ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2024, March, Volume 5 Issue 1
www.ijisea.org

Enhancing Scalability and Privacy in 5G-Enabled IoT Networks through Block chain Integration and AI Solutions

Dr. Sami Al-Ghnimi[1],Dr.Shamganth Kumarapandian[2],Mr.Mohamed Haji Ali[3]
Head of Department, Department of Engineering[1,2]
Technical Instructor, Department of Engineering[3]
University of Technology and Applied Sciences - Ibra, Sultanate of Oman[1,2,3]
sami.alghnimi@utas.edu.om[1] ;shamganth.kumarapandian@utas.edu.om[2];mohamed.haji@utas.edu.om[3]

ABSTRACT

The proliferation of Internet of Things (IoT) devices in the digital landscape has ushered in a new era of connectivity, empowering billions of devices to communicate over the internet. However, the reliance on centralized protocols for data transfer poses significant security challenges. The emergence of 5G technology promises high-speed data transfer, yet it also underscores the need for robust security measures. Integrating Artificial Intelligence (AI) with 5G networks offers solutions to various challenges, including security concerns and the demand for autonomous systems like self-driving vehicles and virtual reality applications. Blockchain technology, known for its decentralized ledger system, presents an opportunity to address security and trust issues in IoT environments. However, integrating blockchain with IoT networks presents its own set of challenges, particularly in terms of throughput limitations. This paper addresses these challenges by proposing a solution that combines a Blockchain Distributed Network with the Raft consensus algorithm to enhance network scalability and throughput. Additionally, privacy concerns inherent in blockchain ledgers are addressed using zkLedger, a zero-knowledge based cryptographic solution. Through these innovations, this research contributes to the development of secure, scalable, and privacy-preserving 5G-enabled IoT networks.

Key words: Blockchain, Artificial Intelligence, Internet of Things, 5G Network, Scalability, Privacy.
Abbreviations: Blockchain (BC), Artificial Intelligence (AI), Internet of Things (IoT), 5G Network, Scalability (SC), Privacy (PR).

I.INTRODUCTION

The communication network serves as the backbone of today's digital landscape, facilitating the rapid transfer of vast amounts of data. With the proliferation of Internet of Things (IoT) devices across various sectors such as smart homes, smart cities, and aerospace, the demand for efficient connectivity is escalating. Fifth-generation (5G) networks are poised to revolutionize IoT by enabling seamless connectivity between people and a myriad of devices including sensors, vehicles, and wearables. The advent of sixth-generation (6G) networks promises even lower latency, further enhancing network capabilities.

Traditional IoT systems often rely on centralized servers and databases, leading to concerns regarding trust and vulnerability to single-point failures. Decentralized architectures offer a solution by facilitating peer-to-peer communication among network nodes, thereby mitigating trust issues. Blockchain technology, a prominent example of decentralized systems, plays a pivotal role in enhancing trust and security among network participants.

To facilitate the operation of a distributed ledger like blockchain, network peers must fulfill key functionalities including wallet services, storage, routing, and mining. Wallet services provide transaction ordering keys, while storage is essential for maintaining copies of the blockchain on each node. Routing functionality ensures efficient block and transaction propagation, while mining involves solving complex cryptographic puzzles to create new blocks. However, the integration of blockchain and IoT presents challenges related to scalability and throughput.

While blockchain holds immense potential across various domains such as drone systems, artificial intelligence, and healthcare, scalability remains a major concern. The initial blockchain implementation, notably utilized by the Bitcoin network, employs a Proof of Work (PoW) consensus mechanism characterized by low throughput and high energy consumption. While newer blockchain iterations offer higher throughput, scalability issues persist, particularly in large-scale IoT deployments.

Additionally, the expanding size of the blockchain poses challenges related to storage capacity and resource consumption. As the blockchain grows with each new block, network nodes must allocate increasing resources to accommodate the expanding chain. Despite these challenges, blockchain comprises four essential components:

1) **Decentralized Ledger:** Utilizing a distributed database, Blockchain employs nodes within the network to maintain replicated copies of the ledger. This distributed nature renders Blockchain immutable, ensuring heightened security for the stored information. New blocks containing data are only appended to the network once they have been validated by a significant portion of the network.
2) **Automated Contracts:** Blockchain incorporates the concept of smart contracts, which are programmable protocols enabling automatic execution of contracts based on predefined conditions. Leading Blockchain systems have adopted smart contracts, with Ethereum pioneering this concept. Additionally, Hyperledger, a blockchain initiative facilitating customized system implementations for enterprises, also leverages smart contracts.
3) **Enhanced Security:** Data blocks within Blockchain are interconnected using cryptographic hash functions. Altering data within a single block disrupts the hash sequence of the entire chain, making it practically infeasible to tamper with stored data.
4) **Consensus Mechanisms:** Each Blockchain employs a consensus algorithm enabling nodes to reach agreement on specific decisions. These consensus mechanisms are crucial for adding new blocks to the network in adherence to predefined rules and agreements.

The Internet of Things (IoT) encompasses a network comprising diverse electrical and electronic devices that communicate with each other via channels such as the internet. Various technologies, including radio frequency identification (RFID), sensor networks, and near field communication (NFC), facilitate this interconnectedness. Nonetheless, certain challenges exist with these IoT devices that necessitate attention:

1) **Latency:** Present-day IoT devices encounter latency issues, characterized by delays in data transfer. While latency might not significantly impact certain scenarios, such as issuing commands to appliances like washing machines or thermostats, it can pose serious challenges in applications like automated vehicles or satellites.

ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2024, March, Volume 5 Issue 1
www.ijisea.org

2) **Privacy:** IoT devices generate vast volumes of data transmitted through channels and stored in various locations. Users must trust third-party providers to store such data, raising concerns about potential data leaks.
3) **Security:** IoT devices possess limited computational power and memory resources. Traditional encryption algorithms like AES are often unsuitable for these devices, necessitating lightweight encryption schemes to ensure security.
4) **Storage:** The sheer volume of real-time data generated by millions of IoT devices presents challenges in storage. Blockchain, which typically stores transactions in blocks of 1-2 MB, faces limitations in accommodating this massive influx of data, serving as a primary bottleneck in integrating IoT devices with blockchain technology.

II.PRELIMINARY OF BLOCKCHAIN

Blockchain, originally developed for the cryptocurrency Bitcoin, has garnered global attention for its transparent and distributed nature. It operates as a distributed ledger technology, with multiple nodes maintaining a peer-to-peer network. Key attributes of blockchain include security, scalability, and decentralization, although achieving all three simultaneously remains a challenge. This challenge is known as "The Blockchain Trilemma." Decentralization, a central concept in blockchain, is often ambiguously defined. It refers to the degree of control within a system, where centralization entails control by a single entity, whereas decentralization involves shared control among multiple entities. Distribution, meanwhile, pertains to the physical dispersal of system components, indicating that they are not all located in the same place. The Bitcoin blockchain exemplifies both decentralization and distributed ledger technology(For all three types, see Figure 1).

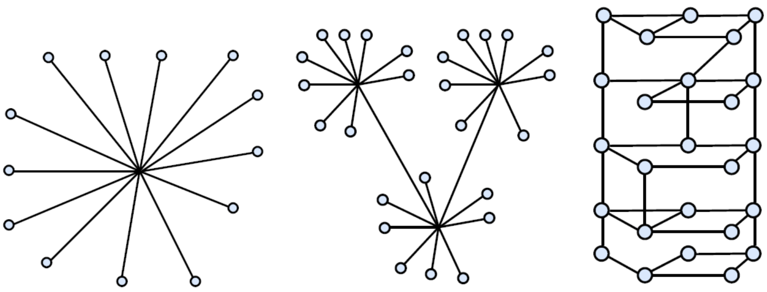

Figure 1:Shows Centralized, Decentralized and Distributed

The blockchain operates by linking together blocks of data containing information, adhering to a strictly append-only structure. While some blockchain variations diverge from this chain model, adopting a Directed Acyclic Graph (DAG) format, they are less widely adopted. The utility of blockchain extends beyond its original conception, finding applications in diverse fields such as electronic voting, supply chain management, healthcare, and digital rights management systems.

A pivotal element within the blockchain ecosystem is the smart contract. These programmable applications execute predefined tasks automatically, governed by specific terms and conditions. Unlike traditional contracts overseen by central authorities, smart contracts operate autonomously within a decentralized framework.

The overarching architecture of a blockchain system is depicted in Figure 2, illustrating various options available within each component to cater to specific requirements.

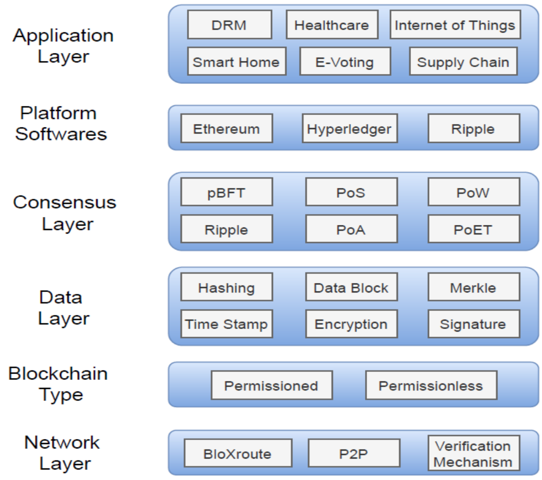

Figure 2:Shows Blockchain Architecture

DISTRIBUTED LEDGER NETWORKS: Public blockchain systems represent fully decentralized networks where any node can participate in block validation and mining activities. Termed as permissionless, these networks, exemplified by Bitcoin and Ethereum, allow unfettered access for all nodes without requiring explicit authorization. Transactions within public blockchains typically incur processing fees, serving as incentives for node participation in block creation.

CLOSED BLOCKCHAIN ENVIRONMENTS: Contrary to public blockchains, private blockchains operate as permissioned networks, restricting access to a select group of authorized nodes rather than being open to the public. Suited for single organizations or enterprise solutions, only designated nodes within the network are empowered to mine new blocks. Unlike their public counterparts, private blockchains do not impose processing fees or tokens for block publication. While offering controlled access, these networks may lack full decentralization, as demonstrated by Ripple, a prominent example of a private blockchain-based cryptocurrency.

COLLABORATIVE BLOCKCHAIN STRUCTURES: Consortium blockchains, also referred to as federated blockchains, blend characteristics of both public and private blockchain models. Combining elements of permissioned networks with participation from multiple organizations, consortium blockchains offer a hybrid approach to distributed ledger technology. Unlike public blockchains, consortium networks typically do not levy processing fees. Examples include Hyperledger and Quorum, which facilitate collaborative blockchain initiatives across diverse organizational landscapes.

The consensus mechanism is a pivotal component within blockchain systems, particularly crucial in networks lacking mutual trust among participants and devoid of central authorities.

PROOF OF WORK (PoW): PoW, the pioneering consensus protocol introduced by Bitcoin, operates in a permissionless blockchain environment. In this setup, any node can partake in network activities to generate blocks, with those responsible for block creation termed as miners. These miners engage in solving cryptographic puzzles of varying complexity, necessitating significant computational resources. Upon successful puzzle resolution, the miner broadcasts the new block to the entire network for verification. Subsequently, upon validation and addition to the blockchain, the miner receives rewards in bitcoin along with transaction fees. However, PoW is marred by its substantial computational requirements, leading to heightened energy consumption.

PROOF OF STAKE (PoS): In contrast, PoS, another permissionless blockchain protocol, replaces miners with validators. Validators, instead of puzzle-solving, directly add blocks to the network. Every validator must possess a stake in the network, requiring a deposit into the system. Validators are chosen through pseudorandom selection, with those holding larger stakes having a greater likelihood of validation. Unlike PoW, PoS demands minimal computational power for block mining, resulting in lower energy consumption. While PoS lacks direct rewards, validators receive transaction fees as incentives.

PRACTICAL BYZANTINE FAULT TOLERANCE (pBFT):pBFT, employed in permissioned blockchain systems, addresses the challenge of potential malicious nodes within the network. Byzantine Fault Tolerance (BFT) refers to the network's ability to maintain consensus even in the presence of malicious nodes disseminating false information. pBFT offers 33% Byzantine Fault Tolerance, ensuring optimal network performance as long as malicious nodes constitute less than 33% of the network.

III.BLOCKCHAIN USAGE IN 5G-ENABLED SMART INDUSTRIAL AUTOMATION

Blockchain technology finds numerous applications within 5G-enabled networks across various industries, spanning Healthcare 5.0, Autonomous Vehicles, Industry 5.0, Supply Chain Management, e-Voting, Smart Homes, among others. By integrating blockchain with 5G, significant enhancements can be achieved in both performance and security aspects, as elaborated in the preceding sections.
The utilization of blockchain within these industrial networks is outlined as follows.

HEALTHCARE 5.0: The global rise in population necessitates advancements in healthcare technology. Remote health monitoring has gained significant traction, leveraging wireless healthcare applications. Incorporating Artificial Intelligence (AI), high-speed data transmission, and intelligent devices has revolutionized the healthcare sector.

Electronic Health Records (EHR) encompass patients' information, while Personal Health Records (PHR) are specific to individual patients. EHR enables real-time patient monitoring through shared medical data. Dwivedi et al. introduced a decentralized, privacy-preserving healthcare system for IoT devices utilizing blockchain as a distributed ledger for storing healthcare events. Their approach involved an overlay network based on cloud servers for storing patient healthcare records, with the hash of cloud data stored on the blockchain. This setup ensures that any alterations to cloud data can be easily detected, as modifying even a single bit alters the hash value stored on the blockchain. Additionally, the authors proposed lightweight cryptographic algorithms to expedite network implementation.

SMART HOME: The preservation of privacy and security in the realm of the Internet of Things (IoT) poses a significant challenge, particularly in light of the widespread adoption of numerous devices. Dorri et al. conducted a case study exploring the application of blockchain technology to address security and privacy concerns within smart home environments. Their approach involved the introduction of a blockchain-based network that eschewed conventional proof-of-work mechanisms and the notion of cryptocurrencies.

Their network architecture comprised three primary components: the smart home, cloud storage, and an overlay network. The overlay network, also referred to as a peer-to-peer network, served as the backbone for the distributed architecture. To mitigate data transmission and overhead delays, nodes were organized into clusters, with each cluster electing a Cluster Head (CH) to oversee operations.

The paper discussed these concepts within the context of a smart home scenario, providing a practical illustration of their application. Additionally, the authors conducted a thorough analysis of the system's

ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2024, March, Volume 5 Issue 1
www.ijisea.org

privacy and security implications. Simulation results indicated that their approach resulted in reduced network overhead and was well-suited for IoT devices with limited resources.

SUPPLY CHAIN MANAGEMENT: Singh et al. introduced a research paper focused on enhancing supply chain management by integrating blockchain and the Internet of Things (IoT). Their aim was to combat the issue of counterfeit pharmaceuticals and ensure the proper monitoring of medication temperatures throughout the supply chain. The pharmaceutical supply chain typically comprises three key entities: manufacturers, wholesalers, and pharmacies. Their proposed solution, leveraging IoT and blockchain technologies, also encompasses the management of the cold chain process for medications.

The cold chain process in pharmaceutical distribution typically involves three essential components: cold storage facilities, cold transportation systems, and cold processing and distribution channels. Maintaining sanitary conditions during the distribution and transportation of pharmaceuticals is crucial within the cold chain. This necessitates the use of specialized containers capable of sustaining required temperatures. Consequently, a continuous monitoring mechanism is essential throughout the supply chain to ensure compliance with temperature regulations and safeguard the integrity of the medications.

INDUSTRY 5.0: In today's landscape, industries are rapidly transitioning towards full automation. This advancement in technology has ushered in a new era of production methods known as Industry 5.0, which integrates various technological facets such as Cyber-Physical Systems (CPS), Blockchain, Artificial Intelligence (AI), and the Internet of Things (IoT). Amidst intense competition, businesses are striving to minimize costs and gain competitive advantages. While adopting automated processes can yield substantial benefits, it also introduces security vulnerabilities. Within Industry 5.0, the implementation of Business Process Management (BPM) systems plays a pivotal role in automating and digitizing operations to enhance efficiency and profitability.

IV.BLOCKCHAIN FOR AI ENABLED 5G

At a high level of abstraction, blockchain represents a structured linkage of blocks using cryptographic hashes, offering transparency, consistency, and reliability. It stands as a pivotal technology in the realm of 5G networks, which herald a significant advancement in mobile telecommunications, promising speeds up to 20 times faster than current 4G technology. The latest features of 5G hold immense potential to facilitate novel business models and initiatives, fostering seamless connectivity among diverse stakeholders such as network carriers, enterprises, broadband providers, government agencies, regulators, and infrastructure suppliers.

In parallel, blockchain technology has emerged as a transformative force, disrupting various sectors across industries. It serves as a trusted, decentralized, and secure framework, extensively employed for tasks like registering, authenticating, and validating assets and transactions, managing communications, recording data, and handling identity verification across multiple parties. The integration of blockchain into 5G technology, empowered by artificial intelligence (AI), amplifies its impact and potential. Figure 3 delineates the broad scope of blockchain within AI-enabled 5G ecosystems. Below are succinct descriptions of each subcategory.

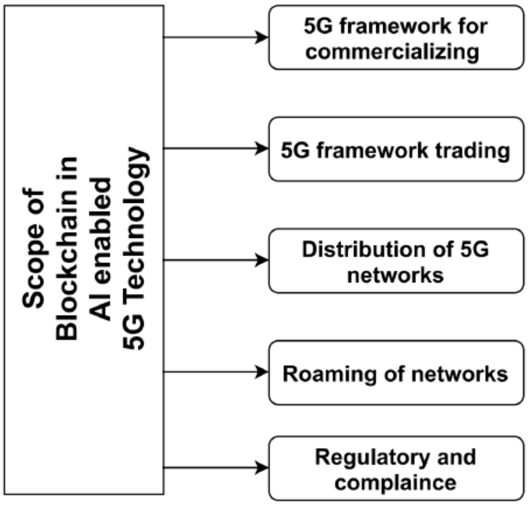

Figure 3:Shows Scope of Blockchain in AI-enabled 5G technology

5G FRAMEWORK FOR COMMERCIALIZING: Utilizing crowdsourcing can empower smaller entities within networks to establish telecommunications towers, which can become integral components of the overarching provider's infrastructure. These individual investors must undergo licensing, approval, management, and often receive immediate compensation for the utilization of their towers. The deployment of telecommunications services to specific areas can involve the independent or collective operation of dispersed cellular sites by these investors or operators.

In various geographical regions, multiple coalitions may exist, necessitating a central authority to oversee the distribution of signatures for each coalition. A pragmatic approach to registering towers, managing utilized services, and automating fees, billing, and payments through crypto tokens can be facilitated via blockchain technology and smart contracts. This decentralized approach ensures trust while ensuring transparency and traceability concurrently.

5G FRAMEWORK TRADING: The trading framework within the realm of 5G holds significant importance, facilitating the sharing of telecom services among Mobile Network Operators (MNOs). This approach involves the sharing of mobile cellular towers, either wholly or partially. Broadly, it is categorized into two types: Active and Passive trading of 5G infrastructure.

Active sharing is notably favoured due to the advent of network virtualization, as it proves to be the most efficient strategy. Under this model, MNOs share not only the physical infrastructure but also the network resources and functionalities.

On the other hand, passive sharing occurs when MNOs share infrastructure components such as the cellular tower mast, as well as ancillary facilities like rooms and cooling systems. This sharing extends to telecommunication rooms housed in separate buildings, fostering collaboration and resource optimization among operators.

DISTRIBUTION OF 5G NETWORKS: In wireless networks, the availability of bandwidth has become increasingly scarce and expensive. Typically, providers are required to pay substantial fees to spectrum regulators for access. Often, an operator acquires a sub-band or multiple sub-bands from a regulator, which can then be utilized for their own operations or leased out to other operators. To address this issue, telecommunications operators may leverage their existing infrastructure to enable new small operators to provide 5G coverage without incurring significant license fees. Furthermore, it's evident that the spectrum bands are predominantly occupied by established users, such as cable, digital radio, government systems, and satellite communications.

ROAMING OF NETWORKS: The challenge of roaming remains a significant hurdle within the telecommunications sector, necessitating intricate negotiations between brokers and third parties to establish payment and fee agreements. With the advent of 5G technology, there is a heightened interest from multiple stakeholders seeking to leverage its capabilities. These stakeholders encompass various carriers, international broker exchanges, and broker networks. Smart contracts offer a promising solution by encapsulating the terms of agreements and the intentions of all involved parties. By facilitating the recording, verification, and monitoring of all communications, smart contracts enable transparent and traceable transactions that can be audited by all parties in a cost-effective manner.

REGULATORY AND COMPLIANCE: The deployment of numerous IoT devices presents opportunities for introducing inventive business models and services to modern smartphone users. It is anticipated that 5G technology will manage these IoT devices through trusted centralized intermediaries. However, blockchain-based smart contracts offer a more efficient and practical alternative to these centralized providers. By utilizing blockchain technology, tasks can be decentralized, ensuring high levels of trust, transparency, regulatory compliance, and automated payment processing.

V.CHALLENGES IN IOT-BLOCKCHAIN INTEGRATION

This section delves into the significant hurdles that arise when integrating blockchain with IoT systems. Originally crafted for digital currency, blockchain technology emerged with Bitcoin as its pioneering platform. However, the conventional setup of blockchain, tailored for powerful computer nodes, doesn't align well with the realities of IoT networks, which predominantly consist of resource-constrained devices. The integration poses several challenges:

SCALABILITY IN STORAGE AND THROUGHPUT: One of the primary challenges in merging blockchain with IoT is ensuring scalability in both storage and throughput. In systems like Bitcoin, throughput is gauged by transactions per second (TPS), with Bitcoin averaging around 2.5-3.5 TPS and Ethereum around 12-15 TPS. Contrastingly, the sheer volume of IoT devices, estimated at 20.4 billion by 2020, demands significantly higher throughput to handle the data generated. Additionally, blockchain's inherent design isn't optimized for storing large datasets, with typical block sizes being mere megabytes, whereas IoT systems can churn out gigabytes (GBs) of data per second.

PRIVACY AND ANONYMITY CONCERNS: Many IoT applications necessitate data privacy, especially for sensitive information such as health records. Take, for instance, remote patient monitoring scenarios where wearable IoT devices transmit data to healthcare providers. The challenge here lies in ensuring privacy on a public blockchain network, a concern already acknowledged and debated. Cryptocurrencies like Monero utilize ring signatures to safeguard user privacy. However, ensuring privacy for resource-constrained IoT devices is more intricate, as standard cryptographic algorithms might not be feasible in such scenarios.

AGREEMENT: Given the resource constraints of IoT devices, conventional consensus algorithms like Proof of Work (PoW) are impractical due to their reliance on high computational power, which is not feasible for IoT devices. While various consensus proposals exist, they lack standardization and require validation for IoT applications. A significant challenge in resource-limited IoT environments is the mining process. One potential solution is off-chain processing, although this necessitates moving data outside the blockchain to reduce latency. Additionally, the energy-intensive nature of PoW-based blockchains renders them unsuitable for IoT devices.

NETWORK SCALABILITY: Several consensus algorithms have been proposed to enhance blockchain throughput, yet their effectiveness is hindered by network limitations. For a truly distributed ledger, each added block must be validated by the maximum number of nodes in the network. However, the slow propagation speed of the network results in delays in block verification. Accelerating the propagation of transactions and blocks throughout the network would expedite mining and block verification processes. Enhancing network scalability requires all nodes to efficiently propagate blocks, a task that poses significant challenges in a public network setting. Many IoT applications necessitate data privacy, especially for sensitive information such as health records. Take, for instance, remote patient monitoring scenarios where wearable IoT devices transmit data to healthcare providers. The challenge here lies in ensuring privacy on a public blockchain network, a concern already acknowledged and debated. Cryptocurrencies like Monero utilize ring signatures to safeguard user privacy. However, ensuring privacy for resource-constrained IoT devices is more intricate, as standard cryptographic algorithms might not be feasible in such scenarios.

V.CHALLENGES IN IOT-BLOCKCHAIN INTEGRATION

A SCALABLE BLOCKCHAIN DISTRIBUTION NETWORK (BDN): The Blockchain Trilemma poses a significant challenge for blockchain systems, as it involves three crucial components: scalability, decentralization, and security. Achieving all three simultaneously is difficult. Scalability refers to the network's capacity to handle growth. For instance, while Bitcoin boasts robust security with around 6 million users, its throughput and latency performance are subpar. Latency in a blockchain context refers to the time taken from submitting a transaction to its confirmation. When a miner adds transactions to a block, other network nodes validate it. The addition of a new block necessitates communication between nodes, making network communication capacity crucial. Peer-to-peer networks comprise nodes with varying computational speeds, including both fast and slow nodes. Slow nodes can impede data propagation within the network. To address scalability challenges, bloXroute, a Blockchain Distribution Network (BDN), has been developed as a global network aimed at enhancing scalability.

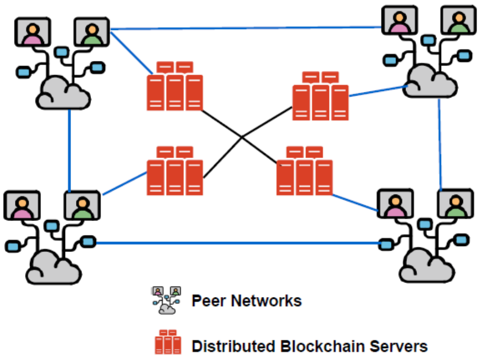

Figure 4:Shows Blockchain Distribution Network (BDN)

DISTRIBUTED LEDGER SOFTWARE: Hyperledger Fabric, developed within the Linux Foundation, is an open-source distributed ledger technology (DLT) that operates within permissioned networks. One of its notable features is its support for pluggable consensus protocols, allowing for flexibility in consensus mechanisms based on specific requirements. Presently, Fabric utilizes the Raft consensus protocol, primarily suitable for single enterprises where only trusted nodes participate. However, Raft lacks Byzantine fault tolerance, which is essential for scenarios involving untrusted nodes, such as public blockchains. In such cases, Byzantine fault-tolerant consensus mechanisms like Practical Byzantine Fault Tolerance (pBFT) are more appropriate.

Privacy concerns are inherent in blockchain systems, and Hyperledger Fabric addresses this through its channel architecture. Channels enable different subnetworks to maintain privacy by segregating transaction information. For instance, if a subnetwork wishes to restrict access to its data from other subnetworks, Fabric facilitates this by creating separate channels. Members within one channel are unable to view transaction details from other channels, thereby enhancing privacy and confidentiality.

CONSENSUS MECHANISM (RAFT): Consensus entails reaching an agreement among various peers or servers within a network regarding specific values or decisions. Once a consensus is achieved among these network participants, the decision is considered final. This process typically requires the majority of peers to be operational; for instance, in a network with 5 nodes, if 3 nodes reach an agreement while the other 2 are inactive, the network can proceed with the active nodes.

In the proposed framework, we advocate for implementing Raft consensus within Hyperledger. Raft is particularly suitable for smaller, private networks due to its ability to deliver high throughput. However, for scaling the network to accommodate a larger number of nodes, bloXroute servers can be integrated alongside Raft or any other consensus mechanism.

Raft consensus operates by maintaining a replicated log across all nodes. This log adheres to the blockchain data structure, wherein data can only be appended. The consensus process involves three types of nodes: Leader, Follower, and Candidate. These nodes dynamically transition between roles, and any node can assume the role of a leader through a voting process. Write requests are directed to the leader, who subsequently disseminates them to the follower nodes.

DISTRIBUTED DATABASE NETWORK:

Storing gigabytes (GBs) of data generated by IoT devices on a continuous basis presents significant challenges. Cloud storage emerges as the primary solution due to its scalability and accessibility. However, to achieve the benefits of a distributed database, the proposed framework incorporates the concept of data sharding. Here's how the distributed database network operates:

a) Data Storage: The data generated is fragmented into multiple chunks, a process known as data sharding. Let's assume the data is divided into n pieces, with only k (where $k < n$) fragments necessary to reconstruct the original file. To compromise the data, an attacker would require access to the secret key for all k files, each stored on distinct and randomized storage nodes. Metadata is generated for all these fragments, akin to Shamir's Secret Sharing Scheme developed by Adi Shamir in 1952. In this scheme, a secret is divided into multiple parts, with each part distributed to different participants. To reconstruct the secret, a minimum number of parts is essential.
b) Data Retrieval: Utilizing the metadata, the client or user can easily determine the locations of previously stored fragments. It's unnecessary to pinpoint all n fragments scattered across various locations; instead, a predefined threshold, say k, is established. Original data can be retrieved by utilizing k fragments out of n stored within the client's computer system.
c) Data Maintenance: This technology ensures data retrieval even if some storage nodes malfunction or certain fragments become corrupted. The original data can be reconstructed with the minimum number of fragments required for message reconstruction, thus ensuring data integrity and availability.

DISTRIBUTED DATABASE NETWORK: The negative aspect of the Internet of Things (IoT) lies in the breach of user privacy. Many IoT users are unaware of the implications of data privacy, leading them to unwittingly forfeit their privacy and data ownership. Consider when you visit a website; typically, you encounter a lengthy privacy policy that users often disregard, simply accepting the terms and conditions. This acceptance necessitates sharing personal details like location and contact information. However, these seemingly innocuous data points hold significant monetary value. Companies or organizations gather such data for their own gain, subsequently selling them in data markets. For instance, health data collected through sensors or wearable devices is particularly valuable, with the collecting entity often selling it without your knowledge or consent.

Furthermore, IoT devices and networks are increasingly vulnerable to cyber-attacks, making them prime targets for cybercriminals. This vulnerability compromises both the security and privacy of IoT user data. A recent threat report by security firm Symantec highlighted a staggering 600% increase in IoT attacks within a single year. In 2016, there were 6,000 reported attacks, whereas in 2017, this figure skyrocketed to 50,000. Notably, a significant portion of these attacks originates from China, comprising approximately 21%, followed by the USA (around 11%), Brazil (about 7%), and Russia (roughly 6%).

VI.CONCLUSION

In the 5G era, the fusion of blockchain technology with the Internet of Things (IoT) holds significant importance. This study explores diverse opportunities and industrial applications arising from 5G-enabled IoT devices, including but not limited to supply chain management, e-voting systems, Industry 5.0 initiatives, and smart home automation. Additionally, it addresses the primary challenges associated with integrating blockchain into IoT devices, such as scalability concerns related to storage, throughput, and network infrastructure, as well as privacy issues.

To tackle these challenges, a novel framework is proposed. It resolves network scalability limitations through the implementation of a Blockchain Distributed Network (BDN) and addresses throughput constraints by adopting the Raft consensus mechanism. Detailed solutions are provided to effectively address the integration hurdles between blockchain and IoT technologies.

Privacy emerges as another critical issue within blockchain systems. To mitigate privacy concerns, the proposed framework incorporates a ZK Ledger, which relies on Zero-Knowledge Proof techniques. Zero-Knowledge Proof represents a burgeoning area within computer science, still undergoing extensive research to resolve various unsolved challenges.

VII.DISCUSSIONS

Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions. Authors are strongly encouraged not to call out multiple figures or tables in the conclusion—these should be referenced in the body of the paper.

ACKNOWLEDGEMENT(S)

We would like to express our sincere gratitude to all those who have contributed to the completion of this research paper. Special thanks to our department support throughout the research process. Additionally, we extend our appreciation to the institutions and organizations that provided resources and facilities essential for this study. Lastly, we thank our friends and family for their unwavering encouragement and understanding during this endeavor.

REFERENCES:

1. Gupta R, Shukla A, Tanwar S. BATS: A Blockchain and AI-empowered Drone-assisted Telesurgery System towards 6G. IEEE Transactions on Network Science and Engineering 2020: 1-1. doi: 10.1109/TNSE.2020.30432622.
2. Singh SK, Rathore S, Park JH. BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence. Future Gener. Comput. Syst. 2020; 110: 721–743. doi: 10.1016/j.future.2019.09.002
3. Qu Y, Gao L, Luan TH, et al. Decentralized Privacy Using Blockchain-Enabled Federated Learning in Fog Computing. IEEE Internet of Things Journal 2020; 7(6): 5171-5183. doi: 10.1109/JIOT.2020.2977383
4. Srivastava G, Dwivedi AD, Singh R. Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology. in Samarati and Obaidat56: 674–679
5. Singh R, Dwivedi AD, Srivastava G. Internet of Things Based Blockchain for Temperature Monitoring and Counterfeit Pharmaceutical Prevention. Sensors 2020; 20(14): 3951. doi: 10.3390/s20143951
6. Wu H, Dwivedi AD, Srivastava G. Security and Privacy of Patient Information in Medical Systems Based on Blockchain Technology. ACM Trans. Multimedia Comput. Commun. Appl. 2021; 17(2s). doi: 10.1145/3408321
7. Dwivedi AD, Singh R, Dhall S, Srivastava G, Pal SK. Tracing the Source of Fake News using a Scalable Blockchain Distributed Network. In: IEEE; 2020: 38–43
8. Kaushik K, Dahiya S, Singh R, Dwivedi AD. Role of Blockchain in Forestalling Pandemics. In: IEEE; 2020: 32–37
9. Garba A, Dwivedi A, Kamal M, et al. A digital rights management system based on a scalable blockchain. Peer-to-Peer Networking and Applications 2020(Special Issue on Blockchain for Peer-to-Peer Computing). This article is part of the Topical Collection: Special Issue on Blockchain for Peer-to-Peer Computing Guest Editors: Keping Yu, Chunming Rong, Yang Cao, and Wenjuan Lidoi: 10.1007/s12083-020-01023-z
10. Ethereum white paper. .
11. Androulaki E, BargerA, BortnikovV, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. in Oliveira et al. 57: 30:1–30:15
12. Liu CH, Lin Q, Wen S. Blockchain-Enabled Data Collection and Sharing for Industrial IoT With Deep Reinforcement Learning. IEEE Transactions on Industrial Informatics 2019; 15(6): 3516-3526. doi: 10.1109/TII.2018.2890203
13. Giordani M, Polese M, Mezzavilla M, Rangan S, Zorzi M. Towards 6G Networks: Use Cases and Technologies. CoRR 2019; abs/1903.12216.
14. Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for 5G and Beyond Networks: A State of the Art Survey.CoRR 2019; abs/1912.05062.
15. Shen M, Tang X, Zhu L, Du X, Guizani M. Privacy-Preserving Support Vector Machine Training Over Blockchain-Based Encrypted IoT Data in Smart Cities. IEEE Internet of Things Journal 2019; 6(5): 7702-7712. doi:10.1109/JIOT.2019.2901840
16. Wu J, Dong M, Ota K, Li J, Yang W. Application-Aware Consensus Management for Software-Defined IntelligentBlockchain in IoT. IEEE Network 2020; 34(1): 69-75. doi: 10.1109/MNET.001.1900179
17. Hewa T, Gür G, Kalla A, Ylianttila M, Bracken A, Liyanage M. The Role of Blockchain in 6G: Challenges, Opportunitiesand Research Directions. In: IEEE; 2020: 1–5

18. Alsharif MH, Kelechi AH, Albreem MA, Chaudhry SA, Zia MS, Kim S. Sixth Generation (6G)Wireless Networks: Vision,Research Activities, Challenges and Potential Solutions. Symmetry 2020; 12(4). doi: 10.3390/sym12040676
19. Mistry I, Tanwar S, Tyagi S, Kumar N. Blockchain for 5G-enabled IoT for industrial automation: A systematicreview, solutions, and challenges. Mechanical Systems and Signal Processing 2020; 135: 106382. doi:https://doi.org/10.1016/j.ymssp.2019.106382
20. Qu Y, Pokhrel SR, Garg S, Gao L, Xiang Y. A Blockchained Federated Learning Framework for Cognitive Computingin Industry 4.0 Networks. IEEE Transactions on Industrial Informatics 2021; 17(4): 2964-2973. doi:10.1109/TII.2020.3007817
21. Gupta R, Kumari A, Tanwar S. Fusion of blockchain and artificial intelligence for secure drone networking underlying 5Gcommunications. Trans. Emerg. Telecommun. Technol. 2021; 32(1). doi: 10.1002/ett.4176
22. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. 2008.
23. Srivastava G, Dwivedi AD, Singh R. PHANTOM Protocol as the New Crypto-Democracy. in Saeed and Homenda58:499–509
24. Ghode D, Yadav V, Jain R, Soni G. Adoption of blockchain in supply chain: an analysis of influencing factors. J. Enterp.Inf. Manag. 2020; 33(3): 437–456. doi: 10.1108/JEIM-07-2019-0186
25. Srivastava G, Dwivedi AD, Singh R. Automated Remote Patient Monitoring: Data Sharing and Privacy Using Blockchain.CoRR 2018; abs/1811.03417.
26. Dwivedi AD. A Scalable Blockchain Based Digital Rights Management System. IACR Cryptol. ePrint Arch. 2019; 2019:1217.
27. Ripple. .
28. Androulaki E, Barger A, Bortnikov V, et al. Hyperledger Fabric: A Distributed Operating System for PermissionedBlockchains. CoRR 2018; abs/1801.10228.
29. Quorum. .
30. Singh R, Dwivedi A, Srivastava G, Wiszniewska-Matyszkiel A, Cheng X. A game theoretic analysis of resource miningin blockchain. Cluster Computing: The Journal of Networks, Software Tools and Applications 2020. doi: 10.1007/s10586-020-03046-w
31. Srivastava G, Dhar S, Dwivedi AD, Crichigno J. Blockchain Education. in 2019 IEEE Canadian Conference of Electricaland Computer Engineering, CCECE 2019, Edmonton, AB, Canada, May 5-8, 201959: 1–5
32. Proof of Stake. .
33. Castro dMOT. Practical Byzantine fault tolerance. PhD thesis. Massachusetts Institute of Technology, Cambridge, MA,USA, 2000.
34. D. Schwartz NY, Britto A. The Ripple protocol consensus algorithm. 2000.
35. Popov S. The tangle. .
36. Ben-Sasson E, Chiesa A, Garman C, et al. Zerocash: Decentralized Anonymous Payments from Bitcoin. in 2014 IEEESymposium on Security and Privacy, SP 2014, Berkeley, CA, USA, May 18-21, 201460: 459–474
37. Litecoin: An open source P2P digital currency. .
38. Dwivedi AD, Srivastava G, Dhar S, Singh R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. Sensors2019; 19(2). doi: 10.3390/s19020326
39. Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: The case study of a smart home.In: IEEE; 2017: 618–623
40. Singh R, Dwivedi AD, Srivastava G. Internet of Things Based Blockchain for Temperature Monitoring and CounterfeitPharmaceutical Prevention. Sensors 2020; 20(14). doi: 10.3390/s20143951
41. "The Internet of Things (IoT) - An Overview" - https://www.internetsociety.org/issues/iot/
42. "5G Technology Overview" - https://www.qualcomm.com/invention/5g/what-is-5g
43. "Artificial Intelligence (AI) - A Primer" - https://www.ibm.com/cloud/learn/ai
44. "Blockchain Technology Explained" - https://www.investopedia.com/terms/b/blockchain.asp

45. "Challenges and Opportunities in Integrating Blockchain with IoT" - https://www2.deloitte.com/us/en/insights/industry/financial-services/blockchain-in-iot-applications.html
46. "Raft Consensus Algorithm Explained" - https://raft.github.io/
47. "Scalability Solutions for Blockchain Networks" - https://ethereum.org/en/developers/docs/scalability/
48. "zkLedger: A Zero-Knowledge Cryptographic Solution" - https://zkledger.org/
49. "Privacy Concerns in Blockchain Technology" - https://www.privacy-concerns.org/blockchain-privacy/
50. "Secure and Scalable IoT Networks: Research Trends and Challenges" - https://ieeexplore.ieee.org/document/9144519.

IJISEA
Original Papers

www.ijisea.org