POWER EFFICIENT BLOCKCHAIN MINER ACCELERATOR DESIGN

LIM CALVIN

UNIVERSITI TEKNOLOGI MALAYSIA

POWER EFFICIENT BLOCKCHAIN MINER ACCELERATOR DESIGN

LIM CALVIN

A project report submitted in fulfilment of the
requirements for the award of the degree of
Master of Engineering (Computer and Microelectronic Systems)

School of Electrical Engineering
Faculty of Engineering
Universiti Teknologi Malaysia

JULY 2022

DEDICATION

This thesis is dedicated to my father, who taught me that the best kind of knowledge to have been that which is learned for its own sake. It is also dedicated to my mother, who taught me that even the largest task can be accomplished if it is done one step at a time.

ACKNOWLEDGEMENT

In preparing this thesis, I was in contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to my main thesis supervisor, Dr. Shahidatul Sadiah Binti Abdul Manan, for encouragement, guidance, critics and friendship. Without her continued support and interest, this thesis would not have been the same as presented here.

My fellow postgraduate student should also be recognised for their support. My sincere appreciation also extends to all my colleagues and others who have provided assistance at various occasions. Their views and tips are useful indeed. Unfortunately, it is not possible to list all of them in this limited space. I am grateful to all my family member.

ABSTRACT

Blockchain related technology nowadays involves cryptocurrency, supply chains, global trades, land registration, and logistics. While blockchain's unique characteristics provides benefits such as increase transparency, integrity and security of data that is shared across the network, employing blockchain requires very high energy consumption due to its mining process. Mining process’s high energy consumption was due to the Proof of work (PoW) consensus protocols on the blockchain network which utilizing the double SHA-256 algorithm to compute the hash of the block header. This ensures that each block of database entry that is distributed on the network is confirmed and encrypted, increasing integrity and data security. Most of the researches and improvement are focus on throughput and performance on the hardware as a standalone accelerator, overlooking the importance of power efficiency which is also one of the main factors in current industry system-on-a-chip (SoC) design. The data dependency among loops in the double SHA-256 algorithm was one of the main aspects which leads to high energy consumption due to the extensive calculation process for multiple loops. This paper proposing a power efficient blockchain miner accelerator design to optimize the power consumption of the blockchain miner accelerator from the design perspective which relates to clock gating, high voltage and low voltage threshold (HVT & LVT) standard cell technology library. There are 3 main intensions, first is to implement a SHA-256 baseline architecture in ASIC with Synopsys Verilog Compiler and Simulator (VCS) for circuit design verification and Design compiler (DC) for circuit synthesis using SAED 32nm standard cell library as the PDK (Process Design Kit). Next is to design a double SHA-256 accelerator using the same tools and technology and compare the two algorithms in terms of power consumption. Last is to analyse the power consumption of double SHA-256 accelerator with the implementation of clock gating optimization and different voltage threshold cell (HVT & LVT) setup. Results from the research shows that HVT synthesized circuit design with clock gating implementation for the accelerator produced good power efficiency.

ABSTRAK

Teknologi berkaitan rantaian blok pada masa kini melibatkan mata wang kripto, rantaian bekalan, perdagangan global, pendaftaran tanah dan logistik. Walaupun ciri-ciri unik blockchain memberikan faedah seperti meningkatkan ketelusan, integriti dan keselamatan data yang dikongsi merentasi rangkaian, menggunakan blockchain memerlukan penggunaan tenaga yang sangat tinggi kerana proses perlombongannya. Penggunaan tenaga yang tinggi dalam proses perlombongan melibatkan protokol konsensus bukti kerja (PoW) pada rangkaian blockchain yang menggunakan algoritma SHA-256 berganda untuk mengira nilai hash pengepala blok. Ini memastikan bahawa setiap blok disahkan dan disulitkan, meningkatkan integriti dan keselamatan data. Kebanyakan penyelidikan dan penambahbaikan tertumpu pada daya pemprosesan dan prestasi pada perkakasan sebagai pemecut kendiri, mengabaikan kepentingan kecekapan kuasa yang juga merupakan salah satu faktor utama dalam reka bentuk sistem-on-a-cip (SoC) industri semasa. Kebergantungan data antara gelung dalam algoritma SHA-256 berganda merupakan salah satu aspek utama yang membawa kepada penggunaan tenaga yang tinggi disebabkan oleh proses pengiraan yang meluas untuk berbilang gelung. Projek ini mencadangkan reka bentuk pemecut pelombong blok blok yang cekap kuasa untuk mengoptimumkan penggunaan kuasa pemecut penambang blok blok dari perspektif reka bentuk yang berkaitan dengan *standard cell technology library*, voltan tinggi dan ambang voltan rendah (HVT & LVT). Terdapat 3 intensi utama, pertama adalah untuk melaksanakan seni bina garis dasar SHA-256 dalam ASIC dengan Synopsys Verilog Compiler and Simulator (VCS) untuk pengesahan reka bentuk litar dan Reka bentuk pengkompil (DC) untuk sintesis litar menggunakan perpustakaan sel standard SAED 32nm sebagai PDK (Kit Reka Bentuk Proses). Seterusnya adalah untuk mereka bentuk pemecut SHA-256 berganda menggunakan alat dan teknologi yang sama dan membandingkan kedua-dua algoritma dari segi penggunaan kuasa. Terakhir adalah untuk menganalisis penggunaan kuasa pemecut SHA-256 berganda dengan pelaksanaan pengoptimuman gating jam dan persediaan sel ambang voltan yang berbeza (HVT & LVT). Hasil daripada penyelidikan menunjukkan bahawa reka bentuk litar sintesis HVT dengan pelaksanaan gating jam untuk pemecut menghasilkan kecekapan kuasa yang baik.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Problem Background

Blockchain utilizing a decentralized way to provide a variety of security related benefits such as transparency, integrity and data security. Its unique characteristics leads to its contribution on cryptocurrency, supply chains, insurance, logistics and global trades[1]–[3].

However, appreciating the benefits of blockchain comes with a trade-off, which is the high power and energy consumption problem. Blockchain as one type of distributed ledgers, every block of the database that is uploaded to the network was encrypted and secured through consensus protocols. The reason behind blockchain decentralize network that helps to provide high data integrity level is the selection of hashing algorithm for blockchain consensus protocols.

Consensus protocols involves the hashing computation (mining process) effort which leads to extreme high power consumption problem. Proof of work (PoW) is widely believed to be the consensus that provides high security level which is secure enough for public network which utilizing double Secure Hash Algorithm 256-bit (SHA-256) algorithm to hash every block header of a database that is uploaded to the network. The complexity of this algorithm prevents hacker to tamper with the data that is share across the network, guarantee data integrity and data security. The hashing complexity utilize high calculation power provides security to the databases but at the same time it is consuming high energy and powers, leading to its poor power efficiency.

1.2 Problem Statement

The problem statements of the research are:

(a) Blockchain mining process has a very high-power consumption due to the Proof of work (PoW) consensus protocols which utilizing the double SHA-256 algorithm to compute the hash of the block header.

(b) There have been numerous proposed designs to increase the throughput, but few focuses on optimizing the power consumption of the design.

1.3 Research Objective

The objectives of the research are:

(c) To implement a SHA-256 baseline architecture in ASIC which focus on Proof of Work consensus algorithms.

(d) To design a double SHA-256 accelerator in ASIC which focus on Proof of Work consensus algorithms and compare it with SHA-256 baseline architecture in terms of power consumption.

(e) To analyze the power consumption of double SHA-256 accelerator with the implementation of clock gating optimization and different voltage threshold cell (HVT & LVT) setup.

1.4 Research Scope

The scopes of this project are:

(f) Design implemented in this project:

   a. SHA-256 baseline architecture

   b. double SHA-256 accelerator

(g) Synopsys EDA tools, with Verilog Compiler and Simulator (VCS) for circuit design verification, Design compiler (DC) for circuit synthesis and target library is SAED 32 nm technology.

(h) Double SHA-256 accelerator design limits to the implementations of clock gating optimization, along with LVT & HVT voltage threshold cell setup.

(i) Only focus on power efficiency design improvement.

(j) Design flow only includes circuit design verification and logic synthesis.

REFERENCES

[1] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Bus. Horiz.*, vol. 58, no. 4, pp. 431–440, Jul. 2015, doi: 10.1016/J.BUSHOR.2015.03.008.

[2] T. H. Tran, H. L. Pham, T. D. Phan, and Y. Nakashima, "BCA: A 530-mW Multicore Blockchain Accelerator for Power-Constrained Devices in Securing Decentralized Networks," *IEEE Trans. Circuits Syst. I Regul. Pap.*, vol. 68, no. 10, pp. 4245–4258, 2021, doi: 10.1109/TCSI.2021.3102618.

[3] S. Krishnapriya and G. Sarath, "Securing Land Registration using Blockchain," *Procedia Comput. Sci.*, vol. 171, no. 2019, pp. 1708–1715, 2020, doi: 10.1016/j.procs.2020.04.183.

[4] M. A. Safana, Y. Arafa, and J. Ma, "Improving the performance of the Proof-of-Work Consensus Protocol Using Machine learning," *2020 2nd Int. Conf. Blockchain Comput. Appl. BCCA 2020*, pp. 16–21, 2020, doi: 10.1109/BCCA50787.2020.9274082.

[5] Z. Cekerevac, L. Prigoda, and J. Maletic, "Blockchain Technology and Industrial Internet of Things in the Supply Chains," *MEST J.*, vol. 6, no. 2, pp. 39–47, 2018, doi: 10.12709/mest.06.06.02.05.

[6] M. Kim, J. Ryou, and S. Jun, "Efficient hardware architecture of SHA-256 algorithm for trusted mobile computing," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5487, pp. 240–252, 2009, doi: 10.1007/978-3-642-01440-6_19.

[7] "Blockchain Explained: What is blockchain? | Euromoney Learning." https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain (accessed Feb. 17, 2022).

[8] P. Classification and S. Clara, "The latendimentului umani," vol. 1, 2018.

[9] Y. Zhang *et al.*, "A New Message Expansion Structure for Full Pipeline SHA-2," *IEEE Trans. Circuits Syst. I Regul. Pap.*, vol. 68, no. 4, pp. 1553–1566, 2021, doi: 10.1109/TCSI.2021.3054758.

[10] H. L. Pham, T. H. Tran, T. D. Phan, V. T. Duong Le, D. K. Lam, and Y. Nakashima, "Double SHA-256 Hardware Architecture with Compact Message

Expander for Bitcoin Mining,” *IEEE Access*, vol. 8, pp. 139634–139646, 2020, doi: 10.1109/ACCESS.2020.3012581.

[11] T. H. Tran, H. L. Pham, and Y. Nakashima, “A High-Performance Multimem SHA-256 Accelerator for Society 5.0,” *IEEE Access*, vol. 9, pp. 39182–39192, 2021, doi: 10.1109/ACCESS.2021.3063485.

[12] H. I. A. Chen, E. K. W. Loo, J. B. Kuo, and M. J. Syrzycki, “Triple-threshold static power minimization technique in high-level synthesis for designing high-speed low-power SOC applications using 90nm MTCMOS technology,” *Can. Conf. Electr. Comput. Eng.*, pp. 1671–1674, 2007, doi: 10.1109/CCECE.2007.418.

[13] N. Agnes Shiny Rachel, B. Fahimunnisha, S. Akilandeswari, and S. Joyes Venula, “Integration of Clock Gating and Power Gating in Digital Circuits,” *2019 5th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2019*, pp. 704–707, 2019, doi: 10.1109/ICACCS.2019.8728370.

[14] P. Sahu and S. K. Agrahari, “Comparative Analysis of Different Clock Gating Techniques,” *2020 5th IEEE Int. Conf. Recent Adv. Innov. Eng. ICRAIE 2020 - Proceeding*, vol. 2020, pp. 4–9, 2020, doi: 10.1109/ICRAIE51050.2020.9358375.

[15] T. Fanni, C. Sau, P. Meloni, L. Raffo, and F. Palumbo, “Power and clock gating modelling in coarse grained reconfigurable systems,” *2016 ACM Int. Conf. Comput. Front. - Proc.*, pp. 384–391, 2016, doi: 10.1145/2903150.2911713.

[16] R. P. McEvoy, F. M. Crowe, C. C. Murphy, and W. P. Marnane, “Optimisation of the SHA-2 family of hash functions on FPGAs,” *Proc. - IEEE Comput. Soc. Annu. Symp. Emerg. VLSI Technol. Archit. 2006*, vol. 2006, pp. 317–322, 2006, doi: 10.1109/ISVLSI.2006.70.

[17] S. Binti Suhaili and T. Watanabe, “Design of high-throughput SHA-256 hash function based on FPGA,” *Proc. 2017 6th Int. Conf. Electr. Eng. Informatics Sustain. Soc. Through Digit. Innov. ICEEI 2017*, vol. 2017-Novem, pp. 1–6, 2018, doi: 10.1109/ICEEI.2017.8312449.

[18] H. E. Michail, G. S. Athanasiou, V. Kelefouras, G. Theodoridis, and C. E. Goutis, “On the exploitation of a high-throughput SHA-256 FPGA design for HMAC,” *ACM Trans. Reconfigurable Technol. Syst.*, vol. 5, no. 1, pp. 1–28, 2012, doi: 10.1145/2133352.2133354.

[19] F. Opritoiu, S. L. Jurj, and M. Vladutiu, “Technological solutions for throughput improvement of a Secure Hash Algorithm-256 engine,” *2017 IEEE 23rd Int. Symp. Des. Technol. Electron. Packag. SIITME 2017 - Proc.*, vol. 2018-Janua, pp. 159–164, 2017, doi: 10.1109/SIITME.2017.8259881.

[20] R. Martino and A. Cilardo, “A Flexible Framework for Exploring, Evaluating, and Comparing SHA-2 Designs,” *IEEE Access*, vol. 7, pp. 72443–72456, 2019, doi: 10.1109/ACCESS.2019.2920089.

[21] F. Kahri, B. Bouallegue, M. MacHhout, and R. Tourki, “An FPGA implementation and comparison of the SHA-256 and Blake-256,” *14th Int. Conf. Sci. Tech. Autom. Control Comput. Eng. STA 2013*, pp. 152–157, 2013, doi: 10.1109/STA.2013.6783122.

[22] R. García, I. Algredo-Badillo, M. Morales-Sandoval, C. Feregrino-Uribe, and R. Cumplido, “A compact FPGA-based processor for the Secure Hash Algorithm SHA-256,” *Comput. Electr. Eng.*, vol. 40, no. 1, pp. 194–202, 2014, doi: 10.1016/j.compeleceng.2013.11.014.

[23] M. D. Rote, N. Vijendran, and D. Selvakumar, “High performance SHA-2 core using the Round Pipelined Technique,” *2015 IEEE Int. Conf. Electron. Comput. Commun. Technol. CONECCT 2015*, pp. 1–6, 2016, doi: 10.1109/CONECCT.2015.7383912.

[24] R. Chaves, G. Kuzmanov, L. Sousa, and S. Vassiliadis, “Cost-efficient SHA hardware accelerators,” *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 16, no. 8, pp. 999–1008, 2008, doi: 10.1109/TVLSI.2008.2000450.

[25] L. Dadda, M. Macchetti, and J. Owen, “The design of a high speed ASIC unit for the hash function SHA-256 (384, 512),” *Proc. -Design, Autom. Test Eur. DATE*, vol. 3, pp. 70–75, 2004, doi: 10.1109/DATE.2004.1269207.

[26] “Synopsys | EDA Tools, Semiconductor IP and Application Security Solutions.” https://www.synopsys.com/ (accessed Feb. 18, 2022).