Implementation of Double SHA-256 in HLS for FPGA Using Real Bitcoin Blocks

Bernardo V. S. Pinto*, Douglas R. Melo*, Cesar A. Zeferino*, Eduardo A. Bezerra†, and Felipe Viel*†
* Laboratory of Embedded and Distributed Systems (LEDS), University of Vale do Itajaí, Brazil
† Space Systems Research Laboratory (SpaceLab), Federal University of Santa Catarina, Brazil
berna@edu.univali.br, drm@univali.br, zeferino@univali.br, eduardo.bezerra@ufsc.br, viel@univali.br

***Abstract*—The SHA-256 cryptographic algorithm plays a central role in the integrity and security of the Bitcoin blockchain, being applied twice consecutively in the process known as Double SHA-256. Despite its reliability, the algorithm demands significant computational power, which poses challenges for embedded systems with strict energy and performance constraints. This work aims to evaluate the feasibility of implementing Double SHA-256 in reconfigurable hardware using High-Level Synthesis (HLS) on commercial FPGA platforms. The architecture was developed as a custom IP core and integrated into bare-metal systems on the ZedBoard (Zynq-7000) and ZCU104 (Zynq UltraScale+ MPSoC) platforms, validating real blockchain blocks to ensure functional accuracy. Results showed that the ZCU104 achieved a performance of 319 kH/s with an execution time of 3.1 µs per hash, while the ZedBoard excelled in energy efficiency, delivering 29.625 hashes per watt. Both implementations utilized a single logic core, achieving low FPGA resource utilization. The proposed approach proved to be effective and energy-efficient, making it suitable for embedded applications requiring high-performance cryptography.**

***Index Terms*—SHA-256, Double Hashing, FPGA, High-Level Synthesis, Bitcoin, Blockchain, Embedded Systems.**

I. Introduction

In the current landscape of technological advancement, digital processing technologies play a fundamental role in solving complex computational problems. With the exponential growth of data and the demand for efficient processing, Field-Programmable Gate Arrays (FPGAs) have gained prominence due to their reconfigurability and high degree of customization [1]. These devices are widely used in applications requiring high performance, such as embedded systems, machine learning, and, more recently, blockchain operations [2].

Given the growing complexity of blockchain operations and the increasing demand for energy-efficient solutions, High-Level Synthesis (HLS) has emerged as a viable method to achieve high performance in FPGA-based systems. HLS enables the translation of high-level languages, such as C/C++, into hardware descriptions compatible with FPGA logic, allowing for optimizations and parallelism inherent to hardware architectures [3]. This approach significantly reduces development time compared to traditional Hardware Description Languages (HDLs), while maintaining the flexibility to explore architectural optimizations. In addition, HLS bridges the gap between software-oriented developers and hardware design, making FPGA-based cryptographic accelerators more accessible for research and prototyping. [4]

In this context, this work explores the use of FPGAs programmed via HLS to validate the Double SHA-256 algorithm, a core component in Bitcoin's block verification process. Unlike traditional mining approaches, this project focuses on block validation using real headers extracted from the Bitcoin blockchain. The adoption of HLS is motivated not only by the need to achieve competitive performance but also by the possibility of rapidly iterating and testing hardware-software co-design strategies. This approach makes it possible to evaluate trade-offs between latency, throughput, and resource consumption, ensuring that the resulting implementation is both computationally effective and energy-efficient. [5]–[7].

The blockchain is a decentralized system in which each participant node is responsible for recording and verifying transactions, thereby eliminating the need for a central authority. Security is ensured by the network's consensus and computational difficulty, making fraudulent alterations practically infeasible due to the immense computing power required [8]. In this scenario, accelerating the validation process through specialized hardware becomes an essential contribution to the sustainability and scalability of blockchain networks. For instance, hardware accelerators have been shown to boost block validation throughput in permissioned blockchains by factors of 10× or more [9]. Similarly, FPGA-based signature verification engines help offload expensive cryptographic checks from CPUs, improving overall system scalability [10].

The remainder of this paper is structured as follows. Section II provides Background information on Bitcoin mining, FPGA platforms, and High-Level Synthesis, while Section III reviews related works. The proposed architecture is demonstrated in Section IV and the results obtained from our experiments are detailed in Section V. Finally, the conclusions of this study are presented in Section VI.

II. Background

The process of Bitcoin mining relies on the validation of block headers using the double SHA-256 algorithm, which is computationally intensive and requires massive parallelism. In the early stages of Bitcoin, mining was feasible using

This work was supported by CAPES – the Brazilian Federal Agency for Support and Evaluation of Graduate Education – Finance Code 001, FAPESC – the Foundation for Support of Research and Innovation, Santa Catarina – Call 51/2024 Grants 2023TR000880 and 2024TR001897, and CNPq – the Brazilian National Council for Scientific and Technological Development – Processes 140368/2021-3, 408641/2023-1, and 306478/2025-0.

CPUs, but as the network's difficulty increased, the adoption of Application-Specific Integrated Circuits (ASICs) became necessary. Although ASICs provide high performance, they lack flexibility and demand substantial investments in hardware and infrastructure [11].

In this context, Field-Programmable Gate Arrays (FPGAs) emerge as a cost-effective and reconfigurable solution. Unlike ASICs, FPGAs allow design exploration and hardware acceleration tailored to specific applications while maintaining lower power consumption than GPUs [3]. High-Level Synthesis (HLS) further enhances this approach by enabling the description of complex algorithms in C/C++, which are then automatically synthesized into hardware logic, significantly reducing design time and complexity [3].

This work leverages HLS to implement and optimize a Double SHA-256 hashing architecture on FPGA platforms, validating its feasibility in real blockchain environments.

III. Related Work

Santos Júnior et al. [12] proposed a reconfigurable hardware architecture for SHA-256 hashing, targeting blockchain and IoT applications. The authors developed the proposed architecture on an Xilinx Virtex-6 FPGA, supporting up to 16 parallel SHA-256 cores. The architecture enables dynamic reconfiguration, allowing the system to optimize for either performance or power efficiency, depending on the deployment context. Experimental results showed a throughput of approximately 1.4 Gbps with 16 cores and a reduction of up to 234× in dynamic power consumption compared to previous designs. This work demonstrates the potential of deploying SHA-256 accelerators in embedded and low-power systems, offering a valuable benchmark for blockchain-oriented hardware solutions.

Recent studies have explored the use of FPGAs in computationally intensive applications, leveraging HLS to accelerate specific algorithms. Dang and Skadron (2017) investigated the acceleration of Frequent Itemset Mining (FIM) on FPGAs using SDAccel and Vivado HLS. Their work demonstrated a speedup of up to 3.2× over CPU implementations and showed higher energy efficiency than GPUs [4].

Kammoun et al. (2020) proposed an FPGA-based implementation of the SHA-256 algorithm, aiming to enhance performance and reduce energy consumption in security-focused applications. Their approach used Vivado HLS and hybrid ARM-FPGA architectures, employing directives such as loop unrolling and pipelining to optimize throughput. Their results indicated a 73% reduction in energy usage and a 17% increase in execution speed compared to software-only implementations [13].

Although these works have made significant contributions to the field of hardware acceleration and blockchain processing, most focus on mining or synthetic benchmark scenarios. In contrast, this work presents a novel implementation of Double SHA-256 on an FPGA for validating real Bitcoin blocks, ensuring compatibility with existing blockchain standards while emphasizing energy-efficient embedded processing.

IV. Proposed Architecture

This section presents the hardware architecture designed for validating real Bitcoin blocks using the Double SHA-256 algorithm, implemented through High-Level Synthesis (HLS) on commercial FPGA platforms.

A. System Overview

The proposed system targets the execution of the double SHA-256 hash function on the header of real Bitcoin blocks, replicating the validation mechanism used in the Bitcoin network [8]. This approach was chosen to demonstrate not only the feasibility of FPGA-based cryptographic acceleration but also its direct applicability in real blockchain environments. The architecture consists of two main components: a custom HLS-based IP core for SHA-256 hashing and a bare-metal software application running on the ARM processor of Xilinx's Zynq platforms. Communication between the processing system (PS) and the programmable logic (PL) is carried out through AXI4-Lite interfaces, ensuring low-latency and memory-mapped access to the accelerator. The overall interaction between hardware and software components in the proposed architecture is depicted in Fig. 1, highlighting how real Bitcoin block headers are processed through the ARM processor, FPGA IP, and external blockchain node.

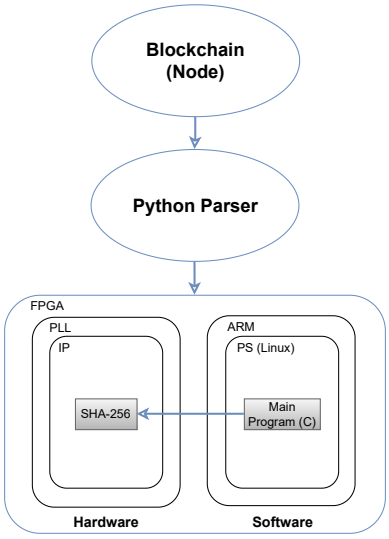

Fig. 1. Overview of the proposed architecture using real Bitcoin blocks.

The system receives pre-assembled 80-byte headers, applies the double SHA-256 procedure, and returns the resulting 256-bit hash for verification against the target value. By reproducing the same hashing and validation procedure used by Bitcoin full nodes, the design bridges academic experimentation with practical blockchain applications, emphasizing both computational performance and functional correctness.

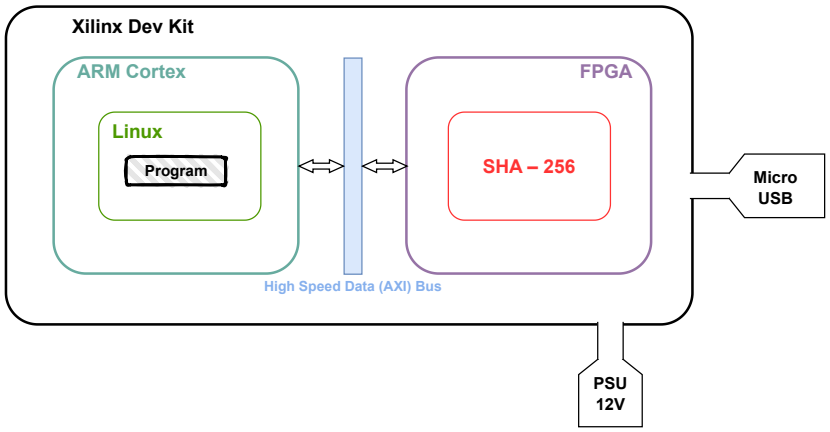

Fig. 2. Internal hardware architecture with SHA-256 core implemented on FPGA.

B. Double SHA-256 IP Design

The SHA-256 core was developed in C and synthesized using Vivado HLS to generate RTL code optimized for FPGA logic. The implementation follows a pipelined architecture, divided into two sequential SHA-256 hashing stages, which corresponds to the Bitcoin double hashing requirement. Each stage processes 512-bit message blocks through 64 compression rounds, using a combination of shift, rotate, and modular addition operations characteristic of the SHA-2 family.

Optimization directives such as loop unrolling, pipeline initiation intervals, and resource constraints were carefully applied to balance latency, throughput, and area utilization. This process highlights the advantages of HLS, which enables fast design space exploration without requiring manual low-level HDL coding. The IP exposes memory-mapped registers for input messages, nonces, targets, and control flags (e.g., `ap_start`, `ap_done`, `ap_idle`), making it seamlessly integrable into larger system-on-chip architectures. This modular design ensures scalability, allowing for the instantiation of multiple cores or parallel pipelines in future extensions of the work. A detailed representation of the hardware organization, including the integration of the SHA-256 IP core inside the FPGA fabric, is shown in Fig. 2. This view emphasizes the internal data paths and power supply connections required for operation.

C. Implementation Details

The internal flow of the `sha256_top` function represents the complete Double SHA-256 calculation, fully compliant with the Bitcoin specification. This block receives an 80-byte header (organized as 20 words of 32 bits), executes two consecutive SHA-256 rounds, and outputs the final 256-bit hash. The design was structured to be fully sequential, including initialization, variable setup, and buffer conversion between `uint32_t` and byte arrays, ensuring compatibility with the standard algorithm and deterministic results.

Special care was taken to maintain algorithmic fidelity while enabling efficient synthesis into hardware logic. Intermediate buffers and endianness adjustments were handled explicitly to ensure that the hardware implementation would produce the same results as reference Bitcoin clients and cryptographic libraries. This methodology ensures that the accelerator is not merely a proof of concept but a functionally reliable component for blockchain validation. The overall procedure is summarized in Fig. 3.

D. System Architecture

The block design implemented in Vivado for the ZCU104 platform utilizes AXI interconnect channels to facilitate communication between the Processing System (PS) and the Programmable Logic (PL). In this architecture, the High-Performance Master (HPM) and High-Performance Slave (HP) interfaces provide significantly higher bandwidth compared to the previous Zynq generation, ensuring efficient data transfer and improved throughput during mining operations. The overall integration of the Processing System (PS) and the Programmable Logic (PL) in the ZCU104 platform is depicted in Fig. 4. The block diagram illustrates the connections between the ARM cores, the custom SHA-256 IP, and auxiliary modules, including GPIO and performance counters, demonstrating how the accelerator is orchestrated through AXI interconnects.

E. Integration with Bare-Metal Systems

The generated IP was integrated into a custom hardware design using Vivado's Block Design environment. The ZedBoard (Zynq-7000) and ZCU104 (Zynq UltraScale+ MPSoC) platforms were used for implementation and testing, allowing the evaluation of trade-offs between low-cost and high-performance FPGA devices. A bare-metal application written in C runs on the ARM processor and is responsible for orchestrating the accelerator. The main steps include:

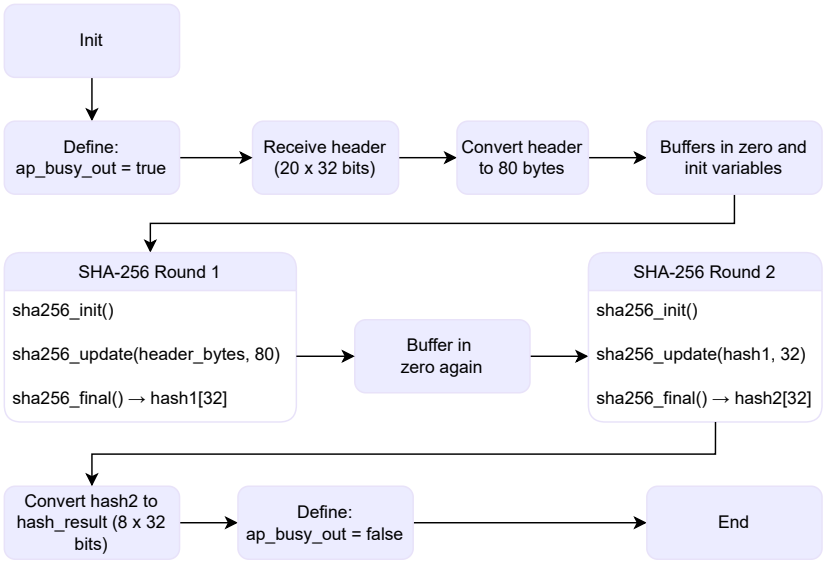

Fig. 3. Flowchart of SHA256_TOP

- Receiving block header data and target via UART.
- Writing inputs to the IP registers using AXI interfaces.
- Starting the hashing process through control signals.
- Polling for completion and retrieving the 256-bit hash result.
- Comparing the result against the target to validate the block.

This integration ensures minimal software overhead while leveraging the performance of the hardware accelerator. By avoiding operating system overhead, the system achieves deterministic execution and low-latency communication between software and hardware, which is crucial in real-time blockchain validation scenarios.

F. Validation Using Real Bitcoin Blocks

To guarantee the system's functional correctness, real block headers were extracted from the Bitcoin blockchain, including fields such as version, previous block hash, Merkle root, timestamp, bits, and nonce. The system was tested using block 100000 and others with increasing difficulty levels, ensuring that the design could handle real-world complexity. The results obtained from the FPGA were cross-verified with reference hashes computed using Python scripts and blockchain explorers, confirming bit-accurate compliance with the Bitcoin specification.

Only valid shares that matched the network's target were accepted, demonstrating that the hardware design adheres to the consensus rules enforced by the blockchain. This validation methodology emphasizes not only performance but also the trustworthiness of the system in a real cryptographic context. By reproducing the exact node validation procedure in hardware, the design demonstrates its suitability for embedded blockchain verification tasks, as illustrated in Fig. 5. This approach contributes to the vision of lightweight, energy-efficient blockchain nodes that can operate in constrained environments while maintaining full compliance with the protocol.

V. Experimental Results

This section presents the results of performance, energy efficiency, and resource utilization obtained by implementing the Double SHA-256 architecture on two FPGA platforms: the ZedBoard 7000 and the ZCU104. In addition to these

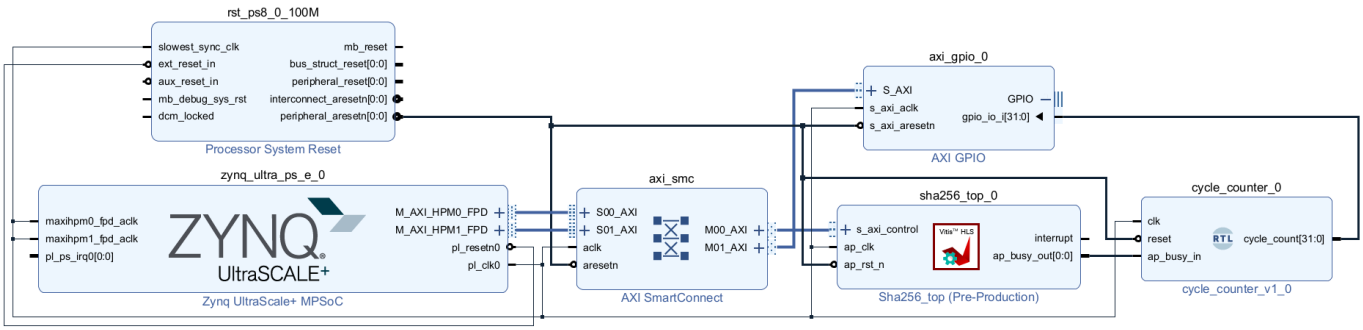

Fig. 4. ZCU104 Block Diagram

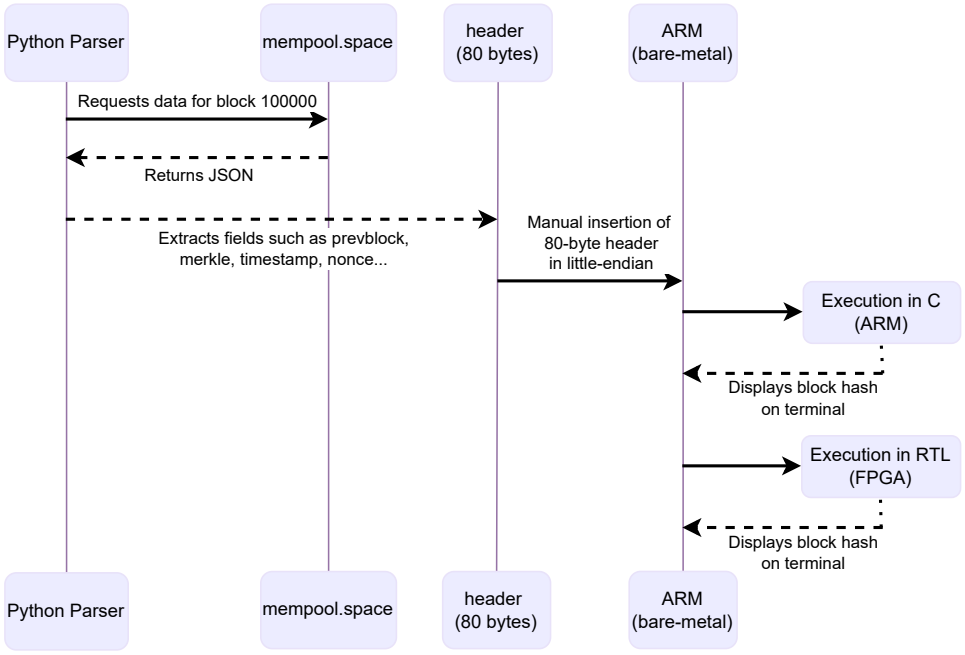

Fig. 5. Validation flow using real Bitcoin block headers with Double SHA-256.

embedded systems, a desktop-class AMD Ryzen 7 5800x3D CPU was also used as a performance reference to provide a comparative baseline against a high-end general-purpose processor.

A. Performance Metrics

The hashrate was computed by measuring the time required to process a single 80-byte Bitcoin block header. This was achieved both in ARM software (bare metal) and using the custom FPGA IP.

On the ZedBoard platform, the FPGA implementation achieved an execution time of 7.850 ns per hash, resulting in an estimated performance of 127.388 H/s. In contrast, the ARM (Cortex-A9) implementation required 58.607 ns, yielding 17.061 H/s.

On the ZCU104, the FPGA achieved a significantly higher performance: 3.128 ns per hash and 319.693 H/s, while the ARM (Cortex-A53) implementation reached only 23.736 H/s with a latency of 42.03 ns.

For reference, the Double SHA-256 algorithm was also executed on a single core of the AMD Ryzen 7 5800x3D, using an optimized C implementation under Microsoft Windows 10. The measured execution time was 3.4 µs per hash, corresponding to a hashrate of approximately 294,118 H/s. While this result outperforms the embedded systems in raw speed, it comes with substantially higher power consumption, making it less suitable for energy-constrained or embedded blockchain applications. These results highlight the effectiveness of FPGA-based accelerators in providing a balanced trade-off between performance and energy efficiency. The comparative hashrates across platforms are summarized in Fig. 6, demonstrating the performance advantage of FPGA-based execution over ARM software implementations.

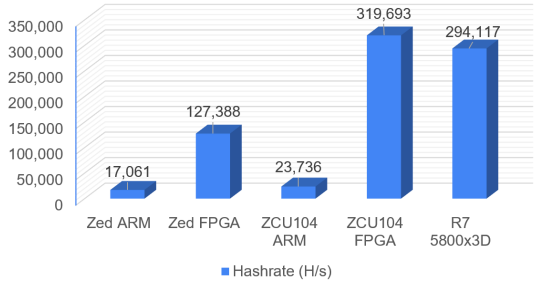

Fig. 6. Hashrate achieved by each platform (ARM, FPGA and CPU).

B. Energy Efficiency

Energy measurements were performed using external wattmeters during the execution of the hashing algorithm. To provide a comparative perspective, the energy efficiency of the AMD Ryzen 7 5800x3D was estimated using its Thermal Design Power (TDP), which is officially rated at 105 W. Although TDP does not represent the exact real-time power consumption—especially for short, bursty workloads—it serves as a reasonable upper-bound approximation in the absence of direct power measurements. Based on this assumption, a summary of the performance and energy efficiency results for each platform is presented in Table I, consolidating both the hashrate and estimated power consumption into a direct efficiency metric.

TABLE I
PERFORMANCE AND ENERGY EFFICIENCY SUMMARY

Platform	Hashrate (H/s)	Power (W)	Efficiency (H/W)
ZedBoard FPGA	127,388	4.3	29,625
ZCU104 FPGA	319,693	11.0	29,063
Ryzen 7 5800X3D	294,117	105.0	2,801

Despite the Ryzen achieving significantly higher raw performance, its estimated energy efficiency is nearly one order of magnitude lower than that of the FPGA-based implementations. This reinforces the suitability of FPGA accelerators in scenarios where both performance and power consumption must be carefully balanced, such as in embedded blockchain validation nodes. Fig. 7 illustrates the hashrate-per-watt efficiency of each platform, reinforcing the suitability of FPGAs for energy-constrained blockchain validation tasks.

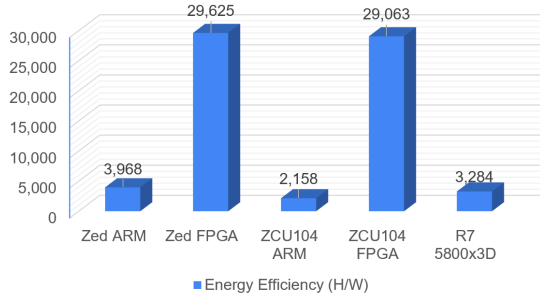

Fig. 7. Energy efficiency comparison (Hashrate per Watt) among different platforms.

Despite the higher raw performance of the ZCU104, both platforms achieved comparable energy efficiency, reinforcing the suitability of FPGAs for energy-sensitive cryptography.

C. Resource Utilization

A summary of the performance and energy efficiency results for each platform is presented in Table II, consolidating both the hashrate and estimated power consumption into a direct efficiency metric.

TABLE II
FPGA RESOURCE UTILIZATION

Resource	ZedBoard (Zynq-7000)	ZCU104 (UltraScale+)
LUTs	10,709 / 53,200 (20.1%)	13,231 / 230,400 (5.74%)
FFs	12,804 / 106,400 (12.0%)	14,062 / 460,800 (3.05%)
BRAMs	2 / 140 (1.43%)	2.5 / 312 (0.80%)
LUTRAM	222 / 17,400 (1.28%)	544 / 101,760 (0.53%)

The post-implementation utilization of LUTs, FFs, BRAMs, and LUTRAM is shown in Fig. 8, confirming that the accelerator occupies only a small fraction of the available FPGA logic resources.

The results demonstrate that the proposed IP core occupies only a small fraction of the available FPGA resources, even on the entry-level Zynq-7000 device. Although the relative usage is higher in the ZedBoard due to its smaller capacity, the design still consumes less than one-fifth of the LUTs,

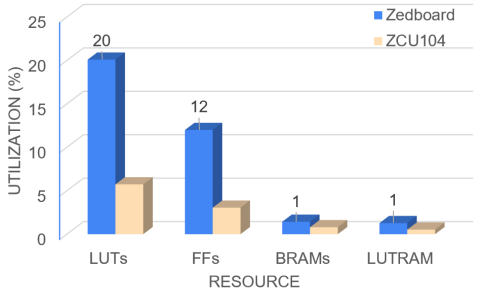

Fig. 8. FPGA logic resource utilization on each platform.

leaving sufficient headroom for integrating additional system logic. On the larger ZCU104 platform, utilization is negligible, confirming the scalability of the architecture.

This analysis reinforces the main objective of this work: to evaluate the feasibility of implementing Bitcoin's Double SHA-256 in reconfigurable hardware through High-Level Synthesis. Despite the algorithm's computational complexity, the architecture achieved an efficient balance between performance and area utilization, showing that FPGA-based accelerators can provide an energy-efficient and flexible alternative to GPUs and ASICs in blockchain applications.

VI. CONCLUSION

This paper presented the design and implementation of a Double SHA-256 hardware accelerator using High-Level Synthesis (HLS) targeting FPGA platforms, specifically for validating real Bitcoin blocks. The proposed architecture was successfully deployed on two commercial FPGA boards, ZedBoard (Zynq-7000) and ZCU104 (Zynq UltraScale+ MPSoC), using a custom IP core integrated into a bare-metal system.

Experimental results demonstrated that the FPGA-based solution achieved substantial performance gains compared to software execution on ARM processors, while maintaining low power consumption and minimal hardware resource usage. The ZCU104 achieved a throughput of 319 kH/s with an execution time of 3.1 µs per hash, while the ZedBoard stood out in energy efficiency with 29.625 hashes per watt. These results reinforce the potential of FPGAs as viable alternatives for cryptographic workloads in scenarios where both efficiency and flexibility are critical.

Future work may include the parallelization of multiple SHA-256 cores, dynamic clock scaling for improved power efficiency, and extending the architecture to support other blockchain algorithms, such as SHA-3 or Blake2b. Additionally, exploring partial reconfiguration and integration with lightweight operating systems could further enhance the applicability of this architecture in real-world blockchain nodes and IoT-oriented cryptographic systems.

REFERENCES

[1] F. Vahid and T. D. Givargis, *Embedded system design: a unified hardware/software introduction*. John Wiley & Sons, 2001.

[2] L. Cocco and M. Marchesi, "Modeling and simulation of the economics of mining in the bitcoin market," *PloS one*, vol. 11, no. 10, p. e0164603, 2016.

[3] P. Coussy and D. D. Gajski, "An introduction to high-level synthesis," *IEEE Design & Test of Computers*, vol. 26, no. 4, pp. 8–17, 2009.

[4] V. Dang and K. Skadron, "Acceleration of frequent itemset mining on fpga using sdaccel and vivado hls," in *2017 IEEE 28th International Conference on Application-specific Systems, Architectures and Processors (ASAP)*, 2017, pp. 195–200.

[5] M. Bedford Taylor, "The evolution of bitcoin hardware," *Computer*, vol. 50, no. 9, pp. 58–66, 2017.

[6] M. J. et al., "Energy and cost efficiency of bitcoin mining endeavor," *PLOS ONE*, 2023, accessed: 09/30/2024. [Online]. Available: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0281327

[7] J. I. Ibañez and A. Freier, "Bitcoin's carbon footprint revisited: Proof of work mining for renewable energy expansion," *Challenges*, vol. 14, no. 3, p. 35, 2023, accessed: 09/18/2024. [Online]. Available: https://doi.org/10.3390/challe14030035

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, accessed: Sep. 18, 2024. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[9] H. Javaid, J. Yang, N. Santoso, M. Upadhyay, S. Mohan, C. Hu, and G. Brebner, "Blockchain machine: A network-attached hardware accelerator for hyperledger fabric," in *2022 32nd International Conference on Field-Programmable Logic and Applications (FPL)*, 2022, pp. 191–197.

[10] R. Agrawal, H. Javaid, and J. Yang, "Efficient fpga-based ecdsa verification engine for permissioned blockchains," in *2022 32nd International Conference on Field-Programmable Logic and Applications (FPL)*, 2022, pp. 139–145.

[11] Minerset, "Energy efficiency in bitcoin mining: Tips for reducing cost," 2021. [Online]. Available: https://minerset.com/energy-efficiency-in-bitcoin-mining-tips-for-reducing-minimising-costs/

[12] F. D. d. S. Santos Júnior, "Reconfigurable hardware architecture for sha-256 hashing in blockchain and iot applications," Master's thesis, Universidade Federal do Rio Grande do Norte (UFRN), 2024, accessed: 2025-07-11. [Online]. Available: https://repositorio.ufrn.br/handle/123456789/63475

[13] M. Kammoun, M. Elleuchi, M. Abid, and M. S. BenSaleh, "Fpga-based implementation of the sha-256 hash algorithm," in *2020 IEEE International Conference on Design & Test of Integrated Micro & Nano-Systems (DTS)*, 2020, pp. 1–6.