IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 14 February 2024, accepted 8 March 2024, date of publication 18 March 2024, date of current version 22 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3377119

RESEARCH ARTICLE

Scalable EdgeIoT Blockchain Framework Using EOSIO

EHTISHAM UL HAQUE[1], M. SHAMIM BAIG[1], ASAD AHMED[1], ASHFAQ AHMAD[1], MASOUD ALAJMI[2], (Member, IEEE), YAZEED YASIN GHADI[3], HEND KHALID ALKAHTANI[4], (Member, IEEE), AND AINUR AKHMEDIYAROVA[5]

[1]Department of Computer Science, MY University, Islamabad 44000, Pakistan
[2]Department of Computer Engineering, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia
[3]Department of Computer Science, Al Ain University, Abu Dhabi, United Arab Emirates
[4]Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia
[5]Department Computer Engineering, Satbayev University, Almaty 050000, Kazakhstan

Corresponding authors: Hend Khalid Alkahtani (hkalqahtani@pnu.edu.sa) and Ashfaq Ahmad (ashfaq.ahmad@myu.edu.pk)

This work was supported by Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia, through the Princess Nourah bint Abdulrahman University Researchers Supporting Project, under Grant PNURSP2023R384.

ABSTRACT Widespread adoption of internet of things (IoT) for automation, monitoring and control in various engineering, business and industrial applications poses serious challenges of data security and cyber-attacks to IoT networks. Blockchain enabled IoT networks, due to their immutability, transparency, and accountability, are commonly employed to ensure safe and secure implementation of the IoT networks. However, blockchain technology is prone to degradation in performance and efficiency in the presence of large number of IoT devices and massive data generated by these networks and does not scale well with the growing size of the networks. This research proposes a Scalable EdgeIoT Blockchain (SEB) framework using EOSIO to enhance the performance and efficiency of the blockchain enabled IoT networks. The proposed framework leverages upon the concepts of sharding for parallel execution of smart contracts, Delegated Proof of Stake (DPoS) for consensus in the network with large number of devices and Interplanetary File System (IPFS) for the data storage and management of massive data in the IoT networks. The proposed framework is implemented in the EOSIO blockchain. This study experiments show significant improvement in the throughput, latency and resource utilization compared to the state-of-the-art solutions in the blockchain enabled IoT networks.

INDEX TERMS Blockchain, consensus algorithm, the Internet of Things, edge computing, data sharding, delegated proof of stake, EOSIO, interplanetary file system.

I. INTRODUCTION

Blockchain technology-based Internet of Things (IoT) networks have been widely adopted for secure and safe connectivity for the exchange of information and control over the physical or virtual objects in medical, agriculture and business applications [1]. However, blockchain enabled IoT networks suffer from the scalability, high latency and low throughput issues due to high computational demands of blockchain technology, scarce resources and large size of the IoT networks.

IoT networks consist of devices, nodes, wireless sensor nodes (WSNs), actuators, embedded systems and things or objects which are interconnected via the internet. Due to many factors, such as low cost IoT devices, state-of-the-art ICT infrastructure, IoT networks have been widely adopted for the variety of applications including healthcare, industry, smart homes, smart grids, security, and surveillance and many more [2]. Conventionally, IoT networks are implemented with existing infrastructure and technology which is

The associate editor coordinating the review of this manuscript and approving it for publication was Liang-Bi Chen.

centralized, i.e., data from IoT devices is accumulated and processed through a central server. This approach results in the vulnerabilities to security and privacy of IoT network from cyber and physical attacks [3]. To alleviate the issues, blockchain technologies are used to provide safe and secure implementation of the IoT networks [4].

Blockchain is a database concept which relies upon decentralization and cryptography to store and retrieve the related database. In a blockchain system, participant nodes have digital ledgers which contain blocks to keep record of transaction or data. All nodes in a blockchain system update their digital ledgers with a new block using cryptographic hash-function and consensus algorithm to ensure security, integrity, and immutability of the data [2]. Consensus algorithms, such as Proof of Stake (PoS) and Proof of Work (PoW), are set of rules agreed upon by the nodes to add a new block in the distributed digital ledger. However, integration of IoT using blockchain technology is severely limited by the scalability in terms of transaction per second and energy consumption limitations due to computationally extensive and demanding consensus algorithms [5], [6]. There are various approaches to preventing energy consumption in blockchain-based systems, and they are still inadequate compared to the performance of lower-end devices [4]. Moreover, in large data applications, such as IoT, data storage and management are crucial in the performance and efficiency of the blockchain enabled networks [1].

Recently, significant research attention has been drawn to the blockchain enabled IoT networks. A combination of public and private blockchain is used to achieve performance and security for IoT applications [7]. The hybrid blockchain utilizes PoW and Practical Byzantine Fault Tolerant (PBFT) consensus algorithms for the consensus in their work [8]. Scalable Distributed Intelligence Tangle (SDIT) [9] approach leveraging PoW and Tangle architecture achieves improved scalability in an IoT network. A framework using local blockchain in wireless sensor network (WSN) is utilized for the secure management and storage of large data due to the integration of the WSN IoTs [10]. The consensus among the network nodes is achieved using PoS consensus algorithm. A scalable lightweight Blockchain integrated model (Light-Block) based on the optimization of the scalable Blockchain architecture (SBA), lightweight consensus algorithm (LCA), and throughput management scheme (TMS) is presented to coup with the scalability issue of blockchains in IoT environment [11]. Edge based Coded Sharding technology and cloud storage has been used [12] to improve scalability, fault tolerance and data storage and management by proposing a cryptographic accumulator with the sharding nodes. However, addition of cryptographic accumulator increases the latency which is around 80s. Moreover, the cloud-based storage is a centralized solution thus can jeopardize the security and privacy of the data. Interplanetary File system (IPFS) in combination with edge computing has been proposed to mitigate the cloud-based centralization issue using PoW and PoA consensus algorithms [13]. However, PoW, PBFT, PoW and PoS consensus algorithms limit the scalability of the blockchains for IoT applications due to the large number of IoT devices. An EOSIO based food traceability framework is presented for the smart cities' environment. Authors have compared and proved the superiority of the EOSIO based framework with the Ethereum based solution in terms of consensus algorithm, throughput, block production and block confirmation rate [14]. However, authors do not address the issues of data storage and management of large data associated with the IoT echo system. IPFS as an off-chain storage in EOSIO platform is used for the threat intelligence sharing and exchange but authors does not address the IoT based application [15].

The aforementioned approaches mainly focus on the use of consensus algorithms, storage and management techniques and mechanisms, edge computing and sharding to cater the issues of security, performance, efficiency and scalability in the blockchain enabled IoT networks. However, blockchain enabled IoT networks pose multifaceted challenges due to scarce resources, in terms of computation and memory, and large sized data. In this paper, we propose a comprehensive framework which is aimed to harness the potential benefits of the different techniques and technologies to cater the challenges in the realization of a scalable and high performance blockchain enabled IoT solution for IoT applications. To the best of our knowledge, no blockchain enabled IoT network approach has been proposed to address the whole spectrum of challenges so far, which is the scope of the current paper.

However, our contributions in this paper are:

- In this paper, we propose a framework referred to as Scalable EdgeIoT Blockchain (SEB), leveraging upon the edge computing, sharding, IPFS and DPoS to mitigate efficiency, performance, data storage and management issues in blockchain enabled IoT networks.
- We develop smart contracts in EOSIO for the authentication and verification of the IoT devices in our proposed design.
- We implement the proposed design in EOSIO blockchain platform to evaluate the performance of the proposed architecture for varying number of IoT devices in terms of resource utilization, CPU, and net bandwidth (NET).

The rest of the paper is organized as follows: In Section II, we present preliminary concepts and technologies including data storage management, edge computing, blockchain technology and EOSIO blockchain platform relevant to the proposed framework. In Section III, we present our proposed framework for the blockchain enabled IoT networks. Then, in Section IV, we present our experimental results and discussions. Finally, Section V concludes the paper.

TABLE 1. Comparison of leading blockchain system.

Features	Bitcoin	Ethereum 2.0	Hyperledger-Fabric	IoTA	EOSIO
Consensus	POW	POS	PBFT	Tangle	DPOS
Consensus finality	×	×	✓	×	✓
Run SC	×	×	✓	×	✓
Interchain	×	×	×	×	✓
Feeless	×	×	×	✓	✓
Scalable	×	✓	×	✓	✓
Energy efficient	×	×	×	✓	✓
TX throughput	7	100+	1,000	7-12	4000+

II. PRELIMINARIES

This section presents preliminaries to facilitate the understanding of the rest of the paper.

A. DATA STORAGE AND MANAGEMENT

Blockchain stores data in the blocks which is referred to as on-chain storage mechanism [16]. Due to immutability, reliability, fault-tolerance, and decentralization features of blockchain, on-chain mechanism ensures security of the data from the potential threats and misuse of the data [2], [17]. However, blockchains, such as bitcoin have limited storage space and cost associated with the transactions and hence results in increased cost and limited scalability [5].

Off-chain storage mechanism is utilized to overcome above mentioned issues [18], [19]. In off-chain mechanism, data is managed outside of the blockchain, such as databases systems, networks, and storages. This allows us to overcome the storage space problem in on-chain blockchains.

In the IoT networks, large data is generated and therefore on-chain mechanism does not suit well to the blockchain enabled IoT networks [20], [21]. Therefore, in our proposed solution we use Inter Planetary File System (IPFS), which is an off-storage solution, to alleviate the data storage and management issues in blockchain enabled IoT networks. IPFS is a data storage and management system relying upon the notions of decentralized and distributed storage and sharing of the data [18]. IPFS is a peer-to-peer network which uses content addressing approach rather than conventional location addressing methods to access of retrieve the data [22]. The network nodes maintain a hash table corresponding to the data which is termed as Content Identifier (CID) [23]. The user can access the data distributed over the network by providing the corresponding CID. IPFS ensures reliable and scalable solutions for data storage and retrieval and has been used in blockchain technology, such as Ethereum, to mitigate the scalability issues due to large data size [13]. In this paper, we have employed IPFS in our proposed framework to store, access and retrieve the large data associated with the IoT networks.

1) EDGE COMPUTING

Edge computing is a concept in networks which relies upon the computing power of the network nodes to reduce latency, enhance scalability, optimize the operation cost and ensure the privacy and security of the networks [24]. Edge device in a network refers to a node capable of sensing and collecting data, computing power to process the data and enabling communication technology and on-board memory and storage to perform the network operations [13]. Edge computing plays a vital role in the IoT based applications to implement demanding real-world applications [25]. Particularly, in conjunction with blockchain technology, edge computing has been crucial in ensuring scalable solutions for the privacy and security of data [13], [12], [24]. In this paper, our proposed solution leverages upon the computing power of the edge devices in a network to shard the IoT network and perform consensus which play pivotal role in the improving the efficiency networks.

B. BLOCKCHAIN TECHNOLOGY

Blockchain technology has been widely adopted for growing and diverse IoT applications [2]. Blockchain platforms, such as Bitcoin, Ethereum, Hyperledger, IOTA and EOSIO facilitate the development and deployment of blockchain enabled IoT frameworks and allows achieving security, integrity, and privacy [4]. Table 1 provides a comparison of some widely used blockchains with respect to features, such as consensus mechanism and Transactions per second (TPS) and cost. In the context of IoT networks, consensus mechanism and cost associated with the transactions in the blockchains are major concerns due to the large size and data generated by these networks [2]. As shown in Table 1, EOSIO which utilizes delegated proof of stake consensus algorithm is well suited to the blockchain enable IoTs. Therefore, we have opted EOSIO for the proposed framework, in this paper.

1) EOSIO

EOSIO [26] is an open source blockchain framework specifically designed to facilitate and ease the development and deployment of blockchain enabled large-scale industrial and business applications. ESIO has three main

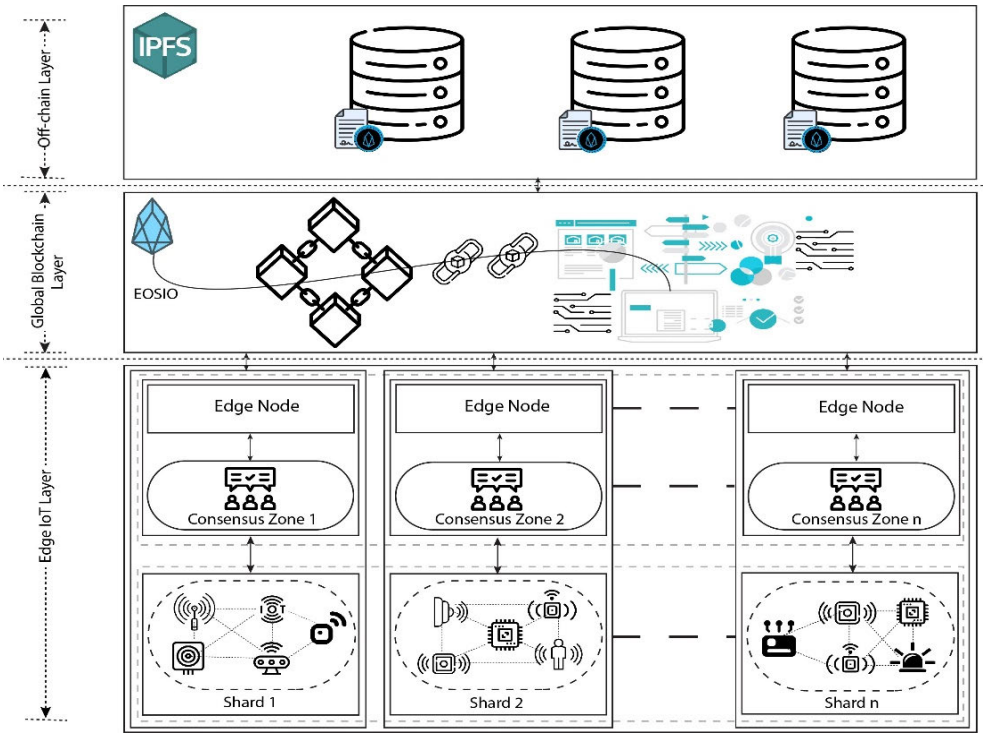


FIGURE 1. Proposed scalable EdgeIoT blockchain framework.

components namely: *Nodeos*, *Cleos* and *Keosd,* to create and operate nodes and manage keys in the blockchain. EOSIO allows users to write smart contracts in C++ which communicates with the rest of the blockchain through a toolchain for WebAssembly (Wasm) and set of tools called Contract Development Toolkit (CDT). Smart contracts are self-executing programs that encode the rules of certain network transactions. The main features of the EOSIO are high throughput, faster confirmation, low latency, efficient energy consumption, programmability, upgradeability, creating custom permission schemata and cost-effective operations [5].

EOSIO employs Delegated Proof of Stake (DPoS) consensus to select a limited set of representative nodes called Block Producers (BPs), to oversee node functions. In EOSIO, a voting procedure selects limited BPs responsibility with authority to create new blocks to the chain notably enhancing transaction speed. Moreover, EOSIO does not levy transaction fees unlike Bitcoin and Ethereum. These are the distinctive features which make EOSIO platform fit for the development of efficient, scalable, and cost-effective blockchain enabled IoT application.

EOSIO provides three types of resources: *RAM, CPU* and *NET* to the users. *RAM* is an on-chain storage for accounts names, permissions, and other data of the blockchain. On-chain storage ensures fast access of the data in the blockchain. *CPU* is a system resource used to measure the processing time of the users' transactions in microseconds and is referred to as *CPU* bandwidth. Whereas *NET* measures the network bandwidth utilized during a transaction and measured in bytes and stored on the blockchain database as net bandwidth.

2) SHARDING

Sharding is a blockchain technology optimization technique, with respect to throughput and latency, which allows the network nodes to contribute to the processing and verification of the part of the blockchain termed as a shard [5], [27]. Sharding approach enables to exploit the size of the blockchain, i.e., increasing size increases the resource of the network, therefore, throughput of the network increases linearly with the increase in the size of the nodes [12]. Sharding has been employed in our proposed framework to improve throughput and latency of the blockchain enabled IoT networks.

III. PROPOSED SCALABLE EDGEIOT BLOCKCHAIN (SEB) FRAMEWORK

Figure 1 shows our proposed architecture for blockchain enabled IoT networks. It consists of three layers; Edge, global blockchain and off-chain storage layer. The functionality of the layers is as follows:

1. Edge layer constitutes IoT network nodes. There are two types of nodes, i.e., edge and sensor nodes. In our proposed architecture sharding is performed at the edge node which is also responsible for the collecting and processing data from the sensor nodes. It allows the network to process the data in

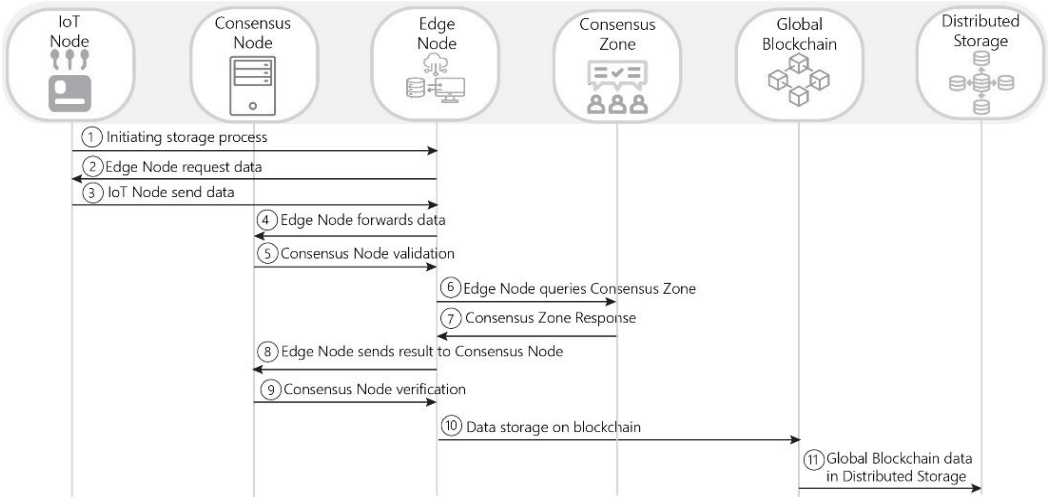


FIGURE 2. Sequence workflow of storing IoT data.

parallel and thus ensures fast processing in the presence of large number of IoT devices. The effect of sharding has been investigated in the next section. Moreover, edge nodes are also responsible for the authentication and verification of the network nodes and communication with Global blockchain layer.

2. Global Blockchain is responsible for the implementation of the blockchain for IoT network through edge nodes. Consensus and Smart contract are two main tasks performed by the global blockchain. DPoS is used to produce BPs among the edge nodes which are then delegated to the authority to verify, authorize and append new blocks. Smart contracts are also implemented at this layer which is responsible for the variety of operations within the network, such as data requests and retrieval. Throughput and latency of the proposed framework is tested for varying size of the IoT network nodes is presented in Section IV.

3. The off-chain distributed storage layer is responsible for maintaining the fully encrypted data. The process of storing and retrieving files on IPFS functions is similar to the web. Each uploaded file is assigned a unique hash string serving as a retrieval identifier akin to a URL. This approach differs from using blockchains for large file storage as current blockchain platforms prioritize transparency which is not suitable for large sized files. In our proposed solution, data exchange between off-chain, i.e., IPFS, and global chain is accomplished using smart contracts. When a user requests an operation on a specific resource, IPFS leverages traditional smart contracts within the blockchain for granting access to the file location only subject to successful authentication. A comparison of upload time and speed of the files is presented in Section IV.

Pseudocode 1 and Figure 2 depict the intricacies of the storing IoT data process within a blockchain framework encompassing various stages to ensure secure and transparent handling of information. The initiation of this process involves the commencement of storage for IoT data on the blockchain, establishing the foundation for subsequent operations. As the workflow progresses, an edge node, playing a pivotal role in the network, requests specific data essential for its processing tasks. The responsive IoT node promptly transmits the complete dataset to the edge node, setting the stage for further validation.

The data validation phase is facilitated by a consensus node selected through the DPoS consensus algorithm. Acting as

Pseudocode 1 Data Storage Proces

```
initializeStorageProcess()
while ! AllDataSent:
requestedData = EdgeNode.RequestData()
sentData = IoTNode.SendData(requestedData)
forwardedData = EdgeNode.ForwardData(sentData)
is Valid=
  ConsensusNode.ValidateData(forwardedData)
if isValid:
queriedData = EdgeNode.QueryConsensusZone()
 if queriedData is not empty :
    result = EdgeNode.SendResult(queriedData)
    verified = IoTConsensusNode.VerifyData(result)
     if verified :
        EdgeNode.StoreDataOnBlockchain(result)

    else:
         RejectData()

else:
     NoDataReturned()
StoreGlobalBlockchainData()
endProcess()
```

a validator, this consensus node instructs the edge node to verify the existence of data within the consensus zone. The edge node, in turn, queries the consensus zone to retrieve the requested information, and the consensus zone responds accordingly, either providing the required data or signaling its absence.

Following this, the edge node relays the outcome to the IoT consensus node, which takes on the critical task of verification. By comparing the information from the IoT node with the data retrieved from the consensus zone, the IoT consensus node generates a response indicating whether the data is accepted or rejected. Upon acceptance, the edge node securely stores the validated data on the blockchain, contributing to the global repository of distributed storage. This comprehensive process ensures the integrity, transparency, and secure storage of IoT data within the evolving landscape of blockchain technology.

IV. IMPLEMENTATION AND EXPERIMENTAL ANALYSIS

Our proposed framework was deployed using EOSIO (v2.2) along with the EOSIO Contract Development Tool (v1.8.1) required for compiling smart contracts and System Contracts (v1.6.0), which provides fundamental functions of the EOSIO blockchain. Additionally, we used Docker to initiate a local EOSIO node. To further assess the performance of the edge IoT framework, we modified the EOS-VM [28] test chain for parallel execution to facilitate testing and evaluation. The setup runs on Linux distribution (Ubuntu 20.04 LTS) installed on a laptop equipped with an Intel Core i3 CPU, 8 GB of RAM, and a 1 TB HDD.

The EOSIO implementation of the SEB framework allows us to analyze and evaluate the performance metrics, i.e., latency, throughput and resource utilization. We evaluate our proposed framework performance for scalability using latency and throughput metrics. Latency measures the time it takes for a data packet to be received by the edge node and added to the blockchain. This performance measure is directly related to the processing speed of the proposed framework. A higher latency value indicates increased difficulty in adding data packets to blocks the in blockchain. Whereas throughput is defined as the number of transactions processed per edge node.

We evaluate our proposed framework performance for scalability using latency and throughput metrics. Latency measures the time it takes for a data packet to be received by the edge node and added to the blockchain. This performance measure is directly related to the processing speed of the proposed framework. A higher latency value indicates increased difficulty in adding data packets to blocks. Whereas throughput is defined as the number of transactions processed per edge node. To assess the scalability of the proposed framework, we use network and data packet size as parameters. Network size refers to the number of IoT nodes which range from 500 to around 20, 000. On the other hand, data packet size is set to 1 MB while payload size is 50 bytes [29].

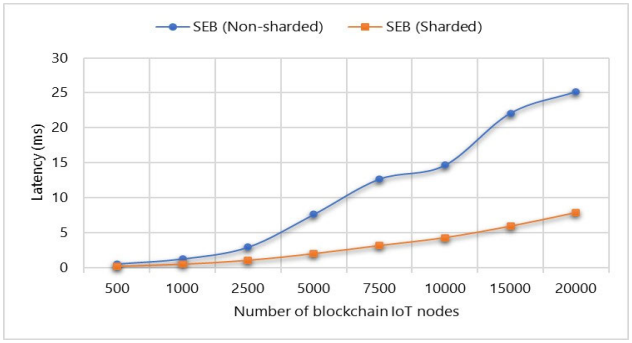


FIGURE 3. Latency comparison between SEB with sharding and without sharding for 500, 1000, 2500, 5000, 7500, 10000, 15000, 20000 IoT node.

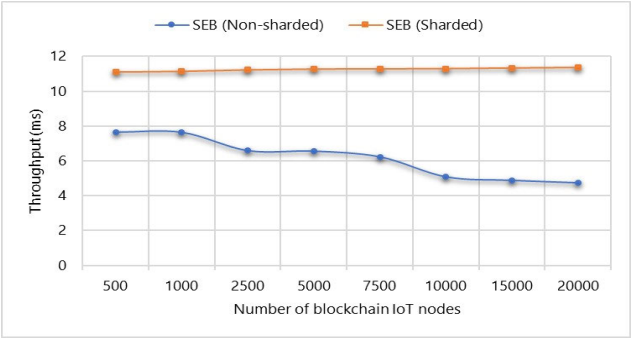


FIGURE 4. Throughput comparison between SEB with sharding and without sharding for 500, 1000, 2500, 5000, 7500, 10000, 15000, 20000 IoT nodes.

A. PERFORMANCE OF SEB DUE TO SHARDING

We evaluate the latency, throughput and resource utilization of proposed framework with sharding and without sharding.

Fig. 3 and 4 show the latency and throughput of the network with IoT nodes ranging from 500 to 20, 000 nodes. Sharding results in remarkable improvement in latency and throughput of the proposed framework.

To assess the effect of the size of the IoT network on the resource utilization, IoT nodes are varied in the range of 500 to 20, 000 for SEB framework. Figure 5 presents the bandwidth, i.e., NET, and CPU utilization of the SEB, illustrating very small changes in the bandwidth and CPU utilization with increasing size of the network.

B. COMPARISON WITH THE STATE-OF-THE-ART

Table 2 presents a comparison between SEB and [10] which utilizes PoS consensus algorithm. The comparison clearly shows the improved performance of SEB framework in terms of latency and throughput.

In Table 2 it is tabulated that the latency of accepting a single data packet increases when utilizing the PoS approach, whereas the DPoS approach exhibits less latency. This discrepancy arises from the significantly faster validation

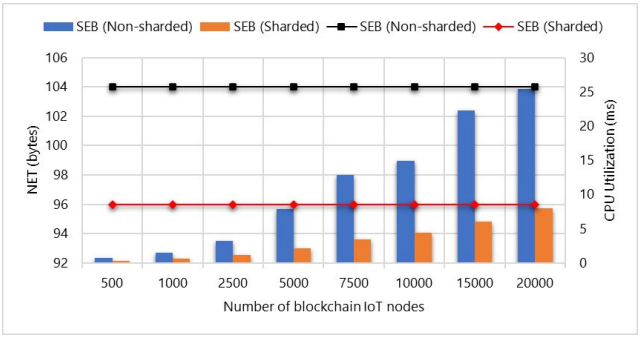


FIGURE 5. Resource utilization of SEB with sharding and without sharding for 500, 1000, 2500, 5000, 7500, 10000, 15000, 20000 IoT node.

TABLE 2. Performance comparison of PoS and DPoS consensus algorithm.

No. of BC IoT nodes	PoS [10] Latency (ms)	DPoS Latency (ms)	PoS [10] Throughput (s)	DPoS Throughput (ms)
500	55.4	0.528	1.008	7.652
1000	60.5	1.305	1.031	7.640
2500	61.5	2.984	1.034	6.586
5000	69	7.649	1.043	6.558
7500	92	12.690	1.071	6.227
10000	221	14.670	1.089	5.076
15000	2300	22.113	1.31	4.875
20000	4261	25.183	1.25	4.734

process in the DPoS approach. In this method, data packets sent by the blockchain IoT nodes are swiftly validated and added to blocks. Conversely, the PoS validation process for a single data packet experiences a longer duration, as it is not performed instantaneously. Consequently, the data packets are placed in a waiting list awaiting validation and subsequent addition to blocks thereby prolonging the validation process for each individual data packet.

In terms of system throughput, we conducted measurements on the number of successful transactions from the initial deployment of the first transaction to the completion of the last transaction in the chain [15]. In this case, transactions are the data packets sent by the blockchain IoT nodes. Throughput based on eight experimental sets with different number of blockchain IoT nodes. The results clearly demonstrate that DPoS approach consistently outperforms PoS approach across all evaluation sets.

C. IPFS STORAGE EVALUATION

SEB implementation in EOSIO is configured with 8GB memory (RAM), 2 cores (CPU) and 8MB bandwidth (NET) to evaluate the upload speed of the data to IPFS. Table 3 shows the effect of increasing file size on the upload time and speed. Upload time increases with increase in the file size; however, upload speed remains almost constant with the increase in the file size.

TABLE 3. IPFS upload time and speed.

Test	File size	Upload time	Upload speed
1	50MB	6.12s	7.85 MB/s
2	100MB	15.03s	6.74 MB/s
3	500MB	117.12s	6.53 MB/s
4	1GB	236.63s	7.28 MB/s

TABLE 4. Performance comparison with the state-of-the-art.

Parameters	[9] 2020	[13] 2020	[16] 2023	[6] 2023	[10] 2023	SEB
Consensus Algorithm	PoW /Tangle	PoW /PoA	PoC	PBFT	PoS	DPoS
TPS	-	400+	-	-	100+	4000+
Block Time	-	15s	-	-	15-20s	0.5s
Scalable	Low	High	Low	Low	Low	High
Security	High	High	High	High	High	High
Power	Low	Low	Low	Low	Low	High
Storage	Low	Low	Low	Low	Low	High

Proposed framework utilizes DPoS and sharding at edge device which result in low latency and high throughput for the blockchain enabled IoT network. Sharding allows to execute the transaction requests in parallel, whereas DPoS is computationally less demanding as compared to PoA, PoW, PoS, PoC and PBFT. Due to implementation of authentication and verification mechanism using smart contracts, SEB is secure from cyber-attacks. Finally, utilizing IPFS off-chain storage and introducing smart contracts for the storing and retrieving the data with global blockchain ensures efficient data storage and management for large sized IoT data.

D. SYSTEM COMPARISON

Implementing a blockchain-based architecture for IoT data management poses scalability challenges. To address this, our paper integrates the DPoS consensus algorithm for efficient scalability. Performance evaluations show superior results compared to existing solutions. Table 4 presents a comparison of proposed framework with blockchain enabled IoT networks based on scalability, security, efficiency and data storage and management features.

DPoS eliminates the need for high computing power, enabling a large number of IoT devices to securely join the network. Additionally, it introduces governance, allowing stakeholders to replace underperforming delegates. This mechanism supports a higher transaction volume without substantial computing power, reducing energy consumption and the carbon footprint. Our system effectively addresses scalability, enhancing security and sustainability in IoT data management.

V. CONCLUSION AND FUTURE WORK

In this paper, we propose Scalable EdgeIoT Blockchain (SEB) framework to mitigate the high latency, low throughput and data storage and management issues, due to scarce resources and high computational and storage demands, in blockchain enabled IoT networks. SEB employs edge devices and sharding for authentication and verification of IoT devices which result in high TPS, DPoS to achieve consensus which has low computational demand, IPFS to store and manage large sized data, efficiently, generated by IoT devices. The proposed framework is implemented on EOSIO blockchain platform to evaluate the performance of the framework. Experimental results show scalability and high efficiency and performance compared to the existing solutions. With reduced latency and throughput, proposed SEB is suitable for real-time applications, such as financial and healthcare industry. Moreover, low-cost is crucial for wide-spread adoption of blockchain technologies for secure and safe data management and storage for medium to large sized organizations.

The security and efficiency of the proposed SEB framework can be improved by incorporating cross-sharding communication and use of PBFT along with DPoS in critical IoT applications, such as medical and business IoT networks. In this context, cross-sharding is crucial for scalability and PBFT enables increased security level for IoT based applications.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] P. K. Kunhahamed and S. Rajak, "Application of blockchain in mining 4.0," in *Blockchain and Its Applications in Industry 4.0*, S. Namasudra and K. Akkaya, eds. Singapore: Springer Nature, 2023, pp. 123–137.

[2] R. Akkaoui, A. Stefanov, P. Palensky, and D. H. J. Epema, "A taxonomy and lessons learned from blockchain adoption within the Internet of Energy paradigm," *IEEE Access*, vol. 10, pp. 106708–106739, 2022.

[3] E. U. Haque, W. Abbasi, S. Murugesan, M. S. Anwar, F. Khan, and Y. Lee, "Cyber forensic investigation infrastructure of Pakistan: An analysis of the cyber threat landscape and readiness," *IEEE Access*, vol. 11, pp. 40049–40063, 2023.

[4] G. Bovenzi, G. Aceto, V. Persico, and A. Pescapé, "Blockchain performance in industry 4.0: Drivers, use cases, and future directions," *J. Ind. Inf. Integr.*, vol. 36, Dec. 2023, Art. no. 100513.

[5] X. Liu, H. Xie, Z. Yan, and X. Liang, "A survey on blockchain sharding," *ISA Trans.*, vol. 141, pp. 30–43, Oct. 2023.

[6] L. Gerrits, E. Kilimou, R. Kromes, L. Faure, and F. Verdier, "A blockchain cloud architecture deployment for an industrial IoT use case," in *Proc. IEEE Int. Conf. Omni-Layer Intell. Syst. (COINS)*, Aug. 2021, pp. 1–6.

[7] X. Wang, P. Yu, G. Yu, X. Zha, W. Ni, R. P. Liu, and Y. J. Guo, "A high-performance hybrid blockchain system for traceable IoT applications," in *Proc. Netw. Syst. Secur., 13th Int. Conf. (NSS)*, Sapporo, Japan. Cham, Switzerland: Springer, Dec. 2019, pp. 721–728.

[8] Y. Wu, P. Song, and F. Wang, "Hybrid consensus algorithm optimization: A mathematical method based on POS and PBFT and its application in blockchain," *Math. Problems Eng.*, vol. 2020, pp. 1–13, Apr. 2020.

[9] T. Alsboui, Y. Qin, R. Hill, and H. Al-Aqrabi, "Towards a scalable IOTA tangle-based distributed intelligence approach for the Internet of Things," in *Proc. Sci. Inf. Conf.* Springer, 2020, pp. 487–501.

[10] A. A. Maftei, A. Lavric, A. I. Petrariu, and V. Popa, "Massive data storage solution for IoT devices using blockchain technologies," *Sensors*, vol. 23, no. 3, p. 1570, Feb. 2023.

[11] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and anonymity," *J. Parallel Distrib. Comput.*, vol. 134, pp. 180–197, Dec. 2019.

[12] Y. Ren, X. Liu, P. K. Sharma, O. Alfarraj, A. Tolba, S. Wang, and J. Wang, "Data storage mechanism of industrial IoT based on LRC sharding blockchain," *Sci. Rep.*, vol. 13, no. 1, p. 2746, Feb. 2023.

[13] R. Akkaoui, X. Hei, and W. Cheng, "EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange," *IEEE Access*, vol. 8, pp. 113467–113486, 2020.

[14] A. K. Tripathi, K. Akul Krishnan, and A. C. Pandey, "A novel blockchain and Internet of Things-based food traceability system for smart cities," *Wireless Pers. Commun.*, vol. 129, no. 3, pp. 2157–2180, Apr. 2023.

[15] F. Menges, B. Putz, and G. Pernul, "DEALER: Decentralized incentives for threat intelligence reporting and exchange," *Int. J. Inf. Secur.*, vol. 20, no. 5, pp. 741–761, Oct. 2021.

[16] H.-A. Pham, N. N. Do, and N. Huynh-Tuong, "A fine-grained access control model with enhanced flexibility and on-chain policy execution for IoT systems," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 6, 2023.

[17] Z. Liu, L. Wan, J. Guo, F. Huang, X. Feng, L. Wang, and J. Ma, "PPRU: A privacy-preserving reputation updating scheme for cloud-assisted vehicular networks," *IEEE Trans. Veh. Technol.*, early access, Dec. 8, 2023, doi: 10.1109/TVT.2023.3340723.

[18] M. Kaur, S. Gupta, D. Kumar, M. S. Raboaca, S. B. Goyal, and C. Verma, "IPFS: An off-chain storage solution for blockchain," in *Proc. Int. Conf. Recent Innov. Comput. (ICRIC)*, vol. 1. Cham, Switzerland: Springer, 2023, pp. 513–525.

[19] P. Khobragade and A. K. Turuk, "On-chain off-chain blockchain model for IoT using IPFS," in *Proc. 27th Int. Conf. Adv. Comput. Commun. (ADCOM)*, 2023, pp. 30–34.

[20] S. Kummar, B. Bhushan, and S. Bhatia, "Blockchain based big data solutions for Internet of Things (IoT) and smart cities," in *New Trends and Applications in Internet of Things (IoT) and Big Data Analytics*. New York, NY, USA: Springer, 2022, pp. 225–253.

[21] J. Guo, Z. Liu, S. Tian, F. Huang, J. Li, X. Li, K. K. Igorevich, and J. Ma, "TFL-DT: A trust evaluation scheme for federated learning in digital twin for mobile networks," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 11, pp. 3548–3560, Nov. 2023.

[22] Q. Zhang and Z. Zhao, "Distributed storage scheme for encryption speech data based on blockchain and IPFS," *J. Supercomput.*, vol. 79, no. 1, pp. 897–923, Jan. 2023.

[23] L. Balduf, S. Henningsen, M. Florian, S. Rust, and B. Scheuermann, "Monitoring data requests in decentralized data storage systems: A case study of IPFS," in *Proc. IEEE 42nd Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2022, pp. 658–668.

[24] Q. Gao, J. Xiao, Y. Cao, S. Deng, C. Ouyang, and Z. Feng, "Blockchain-based collaborative edge computing: Efficiency, incentive and trust," *J. Cloud Comput.*, vol. 12, no. 1, pp. 1–13, May 2023.

[25] O. Ali, M. K. Ishak, M. K. L. Bhatti, I. Khan, and K.-I. Kim, "A comprehensive review of Internet of Things: Technology stack, middlewares, and fog/edge computing interface," *Sensors*, vol. 22, no. 3, p. 995, Jan. 2022.

[26] I. Grigg. *EOSIO-An Introduction*. Accessed: Nov. 11, 2022. [Online]. Available: https://developers.eos.io/welcome/v2.2/index

[27] E. Mehraein, Z. Ahmadian, and R. Nourmohammadi, "IGD-scorechain: A lightweight and scalable blockchain based on node sharding for the Internet of Things," Cryptol. ePrint Arch., Tech. Paper 2023/576, 2023. [Online]. Available: https://eprint.iacr.org/2023/576

[28] B. Kittinger. *EOS VM—A Low-Latency, High Performance and Extensible WebAssembly Engine*. Accessed: Nov. 15, 2022. [Online]. Available: https://github.com/EOSIO/eos-vm

[29] M. I. Hossain and J. I. Markendahl, "Comparison of LPWAN technologies: Cost structure and scalability," *Wireless Pers. Commun.*, vol. 121, no. 1, pp. 887–903, Nov. 2021.

EHTISHAM UL HAQUE received the Master of Science degree in cyber security. His academic journey reflects his diverse interests, encompassing information security, digital forensics, the Internet of Things, blockchain, artificial intelligence, and cybersecurity. His passion for exploring the intricate domains of information systems and cybersecurity positions him at the forefront of cutting-edge developments in these fields. Driven by a commitment to excellence, he stands poised to make significant contributions to the ever-evolving landscape of cybersecurity.

M. SHAMIM BAIG received the B.S. degree in avionics engineering from the College of Aeronautical Engineering (CAE), PAF Academy, the M.S. degree in industrial systems from Cranfield Institute of Technology (CIT), U.K., and the Ph.D. degree in computer science (hardware systems) from The George Washington University (GWU), Washington, DC, USA.

He is currently a qualified Lead Auditor of information security management systems (ISMSs) with British Standards Institute, U.K. He has more than 40 years of academic and research engineering management experience in the field of high-performance computing, digital system design, and AI networks/info security. He has been the Air Vice Marshal with the PAF Academy, the Principle Scientific Officer with the A. Q. Khan Research Laboratories, and the Founding Director General/the Dean of the Centre of Excellence for Cyber Security, National University of Science Technology (NUST), Islamabad. He has been a Professor and the Director of Advanced Studies Research with the Center for Advanced Studies in Engineering (CASE), Islamabad, and the PG/UG Faculty, Hitec University Taxila. He has taught the following courses at the undergraduate/graduate level in various well-reputed universities (GWU USA, CAE PAF, NUST, and CASE Hitec): parallel distributed computing (GPU/multicore/cluster, cudaC, openMP, and MPI), advanced computer networks (Python, Wireshark, and SDN), cryptography network security, reconfigurable computing (FPGA/P-SOC/HLS/systemC), DSP system design (VLIW-DSP), information coding theory, and parallel algorithm design analysis. He has published more than 36 international journals/conference papers in the field of HPC and SDNINFOSEC. His current research interest includes integrating HPC (GPU/SOC) in SDN using AI (machine/deep learning) to find innovative/efficient solutions for cloud/the IoT/cyber security applications.

Dr. Baig is a member of PEC. He has been the Chair of IEEE Educational Activities and a reviewer/the session chair of international conferences keynote/invited speaker for seminars in these fields.

ASAD AHMED received the M.Phil. and M.Sc. degrees in electronics from Quaid-i-Azam University, Islamabad, Pakistan, and the Ph.D. degree in information technology from the National University of Sciences and Technology (NUST), Islamabad, in 2022.

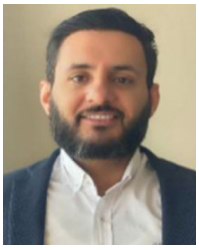
His Ph.D. thesis titled "Formal Analysis of Power Electronics Circuits Using Theorem Proving." He has significant experience in academia and industry. He was a Research Assistant with the System Analysis and Verification Laboratory (SAVe Lab), from 2013 to 2022. He was able to publish his research in well-reputed journals and conferences. His book entitled: *Formal Analysis of Future Energy Systems Using Interactive Theorem Proving* (Springer International Publishing) is the culmination of his research with SAVe Lab. Before that, he was an Instructor with the National Institute of Engineering and Technology, for four years. He was a Telecom Engineer after the M.Sc. degree in the telecom field. During the Ph.D. degree, he has published a book, three international journals, and three international conference papers. His research interests include the formal analysis and verification of safety- or mission-critical systems using formal methods techniques, i.e., model checking and theorem proving. Currently, he is interested in using state-of-the-art formal methods and techniques in the domains of power electronics, control systems, smart grids, e-health, weather forecasting, and microeconomics.

ASHFAQ AHMAD received the B.S. degree in computer science from the University of Peshawar and the M.S. and Ph.D. degrees in computer science from Abdul Wali Khan University Mardan, Khyber Pakhtunkhwa, Pakistan.

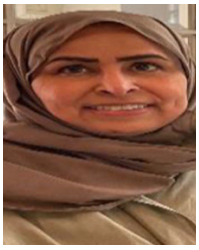
Moreover, he has more than ten years of academic and research management skills. During the Ph.D. degree, he worked in the direction of the interface of deep learning, machine learning, image processing, and some emerging data-rich areas, such as bioinformatics. He has published more than ten research articles in the reputed Q1 journals. His research interests include machine learning, deep learning, and bioinformatics. He also takes an interest in theoretically sound and empirically efficient evolutionary and machine learning algorithms to analyze, understand, and develop computational models on high volumes of multidimensional and heterogeneous data. Furthermore, he developed novel deep learning and machine learning-based models using massive sets of biological sequences for addressing a specific challenging problem by taking full advantage of domain-specific knowledge.

MASOUD ALAJMI (Member, IEEE) received the B.S. degree in electrical engineering from the King Fahad University of Petroleum and Minerals (KFUPM), in 2004, and the M.S. degree in electrical engineering and the Ph.D. degree in electrical and computer engineering from Western Michigan University, Kalamazoo, MI, USA, in 2010 and 2016, respectively.

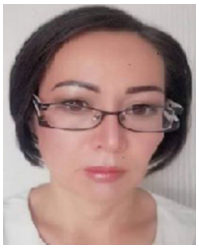
He has over four years of experience in industry. He was with Zamel and Turbag Consulting Engineers, Al-Khobar, Saudi Arabia, as an Electrical Engineer, for three months. Then, he was with Saudi Electricity Company (SEC), Abha, Saudi Arabia, where he was a Pre-Commissioning Engineer, from 2004 to 2008. During that period, he completed many training programs in the technical and administrative fields with well-known institutes. Also, he was assigned to be a commissioning leader of many projects in Saudi Arabia. He was assigned to be the SEC Representative to supervise factory acceptance tests for Siemens Company, Berlin, Germany, in 2007, and Hyundai Heavy Industries Company Ltd., Ulsan, South Korea, in 2008. From 2012 to 2015, he was a Teaching Assistant with the Electrical and Computer Engineering Department, Western Michigan University. He is currently an Associate Professor with the Computer Engineering Department, Taif University, Taif, Saudi Arabia. He has involved in various technical committees. He is the coauthor of about 30 papers in international journals and conference proceedings. His research interests include signal processing, biomedical image processing, image encryption, watermarking, steganography, data hiding, machine learning, smart grids, and renewable energy. He received the 2014–2015 Graduate Teaching Effectiveness Award from Western Michigan University for excellent teaching skills.



YAZEED YASIN GHADI received the Ph.D. degree in electrical and computer engineering from The University of Queensland. He was a Postdoctoral Researcher with The University of Queensland. He is currently an Assistant Professor of software engineering with Al Ain University. He has published more than 80 peer-reviewed journals and conference papers and holds three pending patents. His current research interests include developing novel electro-acoustic-optic neural interfaces for large-scale high-resolution electrophysiology and distributed optogenetic stimulation. He was a recipient of several awards. His dissertation on developing novel hybrid plasmonic photonic on-chip biochemical sensors received the Sigma Xi Best Ph.D. Thesis Award.



HEND KHALID ALKAHTANI (Member, IEEE) received the Bachelor of Science degree in computer science from the School of Engineering and Applied Science, The George Washington University, in1992, the Master of Science degree in information management from the Department of Engineering Management, The George Washington University, in 1993, and the first Ph.D. degree in information security from the Department of Computer Science, Loughborough University, in 2018. She is currently pursuing the second Ph.D. degree with the Information Systems Department, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University. She is an Associate Professor with the Information Systems Department, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University. She has 23 years of working experience as a lecturer, the computer center president, and the statistic center president in faculty colleges. She received the Award from SIDF Academy: Leading Creative Transformation in Critical Time Program, Stanford University, and Center for Professional Development.



AINUR AKHMEDIYAROVA received the master's degree in mathematics from Kazakh National Pedagogical University (named after Abay), in 2001, and the Ph.D. degree in information systems from the Kazakh National Technical University (named after K. I. Satbayev), in July 2018. She is currently an Associate Professor with Satbayev University. She is a specialist in the fields of mathematical modeling, data processing, information security, pattern recognition, speech recognition, system automation, and the development of various software products and software and hardware systems. She is the author of more than 70 scientific articles, three monographs, and five copyright certificates.