process

Plan the core level of the circuit, following the placement of the components with parasitic extractions and timing analysis, in addition, the post-layout verification.