World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Review Article)

Check for updates

Empowering blockchain with SmartNIC: Enhancing performance, security, and scalability

Rahmanul Hoque [1], Md. Maniruzzaman [2, 3], Daniel Lucky Michael [2] and Mahmudul Hoque [4]

[1] *Department of Computer Science, North Dakota State University, Fargo, North Dakota, ND 58105, USA.*
[2] *Department of Electrical Engineering, School of Engineering, San Francisco Bay University, Fremont, CA 94539, USA.*
[3] *Department of Electrical and Computer Engineering, North South University, Dhaka-1229, Bangladesh.*
[4] *Department of Computer Science, Morgan State University, Baltimore, Maryland 21251, USA.*

World Journal of Advanced Research and Reviews, 2024, 22(01), 151–162

Publication history: Received on 22 February 2024; revised on 30 March 2024; accepted on 01 April 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.22.1.1026

Abstract

This paper introduces BlockNIC, an innovative blockchain infrastructure designed to operate exclusively on SmartNICs. Unlike traditional blockchain implementations, BlockNIC leverages the unique capabilities of SmartNICs to execute relatively simple computations directly on the network path, eliminating the need for additional hardware and reducing reliance on host CPUs. By harnessing idle resources within the network, BlockNIC significantly reduces energy consumption and hardware requirements, addressing the environmental concerns associated with conventional blockchain architectures. Through comprehensive performance comparisons between SmartNICs and bare-metal servers, this study demonstrates the promising potential of BlockNIC in achieving scalability, security, and environmental sustainability in blockchain networks. The findings highlight BlockNIC's ability to enhance overall performance and reliability while minimizing resource limitations, thereby unlocking new possibilities for various applications and use cases previously hindered by energy and hardware constraints.

The emergence of BlockNIC aligns with the global sustainability agenda, offering a timely solution to the environmental challenges posed by traditional blockchain technologies. By promoting the adoption of SmartNIC-based blockchain infrastructures, this research contributes to a greener and more secure digital future. It emphasizes the importance of exploring innovative approaches to address the environmental impact of technological innovations, urging researchers, industry professionals, and policymakers to recognize the transformative potential of SmartNIC-based solutions in advancing sustainability and efficiency in blockchain ecosystems.

Keywords: Blockchain; SmartNIC; Performance Enhancement; Security Enhancement; Scalability; Energy Efficiency; Environmental Sustainability; Hardware Offloading.

1. Introduction

For numerous years, network and cloud providers have relied upon the growth of transistors as a means of keeping up with the exponential demand in the market, a phenomenon commonly referred to as Moore's law. Nevertheless, we are presently encountering a conclusion to Moore's law, as the augmentation of CPU clock speeds began to decelerate approximately ten years ago, coinciding with a reduced increase in transistor density [1]. Consequently, researchers and industry experts are exploring diverse solutions to confront this predicament, including edge computing and specialized hardware tailored for specific domains.

* Corresponding author: Rahmanul Hoque

Edge computing, a distributed computing model that adopts an approach whereby computation is brought closer to data sources, such as IoT devices or local edge servers, thereby enabling more efficient and faster data processing, while simultaneously alleviating the burden on network bandwidth availability and data center compute [2]. This paradigm is widely regarded as a viable solution to this predicament, as it underscores the transition from prioritizing the quantity of computation to prioritizing the efficiency of computation. In order to achieve reduced latency and minimize the volume of data processed by the primary data centers, this approach heavily relies on the geographical proximity of its processing devices. It is estimated that a significant proportion, approximately three-quarters, of enterprise data will be generated and processed at the edge, necessitating substantial innovation and giving rise to numerous questions [3].

The issue of trust and security is a significant concern in the realm of edge computing, primarily because edge devices are frequently situated outside the jurisdiction and oversight of centralized data centers. To address this concern, blockchain technology has emerged as a popular solution due to its inherent attributes of decentralization and transparency. Consequently, the adoption of blockchain has been witnessed in various sectors, including cryptocurrency, travel aggregators, and patient records. However, it is worth noting that blockchain is notorious for its high level of computational and energy requirements, rendering it inefficient in many cases. This inefficiency is primarily attributed to the fact that the compute resources within a blockchain system are often employed for unproductive calculations. Additionally, exacerbating the issue, these computations frequently take place on specialized devices that are highly energy-intensive and solely dedicated to performing these unproductive calculations. Consequently, one of the primary objectives of blockchain technology is to mitigate such inefficiency without compromising the level of security it affords.

Since running applications on SmartNICs possess inherent levels of security that surpass user-level applications, it is only logical to leverage SmartNICs as an integral component of server infrastructure for the purpose of offloading security applications such as blockchain. This approach not only enhances the security of the blockchain application, but also mitigates the issues of computational inefficiency and power wastage. Consequently, the focus of this research paper revolves around the introduction of BlockNIC, a Proof of Work blockchain infrastructure that is meticulously optimized and exclusively constructed on SmartNICs. The primary objective of BlockNIC is to enable end users to actively engage in the mining and exchange of BlockNIC's designated currency, aptly named Lampcoin in honor of Leslie Lamport. The framework of BlockNIC is designed to support two distinct functionalities - that of a mining node, which entails the extraction of new Lampcoin, and that of a client node, which facilitates the exchange of currently held Lampcoin. Through the meticulous development and rigorous experimentation of BlockNIC, we have been able to make significant contributions in multiple aspects.

a) Introduction to the initial blockchain infrastructure that has been enhanced for SmartNICs.
b) Examination of the potential for offloading blockchain communication tasks to SmartNICs for forthcoming distributed applications to SmartNICs.
c) Analysis of the potential for offloading blockchain hashing tasks to SmartNICs for forthcoming distributed computing applications.

1.1. Background

In this section, the most recent advancements and pertinent information related to Blockchain and SmartNICs will be discussed, which are the two fundamental pillars of BlockNIC.

To begin with, Blockchain has garnered significant attention and caused quite a sensation in the past decade. The emergence and widespread adoption of blockchain-based cryptocurrencies, such as Bitcoin and Ethereum, have shed light on this revolutionary concept and its potential applications across the technological landscape. The essence of blockchain lies in its ability to serve as a public distributed ledger wherein transactions are meticulously recorded in chronological order, rendering them immutable and impervious to alterations.

In its fundamental structure, each transaction is encapsulated within a "block" within the blockchain. These blocks can contain an array of data types, contingent upon the specific application of the blockchain. However, they all share the commonality of having four primary fields that are integral to their functioning and integrity [5]:

a. The Hash of the Previous Block serves the purpose of establishing the sequence and arrangement of blocks.
b. Data represents a compilation of transactions that are encompassed within a given block.
c. The Nonce, a random value, is employed to introduce variability in the resulting output of the block's hashing value.
d. The Hash, a digital signature, is conventionally derived by subjecting the previous hash, data, and nonce to the SHA-246 algorithm.

The addition of these blocks is not possible for just anyone. Each implementation of a blockchain necessitates some form of verification or consensus mechanism to determine whether to trust a network node that seeks to modify the ledger. The conventional method employed for this purpose is known as proof of work. Under the proof of work approach, the network node endeavoring to include a transaction must engage in a process of "mining" to discover a nonce value that generates a hash value lower than the pre-established condition of the blockchain. The individual who successfully solves this highly intricate mathematical puzzle is duly compensated with a reward, typically in the form of a specific type of digital currency. This "miner" is remunerated for their validation efforts, and the transaction is subsequently appended to the decentralized ledger. It is worth noting that various other consensus mechanisms exist, with proof of stake being particularly noteworthy.

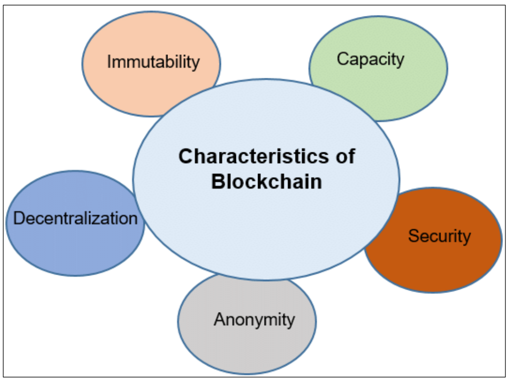

Figure 1 Characteristics of Blockchain

The advantages of the blockchain design are contributing to its widespread adoption worldwide [6]. One of these advantages is the high level of security it offers. This is due to the fact that transactions cannot be deleted or modified, making it extremely difficult for hackers to interfere with the chain. Additionally, the decentralized nature of the ledger, where each node possesses its own version of the ledger, further complicates attempts to falsify transactions. In order for a fake transaction to be validated, it would require the consensus of a significant majority of all nodes.

Another advantage of blockchain is its ability to operate without the need for a central governing authority. In many trust-based systems, such as those involving governments or corporations, a central authority is necessary to mediate and maintain trust among all parties. However, in the case of blockchain, trust is established through the consensus mechanism, where the majority blockchain ledger holds authority. This not only eliminates the need for intermediaries, but also enhances security as the system scales with more users.

In terms of transaction fees, blockchain eliminates the need for intermediaries, resulting in lower costs for users. Instead of paying fees to banks or other intermediaries, users can keep these costs for themselves. Furthermore, the speed of transactions in blockchain is significantly faster compared to other forms of transactions. While traditional transactions may take time to verify or to be reflected in the system, blockchain transactions are almost instantaneous or dependent on network speed, which is typically not a major hurdle.

Nowadays, there have been various novel applications developed for blockchain beyond the realm of cryptocurrency. These applications encompass smart contracts, personal identification, healthcare, and IOT. The exploration of each of these applications is still in its infancy, and as a result, certain areas of improvement have been identified for blockchain. These areas must be addressed in order for blockchain to serve as the algorithmic foundation of our technological future [8].

One area of improvement lies in the computational cost associated with the proof of work consensus algorithm used in Bitcoin. This algorithm is highly computationally intensive, resulting in significant financial and economic implications. The global energy consumption of crypto-assets is estimated to range from 120 to 240 billion kilowatt-hours per year, surpassing the energy usage of entire countries like Australia [9]. To mitigate these concerns, advancements are being made in the form of enhancing proof of work algorithms to reduce computational complexity while maintaining security. Additionally, new consensus algorithms such as proof of identity and proof of stake are being created to address this issue.

The absence of regulation leads to a persistently risky environment for blockchain applications, particularly for newly emerging currencies, as there is no governing authority. The development of "alt-coins" is frequently plagued by scams and market manipulation, which fosters a continuous sense of distrust among the general population. Additionally, there is an inherent risk of cyber-attacks compromising crypto-wallets or causing their loss, and the potential for certain applications to be prohibited by governmental entities.

The widespread adoption of blockchain technology relies on heightened awareness and acceptance. While there has been significant progress in adoption since 2009, it remains insufficient for the technology to reach mainstream status. This is partly due to the substantial computational burden currently associated with blockchain applications, which predominantly rely on high-performance GPUs, field programmable gate arrays (FPGA), or specialized ASICs. Consequently, the energy consumption and device requirements of the technology are inflated.

SmartNICs, or Smart Network Interface Cards, are specialized network interface cards that possess the capability to perform tasks traditionally handled by CPUs. These cards hold a distinctive position within computer systems as they serve as the entry point for all data into a server. Recognizing this uniqueness, vendors such as Mellanox and Netronome have endeavored to harness the advantages offered by SmartNICs by incorporating greater computational power into these cards. This is achieved through the integration of programmable Network Processing Units (NPUs), which are capable of executing customized user programs directly on the NIC. Consequently, computation offloading can occur without the need for data transfer through other server devices. The specific hardware and design of SmartNICs can vary, but generally, they consist of an NPU, a set of network ports, and optionally, a multi-core CPU.

Over time, SmartNICs have become an integral component of forward-thinking data center infrastructures, forming the foundation for initiatives such as VMware's Project Monterey and Microsoft Azure datacenters. Initially, the primary applications of SmartNICs focused on offloading specific networking functions. However, recent academic literature has showcased the numerous potential applications of SmartNICs. Notable examples include offloading network virtualization platforms, distributed applications, and serverless functions onto SmartNICs, yielding remarkable outcomes. These endeavors follow a similar pattern, relieving CPUs of significant computational burdens while simultaneously enhancing latency performance due to the unique placement of SmartNICs. In conclusion, both industry and academia recognize the immense potential for reducing latency and achieving computational offloading through the development of SmartNIC architecture.

2. Motivations and Challenges

SmartNICs are poised to play a crucial role in the advancement of an edge-centric network architecture. Although SmartNICs have been explored in various applications, ranging from virtualization offloading to lambda functions, the utilization of SmartNICs in a distributed application like blockchain has not been extensively examined. Blockchain, by definition, is a distributed system, and its prevailing form is highly computationally demanding. The proof of work mechanism heavily relies on parallelized computation and swift communication among multiple nodes. Each miner node continually computes and verifies the nonce value against the blockchain's hash condition. As we envision the future of blockchain applications, we anticipate market demand to drive a decrease in the computational power required for consensus algorithms in maintaining a blockchain. Progress is already being made in this area. Moreover, we foresee the expansion of hardware devices associated with blockchain, extending beyond ASICs, FPGAs, and GPUs to devices with lesser computational power, such as SmartNICs. We specifically focus on SmartNICs because their fourth-generation design incorporates multicore architecture and hardware accelerators for packet inspection. Consequently, this enables the possibility of parallelized computation and efficient communication, as data packets with packet headers can be processed within the SmartNIC's data processing unit and hardware accelerators. Thus, we identified an opportunity to innovate by establishing the first-ever blockchain infrastructure on SmartNICs and also assessing the SmartNIC's potential as a security node within a larger network. If the SmartNIC can successfully operate a PoW-based blockchain, it serves as a compelling proof of concept for its role as a host for future security functions in a distributed network architecture, irrespective of whether it is blockchain-based or not. The integration of cryptographic hardware accelerators into recent iterations of SmartNICs further supports their broader application in networking security.

2.1. Motivations

A critical aspect of this project is our intention to leverage the data plane capabilities of SmartNICs to alleviate computational workload. Given that data packets are transmitted with headers containing essential information and security measures, it is prudent to exploit this communication for a distributed application, such as blockchain in our case. Our objective is to explore the potential of SmartNICs as a tool in the future of networking and edge computing, while also examining the current computational limits of SmartNICs. Through this project, we aim to contribute to the discourse surrounding the next network foundation that will drive the adoption of the metaverse, autonomous vehicles, artificial intelligence, and other transformative technologies.

2.2. Challenges

The BlockNIC project encountered a multitude of obstacles that were unique not only due to its originality but also because of its interdisciplinary nature.

2.2.1. Designing Blockchain Software

Given that most blockchain applications operate on hardware with significantly different computational capabilities than SmartNIC, it was crucial to consider these design limitations during the development of BlockNIC. This necessitated the use of the lowest-level programming language available and ensuring that the design avoided any unnecessary tasks. Moreover, the design had to account for the possibility that the primary function of the SmartNIC might not be maintaining the blockchain, thus requiring the ability to save, recover, and resume processes.

2.2.2. Harnessing SmartNIC Hardware

As SmartNICs become increasingly accessible to developers, the accompanying documentation and development tools are gradually being developed. Consequently, challenges arise when utilizing built-in accelerators, implementing parallel processing, and debugging, resulting in more time-consuming and arduous tasks. Furthermore, there is still uncertainty surrounding the full potential of leveraging the hardware, necessitating further exploration.

2.2.3. Serialization & Communication:

For BlockNIC to operate optimally, its communication infrastructure must seamlessly serialize and de-serialize specific blockchain information to facilitate consensus. Without proper serialization, critical elements such as a discovered nonce or a new transaction may be misinterpreted or lost, leading to immediate disruption within the entire BlockNIC system.

3. BlockNIC Blockchain Overview

In this section, we present an overarching overview of the various components that constitute BlockNIC. The implementation of BlockNIC's blockchain encompasses several vital elements:

a. Transaction: At the core of BlockNIC's design lies the transaction, which serves as the fundamental building block. This transaction carries valuable information, including the amount of currency being transferred, the timestamp of the transaction, the IP addresses of both the sender and recipient, and the sender's signature. One notable application of the transaction within BlockNIC is the ledger, which records details regarding the exchange and creation of Lampcoin, the blockchain currency devised exclusively for BlockNIC. Lampcoin is generated through incremental deposits into authorized BlockNIC Miner node wallets, serving as a reward for active participation within the BlockNIC community. This Lampcoin can then be exchanged by clients on miner nodes, who can specify recipients through IP addresses and include accompanying messages.
b. Block: In BlockNIC, blocks solely consist of transactions, with each block accommodating approximately 20 transactions. Block data encompasses the index, timestamp, hash of the previous block, the aforementioned list of transactions, and the proof required for the consensus algorithm.
c. Blockchain: Within the system design, the BlockNIC Blockchain assumes the role of the largest entity. It holds all the essential metadata necessary for maintaining the blockchain, such as the database of verified nodes, the length of the chain, the overall number of transactions, the hash of the most recent transaction, the comprehensive ledger, and more. To illustrate further with the example of Lampcoin, transaction data between various clients' wallets are facilitated through this blockchain.

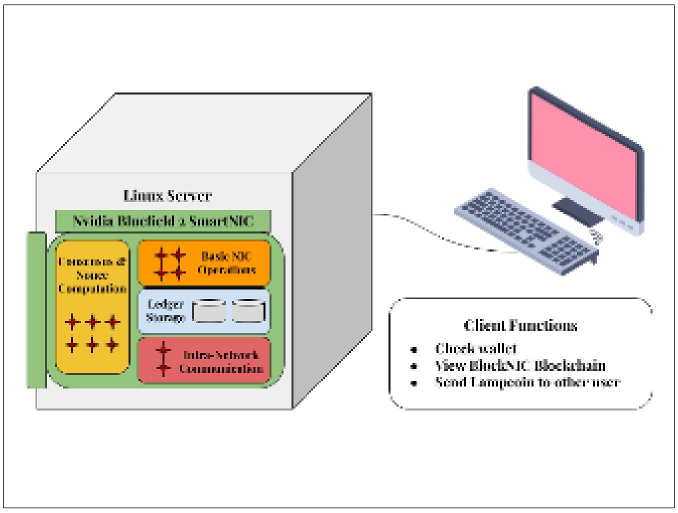

Figure 2 Single Node Abstraction for BlockNIC

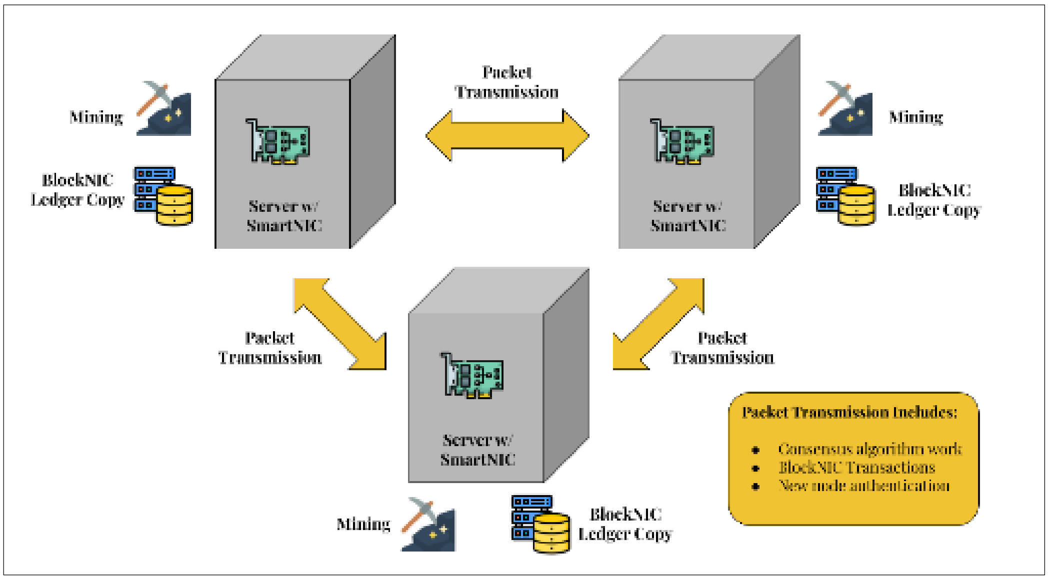

Figure 3 Multi Node Abstraction for BlockNIC

Therefore, BlockNIC comprises these key components, each playing a crucial role in the operation and functionality of the system. The data of the BlockNIC Blockchain is stored in blocks, and clients constantly send transaction data when sending new Lampcoin transactions. With these fundamental components, additional features can be incorporated into the ledger.

Moving to the architectural overview, the BlockNIC architecture can be best understood by considering it from both a single node and multinode perspective. Figure 2 illustrates the design of BlockNIC from a single node standpoint. The bare metal server houses the Nvidia Bluefield-2 SmartNIC, with the I/O devices connected to the same server. By accessing the SmartNIC user space through SSH, the user can initiate the Miner and Client programs. The Miner program should run continuously, whereas the Client program is only necessary when the user intends to check their Lampcoin wallet, the status of the BlockNIC Blockchain, or send a transaction to another BlockNIC user. Meanwhile, the Miner program continues to mine for new Lampcoin and add more blocks to the Blockchain.

Figure 3 provides a comprehensive overview of the BlockNIC architecture. Each BlockNIC node, which consists of a bare metal server with a SmartNIC, is responsible for mining new Lampcoin and maintaining its own copy of the BlockNIC ledger. To accomplish this, the node must communicate with other BlockNIC nodes through packet transmission. This communication includes various types of transactions, such as client Lampcoin transactions and incremental participation Lampcoin transactions, as well as notifications related to the addition or removal of BlockNIC nodes and the discovery of nonce values. All of these tasks are performed by the SmartNIC itself, even though it is housed within the bare metal server.

In terms of consensus model, we are implementing the traditional mining process used in Bitcoin and blockchain. Our blockchain utilizes the proof of work consensus algorithm. In BlockNIC, miner nodes compete to find a nonce value that, when multiplied with the hash value of the most recent block, results in four ending zeros. When a node finds a nonce value that meets this requirement, it notifies the other nodes in the BlockNIC network of its potential success. These nodes independently verify the successful nonce value and respond with confirmation. Once the sending node receives confirmation from a majority of nodes, it is granted permission to forge the next block on the BlockNIC Blockchain. The BlockNIC miner node can then add the block it has been forging, based on transactions recorded through client input or BlockNIC network communication. The node sends a message to all other nodes, presenting the new legitimized BlockNIC chain, which the other nodes accept as the new legitimate chain and override their own. The winning node is rewarded with a small amount of Lampcoin.

Moving on to the design characteristics of BlockNIC, from the user's perspective, it can be simplified into two programs: miner and client. The SmartNIC is ideally always mining, while user transactions are relatively infrequent, hence the division between the two programs. The miner program is responsible for maintaining the node's ledger, continuously guessing the nonce value, and verifying and updating incoming messages from other BlockNIC nodes. It also handles the modification of the chain file and the node list, as it is the primary communication entity. On the other hand, the client program does not modify the chain file. Its main role is to create possible blocks at the node, which can be added if the miner program of the node finds the nonce value first. The client program focuses on reading the BlockNIC Blockchain to ensure transparency and posting new transactions that the user may execute, both within itself and to other nodes.

4. Performance of BlockNIC nodes

In terms of evaluation, the performance of BlockNIC nodes with bare-metal nodes running on a CPU has been compared in this section.

4.1. Testbed Configuration

The assessment testbed comprises a cluster of three Linux servers containing 8-core AMD EPYC 7232P 3.10GHz processors, 8GB 3200MT/S RAM, and 480GB SSD SATA 6Gbps. Two of the servers are equipped with Nvidia Bluefield 2 P-Series DPU 25GbE Dual-Port SFP56, serving as specialized SmartNIC nodes for our blockchain. Additionally, there is a bare metal server functioning as another CPU-based client. The Nvidia Bluefield 2 SmartNIC is equipped with an 8-core Cortex A72 ARM processor running at 2.75GHz, 1MB L2 cache per 2 cores, 6MB L3 cache, and 16GB of DDR4 RAM. The nodes communicate through the university network and are connected via ethernet on the same router to optimize speed. All three nodes continuously run the BlockNIC Miner program, while the BlockNIC Client program is deployed occasionally. The project is implemented in C, with the design heavily influenced by David Gorski's open-source 'blockchain-in-c' repository [13]. Our project utilizes C standard libraries, nng for networking and intra-node communication protocols, and the openssl library for cryptographic computation.

4.2. Benchmark Workloads

BlockNIC's performance was evaluated in [43] on two different types of workloads: (i) the entire program workload and (ii) the hashing workload.

- Entire Program: One of the objectives of the authors in [43] was to evaluate the SmartNIC hardware's effectiveness as a standalone node for future edge networks. To fulfill this role, the SmartNIC must exhibit strong performance while establishing trust, communicating results with other network nodes, and maintaining relatively low latency. To evaluate this, they measured the SmartNIC's performance in terms of user CPU percentage and the time it takes to complete the same task as the bare metal CPU server, which operates as a BlockNIC Miner node.
- Offloads: In their examination of SmartNIC's potential in future distributed computing networks, they project that while they may not operate as standalone nodes, they can act as "executive assistants" by relieving CPUs of specific tasks when integrated with servers. Our assessment focused on SmartNIC's performance in handling specific parts of the BlockNIC workload, particularly the hashing workload and the consensus workload.
- BlockNIC Performance: The BlockNIC system's performance was assessed through trials involving parachute payments to nodes, incentivizing their participation and transactions. However, once the currency cap of 888 Lampcoin is reached, natural processes occur, affecting the BlockNIC Miner program. Nodes operate using the

BlockNIC Client program, enabling transaction generation among registered nodes. Experimental trials revealed that SmartNIC processing times were longer than bare metal CPU due to differences in CPU performance, with SmartNIC utilizing more CPU space due to code optimization for x86 CPUs over ARM cores. The SmartNIC showed greater timing variability attributed to its smaller cache size compared to the bare metal server. Hashing performance evaluations showed the SmartNIC took longer due to increased context switching time.

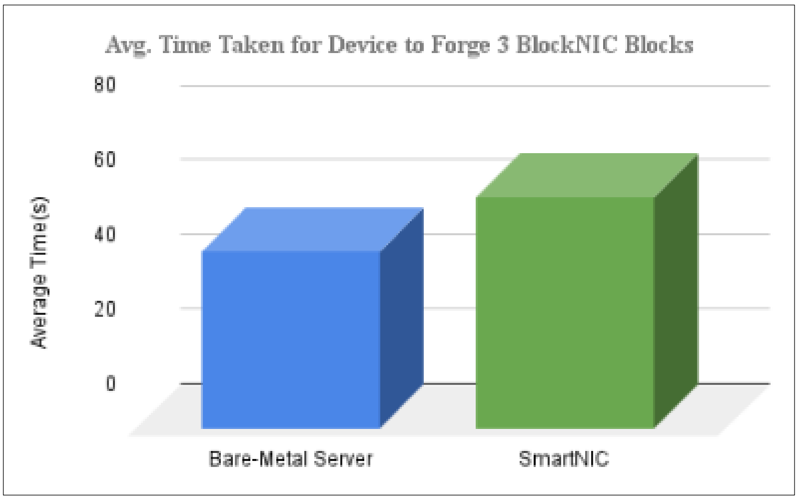

Figure 4 Average Time Taken to Forge 3 BlockNIC Blocks (Adopted from [43])

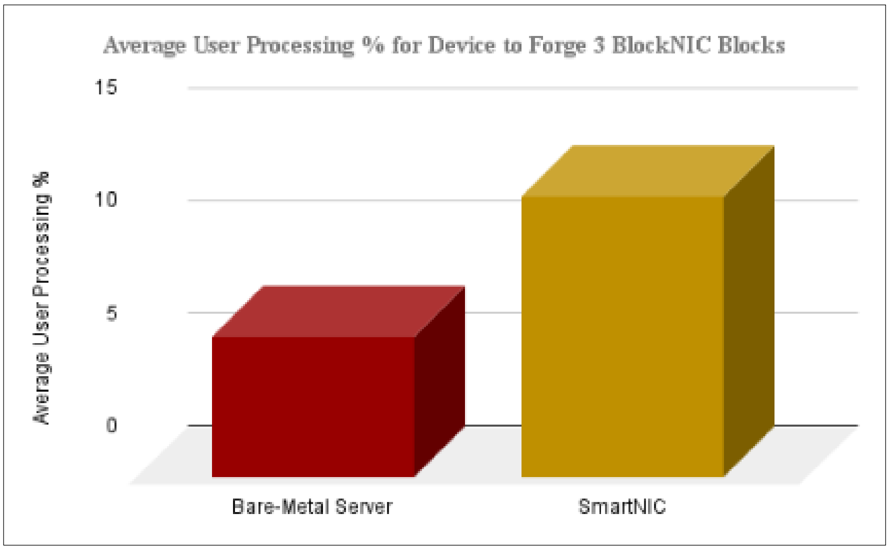

Figure 5 Average CPU Usage (%) to Forge 3 BlockNIC Blocks (Adopted from [43])

Moving on to the next experiment, the focus was solely on monitoring the mining work associated with BlockNIC. In this particular context, mining refers to the process of finding the nonce value that, when multiplied by the most recent block's proof of work hash, produces a result with four zeros at the end. Consequently, the experiment involved computing and verifying the validity of the nonce value. The average time taken for this process was 1.437 seconds for the SmartNIC and 1.053 seconds for the bare-metal server (Figure 7), which aligns with our initial expectations. Furthermore, Figure 8 illustrates that the user space CPU usage for the SmartNIC was 0.29%, while for the bare-metal server it was 0.15%. This discrepancy is relatively small due to the short duration of the mining operation.

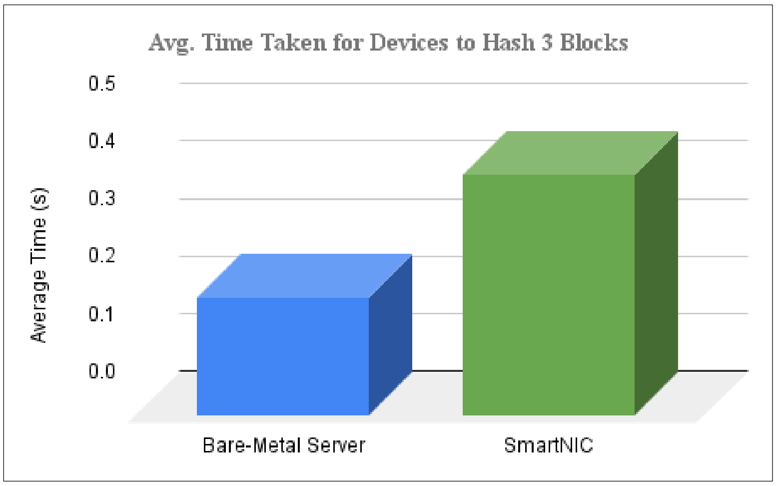

Figure 6 Average Time Taken to Hash 3 BlockNIC Blocks (Adopted from [43])

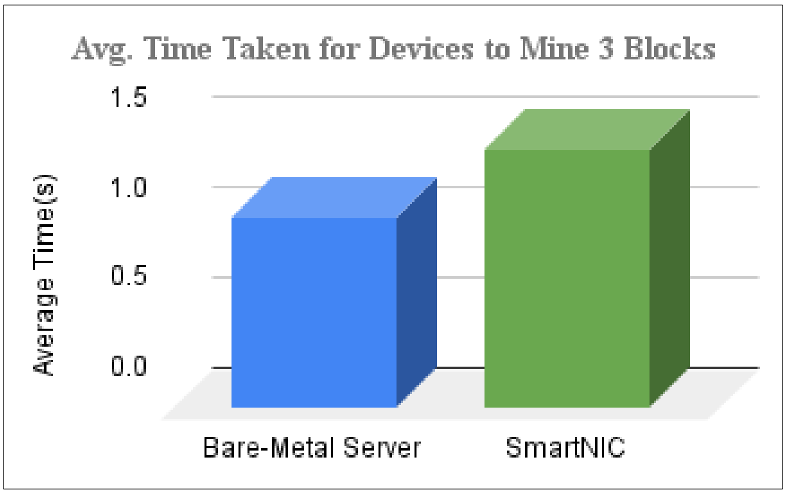

Figure 7 Average Time Taken to Mine 3 BlockNIC Blocks (Adopted from [43])

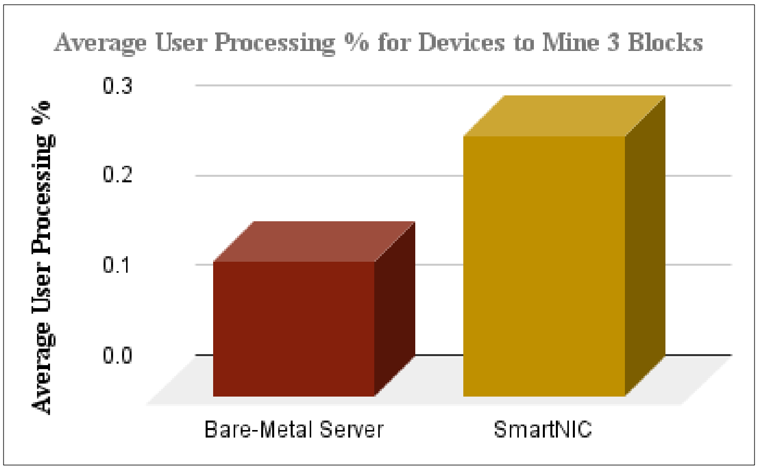

Figure 8 Average CPU usage to Mine 3 Block NIC Blocks

5. Performance Analysis

The initial experiment and its corresponding outcomes exhibited promising results, as they demonstrated the resilience of the SmartNIC in maintaining a lightweight blockchain infrastructure without external assistance. For instance, blockchain operations like communication, ledger maintenance, and nonce computation were intentionally designed to be performed equivalently on both hardware types. Thus, these operations are essentially the same as those performed by any distributed trust-creating node, which the SmartNIC executed with minimal modifications. This indicates that if the operations are further optimized for a SmartNIC, the performance gains will be greater. Therefore, although it is 23.6% slower than its bare-metal counterpart, BlockNIC holds promise for future network deployments where other trust-building functions or mechanisms can exist on the network path and on SmartNICs. It is important to note that the performance difference arises from variations in clock speed, cache sizes for each core, and optimization in the ARM core, rather than architectural limitations, which can be overcome with more powerful hardware. Hence, despite the performance disparity, the proposed architecture strengthens the argument that SmartNICs can function as independent nodes in future blockchain networks while allowing the host to allocate CPU cycles for other operations.

Regarding the second experiment, the results indicated that the SmartNIC was 104% slower than the bare-metal server when performing the same task, which is not favorable for future applications leveraging this technology. This slowdown is significant and cannot be disregarded, as it fails to offset the expected latency gains from having the card at the edge. Hashing, being a repetitive task, is better suited for specialized hardware such as ASIC or FPGA. However, in the case of BlockNIC, we utilize hardware and chips that are not solely dedicated to hashing. Instead, we employ hardware components that are likely to be idle and less valuable than a CPU, thereby reducing environmental impact. To enhance hashing performance, BlockNIC can leverage the crypto engine available in certain SmartNICs.

The third and final experiment showcased the SmartNIC's ability to compete relatively well in terms of performance with the bare-metal server. The SmartNIC was 36% slower in completing the same mining tasks as the bare-metal server, which is expected. It is exciting to observe that the drop-off in performance is not significant, considering that the mining tasks involve trust generation and communication aspects. This finding can be extrapolated to applications that may prefer an intermediate edge device capable of executing work close to the client, thereby conserving valuable compute resources downstream in the network infrastructure.

The use of artificial intelligence (AI) technologies such as machine learning and deep learning to analyze healthcare data, improve diagnostics, personalize treatment plans, and enhance overall patient care [26-40]. Blockchain, coupled with SmartNIC technology, facilitates seamless interoperability among disparate healthcare systems and data sources. This interoperability ensures that AI-driven healthcare applications can access and integrate data from various sources, enabling comprehensive patient care coordination and collaboration among healthcare providers [41].

6. Conclusion

In this paper, we introduce BlockNIC, an initial endeavor to execute a comprehensive range of blockchain operations exclusively on a Network Interface Card (NIC). By deploying a blockchain on SmartNICs, BlockNIC has successfully demonstrated the practicality of employing SmartNICs for blockchain purposes. Although this research is still in its nascent stage and necessitates numerous optimizations and forthcoming efforts, we firmly contend that it establishes an entirely new direction for blockchain development, enabling a more efficient and environmentally friendly approach to blockchain execution.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] A. Huang, "Moore's law is dying (and that could be good)," IEEE Spectrum, vol. 52, no. 4, pp. 43–47, 2015.

[2] I. Cloud, "What is edge computing?" 2019. https://www.ibm.com/cloud/ what-is-edge computing

[3] R.v.d. Meulen, “What edge computing means for infrastructure and operations leaders,” Oct 2018.https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for infrastructure-and-operations-leaders.

[4] B.M.. Co., “How can blockchain technology be applied in real life?” 2021. https://bernardmarr.com/how-can-blockchain-technology-beapplied-in-real-life/

[5] S. Arora, “What is bitcoin mining: How does it work, proof of work & more,” October 2021. https://www.simplilearn.com/bitcoin-miningexplained-article

[6] N. Chalaemwongwan et al., “Notice of violation of ieee publication principles: State of the art and challenges facing consensus protocols on blockchain,” in 2018 International Conference on Information Networking(ICOIN), 2018, pp. 957–962.

[7] Euromoney, “What is blockchain?” 2022, [Online; accessed November 6,2022]. https://www.euromoney.com/learning/blockchainexplained/what-is-blockchain

[8] Y. Huang et al., “Resource allocation and consensus on edge blockchain in pervasive edge computing environments,” in 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), 2019,pp. 1476–1486.

[9] “Fact sheet: Climate and energy implications of crypto-assets in the united states,” September 2022.https://www.whitehouse.gov/ostp/news-updates/2022/09/08/fact-sheetclimate-and energy-implications-of-crypto-assets-in-the-united-states/

[10] X. Zhu et al., “Network function virtualization and software-defined networking: Advancing multimedia distribution,” IEEE MultiMedia,vol. 24, no. 3, pp. 16–18, 2017.

[11] M. Liu et al., “Offloading distributed applications onto smartnics using ipipe,” in Proceedings of the ACM Special Interest Group on Data Communication, ser. SIGCOMM ’19. New York, NY, USA: Association for Computing Machinery, 2019, p. 318–333. https://doi.org/10.1145/3341302.3342079

[12] S. Choi et al., “Lambda-nic: Interactive serverless compute on programmable smartnics,” in 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), 2020, pp. 67–77.

[13] D. Gorski, “blockchain-in-c,” https://github.com/dgski/blockchain-in-c,2018.

[14] D. Firestone et al., “Azure Accelerated Networking: SmartNICs in the Public Cloud,” in USENIX NSDI, 2018.

[15] B. Pfaff et al., “The Design and Implementation of Open vSwitch,” in USENIX NSDI, 2015.

[16] D. Kim et al., “Hyperloop: Group-based NIC-offloading to Accelerate Replicated Transactions in Multi-tenant Storage Systems,” in SIGCOMM,2018.

[17] R. Miao et al., “SilkRoad: Making Stateful Layer-4 Load Balancing Fast and Cheap Using Switching ASICs,” in ACM SIGCOMM, 2017.

[18] N. Katta et al., “HULA: Scalable Load Balancing Using Programmable Data Planes,” in ACM SOSR, 2016.

[19] X. Jin et al., “NetCache: Balancing Key-Value Stores with Fast In-Network Caching,” in ACM SOSP, 2017.

[20] H.T. Dang et al., “NetPaxos: Consensus at Network Speed,” in ACMSOSR, 2015.

[21] NewEgg, “Msi ventus geforce rtx 3060 ti 8gb gddr6 pci express 4.0 video card rtx 3060 ti ventus 2x 8g ocv1 lhr,”https://newegg.com/msi-geforce-rtx-3060-ti-rtx-3060-ti-ventus-2x-8g-ocv1-lhr/p/N82E16814137673?Description=RTX%203060&cm re=RTX 3060- -14-137-673- -Product, 2021.

[22] Bittware, “Cvp-13 fpga cryptocurrency mining board,” https://www.bittware.com/cvp-13/, 2021.

[23] KOI, “Koi miner bitcoin miner c16 max 113th/s with psu and cords —bt-miners,” https://bt-miners.com/products/koi-miner-bitcoin-miner-c16-max-113th-s, 2021.

[24] Y. Zuo et al., “Blockchain storage and computation offloading for cooperative mobile-edge computing,” IEEE Internet of Things Journal, vol. 8, no. 11, pp. 9084–9098, 2021.

[25] X. Xu et al., “Become: Blockchain-enabled computation offloading for iot in mobile edge computing,” IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4187–4195, 2020.

[26] Begum, A.M.; Mondal, M.R.H.; Podder, P.; Kamruzzaman, J. Weighted Rank Difference Ensemble: A New Form of Ensemble Feature Selection Method for Medical Datasets. BioMedInformatics 2024, 4, 477-488. https://doi.org/10.3390/biomedinformatics4010027

[27] Podder, P., Alam, F. B., Mondal, M. R. H., Hasan, M. J., Rohan, A., & Bharati, S. (2023). Rethinking densely connected convolutional networks for diagnosing infectious diseases. Computers, 12(5), 95.

[28] Bharati, S., Mondal, M. R. H., Podder, P., & Kose, U. (2023). Explainable Artificial Intelligence (XAI) with IoHT for Smart Healthcare: A Review. Interpretable Cognitive Internet of Things for Healthcare, 1-24.

[29] Podder, P.; Das, S.R.; Mondal, M.R.H.; Bharati, S.; Maliha, A.; Hasan, M.J.; Piltan, F. LDDNet: A Deep Learning Framework for the Diagnosis of Infectious Lung Diseases. Sensors 2023, 23, 480. https://doi.org/10.3390/s23010480

[30] Bharati, S., Podder, P., Thanh, D. N. H., & Prasath, V. S. (2022). Dementia classification using MR imaging and clinical data with voting based machine learning models. Multimedia Tools and Applications, 81(18), 25971-25992.

[31] Molla, S., Bazgir, E., Mustaquim, S. M., Siddique, I. M., & Siddique, A. A. (2024). Uncovering COVID-19 conversations: Twitter insights and trends. World Journal of Advanced Research and Reviews, 21(1), 836-842.

[32] Rahman, S. M., Ibtisum, S., Bazgir, E., & Barai, T. (2023). The significance of machine learning in clinical disease diagnosis: A review. arXiv preprint arXiv:2310.16978.

[33] Rahman, M. A., Bazgir, E., Hossain, S. S., & Maniruzzaman, M. (2024). Skin cancer classification using NASNet. International Journal of Science and Research Archive, 11(1), 775-785.

[34] Ehsan Bazgir, Ehteshamul Haque, Md. Maniruzzaman and Rahmanul Hoque, "Skin cancer classification using Inception Network", World Journal of Advanced Research and Reviews, 2024, 21(02), 839–849.

[35] Ibtisum, S., Bazgir, E., Rahman, S. A., & Hossain, S. S. (2023). A comparative analysis of big data processing paradigms: Mapreduce vs. apache spark. World Journal of Advanced Research and Reviews, 20(1), 1089-1098.

[36] Rahmanul Hoque, Suman Das, Mahmudul Hoque and Ehteshamul Haque, " Breast Cancer Classification using XGBoost", World Journal of Advanced Research and Reviews, 2024, 21(02), 1985–1994

[37] Bharati, S., Podder, P., Mondal, M. R. H., Surya Prasath, V. B., & Gandhi, N. (2021, December). Ensemble learning for data-driven diagnosis of polycystic ovary syndrome. In International conference on intelligent systems design and applications (pp. 1250-1259). Cham: Springer International Publishing.

[38] Khamparia, A., Pandey, B., Al-Turjman, F., & Podder, P. (2023). An intelligent IoMT enabled feature extraction method for early detection of knee arthritis. Expert Systems, 40(4), e12784.

[39] Rahmanul Hoque, Masum Billah, Amit Debnath, S. M. Saokat Hossain and Numair Bin Sharif, "Heart Disease Prediction using SVM", International Journal of Science and Research Archive, 2024, 11(02), 412–420.

[40] Begum, A. M., Mondal, M. R. H., Podder, P., & Bharati, S. (2021, December). Detecting Spinal Abnormalities using Multilayer Perceptron Algorithm. In International Conference on Innovations in Bio-Inspired Computing and Applications (pp. 654-664). Cham: Springer International Publishing.

[41] Saeed H, Malik H, Bashir U, Ahmad A, Riaz S, Ilyas M, Bukhari WA, Khan MIA. Blockchain technology in healthcare: A systematic review. PLoS One. 2022 Apr 11;17(4):e0266462. doi: 10.1371/journal.pone.0266462. PMID: 35404955; PMCID: PMC9000089.

[42] E. Kapoor, G. Jampani and S. Choi, "BlockNIC: SmartNIC assisted Blockchain," 2023 Silicon Valley Cybersecurity Conference (SVCC), San Jose, CA, USA, 2023, pp. 1-8, doi: 10.1109/SVCC56964.2023.10165427.

[43] Bharati, S., & Podder, P. (2022). Machine and deep learning for iot security and privacy: applications, challenges, and future directions. Security and communication networks, 2022, 1-41.