IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 23 February 2024, accepted 15 March 2024, date of publication 19 March 2024, date of current version 29 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3379374

RESEARCH ARTICLE

Enhancing Blockchain Consensus With FPGA: Accelerating Implementation for Efficiency

JALEL KTARI[1], TAREK FRIKHA[2,3], (Member, IEEE), MONIA HAMDI[4], AND HABIB HAMAM[5,6,7,8], (Senior Member, IEEE)

[1]CES Laboratory, National Engineering School of Sfax (ENIS), University of Sfax, Sfax 3029, Tunisia
[2]ENIS, University of Sfax, Sfax 3029, Tunisia
[3]Data Engineering and Semantics Research Unit, Faculty of Sciences of Sfax, University of Sfax, Sfax 3029, Tunisia
[4]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O.Box 84428, Riyadh 11671, Saudi Arabia
[5]Faculty of Engineering, Uni de Moncton, Moncton, NB E1A 3E9, Canada
[6]Graduate School of Engineering and Technology, Hodmas University College, Mogadishu 2021, Somalia
[7]Bridges for Academic Excellence, Tunis, Tunisia
[8]School of Electrical Engineering, University of Johannesburg, Johannesburg 2006, South Africa

Corresponding author: Jalel Ktari (jalel.ktari@enis.tn)

This work was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) and in part by the New Brunswick Innovation Foundation (NBIF).

ABSTRACT Because of its versatility across various applications, Blockchain has emerged as a technology garnering significant interest. It has effectively addressed the challenge of transitioning from a low-trust, centralized ledger maintained by a single third-party to a high-trust, decentralized structure maintained by multiple entities, often referred to as validating nodes. Consequently, numerous blockchain systems have arisen for a multitude of purposes. Nevertheless, a considerable number of these blockchain systems are plagued by significant deficiencies concerning their performance and security. These issues have to be rectified before the realization of a widespread adoption. An essential element within any blockchain system is its foundational consensus algorithm, a crucial determinant of both its performance and security attributes. Consequently, to tackle the shortcomings observed in various blockchain systems, the hardware implementation of a series of established and innovative consensus algorithms was carried out as part of this work. This paper aims to compare and analyze the different consensus methods in blockchain, namely PoS (Proof of Stake), PoW (Proof of Work) and PoA (Proof of Authority) using VHDL (Very High-Speed Integrated Circuit Hardware Description Language). Each of these methods has unique characteristics that influence the validation of transactions and the addition of blocks to the blockchain. In this context, we aim to demonstrate the importance of optimizing consensus execution time via IPs (Intellectual Property) in VHDL. We also evaluate their impact on security, scalability and performance for IoT applications.

INDEX TERMS Ethereum, PoW, PoS, PoA, embedded system, Xilinx, IP.

I. INTRODUCTION

Blockchain has emerged as a technology with significant potential in recent times. Its prominence began to rise with the introduction of Bitcoin by Nakamoto [1]. Bitcoin has addressed a critical issue inherent in traditional payment systems, namely, the reliance on trust in a single third party. Blockchain involves the utilization of multiple independent organizations to validate transactions, thereby shifting the paradigm from centralization to decentralization [2], [3], [4].

To mitigate the potential for tampering in public settings, distributed operational approaches have been adopted. In particular, all participants synchronize and concurrently store chain states through consensus mechanisms [5] and gossiping protocols, establishing a peer-to-peer (P2P) network. Unlike traditional systems that depend on certificate authorities (CAs), blockchain significantly enhances both decentralization and security. However, these achievements come at the expense of substantial resources and energy consumption [6], [7]. Figure 1 illustrates the evolution of computation and storage overhead in popular blockchain networks over the past decade, demonstrating a clear trend

The associate editor coordinating the review of this manuscript and approving it for publication was Mehdi Sookhak.

of exponential growth. Moreover, the increasing resource consumption does little to improve the transaction processing performance of blockchain. In reality, a significant portion of resources is invested in reinforcing security and enhancing robustness. As the field progresses, the inadequacies in performance are becoming a bottleneck hindering broader adoption of blockchain, particularly in scenarios with resource constraints and high workloads [8], [9].

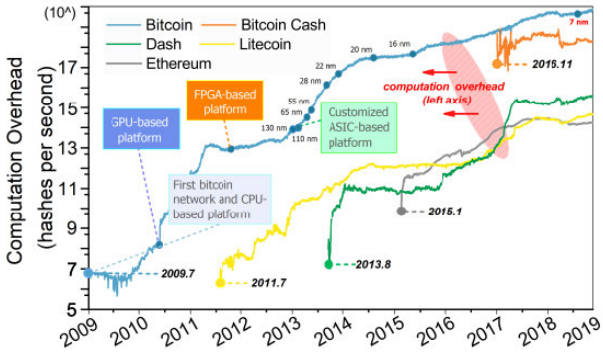

FIGURE 1. Computation overhead in blockchain network [9].

To address these challenges, researchers have embedded on exploring techniques to optimize blockchain performance. The ultimate assessment of these optimizations revolves around scalability, which is defined as the ability to expand the P2P network while maintaining satisfactory performance levels. In simpler terms, the performance of a blockchain network should exhibit a linear or positive correlation with its scale, measured by the number of full nodes and/or total available resources. At the very least, it should remain stable.

Innovations in consensus mechanisms, particularly in the design of lightweight consensus workflows, offer a relatively promising path towards achieving scalability. However, researchers encounter obstacles when attempting to scale up blockchain significantly as resource efficiency remains a challenge. Concurrently, the evolution of hardware in accordance with Moore's Law, transitioning from central processing units (CPUs) to graphics processing units (GPUs), field-programmable gate arrays (FPGAs), and application-specific integrated circuits (ASICs), appears to exacerbate energy consumption rather than providing scalability improvements. Effectively achieving blockchain scalability without compromising its decentralization and security properties presents a formidable ''trilemma,'' posing significant challenges for researchers [10].

At its core, a blockchain system operates as a distributed network, hinging upon a consensus algorithm to ensure unanimous agreement among distributed nodes regarding the states of specific data. This consensus algorithm serves as the linchpin dictating the system's behavior and the performance it can attain.

The wide spectrum of blockchain applications requires tailor-made consensus mechanisms. Consequently, there exists a growing imperative not only to scrutinize the adaptability of established consensus algorithms in fresh contexts but also to pioneer innovative consensus algorithms. As a result, numerous consensus algorithms have emerged. In this work, we have implemented Blockchain on a Xilinx XC 702 FPGA-based embedded platform. and created from VHDL IPs for different consensus mechanisms: PoS, PoW, and PoA.

The article is structured into five parts. First, we review various applications of Blockchain and its implementation on embedded platforms. Next, we propose different consensus mechanisms and their embedded implementation. In the third part, we present the results obtained, followed by a dedicated discussion section. We end this paper with a conclusion and future research directions.

II. CONTRIBUTION

This research makes significant contributions toward integrating blockchain technology with FPGA-based hardware, aiming to improve efficiency, cost-effectiveness, and industrial suitability.

1. Novel FPGA Implementations: We introduce novel VHDL implementations for PoS, PoW and PoA consensus algorithms, emphasizing adaptability and efficiency in embedded contexts. This deeper exploration of hardware-level intricacies provides valuable insights into their performance characteristics.

2. Comprehensive Comparative Analysis: Extending beyond individual implementations, we offer a detailed comparison of PoS, PoW and PoA using metric-based evaluations of resource consumption, execution time, and energy efficiency. This analysis serves as a crucial reference for selecting optimal consensus mechanisms in embedded systems.

3. VHDL IPs for Diverse Consensus Mechanisms: We developed reusable VHDL IPs for PoW, PoS and PoA, enabling seamless integration into embedded blockchain systems on FPGA platforms. These IPs provide a versatile toolkit for exploring various consensus options.

4. Holistic Perspective on Practical Implications: By merging these contributions, our study offers a holistic perspective on the practical implications of different consensus mechanisms in embedded environments. This integrated approach underscores the importance of hardware considerations alongside software-level aspects when choosing a suitable consensus mechanism.

5. Validating Key Approaches: This work paves the way for validating two important approaches: (a) an on-chain/off-chain hybrid platform with offline consensus calculations and (b) an embedded multi-consensus platform dynamically adapting to different blockchains.

Key Differentiators: Our work distinguishes itself through novel FPGA implementation techniques, particularly for PoW, PoS, and PoA, offering valuable insights into their hardware-level behavior.

This work will validate two important approaches:

a) An on-chain off-chain blockchain-based platform, where the consensus calculation will be performed offline and the rest of the system online.

b) An embedded multi-consensus platform that calculates consensus results according to the Blockchain used. This result can be used to validate approach a)

III. STATE OF THE ART

A. BLOCKCHAIN OVERVIEW

Blockchain is a revolutionary technology that has gained widespread attention and adoption across various industries. At its core, a blockchain is a decentralized and distributed ledger that records transactions securely and transparently (Figure 2).

Blockchain is a decentralized system operating on a network of computers (nodes), ensuring no single entity controls it. It provides transparency by making all transactions visible to participants, enhancing trust and eliminating the need for intermediaries. Security is achieved through advanced cryptographic techniques, creating an immutable chain of blocks that resists tampering. Immutability ensures transactions cannot be altered or deleted, crucial for data integrity in applications like finance and supply chain management. Smart Contracts enable automatic execution based on predefined conditions.

Consensus mechanisms like PoW and PoS validate transactions without a central authority. Cryptocurrencies native to blockchains serve as incentives and transactional tools. Blockchain extends beyond cryptocurrencies, finding applications in various industries, promising increased transparency, fraud reduction, streamlined processes, and cost-cutting.

Despite its potential, blockchain faces challenges such as scalability, energy consumption, and regulatory concerns. Ongoing research and development aim to address these issues.

Here is an overview of some of the key concepts and features of blockchain:

- Decentralization: Unlike traditional centralized systems, where a single entity has control and authority over data and transactions, blockchain operates on a decentralized network of computers (nodes). Each node has a copy of the entire blockchain, ensuring that no single entity has complete control, making it resistant to censorship and tampering.
  - Transparency: All transactions recorded on a blockchain are visible to every participant in the network. This transparency enhances trust among users, as they can independently verify transactions without relying on intermediaries.
  - Security: Blockchain uses advanced cryptographic techniques to secure transactions and data. Transactions are grouped into blocks, and each block contains a cryptographic hash of the previous block, creating a chain of blocks (hence the name ''blockchain''). This makes it extremely difficult to alter past transactions without altering all subsequent blocks, which is computationally infeasible.

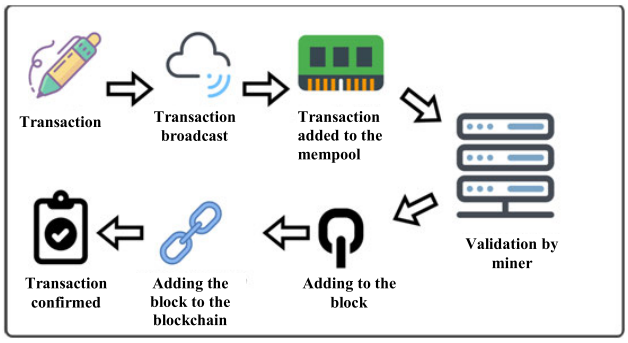

FIGURE 2. Blockchain approach [4].

B. USE CASE AND RELATED WORKS

Blockchain is used in many fields:

- Medical Industry:

Blockchain holds promise in revolutionizing healthcare by securely managing patient data, electronic health records, and clinical trial results. It grants patients greater control over their health data while enhancing transparency and traceability in pharmaceutical supply chains. Additionally, integrating blockchain with edge computing and IPFS, as proposed in [11], ensures data integrity and confidentiality, facilitating real-time processing and fine-grained access control. Meanwhile, research in [12] suggests leveraging blockchain to anonymize COVID-19 patient data within the IoT landscape, preserving confidentiality and privacy. Alsaed et al. reviewed the recently recorded blockchain-based research proposals to control the COVID-19 pandemic [13].

- Agriculture:

In agriculture, blockchain offers supply chain traceability, enabling consumers to trace the origins of food products for safety and authenticity. Smart contracts automate agreements between farmers and buyers, while IoT sensors monitor soil and crop conditions, enhancing farming operations. Blockchain's transparent ledger ensures fair and reliable transactions within the agricultural ecosystem. In [14], authors propose a novel approach to trust management in agricultural green supply chains using blockchain technology, employing game theory to model and analyze trust-related challenges. Reference [15] explores blockchain's application in advancing green energy within smart agriculture, advocating for an innovative ecosystem for clean energy to promote sustainability. Meanwhile, [16] aims to develop a system tracing food from farm to table swiftly, identifying and containing contaminated products to reduce foodborne illnesses and streamline recall procedures.

- Voting:

Blockchain holds the potential to revolutionize the voting process, ensuring secure, transparent, and tamper-proof elections. It enables remote voting, broadening accessibility to citizens, including those residing overseas, and provides instant election results, enhancing efficiency and trustworthiness. Reference [17] introduces a voting platform with remote real-time ballot box auditing capability,

leveraging blockchain technology to verify results' accuracy and detect potential fraud. Reference [18] presents a blockchain-based system for collecting votes via mobile applications, employing biometric data for signature validation to enhance security. Additionally, [19] proposes a low-power blockchain-based e-voting approach utilizing both public Ethereum and private Quorum blockchains for encrypted communication, bolstering security and privacy.

- Industry 4.0:

In the context of Industry 4.0, blockchain optimizes supply chains by providing real-time visibility into goods movement, reducing costs, and enhancing efficiency. It supports quality control by recording IoT sensor data on product performance and fosters interoperability, facilitating seamless data exchange and process automation. Reference [20] introduces a model using blockchain and IoT to monitor product price hikes and corruption, showcasing advanced integration for enhanced monitoring and transparency in Industry 4.0. These examples demonstrate how blockchain's features like security and transparency can transform industries, improving data management, trust, and efficiency in critical processes.

- Security:

In the security context, IoT device security is crucial. Reference [21] proposes an IoT authentication protocol utilizing ID-based encryption to enhance efficiency and stability, surpassing PKI-based methods. Future research should focus on broader authentication protocols, especially for local network device authentication and emerging IoT communication threats. Additionally, a blockchain-based framework is introduced for secure IoT device and resource searches, addressing vulnerabilities in centralized NRS and OID services. This decentralized approach improves security, authentication, and non-repudiation, categorizing nodes into representative and participant nodes with distinct roles. Standardization is recommended to enhance software quality and reduce business risks in implementing the framework, fostering uniformity and heightened security in IoT systems.

- Smart city

In [22], the paper addresses the need for smart cities to accommodate urban population growth while emphasizing sustainability and energy efficiency. Data privacy and security pose significant challenges, especially given smart cities' reliance on IoT devices. The paper explores blockchain technology's application to enhance smart city security, with case studies from cities like Dubai and London illustrating practical implementations. Reference [23] proposes a blockchain-based approach to Citizen e-governance, aiming to modernize government processes. Research by U. Khalil, O. A. Malik, and collaborators focuses on leveraging blockchain for IoT device authentication within smart cities, with a comparative analysis of authentication architectures [24]. Additionally, [25] discusses the hardware design of a customized processor for executing the SHA-256 algorithm, aiming to improve blockchain efficiency on embedded platforms.

C. EMBEDDED SYSTEM AND BLOCKCHAIN

The advancement in electronics and microelectronics has enabled the miniaturization of transistors, leading to an increased integration of electronic components on a single chip. At the heart of this integration is the microprocessor, typically comprising one or more central processing units (CPUs) along with essential modules like memory controllers, cache memory, and I/O controllers.

In [26], the paper introduces the proof-of-concept for leveraging on-chain/off-chain load balancing to facilitate the deployment of Blockchain on Resource Minimization: O-constrained computing environments. This methodology enables the deployment of a Blockchain with an unlimited number of nodes across diverse computing resources, spanning from cloud servers and personal computers to Raspberry Pi 3.

In certain systems, the integrated circuit goes beyond just the microprocessor, incorporating additional components such as microcontrollers and GPUs. Such systems are referred to as System on Chip (SoC). These SoCs prioritize space and power efficiency while maintaining the requisite performance for specific applications. For instance, a modern SoC commonly encompasses the CPU, GPU, communication modules (e.g., Wi-Fi, Bluetooth), localization modules, and various subsystems, including coprocessors dedicated to functions like device security.. Embedded systems have found relevance in blockchain technology. Consequently, domains such as e-health, agriculture, light and heavy industry, e-learning, and augmented reality have increasingly relied on SoCs to establish systems tailored to their unique requirements [27]. As a result, various architectural approaches have emerged to align with these diverse needs. These encompass single-processor systems that leverage hardware accelerators (IPs) to boost performance and massively parallel architectures capitalizing on numerous processors operating in perfect synchronization [28], [29].

Despite embedded systems finding application across multiple domains, their utilization within the blockchain domain, particularly in conjunction with FPGA technology, has remained relatively limited. Although FPGAs possess internal resources like high-speed memory and parallel computing blocks that are well-suited for computationally intensive applications, they have primarily been limited to PoW consensus mechanisms.

In [30], Sakakibara et al. introduce the significance of blockchain technology in handling increasing transactions through IoT products and propose an innovative approach utilizing an in-Network Interface Card (in-NIC) processing method with a Field Programmable Gate Array (FPGA) to enhance performance. They categorize blockchain into public, private, and consortium/community types and explore the use of FPGAs and GPUs to accelerate traditional systems. The primary goal is to achieve high-performance digital asset transfers. Through the proposed in-NIC approach on FPGA, the study successfully enhances throughput and reduces latency for off-chain processing in blockchain-based transfer

systems. However, it acknowledges the need for further enhancements to address increasing transaction volumes and potential discrepancies between current system performance and desired throughput and latency. Future work aims to ensure consistency with existing systems. The methodology involves proposing the in-NIC processing approach, designing and implementing a prototype NIC with a key-value data store using the P4 language on FPGA, and evaluating the prototype's throughput and latency against a blockchain software application.

In [31], the authors proposed a method for implementing various blockchain operations on FPGAs. This implementation involved comparing the implementation of different blocks on FPGA, ASIC, GPU, and processor.

The authors transformed certain PoW-specific blocks, such as hashing, from a simple algorithm into a VHDL IP block. While this work aligns with our hardware implementation for PoW, we delve into greater detail in this paper regarding the implementation of other consensus mechanisms, such as PoA and PoS.

IV. CONSENSUS

Consensus algorithms presented in Figure 3 lie at the core of blockchain technology, determining how transactions are validated, added to the ledger, and ultimately, how trust is established within the network. In this discussion, we delve into four prominent consensus algorithms: Proof of Stake (PoS), Proof of Work (PoW), Proof of Authority (PoA), and Practical Byzantine Fault Tolerance (PBFT), shedding light on their underlying principles and applications [4]

- PoS is a consensus mechanism in which validators, or ''stakers,'' are chosen to create new blocks and validate transactions based on the number of coins they hold and are willing to ''stake'' as collateral. PoS is energy-efficient compared to PoW, making it an attractive option for environmentally conscious blockchain networks [4], [33]

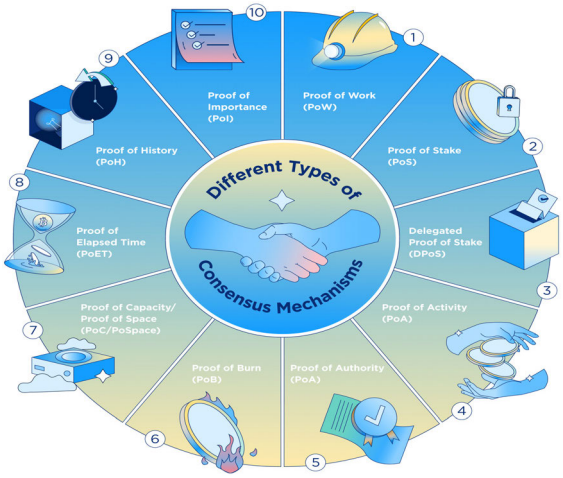

FIGURE 3. Consensus algorithms [32].

- PoW is the original consensus algorithm used in Bitcoin and many other cryptocurrencies. It requires miners to solve complex mathematical puzzles through brute-force computation. The first miner to find a solution gets the right to create a new block and add it to the blockchain. PoW is known for its security but is energy-intensive and computationally expensive, leading to concerns about its sustainability [2], [3], [4].

- PoA is a consensus mechanism often used in private and consortium blockchains. In PoA, a predetermined set of authorities, known and trusted nodes, validate transactions and create new blocks. This approach prioritizes network performance and scalability over decentralization and security, making it suitable for permissioned blockchain networks where trust among participants is established [27]

- Practical Byzantine Fault Tolerance (PBFT) is a consensus algorithm designed for achieving consensus in distributed systems with Byzantine faults, where nodes may be malicious or faulty. PBFT requires a fixed number of nodes to agree on the order and validity of transactions [33], [34].

These consensus algorithms represent a spectrum of trade-offs between factors like security, decentralization, scalability, and energy efficiency. The choice of which consensus mechanism to use depends on the specific goals and requirements of a blockchain network and its use case.

In our context, we choose the FPGA implementation. In fact, the FPGAs can be highly optimized for specific tasks, providing superior performance compared to general-purpose processors. Moreover, FPGA can significantly reduce energy consumption, making blockchain networks more eco-friendly, especially in PoW-based systems. This solution allows developers to tailor hardware to the specific requirements of a consensus algorithm, optimizing resource usage. In terms of security, FPGAs can provide a high level of hardware security, protecting against various attacks and ensuring the integrity of the consensus process. Finally, FPGA-based implementations can be scaled to handle increasing transaction volumes and network demands.

Several studies (Table 1) have addressed Blockchain, particularly embedded Blockchain. The majority of them focused on Ethereum, predominantly utilizing PoW as a consensus mechanism. In [35] and [36], the research exclusively employed FPGA, whereas in [37], the work was purely software-based on Raspberry Pi.

In [27], the authors tackled this by implementing an on-chain/off-chain system on FPGA exclusively for PoW consensus. As for our work, we aimed to manipulate various consensus mechanisms and demonstrate not only their feasibility but also the potential gains in terms of execution time for a system that processes consensus outside the main network connected to the Blockchain

Our hybrid model offers increased flexibility and scalability, which are crucial in the practical implementation of blockchain technologies in embedded systems. By integrating off-chain computations, we reduce the burden on the embedded system itself, which typically has limited resources. This also allows for more complex processing to

TABLE 1. Comparison of our approach with existing work.

Paper	Platform	PoW	PoS	PoA	On chain	Off chain
[38]	FPGA	☒	☒	☒	☑	☒
[39]	FPGA	☑	☒	☒	☑	☒
[30]	FPGA	☑	☒	☒	☑	☑
[34]	FPGA	☑	☒	☒	☑	☒
[40]	Raspberry PI	☑	☒	☒	☑	☒
Our work	FPGA	☑	☑	☑	☑	☑

occur off-chain, thereby improving overall system efficiency and performance.

V. HW IMPLEMENTATION AND METHODOLOGY

Bitcoin's hash rate exceeds 400EH/s. This increase is largely attributed to ongoing improvements in mining hardware and the overall growth of the Bitcoin network. For Ethereum, which initially used a proof-of-work consensus mechanism, the hash rate was around 300 tera hashs per second (TH/s). However, Ethereum 2.0 aims to replace the energy-intensive proof-of-work with a more environmentally friendly consensus mechanism. Currently, the hash rate is 10Thash/s [36].

It is important to note that transaction confirmation speed is one of the aspects of blockchain performance. Other factors, such as scalability, security and decentralization, must also be taken into account when evaluating consensus mechanisms. Execution time can also vary as consensus protocols are updated and improved over time.

Since parallelization of the blocks created in VHDL speeds up execution time, it seems important to change the implementation from a 100% SW implementation to a mixed HW SW system. The least greedy functions (Block Version, Id, Merkle Tree, Time Stamp, Difficulty) while the greediest function is transformed into an HW Block (Consensus). This description is detailed in figure 4.

A. THE CHOICE OF FPGA

FPGAs were considered a flexible alternative to ASICs (Application-Specific Integrated Circuits) in the field of cryptocurrency mining. Unlike ASICs, which are specifically designed for a particular task, FPGAs can be programmed and reprogrammed for different applications, providing a degree of flexibility. However, the rapid evolution of mining algorithms, especially for cryptocurrencies like Bitcoin, has rendered FPGAs less competitive compared to specialized ASICs [38], [39]. Here are some considerations:

- Flexibility: FPGAs offer flexibility in programming, meaning they can be adapted to different mining algorithms. This can be an advantage when new algorithms emerge.

- Computational Power: ASICs have computational power specifically optimized for mining tasks, making them much more energy-efficient compared to FPGAs. FPGAs can have performance levels between ASICs and GPUs.

In our context, the ZedBoard featuring the Zynq-7000 SoC ZC 702, holds significance in blockchain mining because of its unique combination of a dual-core ARM Cortex-A9 processor and programmable logic (FPGA). This integration allows for the execution of both software tasks on the ARM processor and hardware tasks on the FPGA, providing a versatile platform for blockchain mining applications.

In order to implement hardware (HW) in VHDL, a methodology based on codesign is used. Indeed, when establishing an embedded system, conducting a mixed HW/SW study is crucial to ensure the implemented system is well-optimized. However, in the context of our work, since the software (SW) already exists, we analyzed the SW algorithm used for each consensus. This algorithm was profiled to break it down into different functions, outlining the relationship of each function to the others, the number of iterations of each part, and their execution time. Once this task was completed, the most frequently executed and time-consuming functions were divided into blocks running in parallel, while the non-repetitive sequential parts were directly coded in VHDL (in process form). Once this block is implemented, it is transformed into an intellectual property (IP). This IP is then executed on the FPGA to finally achieve the HW consensus.

The dual-core ARM Cortex-A9 processor on the ZedBoard facilitates the execution of software-based mining algorithms, enabling compatibility with various blockchain protocols. This capability is essential for handling tasks that are better suited for sequential processing. Moreover, the ZedBoard's array of ports and interfaces, including USB, Ethernet, HDMI, and GPIO connectors, facilitates connectivity with mining networks and other devices. Efficient communication is vital for participating in blockchain mining pools [39].

The process involves the transformation of the PoW consensus algorithm from a software implementation into a hardware-friendly description using VHDL. This representation is encapsulated into an IP (Intellectual Property) block, designed to be versatile and easily integrated into larger FPGA-based systems.

Following this VHDL transformation, the IP block is seamlessly integrated with the ARM processor, forming a cohesive unit that orchestrates the entire blockchain system. Simulation using ModelSim is employed to validate the functionality and correctness of the PoW IP block before the final deployment on the Zedboard ZC702 FPGA platform.

Importance in Blockchain Mining: The ZedBoard's significance in blockchain mining lies in its capacity to blend the strengths of both hardware and software processing. The FPGA's programmable logic enables the acceleration of specific cryptographic computations, optimizing the mining process. This flexibility is crucial in an environment where mining algorithms can undergo frequent updates or changes. Additionally, the combination of the ARM processor and FPGA allows for a balanced approach, leveraging the strengths of each component for efficient and adaptable blockchain mining operations.

B. CONSENSUS IMPLEMENTATION

Our previous work in [27] involved the PoW consensus only. We implemented the PoW consensus IP directly on FPGA,

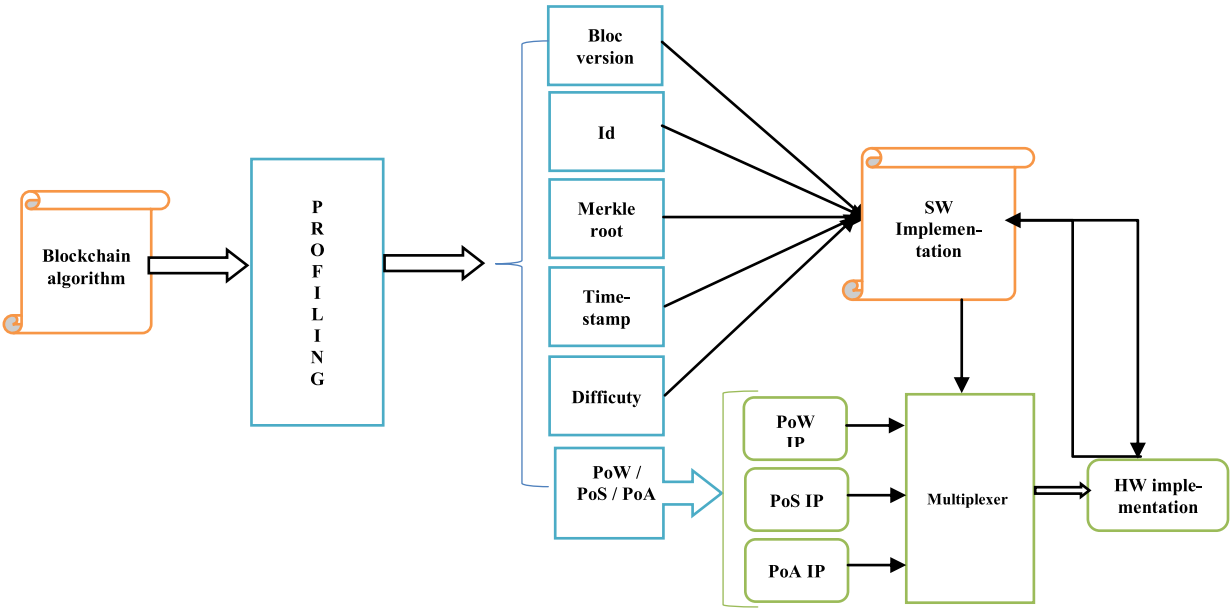

FIGURE 4. Implementation details.

while the rest of the work was realized on a Raspberry PI. In order to generalize this work, we turned our attention to the other consensuses (PoA, PoS). The implementation and the comparison are realized on the Xilinx Zynq 7000 platform.

In order to accelerate the embedded blockchain, we profiled the various elements making up our blockchain. The profiling carried out was software profiling. It demonstrated that the consensus execution part far exceeds the other functionalities.

1) POW CONSENSUS IMPLEMENTATION

In our VHDL implementation, we utilize established and optimized libraries or modules for hash functions, such as SHA256. These modules are well-tested, widely adopted, and ensure the cryptographic security required for consensus protocols. By adopting proven implementations of hash functions, our focus shifts to the integration of these functions within the broader consensus mechanism, as well as the optimization and adaptability of the overall system.

In a block, 6 parts must always exist [40]:

- The block version: In addition to its pure versioning role, this field allows miners to signal their approval (or not) for a change in the protocol.
- The identifier of the previous block, which enables the header to be chained to the header of the previous block.
- The Merkle root, whose role is to link the header to the rest of the block as described above.
- Timestamp: the date and time of mining.
- Data indicating the difficulty of mining the block.
- The nonce relative to the proof of work.

To set up a block, the most computationally intensive part is ineluctably the consensus. In the case of PoW (Figure 5), it consists in finding the value of the nonce that enables the problem and its difficulty to be solved.

Table 2 shows the PoW execution time in ms compared with the other parts of setting up a block in the blockchain.

TABLE 2. PoW execution time (ms) & percentage.

	Block version	Identifier	Merkle root	Timestamp	Difficulty	PoA
Time (ms)	0,12	0.12	1.92	0.12	0.12	3.98
Percent	1.90%	1.90%	30 %	1.90%	1.90%	62%

To speed things up in terms of hardware, we have decided to transform the PoW consensus into an IP HW. This is done by:

1. VHDL Transformation: The first crucial step in this process is the conversion of the PoW consensus algorithm from a software implementation into a hardware-friendly description using VHDL. VHDL facilitates the modeling of electronic systems, and in this context, it entails defining the logical operations, data paths, and control structures required for PoW within the VHDL code.

2. IP Design: Following the VHDL transformation, the PoW algorithm is encapsulated into an IP block. This involves packaging the VHDL code into a modular and reusable component with well-defined input and output interfaces. The IP block is designed to be versatile and easily integrated into larger FPGA-based systems.

3. Integration with ARM Processor: The FPGA, now equipped with the PoW IP block, is connected to an ARM processor. The ARM processor assumes the role of orchestrating the entire blockchain system and interacting with the PoW IP block. The integration process establishes seamless communication between the ARM processor and the PoW IP

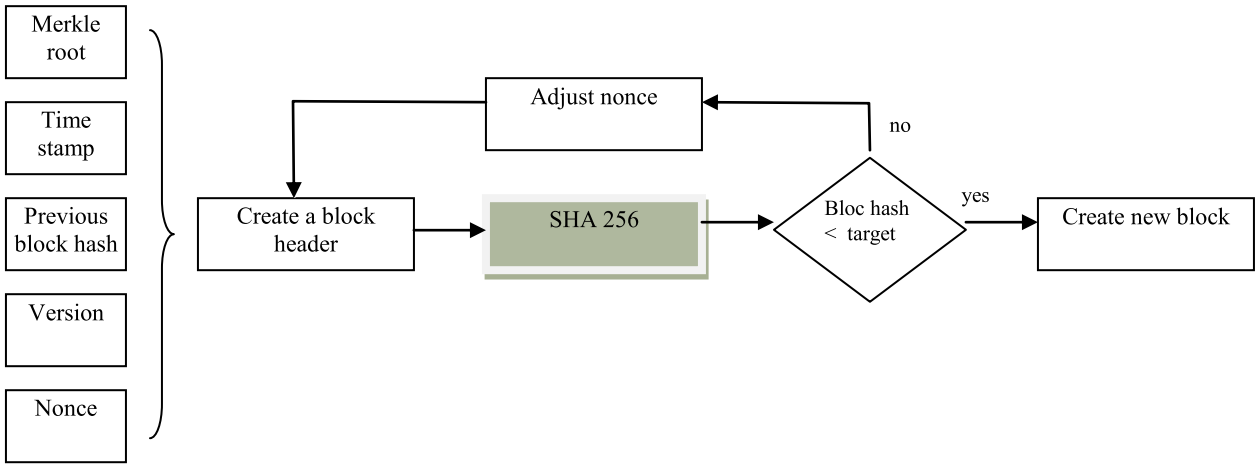

FIGURE 5. The flow of PoW [41].

block, enabling the ARM processor to initiate and control the PoW consensus process.

4. Simulation using ModelSim: To validate the functionality and correctness of the PoW IP block, the VHDL implementation undergoes simulation using ModelSim. ModelSim serves as a powerful simulation tool for hardware description languages, providing insights into how the PoW IP block operates within the FPGA environment. This step is crucial for identifying and rectifying any potential issues before the final deployment.

5. Zedboard ZC702 FPGA Platform: The ultimate implementation is deployed and tested on the Zedboard ZC702 FPGA platform. This platform serves as the real-world environment where the FPGA, ARM processor, and PoW IP block collaboratively perform the consensus process. Testing on the Zedboard ZC702 ensures that the entire system operates seamlessly and efficiently under practical conditions.

To achieve this, the block will be transformed into VHDL (the SHA 256 (Figure 6) and the PoW IP). The IP is connected to the ARM processor to find the nonce value. The code will then be simulated via ModelSim, using the Zedboard ZC702 FPGA as a platform.

The hash function typically used is SHA-256, which produces a 256-bit (32-byte). In the PoW VHDL code, the size of the output nonce is 32 bits (std_logic_vector(31 downto 0)), and the size of the output block_data is determined by the generic constant BLOCK_SIZE. The size of block_data is BLOCK_SIZE bits (std_logic_vector (BLOCK_SIZE-1 downto 0)). In FPGA implementations, the 256-bit output of SHA-256 (PoW) would require calculating the correct 32-bit nonce.

2) POA CONSENSUS IMPLEMENTATION

The block header in a PoA network contains specific information related to block validation and creation. Unlike other consensus algorithms such as PoW used in Bitcoin, where miners solve complex mathematical problems to create a new block, PoA relies on a limited group of

```
entity pow is
    generic (
        BLOCK_SIZE : natural := 256; -
        TARGET : std_logic_vector(255 downto 0) := (others => '0') & '1' & (others => '0')
    );
    port (
        clk : in std_logic; -- Horloge
        rst : in std_logic; -- Reset
        tx_data : in std_logic_vector(BLOCK_SIZE-1 downto 0); --  transaction  Data
        tx_valid : in std_logic; -- transaction validity
        nonce : out std_logic_vector(31 downto 0); -- Nonce
        block_data : out std_logic_vector(BLOCK_SIZE-1 downto 0); -- data block
        block_valid : out std_logic --  block validity
    );
end pow;
```

FIGURE 6. PoW entity.

trusted entities authorized to validate transactions and create blocks.

In a PoA network, each block typically has a header that may include the following:

- Block Number: A unique identifier assigned to each block in the chain.
- Timestamp: The time at which the block was created.
- Merkle Root: A digital fingerprint of all transactions included in the block, ensuring transaction integrity.
- Nonce: A random number used during block creation to ensure that the block meets validation conditions.
- Block Signature: In PoA networks, blocks are usually digitally signed by authorized validators..
- Previous State: A summary of the blockchain's state before adding the transactions from the current block.
- Difficulty: In PoW, difficulty is adjusted to maintain an average block creation time. In PoA, this may be replaced by other mechanisms relevant to the consensus.
- Previous Block Reference: The identifier of the previous block in the chain.

In Table 3 and Figure 7, we show the PoA execution time in ms compared with the other parts of setting up a block in the blockchain.

TABLE 3. PoA execution time (ms) & percentage.

	Block version	Identifier	Merkle root	Time-stamp	Difficulty	PoA
Time (ms)	0.06	0.06	0.46	0.07	0.07	0.54
Percent	4.90%	4.95%	36%	5.50%	5.60%	43%

FIGURE 7. Percentage of execution time.

```
entity poa is
    generic (
        VALIDATOR_COUNT : natural := 5; -- Validator number
        BLOCK_SIZE : natural := 256 -- Block size (bit)
    );
    port (
        clk : in std_logic; -- clk
        rst : in std_logic; -- Reset
        tx_data : in std_logic_vector(BLOCK_SIZE-1 downto 0); -- Transaction data
        tx_valid : in std_logic; --  transaction validity
        validator_list : in std_logic_vector(VALIDATOR_COUNT-1 downto 0); -- Validators list
        validator_sig : in std_logic_vector(BLOCK_SIZE-1 downto 0); -- Validator signature
        block_data : out std_logic_vector(BLOCK_SIZE-1 downto 0); -- Data Block
        block_valid : out std_logic -- Block validity
    );
end poa;
```

FIGURE 8. PoA VHDL entity.

As mentioned above, PoA minimizes runtime. As shown in the table 3, execution time has been reduced. In fact, the execution time of Block version, Identifier, Timestamp and Difficulty, which are identical, use up almost 2.5 times more percentage execution time, even though they have the same algorithmic complexity. To confirm this, the Merkle root execution time increases to 36%, which is close to the PoA execution time. This means that the PoA execution time is much lower than the PoW.

In fact, PoA takes 7.2 times less time than PoW.

3) PoS CONSENSUS IMPLEMENTATION

PoS is another consensus algorithm used in blockchain networks. Unlike PoW, where miners compete to solve complex mathematical problems, PoS relies on validators who are chosen to create new blocks and validate transactions based on the amount of cryptocurrency they hold or are willing to ''stake'' as collateral.

Here are key characteristics of a block header in a PoS network: (Figure 9)

- Block Number: A unique identifier for each block in the blockchain.
- Timestamp: The time when the block was created.
- Validator's Signature: A digital signature from the validator who created the block, demonstrating their authority.
- Previous State: A summary of the blockchain's state before incorporating the transactions from the current block.
- Merkle Root: A cryptographic hash of all transactions included in the block, ensuring data integrity.
- Previous Block Reference: The identifier of the previous block in the blockchain.
- List of Transactions: The transactions included in the block.
- Staking Information: Details about the validators, such as the amount of cryptocurrency they staked, which determines their chances of being chosen to create a new block.
- Randomization Details: In some PoS implementations, a randomization process is used to select the validator who will create the next block.

In Table 4, we show the PoS execution time in ms compared with the other parts of setting up a block in the blockchain.

TABLE 4. The PoS execution time (ms) & percentage.

	Block version	Identifier	Merkle root	Time-stamp	Difficulty	PoS
Time (ms)	0.05	0.05	0.64	0.06	0.05	0.94
Percent	3.20%	3.20%	35%	3.70%	3.2%	51%

As mentioned above, PoS minimizes execution time. As shown in the table 4 and 5, execution time has been reduced. The code (Figure 10) will be simulated via modelsim.

In fact, the execution time of the Version, Identifier, Timestamp and Difficulty blocks, which are identical, consumes almost half in terms of percentage of execution time, despite the same algorithmic complexity..

To confirm this, the Merkle root execution time is 35%, whereas the PoS consensus takes 51% of the execution time. We deduce that PoS execution time is lower than PoW but takes longer than PoA. In fact, PoW takes 3.5 more time than PoS.

Table 5 presents the advantages of PoS and PoA over PoW in blockchain.

TABLE 5. Gain of PoS and PoA over PoW.

Consensus	Performance Gain over PoW
PoA	7.24 x
PoS	4.13 x

VI. RESULTS AND DISCUSSIONS

First, the PoW algorithm was made in VHDL, then it was implemented on FPGA to prove the realization. Having

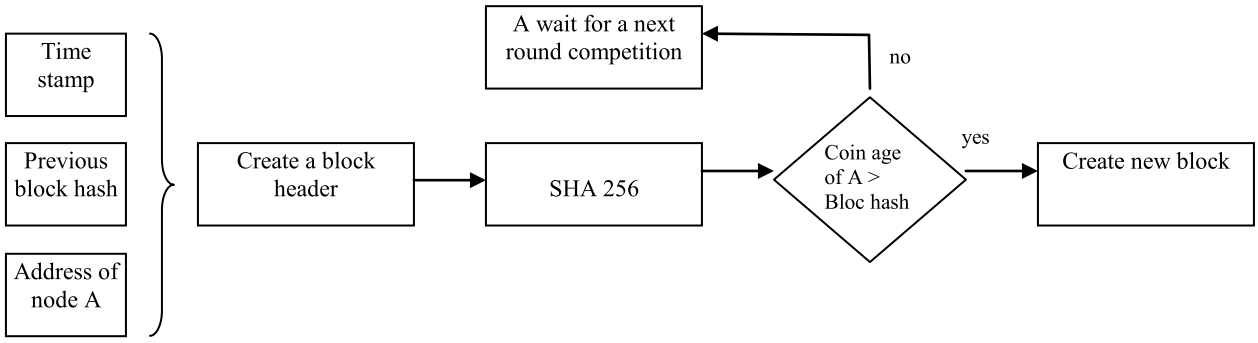

FIGURE 9. Flow of PoS [41].

```
entity pos is
    generic (
        VALIDATOR_COUNT : natural := 5; -- Validator number
        BLOCK_SIZE : natural := 256; -- in bits
        TOKEN_SIZE : natural := 128 --
    );
    port (
        clk : in std_logic; -- clk
        rst : in std_logic; -- Reset
        tx_data : in std_logic_vector(BLOCK_SIZE-1 downto 0); -- transaction data
        tx_valid : in std_logic; -- transaction validity
        validator_token : in std_logic_vector(VALIDATOR_COUNT-1 downto 0)(TOKEN_SIZE-1 downto 0); -- Token
        block_data : out std_logic_vector(BLOCK_SIZE-1 downto 0); -- data
        block_valid : out std_logic -- validity indicator
    );
end pos;
```

FIGURE 10. PoS entity.

53200 slices, the PoW consumed 1100 slices or 2.06% of the platform. The PoS used 709 slices, or 1.33% of the FPGA's Lookup Tables resources. Finally, PoA required 521 slices, or 0.98% of resources.

Table 6, 7 and Figure 11 summarize the results. This confirms that POW remains the greediest consensus in terms of FPGA resource consumption.

TABLE 6. FPGA implementation.

Consensus	PoW	PoS	PoA
Nb of slices	1100	709	521
% Use	2.06%	1.33%	0.98%
Slices gain %PoW	100%	64,45%	47,36%

In our energy study, we employed a software tool recommended by Xilinx and accessed through the Xilinx University program. This tool, known as the Xilinx Power Estimator (XPE), enabled us to estimate the power consumption of the HW implementation we had configured. XPE, a part of the Vivado Design Suite, was also utilized to analyze the power consumption of the prototype system.. The use of the Xilinx Power Simulator allowed us to assess the energy consumption of each consensus algorithm implementation, offering a nuanced understanding of their respective impacts on power utilization. These simulation results serve as a crucial reference point for evaluating the energy efficiency of PoW, PoS, and PoA on the chosen FPGA platform.

We have obtained results that remain simulation data. In Table 7, a comparison of energy efficiency on the one hand, and performance/speed quotient on the other, confirm the results already obtained.

TABLE 7. Criteria comparison.

Criteria	PoW	PoS	PoA
Energy Efficiency	No	Yes	Yes
Performance/Speed	Slow to Moderate	Moderate to Fast	Fast

Undoubtedly, PoW stands out for its significant computational power consumption, notably evident in Bitcoin's transaction throughput per second (TPS) range of 3–7. This limitation significantly hampers PoW's practical application in real-time payment scenarios. While PoS and Delegated Proof of Stake (DPoS) address some computational inefficiency, they introduce their own challenges. In DPoS, for instance, the concentration of block rewards among stakeholders leads to reduced coin liquidity, fostering economic disparities.

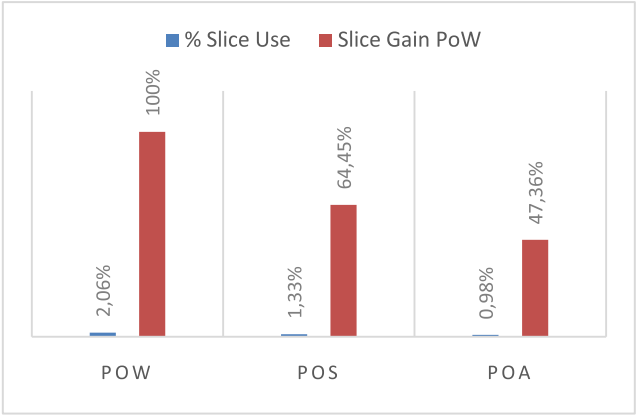

FIGURE 11. Consensus implementation comparison.

Practical Byzantine Fault Tolerance (PBFT) demands frequent communication among nodes during each consensus round, imposing high-performance criteria on the network. Additionally, PBFT's reliance on known node identities raises concerns about anonymity. Ripple, despite achieving

rapid consensus processing in a few seconds, diverges from the decentralized essence of blockchain due to its management by a select few organizations. This centralized control contradicts the fundamental principles of blockchain decentralization.

Regarding security, PoW demonstrates robust security through its hash cash and micro mint methods, although its data handling security is considered only fair. PoA similarly upholds high-security standards and is regarded as safer and more reliable than PoS. Its Byzantine fault tolerance model serves as a superior alternative to the non-distributed protocols of a centralized system. PoS exhibits lower security compared to PoW when it cannot prevent pool mining but performing a double-spending attack in PoS is exceedingly difficult [9], [38]. The evaluation metrics employed in this study include hardware resource consumption (number of slices) and execution time percentages for different components of the consensus algorithms. The study does not extend to cover a comprehensive set of performance metrics, and the conclusions drawn are based on the selected metrics relevant to the study objectives.

In terms of security, Blockchain systems face various potential attacks, as highlighted by recent surveys [41]. In our proposed on-chain/off-chain system, a single node is exposed to the external network, while the other nodes responsible for block generation connect to the external network through this central node. This architecture reduces security vulnerabilities by concentrating potential attacks on a single point. Communication between the central node and other blockchain nodes can be managed using a firewall, allowing for more focused security control on the central node.

This solution addresses the security challenges of deploying blockchain systems without Proof of Work (PoW) consensus by introducing a robust security component. The suggested architecture utilizes an on-chain/off-chain approach, where consensus is conducted offline, ensuring complete isolation of the off-chain segment from external connections. Communication is restricted to the specific node, and once the hash is prepared and accepted, it is directly added to the block as a transaction. This design significantly reduces the risk of hacking or tampering with transactions, as compromising the node and understanding its communication protocol with the FPGA would be the only viable method. Therefore, the utilization of an on-chain/off-chain system is crucial for securing hardware IPs for various consensuses, including PoW.

Concerning energy consumption, traditional PoW is notably inefficient. However, the development of the proposed Green-PoW technology has the potential to reduce energy consumption by 50%. PoA, in comparison, yields better results than both PoW and PoS and forges its path through higher energy efficiency. PoS also requires lower energy consumption than PoW as it avoids the complex puzzle solutions inherent in PoW.

In fact, green PoW make it possible to implement the consensus algorithm and particularly PoW without the use of significant resources in terms of CPU and GPU, but only IPs realized on FPGA.

Minimizing energy consumption is moving in the direction of low-power systems and thus green platforms ou green PoW.

While in this work we studied a comparison of the feasibility of different embedded consensuses, this work could be improved by implementing several IPs in parallel. These IPs will further minimize the execution time and operate like GPUs in perfect parallelism.

VII. CONCLUSION

As part of this work, a comparative study between different Blockchain consensuses was carried out. In this study, we have confirmed that PoW is more demanding than PoS and PoA. This confirmation was demonstrated after implementing the various IPs on an. Xilinx XC 702 FPGA-based embedded platform. We have shown that PoW requires 3.5 times more hardware resources than PoS and 5.2 times more than PoA. This result is also demonstrated by the energy consumption required to implement these different platforms. Thus, this study serves as a benchmark for evaluating blockchain consensus algorithms in hardware, emphasizing their relevance and adaptability in IoT environments. As the landscape of distributed ledger technologies continues to evolve, the insights gained from this research contribute to informed decision-making in selecting consensus mechanisms that align with the energy-efficient demands of future applications. our study distinguishes itself by its emphasis on hardware resource consumption and execution time metrics.

Our approach addresses a critical research gap in the field: the development of blockchain solutions that are not only technically feasible but also practical for real-world applications in embedded systems. By demonstrating a viable model that operates effectively in both on-chain and off-chain environments, we pave the way to future research and development in this area.

As a follow-up to this work, we can propose a dynamically reconfigurable multi-IP embedded system that can switch according to the consensus required by the implemented blockchain. This system could solve the resource constraints of supply-chain applications used in extreme industrial environments (heat, cold, pollution, etc.), while minimizing energy consumption and therefore having a less harmful impact on the environment.

ACKNOWLEDGMENT

The authors thank Natural Sciences and Engineering Research Council of Canada (NSERC) and New Brunswick Innovation Foundation (NBIF) for the financial support of the global project. These granting agencies did not contribute in the design of the study and collection, analysis, and interpretation of data.

REFERENCES

[1] S. Squarepants, "Bitcoin: A peer-to-peer electronic cash system," *SSRN Electron. J.*, vol. 4, no. 2, p. 15, 2008.

[2] S. A. Yousiff, R. A. Muhajjar, and M. H. Al-Zubaidie, "Design and implementation of a blockchain-based approach for ensuring security in Internet of Things-enabled firefighting stations," *Informatica*, vol. 47, no. 10, pp. 9–26, 2023.
[3] S. Tanwar, N. Gupta, P. Kumar, and Y. C. Hu, "Implementation of a blockchain-based E-voting system," *Multimedia Tools Appl.*, vol. 83, no. 1, pp. 1449–1480, 2024.
[4] S. Fahim, S. Katibur Rahman, and S. Mahmood, "Blockchain: A comparative study of consensus algorithms PoW, PoS, PoA, PoV," *Int. J. Math. Sci. Comput.*, vol. 9, no. 3, pp. 46–57, Aug. 2023.
[5] T. Frikha, J. Ktari, B. Zalila, O. Ghorbel, and N. B. Amor, "Integrating blockchain and deep learning for intelligent greenhouse control and traceability," *Alexandria Eng. J.*, vol. 79, pp. 259–273, Sep. 2023.
[6] A. Alsirhani, M. A. Khan, A. Alomari, S. Maryam, A. Younas, M. Iqbal, M. H. Siqqidi, and A. Ali, "Securing low-power blockchain-enabled IoT devices against energy depletion attack," *ACM Trans. Internet Technol.*, vol. 23, no. 3, pp. 1–17, Aug. 2023.
[7] H. Luo, S. Liu, S. Xu, and J. Luo, "LECast: A low-energy-consumption broadcast protocol for UAV blockchain networks," *Drones*, vol. 7, no. 2, p. 76, Jan. 2023.
[8] B. Dammak, M. Turki, S. Cheikhrouhou, M. Baklouti, R. Mars, and A. Dhahbi, "LoRaChainCare: An IoT architecture integrating blockchain and LoRa network for personal health care data monitoring," *Sensors*, vol. 22, no. 4, p. 1497, Feb. 2022.
[9] Y. Liu, K. Qian, K. Wang, and L. He, "Effective scaling of blockchain beyond consensus innovations and Moore's law: Challenges and opportunities," *IEEE Syst. J.*, vol. 16, no. 1, pp. 1424–1435, Mar. 2022.
[10] S. B. Pandya, H. A. Sanghvi, R. H. Patel, and A. S. Pandya, "GPU and FPGA based deployment of blockchain for cryptocurrency—A systematic review," in *Proc. Int. Conf. Comput. Intell. Sustain. Eng. Solutions (CISES)*, May 2022, pp. 18–25.
[11] H. Makina, A. B. Letaifa, and A. Rachedi, "Leveraging edge computing, blockchain and IPFS for addressing eHealth records challenges," in *Proc. 15th Int. Conf. Secur. Inf. Netw. (SIN)*, Nov. 2022, pp. 01–04.
[12] O. Samuel, A. B. Omojo, S. M. Mohsin, P. Tiwari, D. Gupta, and S. S. Band, "An anonymous IoT-based E-health monitoring system using blockchain technology," *IEEE Syst. J.*, vol. 17, no. 2, pp. 1–12, May 2022.
[13] Z. Alsaed, R. Khweiled, M. Hamad, E. Daraghmi, O. Cheikhrouhou, W. Alhakami, and H. Hamam, "Role of blockchain technology in combating COVID-19 crisis," *Appl. Sci.*, vol. 11, no. 24, p. 12063, Dec. 2021, doi: 10.3390/app112412063.
[14] Y. Bai, K. Fan, K. Zhang, X. Cheng, H. Li, and Y. Yang, "Blockchain-based trust management for agricultural green supply: A game theoretic approach," *J. Cleaner Prod.*, vol. 310, Aug. 2021, Art. no. 127407.
[15] R. Hou, S. Li, H. Chen, G. Ren, W. Gao, and L. Liu, "Coupling mechanism and development prospect of innovative ecosystem of clean energy in smart agriculture based on blockchain," *J. Cleaner Prod.*, vol. 319, Oct. 2021, Art. no. 128466.
[16] B. Niu, Z. Shen, and F. Xie, "The value of blockchain and agricultural supply chain parties' participation confronting random bacteria pollution," *J. Cleaner Prod.*, vol. 319, Oct. 2021, Art. no. 128579.
[17] F. M. Vote. (2020). *The Secure Mobile Voting Platform of The Future-Follow My Vote*. Accessed: Jul. 28, 2020. [Online]. Available: https://followmyvote.com/
[18] Voatz. (2020). *Voatz-Voting Redefined*. Accessed: Jul. 28, 2020. [Online]. Available: https://voatz.com
[19] F. Chaabane, J. Ktari, T. Frikha, and H. Hamam, "Low power blockchained E-vote platform for university environment," *Future Internet*, vol. 14, no. 9, p. 269, Sep. 2022.
[20] M. K. Hasan, M. Akhtaruzzaman, S. R. Kabir, T. R. Gadekallu, S. Islam, P. Magalingam, R. Hassan, M. Alazab, and M. A. Alazab, "Evolution of industry and blockchain era: Monitoring price hike and corruption using BIoT for smart government and Industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 18, no. 12, pp. 9153–9161, Dec. 2022.
[21] L. Zeng, S. Xin, A. Xu, T. Pang, T. Yang, and M. Zheng, "Seele's new anti-ASIC consensus algorithm with emphasis on matrix computation," 2019, *arXiv:1905.04565*.
[22] S.-K. Kim, U.-M. Kim, and J.-H. Huh, "A study on improvement of blockchain application to overcome vulnerability of IoT multiplatform security," *Energies*, vol. 12, no. 3, p. 402, Jan. 2019, doi: 10.3390/en12030402.
[23] S. Krishnan and L. P. Ganesan, "Smart cities with blockchain technology," in *Blockchain for Smart Cities*. Amsterdam, The Netherlands: Elsevier, 2021, pp. 1–15.
[24] U. Khalil, O. A. Malik, and S. Hussain, "A blockchain footprint for authentication of IoT-enabled smart devices in smart cities: State-of-the-art advancements, challenges and future research directions," *IEEE Access*, vol. 10, pp. 76805–76823, 2022, doi: 10.1109/ACCESS.2022.3189998.
[25] 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, Jan. 2014.
[26] R. Setiya, S. Pandey, A. K. Singh, and D. K. Sharma, "Citizen E-governance using blockchain," in *Blockchain for Smart Cities*. Amsterdam, The Netherlands: Elsevier, 2021, pp. 119–152.
[27] T. Frikha, F. Chaabane, N. Aouinti, O. Cheikhrouhou, N. Ben Amor, and A. Kerrouche, "Implementation of blockchain consensus algorithm on embedded architecture," *Secur. Commun. Netw.*, vol. 2021, pp. 1–11, Apr. 2021.
[28] V. T. D. Le, P. H. Luan, T. H. Tran, and Y. Nakashima, "CSIP: A compact scrypt IP design with single PBKDF2 core for blockchain mining," in *Proc. 35th SBC/SBMicro/IEEE/ACM Symp. Integr. Circuits Syst. Design (SBCCI)*, Aug. 2022, pp. 1–6.
[29] R. Florin and R. Ionut, "FPGA based architecture for securing IoT with blockchain," in *Proc. Int. Conf. Speech Technol. Hum.-Comput. Dialogue (SpeD)*, Oct. 2019, pp. 1–8.
[30] Y. Sakakibara, Y. Tokusashi, S. Morishima, and H. Matsutani, "Accelerating blockchain transfer system using FPGA-based NIC," in *Proc. IEEE Intl. Conf. Parallel Distrib. Process. Appl., Ubiquitous Comput. Commun., Big Data Cloud Comput., Social Comput. Netw., Sustain. Comput. Commun.*, Dec. 2018, pp. 171–178.
[31] N. Schapeler, F. Weiser, T. Eke, and C. Strnecker, "Efficient FPGA implementation of blockchain operations," in *Proc. Conf., Gropraktikum Rechnerarchitektur (TUM)*, 2021.
[32] Crypto.com. (2024). *Consensus Mechanisms in Blockchain*. [Online]. Available: https://crypto.com/university/
[33] M. Wendl, M. H. Doan, and R. Sassen, "The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review," *J. Environ. Manage.*, vol. 326, Jan. 2023, Art. no. 116530.
[34] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain," in *CEUR Workshop Proc.*, vol. 2058, 2018, pp. 1–11.
[35] J. Guo, J. Huang, W. Wang, and Y. Chen, "Design and implementation of consensus control protocol for first-order linear multi-agent systems based on FPGA hardware," in *Proc. Chinese Automation Congr. (CAC)*, 2020, pp. 6585–6589.
[36] H.-Y. Kim, L. Xu, W. Shi, and T. Suh, "A secure and flexible FPGA-based blockchain system for the IIoT," *Computer*, vol. 54, no. 2, pp. 50–59, Feb. 2021.
[37] S. U. Abas, F. Duran, and A. Tekerek, "A Raspberry Pi based blockchain application on IoT security," *Expert Syst. Appl.*, vol. 229, Nov. 2023, Art. no. 120486.
[38] L. Xu, L. Chen, Z. Gao, H. Kim, T. Suh, and W. Shi, "FPGA based blockchain system for industrial IoT," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Guangzhou, China, Dec. 2020, pp. 876–883, doi: 10.1109/TrustCom50675.2020.00118.
[39] M. Kammoun, M. Elleuchi, M. Abid, and M. S. BenSaleh, "FPGA-based implementation of the SHA-256 hash algorithm," in *Proc. IEEE Int. Conf. Design Test Integr. Micro Nano-Syst. (DTS)*, Jun. 2020, pp. 1–6.
[40] S. Zhang and J.-H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Exp.*, vol. 6, no. 2, pp. 93–97, Jun. 2020.
[41] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain, Res. Appl.*, vol. 3, no. 2, Jun. 2022, Art. no. 100067.

JALEL KTARI was born in Sfax, Tunisia, in 1980. He received the Diploma degree in electrical engineering, the M.S. degree in electrical and computer engineering, and the Ph.D. degree in computer engineering from the National Engineering School of Sfax, Tunisia, in 2003, 2005, and 2009, respectively, and the H.D.R. degree in the low-power embedded blockchain. His current research interest includes hardware-software systems on chip.

TAREK FRIKHA (Member, IEEE) was born in Sfax, Tunisia, in 1982. He received the Engineering degree in electronic engineering from the National School of Engineers of Sfax, Tunisia, in 2006, the Master Diploma degree from Polytech Sophia Antipolis, France, and the joint Ph.D. degree in science and technology of information and communication from the University of South Brittany, France, and the National Engineering School of Sfax. He is currently an Assistant Professor with the National Engineering School of Sfax. His research interests include multiprocessor architecture optimization for multimedia domains and hardware/software codesign, approximate computing, blockchain for multimedia applications, medical and paramedical data, and agricultural applications.

MONIA HAMDI received the B.Eng. degree in information technology from Telecom SudParis, Paris-Saclay University, France, in 2008, the M.Sc. degree in telecommunications and networks from Institut National Polytechnique, Toulouse, France, in 2008, and the Ph.D. degree in computer science from the University of Rennes 1, France, in 2012. From 2012 to 2017, she was an Assistant Professor with the Higher Institute of Computer Science and Multimedia, Gabés University, Tunisia. From March 2015 to August 2015, she was a Visiting Researcher with the Department of Science and Technology, Linköping University, Sweden. She is currently an Associate Professor with the College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Saudi Arabia. Her research interests include mobile communications, wireless sensor networks, edge computing, and blockchain.

HABIB HAMAM (Senior Member, IEEE) received the B.Eng. and M.Sc. degrees in information processing from the Technical University of Munich, Germany, 1988 and 1992, respectively, the Ph.D. degree in physics and applications in telecommunications from Université de Rennes I conjointly with France Telecom Graduate School, France, 1995, and the Postdoctoral Diploma degree "Accreditation to Supervise Research in Signal Processing and Telecommunications" from Université de Rennes I, in 2004. From 2006 to 2016, he was the Canada Research Chair of Optics in Information and Communication Technologies, the most prestigious research position in Canada which he held for a decade. The title is awarded by the Head of the Government of Canada after a selection by an international scientific jury in the related field. He is currently a Full Professor with the Department of Electrical Engineering, Université de Moncton. His research interests include optical telecommunications, wireless communications, diffraction, fiber components, RFID, information processing, the IoT, data protection, COVID-19, and deep learning. He is an OSA Senior Member and a Registered Professional Engineer in New Brunswick. He received several pedagogical and scientific awards. He is among others the Editor-in-Chief and the Founder of *CIT Review Journal*, an Academic Editor of *Applied Sciences*, and an Associate Editor of *IEEE Canadian Review*. He also served as a guest editor for several journals.