Adoption of Blockchain With 5G Networks for Industrial IoT: Recent Advances, Challenges, and Potential Solutions

MANPREET KAUR1,2, MOHAMMAD ZUBAIR KHAN3,4, SHIKHA GUPTA1, and ABDULLAH ALSAEEDI5

1Department of Computer Science and Engineering, University Institute of Engineering, Chandigarh University, Gharuan, Mohali, Punjab 140413, India
2Department of Computer Science and Engineering, Guru Nanak Dev Engineering College, Ludhiana, Punjab 141006, India
3Department of Computer Science and Information, Taibah University, Medina 42353, Saudi Arabia
4Department of Computer Science and Engineering, Invertis University, Bareilly 243123, India
5Department of Computer Science, College of Computer Science and Engineering, Taibah University, Medina 42353, Saudi Arabia

Corresponding authors: Manpreet Kaur (preetmand@gmail.com) and Mohammad Zubair Khan (mkhanb@taibahu.edu.sa)

ABSTRACT
It has been proven that Internet of Things (IoT) platforms can improve the performance and efficiency of a wide range of processes. With the acceptance of IoT as a major part of the technology of Industry 4.0, the notion of leveraging the Internet in industries to enable automation and reconfigure existing industrial processes has greatly evolved. By introducing smart technology and intelligent processes, the Industrial Internet of Things (IIoT) is committed to bringing high operational efficiency, enhanced productivity, and effective management to industrial assets. Despite this, the reliance of IIoT on central architecture presents numerous challenges, including the security and maintenance of smart devices, privacy issues owing to third-party participation, and massive computations conducted by a central entity, all of which prevent its widespread adoption in businesses. Emerging blockchain technologies have the potential to transform IIoT platforms and applications. A distributed and decentralized approach followed by blockchain might offer interesting solutions to the challenges raised by IIoT. Furthermore, 5G networks are expected to deliver excellent solutions to meet the demands of decentralized systems, with a focus on application-specific vulnerabilities. Blockchain and IIoT, enabled by 5G, is a viable option to fully explore the potential of contemporary industry. In this context, this article analyzes and examines recent achievements to highlight the major obstacles in blockchain–IIoT convergence and presents a framework for potential solutions. A well-organized literature review by analyzing the existing work in three primary areas: blockchain consensus algorithms used in existing IoT and IIoT applications, blockchain for 5G-enabled IoT networks, and blockchain in industry have been performed, with major findings summarized in each area. Directions for the future are also provided and intend to assist researchers in understanding the full potential of these innovations.

INDEX TERMS
Blockchain, IIoT, Industry 4.0, IoT, 5G.

I. INTRODUCTION
The Internet of Things (IoT) is a network of smart devices and machines that are able to gather data from their surroundings via sensing devices, communicate with other devices in the web, and respond automatically without the need for human contact [1]. The Industrial Internet of Things (IIoT) is an IoT-enabled industrial production system that delivers productivity and financial benefits relating to system implementation, ease of maintenance, growth capability, and interoperability [2]. By automating smart devices for monitoring, recording, analyzing, and exchanging real-time information in industrial systems, IIoT serves as a new vision of IoT in the industrial sector [3]. IIoT could be formally defined as follows [3]: “Industrial IoT (IIoT) consists of a network of smart and extensively coupled industrial elements that are used to attain high production rates while cutting operational expenses through real-time monitoring, optimal management and control of industrial processes, assets, and administrative time.” IIoT is a subset of IoT that requires
increased safety standards, increased protection levels, and more reliable communication without affecting significant industrial processes [3]. The terms Industry 4.0 and IIoT are used to describe the industrial applications of IoT. In reality, Industry 4.0, IIoT, and IoT are all interconnected, although they differ significantly, with IoT being consumer-oriented and IIoT being industry-oriented. When the IoT paradigm is combined with cyber-physical systems (CPSs), Industry 4.0 emerges [4].

IoT serves a variety of various industrial applications to enhance operational efficiency, rate of production, and product quality and to minimize machine breakdown. IoT has several features, such as the decentralization of its systems, its variety of devices, and the heterogeneity of its data. These characteristics have resulted in certain difficulties, such as IoT system heterogeneity, poor interoperability, the resource-restricted nature of IoT devices, and security concerns. Blockchain is a distributed database that is shared by all nodes in a network. Every node in a network has an identical copy of this database, and any changes to the database are mirrored in all copies. A blockchain may simply be viewed as a linked list of blocks, with each block cryptographically connected to the one before it to ensure its immutability. Blockchain, through the use of a consensus mechanism, allows a transaction to take place and be approved in a mutually decentralized environment without the involvement of a third party. Every block contains a number of transactions validated using cryptographic techniques, such as asymmetric encryption algorithms, digital signatures, and hashing functions by dedicated nodes known as miners. This ensures that every node in this distributed ecosystem is up to date with the current version of the database. Any attempt to change a block or its transactions would violate its integrity and make that block invalid. With these features, blockchain could be considered as a perfect complement to the challenges of IoT. In this paper, we provide multiple reasons why Industrial IoT should be coupled with blockchain. Although the integration of blockchain and IIoT has potential challenges, the true worth of both innovations can never be reached without solving such challenges. Therefore, several solutions are also presented in this context.

A. INDUSTRY 4.0

Industry 4.0 is a significant topic in IIoT discussions. Industry 4.0 was the fourth industrial revolution, initially recognized in Germany, and attracted popularity throughout the world afterward [18]. Industry 4.0 refers to the mixture of several Internet technologies, including IoT, big data analytics, artificial intelligence, blockchain, and so on, to optimize the productivity and efficiency of existing systems [18]. Industry 4.0 particularly focuses on the safety and security of manufacturing processes [8]. Industry 4.0 is a sub-domain of IIoT that refers to the incorporation of the IoT idea into smart manufacturing.

1) KEY ELEMENTS OF INDUSTRY 4.0

The key elements of Industry 4.0 are shown in Fig.1 and described briefly below:

- Cyber-physical systems: These are physical devices operated by system-generated algorithms that sense, monitor, and control physical processes and create virtual replicas [5].
- IoT: This is emerging technology that allows communication between the physical objects surrounding us (e.g., a home, car, etc.) [6].
- IoS (Internet of Services): The core idea of this system involves the division of sections into components. Each of these may subsequently convert a product or component into a service of value to a customer [7]. In other words, it is a combination of web- and service-oriented architecture [5].
- Big data analytics: Classical tools and techniques are inadequate for collecting, processing, and analyzing massive amounts of data generated daily by digital operations. Big data analytics is a digital tool for analyzing and extracting useful information under Industry 4.0.
- Cloud computing: This is technology that allows storage and computing resources to be made accessible to customers based on their needs without adding an extra maintenance burden. It is a worldwide network for on-demand resource sharing that allows data storage and processing via remote servers and that is accessible via the web. Hence, businesses with limited storage and computing resources could utilize this technology to improve their productivity levels.
- Augmented reality: The concepts of Industry 4.0 are quite similar to those of industrial augmented reality. Augmented reality is a technique used by industrialists to empower their employees and provide visual training skills to workers in an industrial unit to complete a complex task efficiently and quickly. This undoubtedly enhances process accuracy and reduces the likelihood of fault occurrence. Although IoT, IIoT, and Industry 4.0 are all interconnected, the terms cannot be used interchangeably. IoT could be
FIGURE 2. Paper structure.

referred to as a “web for machines,” emphasizing the purpose of permitting objects to share data. In contrast, IIoT is concerned with connecting all industrial assets, such as machines and control systems, to various information systems and business procedures [8].

B. INDUSTRY 5.0
The main goal of Industry 4.0 is to increase productivity and efficiency by implementing digital technologies that reduce human involvement and enable process automation. Industrial 5.0, on the other hand, is a new revolution in the industrial sector that focuses on allowing humans to collaborate with robots and smart equipment to complete complex tasks in a better and quicker way by using modern technologies such as IoT and big data. Because robots are considerably more precise and efficient at doing tasks, they cannot reason in the same way as humans. Hence, Industry 5.0 acknowledges the necessity for humans to help or oversee robots to make more tailored products. Industry 5.0 allows for the blending of powerful and precise machinery with human cognitive thinking to promote productive and sustainable manufacturing. The key distinctions between Industry 4.0 and Industry 5.0 are presented in Table 1.

C. OUR CONTRIBUTIONS
To the best of our knowledge, no single work has addressed the integration of blockchain and IIoT developed with 5G networks. As a result, this work was carried out with a strong emphasis on blockchain for 5G networks combined with Industry 4.0 and IIoT. The main contribution of this paper is 1) to provide the sound background of Industrial IoT, its architecture, and its challenges, 2) to identify the key differences between Industry 4.0 and Industry 5.0, 3) to provide a summary and direction for the potential future of existing research done in this context, 4) to introduce the application of 5G networks in blockchain with IIoT, 5) to outline the technical challenges and potential solutions in the integration of blockchain and IIoT, and 6) to discuss the insights of existing applications and the future direction required to address the difficulties faced.

D. PAPER ORGANIZATION
The paper is structured with six sections, as depicted in Fig. 2, with Section 1 providing in-depth introductions for IoT, IIoT, Industries 4.0 and 5.0, and blockchain technology. Section 2 discusses the existing literature and outlines the summary of major findings and expected future direction. Section 3 describes the role of blockchain and its structure,
working, and types. Section 4 discusses Industrial IoT, the key differences between IoT and IIoT, IIoT architecture, and the issues involved in IIoT implementation. Section 5 is the core of this paper and provides the scope of the convergence of blockchain and IIoT, the challenges involved in this convergence, and their potential solutions. Finally, Section 6 concludes the paper by listing the outcome of this work as well as direction for future work.

II. LITERATURE REVIEW

This section is a brief review of the existing work done in the field of the integration of blockchain and IIoT. We analyzed the existing literature through three areas: the blockchain consensus algorithms used in existing IoT and IIoT applications, blockchain for 5G-enabled IoT networks, and blockchain in industry. The following subsections explore the literature in these key areas.

A. BLOCKCHAIN CONSENSUS MECHANISMS IN EXISTING IoT/IIoT APPLICATIONS

The consensus algorithm is an essential component of every blockchain application. Before incorporating blockchain into industry, one should exercise extreme caution in selecting the optimal consensus algorithm for a certain application. Many consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), Proof of Activity (PoA), and so on, already exist in the blockchain domain. The widely used consensus algorithms, such as PoW, require a large amount of processing to solve mathematical puzzles; however, owing to the resource constraints of IoT devices, conventional consensus methods are inappropriate. Therefore, there is a marked need to overview the existing blockchain-IoT systems to assess the performance of the consensuses used. Wang et al. [9] created the PoRX reputation-based incentive scheme to distinguish between honest and dishonest nodes. Based on the behavior of nodes, a reward and punishment mechanism was created and a credibility-based equity-proof consensus method was proposed. Zhang et al. [2] devised a lightweight consensus protocol to enable a secure network for data transport, specifically for IIoT. The simulation results achieved great data accuracy while maintaining the IIoT system’s stability and resilience. Mansoor et al. [10] discussed the concept of blockchain and its applications in the IoT infrastructure and the use of federated learning for better privacy and data administration. The blockchain and IoT architectures have already been presented. Because the consensus mechanism in use necessitates many computations, a good consensus algorithm is still needed for blockchain-enabled federated learning. The necessity for blockchain collaboration in IoT and IIoT applications was recognized by Sengupta et al. [11]. The authors explored how this integration may be used to address major security problems in conventional systems. Farahani et al. [12] covered all major elements of Blockchain-IoT, with an emphasis on IoT eHealth, and highlighted its prospects, uses, solutions, and current architectures, and analyzed its significant barriers for a more thorough study of this rapidly-developing area. Wu et al. [13] thoroughly examined the relationship between blockchain and machine learning in IIoT through three important topics: consensus protocol, storage, and communication. The presented work provided an extensive understanding of the privacy issues of blockchain components that will aid in the development of more practical blockchain-enabled solutions for Industrial IoT. The current Merkle tree storage structure in IIoT systems with non-homogeneous devices cannot improve the verification performance for transactions that require frequent verification. To solve the aforementioned issue, Wang et al. [14] presented an enhanced Merkle tree structure for efficient transaction verification in reliable blockchain-enabled IIoT systems. Decentralization, security, and energy consumption are the three major problems faced by blockchain consensus methods that cannot be improved synchronously. Using a consistent hash algorithm, Yu et al. [15] described two novel blockchain consensus protocols: “CHB-consensus” and “CHBD-consensus”. Guan et al. [16] developed a concept of a blockchain-based energy trading system (BCE-ETS) to solve the issues of centralized energy systems. The design objectives of this model included privacy protection, efficiency, and security. Wang et al. [17] explored the blockchain consensus technique’s credibility problem to meet IoT system security requirements. They suggested a reputable-based consensus process with incentives and penalties. If nodes behave well, they receive reputable rewards, and if they do not, they receive reputable punishments. The suggested consensus technique was shown to be highly secure and resistant to threats in an investigation by the authors. Doku et al. [18] solved the problem of existing PoW algorithms in resource-limited IoT devices by grouping the resources of a cluster of IoT devices together to solve computation-intensive tasks or puzzles that lone IoT devices cannot accomplish. Bandara et al. [19] deployed a microservice architecture known as Tikiri—a blockchain-enabled system for resource-constrained IoT devices. It was built in the Hyperledger Fabric and Mystiko blockchain platforms. One of the main features of the proposed architecture was full-text search capability. Huang et al. [20] emphasized that high energy consumption and low throughput restrict the usability of blockchain systems in IoT applications. As a result, a credit-based PoW consensus method was introduced to increase system security and efficiency by lowering the energy needs for honest nodes. The prototype was implemented using a directed acyclic graph structure. The authority management has protected the privacy of IoT devices. Dey et al. [21] described the application of blockchain in agriculture to maximize resource usage and empower decision-making, resulting in smart farming and a sustainable agriculture system. In private blockchain, the Raft consensus method has been found to offer data security in transactions. Fair data sharing concepts and a blockchain-IoT framework for e-agriculture were proposed. A summary of the literature review of blockchain consensus mechanisms in existing IoT and IIoT applications is provided in Table 2.
TABLE 2. Blockchain consensus mechanisms in existing IoT and IIoT applications: Review summary.

| Reference No. (Year of Publication) | Major Contribution                                                                 | IoT/IIoT | Consensus Used       | Privacy | Security | Experimental Results Provided | Application Domain |
|-------------------------------------|-------------------------------------------------------------------------------------|----------|----------------------|---------|----------|-----------------------------|--------------------|
| [12][2021]                          | Blockchain and IoT integration schemes, security attacks, IoT eHealth – reference architecture, challenges and performance comparison. | IoT      | RAPT, BFT, SMaRT consensus | ✓       | ✓        | ✓                          | eHealth            |
| [2][2020]                           | Implemented a distributed ledger as multiple edge gateways and formulated a LDC algorithm for IIoT. | IIoT     | Lightweight data consensus algorithm | ✓       | ✓        | ✓                          | Smart City         |
| [9][2020]                           | The state-of-the-art consensus methods do not ensure the honest behavior of nodes in the consensus process. | IIoT     | PoRX = Proof of reputation + Proof of X consensus | ×       | ✓        | ✓                          | Industry           |
| [18][2019]                          | A PoW-based approach using sharding is proposed enabling IoT devices to solve puzzles in clusters. | IoT      | PoW with sharding | ×       | ×        | ✓                          | Military           |
| [20][2019]                          | DAG - Blockchain is used to develop prototypes through Raspberry Pi.                | IIoT     | B-IoT: A credit-based PoW | ✓       | ✓        | ✓                          | Smart Factory      |
| [21][2021]                          | The use of RAPT consensus in a proposed blockchain-based agriculture platform allows an ecosystem to be more scalable, more energy efficient and faster. | IoT      | RAPT consensus | ✓       | ✓        | ×                          | e-Agriculture      |
| [17][2020]                          | Solved the problem of credibility of blockchain consensus and performed security analysis of the proposed consensus. | IoT      | Proof of X-repute | ×       | ✓        | ✓                          | Edge Computing     |
| [19][2021]                          | The Apache Kafka consensus for resource-constrained IoT devices was implemented. Hyperledger Fabric and the Mystiko blockchain platforms were used. The Tikiri platform facilitates the parallel processing of transaction and real time transaction execution. | IoT      | Apache Kafka consensus | ×       | ✓        | ✓                          | Edge Computing     |
| [16][2020]                          | A credibility based equity proof consensus protocol (PoS+ TOPSIS) that integrates an elliptic curve algorithm with cryptography to enhance security. | IIoT     | Credibility based equity proof consensus protocol | ✓       | ✓        | ✓                          | Energy Trading     |

Hence, traditional consensus algorithms are incompatible with lightweight IoT devices that have limited storage and computing power. To establish agreements regarding resource-constrained industry devices, more efficient, hybrid, and lightweight consensus algorithms are necessary. Most of the consensus protocols mentioned in this context have been implemented through simulation results. As a result, large-scale deployment is still required to fully realize the promise of these innovations in leveraging a better and more personalized user experience in an industrial setting.

B. BLOCKCHAIN FOR 5G-ENABLED IoT NETWORKS

A paper by Mistry et al. [22] discussed the industrial potential for blockchain in 5G-enabled IoT devices. They organized their work into three parts: the background of blockchain, IoT, and 5G is briefly covered first, followed by relevant industrial applications. Finally, unresolved issues and challenges, primarily for industrial applications, have been addressed. Jovovic et al. [3] offered an outline of potential practical use cases for 5G technology and the idea of blockchain technology in the Industry 4.0 context. This study revealed several significant characteristics of this technology and showed its potential to surpass existing solutions and provide remedies to address the numerous issues faced by Industry 4.0. Nguyen et al. [23] examined the opportunities involved in using blockchain in 5G IoT networks. They explored the most recent advancements in integrated blockchain-5G IoT applications in a variety of sectors, including smart healthcare, smart cities, smart transportation, smart grid, and unmanned aerial vehicles (UAVs). Han et al. [24] proposed a technology that captures real-time air pollution readings from industrial locations using IoT sensors based on 5G wireless networks. To avoid data fabrication and manipulation, researchers employed blockchain technology to encrypt and send data to the cloud and provide a real-time air pollution index measurement framework. Zhang et al. [25] stated that intelligent data processing may be provided for edge devices in IIoT systems.
TABLE 3. Blockchain for 5G-enabled IoT networks: Review summary.

| Reference No. (Year of Publication) | Major Contribution | IoT or IIoT | Edge Computing | Cloud Computing | AI | Experimental Results Provided | Application Domain |
|------------------------------------|--------------------|-------------|----------------|----------------|----|-----------------------------|-------------------|
| [24][2019]                         | Blockchain and 5G wireless networks have been used to calculate real-time air pollution data from sensors. | IoT | ✓ | ✗ | ✗ | Environment Control in Industry 4.0 |
| [25][2019]                         | An edge intelligence and blockchain-enabled IIoT architecture for flexible and secure edge service administration. | IoT | ✓ | ✓ | ✗ | Industry 4.0 |
| [28][2020]                         | A conceptual BlockEdge architecture for Industrial IoT was proposed. | IoT | ✓ | ✗ | ✓ | Industry 4.0 |
| [26][2021]                         | A hybrid blockchain method powered by 5G MEC smart grids to identify and register IoT devices was developed. | IoT | ✓ | ✓ | ✗ | Smart Grid |
| [27][2021]                         | The proposed system incorporates security and fault tolerance through blockchain and beyond 5G enabled AVs permit low latency and high reliability. | IoT | ✗ | ✓ | ✓ | Autonomous Vehicles |

employing blockchain and 5G technologies to deliver secure and controlled services. The authors offered a cross-domain sharing and edge resource scheduling strategy and a credit-differentiated edge transaction acceptance mechanism. The results of this method indicated a considerable improvement in service cost and edge device capabilities.

Wang et al. [26] presented an integrated method for blockchain- and 5G-enabled multi-access edge computing smart grids to address smart grid IoT device coding and identification issues. The suggested hybrid approach was evaluated and compared to a variety of consensus procedures, including PoW, PoS, and Practical Byzantine Fault Tolerance (PBFT). Reebadiya et al. [27] highlighted the use of blockchain to provide security for autonomous vehicles (AV) and proposed a secure and intelligent blockchain-based system to sense and track AVs by deploying AI algorithms at edge servers. This proposed architecture was examined against and outperformed a conventional system. Kumar et al. [28] combined blockchain and edge computing to introduce a new framework BlockEdge to overcome the various issues related to IIoT. They evaluated the proposed system on iFogSim with and without blockchain to comprehend the results. As shown in Table 3, the current state-of-the-art technology demonstrates that blockchain and IIoT integration with 5G is still in its infancy. Even the existing implementation is based largely on simulations, test beds, and experiments.

C. BLOCKCHAIN FOR INDUSTRY 4.0

Hu et al. [29] evaluated a credit-based blockchain-enabled P2P transaction system based on distributed energy. The proposed model could enhance transaction efficiency without compromising transaction security. Moin et al. [30] proposed a taxonomy for blockchain-based IoT systems based on a SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis. They suggested a five-layer structure for integrating IoT with blockchain. The blockchain-enabled IoT system’s implementation requirements were provided. After the successful adoption of radio frequency identification (RFID) in industrial processes, Figueroa-Lorenzo et al. [31] investigated the possibilities of IIoT for increased efficiency and production. In a permissioned context, the authors showcased a Hyperledger Fabric blockchain based on a novel execute-order-validate strategy. Khan et al. [3] provided a clear description of IIoT and identified certain key difficulties that hampered the effectiveness of an IIoT system in the intended context. Authors also highlighted the key distinctions between IoT and IIoT. They planned to expand on the study trends in customized manufacturing in IIoT systems in the future. In the context of IIoT, Younan et al. [32] defined IoT as a communication mechanism or channel for facilitating interactions between people and devices. This communication has been extended from device to device. IIoT is a subset of IoT that focuses on interoperability across manufacturing systems to trigger automation and synchronization more quickly for closed environments. Li et al. [8] offered blockchain technology as a new way to handle data in the industrial Internet. Even though there are still many issues with blockchain in various industrial sectors, such as performance limitations, security, privacy protection, and so on, it can boost information exchange, optimize business practices, and cut expenses. The influence of blockchain technology on IoT was examined in a study by Makhdoom et al. [33], and barriers to blockchain’s adoption in IoT were identified. The authors then examined various blockchain-based IoT applications to highlight IoT application trends and blockchain constraints handled by these applications. Finally, a gap analysis was conducted, and a plan of action was proposed to address some of the major barriers to blockchain adoption in the IoT context.
### TABLE 4. Comparison of our work as compared to related work (1. Communication Standard; 2. Proposed a Model; 3. Challenges and Issues; 4. Potential Solutions; 5. Use of Blockchain).

| Reference No. (Year of Publication) | Focused On | Description | Potential Applications | IoT or IIoT | 1 | 2 | 3 | 4 | 5 |
|------------------------------------|------------|-------------|------------------------|-------------|---|---|---|---|---|
| [30][2019]                         | Security and trust issues imposed by blockchain in IoT environment. | SWOT analysis, identify causes of security issues of blockchain integration with IoT, security parameters. | Smart homes, Smart City, Industry 4.0 and Schools | IoT | Not Defined | ✓ | ✓ | × | ✓ |
| [22][2020]                         | Blockchain for 5G - survey. | Survey of enabling 5G technologies, research challenges and future research areas. | Healthcare, Smart City, Smart Transportation, Smart Grid and UAVs. | IoT | 5G | × | ✓ | ✓ | ✓ |
| [22][2020]                         | Blockchain for 5G enabled IoT for industrial automation-survey. | Outline possible use cases of blockchain in 5G enabled industrial devices. | Health Care and Industry 4.0 | IoT, IIoT | 5G | × | ✓ | ✓ | ✓ |
| [3][2018]                          | Applications of 5G and blockchain in Industry 4.0. | Insight to accommodate 5G and blockchain in industry application. | Industry 4.0 | IoT | 5G | × | ✓ | × | ✓ |
| [8][2021]                          | Industrial Blockchain survey. | Statistical analysis of blockchain enabled industrial Internet. | Supply Chain and Manufacturing. | IoT | Not defined | × | ✓ | ✓ | ✓ |
| [32][2020]                         | IoT Challenges: Review. | Reviewed existing IoT search engines and concluded that their performance could be improved by incorporating technologies such as blockchain, cloud computing etc. | Smart Transportation and Health Care | IoT, IIoT | Not defined | ✓ | ✓ | ✓ | ✓ |

| Our work                           | Blockchain with 5G in IIoT. | Analysis of recent advances in blockchain IIoT, challenges and proposed solutions | Industry 4.0 | IoT, IIoT | 5G | × | ✓ | ✓ | ✓ |

Many clients are divided into multiple communities based on the correlation and similarity of the collected data, and the data is only shared among smart factories within the same community [34]. As a result, Nair et al. [35] presented resource-efficient mining, ASIC cloud data-centers, and alternative consensus algorithms, including PoS and PoA. Standardization, scalability, and interoperability are just a few of the key issues identified to integrate blockchain technology into IIoT networks. Table 4 presents the contribution of our work in comparison with related work in blockchain in Industrial IoT.

### III. BLOCKCHAIN TECHNOLOGY

Industry 4.0 plays a critical role in connecting equipment and using new technologies such as IoT, AI, and big data in business processes to meet customers’ high production and accuracy needs. The main issue for Industry 5.0 is to enable massive data transmission while preserving high levels of security, transparency, and trustworthiness. 5G networks integrated with blockchain are capable to resolve these issues [36]. However, 5G and 6G networks are suitable for delivering extremely high capacity channels and eliminating communication delays, whereas distributed data storage feature blockchain provides high levels of information security, transparency, and integrity [3]. Blockchain is now recognized as one of the fastest-growing technologies, and it has grown in popularity as a result of its unique characteristics [37]. Blockchain is a decentralized collection of nodes that offers immutability, privacy, security, and an append-only data structure that is openly distributed among many non-trusting nodes and in which new blocks can only be added to the end of the existing chain without altering the preceding blocks [38]. The ability of a system to confirm the accuracy and trustworthiness of a block without any trusted third party is a key advantage of adopting a blockchain application [39]. The fundamental building block of blockchain is the ability to provide decentralization; thus, there is no need for a trusted third party to manage or control the participating entities. All the entities preserve their identical copies of the distributed database called a “distributed ledger.” To understand the potential blockchain applications in IIoT, it is vital to understand the workings, types, basic structure, and
core components of blockchain. There are two types of nodes in blockchain: full nodes and lightweight nodes [40]:

1) Full node: This is a node that can act as a miner node and add new blocks to a blockchain. A full node can process and store all blocks and transactions.

2) Lightweight node: This is a node with limited resources and can store and process only a part of blockchain data. In IIoT, sensors that are lightweight smart devices can act as lightweight nodes.

A. BLOCKCHAIN STRUCTURE AND KEY COMPONENTS
The key components of blockchain are described as follows:

1) Data block: The block in a blockchain is an elementary component. A block is a group of transactions that have been added to the blockchain [37]. The first block in a blockchain is known as a Genesis Block. The subsequent blocks, with the exception of the Genesis Block, must retain the hash address of its previous block. Every block consists of two parts: the block header and block data [41], as shown in Fig. 3. The block header contains the hash address of the block and its precursor, the hash address of the root of the Merkle tree, the nonce (an arbitrary number used only once), a timestamp, and metadata. The block data part contains all of the transactions and related information [37].

2) Miners: These are dedicated nodes capable of generating new blocks and adding them to the blockchain. Miners are always equipped with an extensive set of computing resources to contribute to the block generation process [37].

3) Distributed ledger: A distributed ledger is a specialized form of an open-source, transparent, and self-regulating database that is duplicated and synchronized over several places to conduct and keep track of transactions. In a blockchain network, each member has a copy of the database. A consensus is also made on the current blockchain instance that is saved and maintained by all members of the network [37].

4) Consensus protocols: Regardless of the lack of centralized control to authenticate and confirm transactions, a blockchain believes that every transaction is safe and certified. The consensus protocol, which is a fundamental component of every blockchain network, is what makes it possible. Hence, the consensus has been defined as the following [42]: “Without needing a trusted third party, blockchain technology enables the development of a distributed database among mutually distrusting parties. This is only feasible with the aid of a distributed) consensus algorithm, which ensures that every node in a network must agree
on a shared database state by obtaining agreement from at least a majority of network nodes.” As a result, a consensus algorithm is vital to any blockchain application as it determines how a system acts and operates [43]. The consensus mechanism used in bitcoin is PoW [44]. However, the main disadvantage of PoW is that it consumes a significant amount of energy and resources, making it unsuitable for real applications with limited resources.

5) Smart contracts: A smart contract is a self-executing set of instructions running on blockchain to manage and process transactions according to pre-specified terms and conditions. A smart contract is a digital version of a traditional contract that allows non-trusted parties to negotiate without the involvement of a third party. Ethereum was the first to introduce the notion of smart contracts. Each blockchain node has its own local virtual computer, which is referred to as the EVM (Ethereum virtual machine) in Ethereum [37].

B. WORKING OF A BLOCKCHAIN

The practical working operation of blockchain would vary from application to application. However, as illustrated in Fig. 4, the process of adding a new block entails six phases, which are as follows [37]:

1) A node initiates a transaction by generating it and then digitally signing it with its private key (created via cryptography).
2) In a blockchain, a transaction can exhibit a variety of actions. A fresh block is then produced to reflect either a transaction or a collection of transactions.
3) A new transaction is broadcast (flooded) to all involved network entities in order to verify it using predetermined procedures. Typically, many nodes are needed to validate a transaction on a blockchain.
4) Miner nodes are responsible for validating new transactions or blocks and storing them on the distributed ledger. Miners compete to solve a hard mathematical challenge or puzzle based on a cryptographic hash method. PoW is a solution to this problem and demonstrates that a miner invested substantial computational work. Miners may be entitled to some incentive for mining, which could be either in the form of cryptocurrency or transactional charges.
5) Once a transaction has been confirmed, it is added to a block, and a new instance of blockchain is broadcast throughout the network to give the most up-to-date information about the block. A transaction receives its initial confirmation at this stage.
6) This most recent block is then placed on the distributed ledger, and following blocks are linked to it through a hash pointer. At this moment, the transaction obtains its second confirmation, while the block receives its first. When a new block is produced, its related transactions are reconfirmed. Normally, a network requires six confirmations before considering a transaction to be complete.

C. TYPES OF BLOCKCHAIN

Private blockchain systems are available to an approved or pre-specified set of users only. In contrast, public blockchain systems are open networks in which all nodes are free to join and leave the network with full access to read, view, and write data in the blockchain. The three different types of blockchain are described as follows [37], [45]:

1) Public
2) Private
3) Consortium
1) Public or permissionless blockchain: This blockchain is a network where all transactions are accessible to all users, and anyone may participate in the consensus mechanism.
2) Private or permissioned blockchain: Private blockchain differs from public blockchain in several ways. To participate in this network type, interested nodes would have to either be members or have privileges. Transactions are only visible to specified users, since they are private. Only nodes connected with a certain enterprise would be permitted to participate in the consensus method.
3) Consortium or federated blockchain: A predetermined set of businesses use these. The groups are generally
established around the common interests of the organizations involved. Like private blockchain, these consortium chains operate as closed systems that rely on few verified nodes to reach an agreement, resulting in a semi-decentralized system. In contrast to a private blockchain, which is controlled by a single organization, a consortium chain is governed by a group of organizations.

IV. INDUSTRIAL INTERNET OF THINGS

With the continued expansion and extensive use of IoT technology, IIoT has now become an integral part of industrial systems [16]. Being a contemporary concept of IoT in industries, the major task of IIoT is to automate smart devices for detecting, collecting, analyzing, controlling, and transmitting real-time events in industrial processes [3]. The term “Industrial IoT” refers to the next stage of smart devices that are capable of managing resources in a more flexible, efficient, and timely manner. Furthermore, these smart devices can monitor complete control systems within industries without human involvement [46]. The major objective of IIoT, as a subset of IoT, is the effective utilization of industrial assets and activities [3]. IoT is a critical part of the technology in Industry 4.0, the fourth industrial revolution. Smart innovations, data automation, interconnection, artificial intelligence, and other technologies and capabilities are highlighted in Industry 4.0. These technologies are drastically changing the operations of factories and industries. IIoT facilitates machine-to-machine communication to understand business processes in a better way. Businesses on a continuing basis could receive complete resource information and use it to regulate equipment (manually or automatically) to improve their function. Businesses could save a significant amount of energy, water, and materials while maintaining or enhancing their output levels.

A. THE INTERNET OF THINGS VS. THE INDUSTRIAL INTERNET OF THINGS

In spite of the fact that IIoT and conventional IoT applications share many of the same principles and functionalities, there are still significant distinctions between them. When comparing IoT and IIoT, the primary distinction is that consumers mostly utilize IoT to simplify their lives, whereas companies use IIoT to enhance their performance and safety levels. Therefore, in Table 5, we have highlighted some major differences between these two.

B. IIoT ARCHITECTURE

The four-layer architecture of IIoT is displayed in Fig. 5 [40]. A layer-modular architecture consists of four layers: a sensing layer, a network layer, a service layer, and an application layer. These are described in this section as follows:

1) Sensing layer: This layer consists of physical devices, such as sensors, actuators, RFID, and programmable logic controllers (PLCs) in an industrial unit. This layer implements various data sensing and acquisition protocols to sense, control, and collect data from physical devices.

2) Network layer: The task of a networking layer is to connect physical devices and allow them to communicate with each other for data exchange. Hence, this layer provides networking support and data transfer over wireless and wired networks. This layer is also capable of integrating data from existing infrastructures.

3) Service layer: This layer serves as a gateway, enabling the successful integration of services and applications. This is a low-cost solution that allows for the reuse of hardware and software platforms. A well-defined service must identify the application requirements and provide an API (Application Programming Interface) and protocols to cater to the needs of users. Also, this layer manages all of the service-oriented issues. Therefore, this layer creates and manages services according to the requirements of the users.

4) Interface layer: As the devices involved in IIoT are heterogeneous and employ different standards and protocols, the interactions between such devices always come with various problems. Moreover, with the growth of the number of connected devices, it becomes harder to manage and communicate in such a scenario. Hence, the interface layer provides interaction methods for users and other applications.

C. ISSUES AND CHALLENGES IN IIoT

IIoT enables numerous corporate activities and transforms conventional industry operations into smarter operations. However, because of the heterogeneous structure and complexity of the IIoT system, several problems and concerns must be addressed to mitigate the risks involved. Some important issues and challenges are discussed under this section:

1) Interoperability: The term interoperability refers to the capability of heterogeneous IoT devices to communicate and exchange information with each other [7]. Due to the diverse nature of machines and protocols employed in business operations, interoperability between such devices becomes a great challenge. The lack of interoperability hinders the use of IIoT systems. More research efforts are required to improve the interoperability.

2) The heterogeneous nature of IoT devices: Because the devices used in the IIoT environment are of various types and utilize unique protocols and approaches, there is a need to build a relationship and enable synchronization in these devices to assure data integrity.

3) Inefficient data management: The system’s complexity grows as the number of devices and sensors in an industrial unit expands. Furthermore, the massive volume of high frequency data generated by IoT devices and sensors makes it difficult to handle and store. As a result, data management becomes exceedingly difficult and necessitates instant solutions.
TABLE 5. IoT vs. IIoT.

| Relation         | IoT                  | IIoT                |
|------------------|----------------------|---------------------|
| Scalability [3]  | Small scale          | Large scale         |
| Operational Reliability | Low                  | High                |
| Data Processing Range [47] | Medium to high       | Huge volume         |
| Communication   | Wireless             | Both wired and wireless |
| Focus [3]        | Consumer oriented applications | Industry oriented applications |
| Interoperability | Autonomous           | CPS-integrated      |
| Programmability  | Easy off-site programming | Remote on-site programming |
| Requirements     | Moderate             | Stringent           |
| Development goal | User convenience     | Process optimization |
| Risk of Failure  | Life-threatening risk does not exist upon failure | Life-threatening situation occurs upon failure |

4) Security and privacy issues: There are security and privacy risks associated with IoT devices’ heterogeneous and centralized nature. Furthermore, data of a non-public nature specific to an industry must be sent over the Internet and access to this data must be provided in accordance with appropriate security standards [48]. Increasing usage of IIoT by enterprises exposes them to an increased risk of cyber-attacks, since it allows users to remotely access their devices, processes, and services.

5) Limited resource support: The majority of IoT devices come with constrained resources in terms of memory and processing capabilities. The volume of data generated in the industrial process puts extra pressure on these lightweight devices for processing, storage, and utilization.

6) Connectivity: In the deployment of IIoT, poor connection becomes a major concern. The appropriate connection of a machine with an IIoT system is a difficult issue yet is needed in order to remotely monitor and maintain the performance of a machine at an ideal level. The typical coordination issues that arise with IoT devices reduce production levels and lead to economic losses.

7) Network performance and bandwidth: Existing networks that support IoT are not designed to handle the challenges posed by Industrial IoT. These integrated networks that support both IoT and IIoT data traffic require better bandwidth to ensure smooth system function. Technologies like 5G need to be exploited to provide higher data rates and improved performance.

V. BLOCKCHAIN-IIoT CONVERGENCE

The decentralized nature of blockchain makes it useful for the elimination of the central point of failure in conventional IIoT devices [7], [14]. IIoT is an open, client–server, and heterogeneous network of smart devices that needs to implement trustworthy communication [9]. The temper-proof nature of blockchain could be a great choice to ensure secure communication between these devices. Since blockchain offers high immutability and unique transparency, it could provide security among IoT devices and servers [19]. IoT solutions are mostly built on the client–server paradigm, which is connected to cloud servers through the web. There will be an increase in demand for decentralized solutions and networks due to the future growth of these networks [7]. P2P networks provided by blockchain system are potential solutions for the creation of a secure and reliable environment for industrial processes. Blockchain has the capabilities to revolutionize the existing IIoT applications to obtain optimal productivity levels and minimize losses.
Blockchain could prove to be a game changer for IIoT, as the impact of blockchain on IIoT and Industry 4.0 has been quite significant. Blockchain provides a unique paradigm for the distribution of digital data among industries to adopt the principles laid out by Industry 4.0. The search query “TITLE-ABS-KEY (“Blockchain-IIoT” OR blockchain AND iiot) AND (EXCLUDE (PUBYEAR,2022)) AND (LIMIT-TO (LANGUAGE, "English"))” was used to search the literature from the Scopus database. Documents written in a language other than English and the search results with publication year 2022 were excluded to analyze the results. A total of 250 research documents have been extracted which was very limited in number if compared with “blockchain” and “IIoT” individually. The chart in Fig. 6 depicts the number of publications per year retrieved from Scopus in “blockchain,” “IIoT,” and “blockchain-IIoT” to highlight research trends in blockchain integration with IIoT during the last five years, beginning in 2017. We attempted to combine the most recent research on blockchain and IIoT integration. The bulk of the research articles in this paper were released in 2021. According to this graph, research into the convergence of blockchain and IIoT gained pace after 2018, while the notion of integrating these two was not suggested previous to 2017.

The graph in Fig. 7 depicts the publisher-specific statistics of the existing literature from the Scopus database to explain the significant contributions of the various publication houses. Based on this analysis, it is possible to infer that IEEE has the largest proportion of retrieved research papers (52%). A list of the top-10 authors in the field of blockchain-IIoT is displayed in Fig. 8, which can help future publications to find reviewers and editors in this field. Although the convergence of both of these innovations could change the working culture of existing industries, several challenges must be resolved to explore the benefits of these technologies.

A. BLOCKCHAIN-IIoT CHALLENGES

Industrial IoT combined with blockchain is now generating a significant amount of attention in the corporate sector. However, when existing blockchain systems are combined with IIoT, the issues represented in Fig. 9 must be solved prior to their deployment.

1) Inefficient consensus mechanism: The mainstream blockchain consensus methods are computationally difficult and complicated when operating with lightweight IoT devices with limited resources [17], [19]. Furthermore, the security and efficiency of consensus methods are critical issues that must be addressed to effectively deploy blockchain in IIoT [9], [49].

2) High throughput requirements of IoT: Existing blockchain systems have a fixed number of transactions per second, and mining is time-consuming. As a result, when integrating a large number of devices and sensors inside an industry, the high throughput and speed demanded by IoT systems would hinder the intended outcome [12].

3) Big data storage requirements: Every node keeps a copy of the whole distributed ledger. However, while replicating data blocks on every node of the blockchain network enhances efficiency and removes the necessity of central control, it places an additional overhead on the limited storage capacity offered by IoT devices [50]. As a result, while dealing with blockchain coupled with IIoT, massive data management has emerged as a potential challenge.

4) Lack of regulation standards: The process of standardizing blockchain with IIoT is still in its early stages, and it must be synchronized with the existing industry standards. Blockchain’s immutability, anonymity, transparency, and decentralized characteristics raise...
new regulatory concerns for businesses [50]. Without specific norms and regulations, communication between diverse blockchain platforms and Industrial IoT systems becomes a key challenge for industrial transactions. Standard processes and clear regulations are critically required to properly integrate Industrial IoT with blockchain [51].

5) Transparency and privacy trade-off: Blockchain ensures a transparent platform for executing transactions, but it is hard to publicize the transaction history of IoT devices in a distributed ledger, as it could reflect the identity of the user [12]. Moreover, due to the permanent nature of blockchain data, it becomes hard to erase sensitive personal information from blockchain [40], placing such persons within the target of malicious users. To maintain a balance between these two, an effective access control method is required [50].

**B. POTENTIAL SOLUTIONS TO BLOCKCHAIN-IIoT CHALLENGES**

The above-mentioned challenges could be critically addressed as shown in Fig. 10 to ensure the successful deployment of blockchain-IIoT integration.

1) Improved consensus mechanism: Existing consensus methods rely on complex computing processes to add new blocks to a blockchain. These tasks and puzzles
FIGURE 9. Blockchain-IIoT challenges.

The challenges of adopting blockchain with 5G networks for industrial IoT devices include:

1) Inefficient consensus mechanism:
   - Transaction verification is required to add valid blocks to a blockchain.
   - It becomes obvious that the speed of a blockchain system will degrade along with an increase in the number of nodes (scalability) and an increase in the number of transactions in a block. However, to maintain the decentralization of a blockchain network, optimal block size and new node addition frequency must be carefully regulated [52]. Efficient consensus mechanisms, high bandwidth, and low latency are needed to boost the throughput of a blockchain [50]. Using 5G communication channels, ultra-high speed and low latency could be obtained [51]. Personalized agents could be assigned to perform a designated set of activities, including the creation of blocks on behalf of IoT devices to reduce the bandwidth requirements of the blockchain network [7].

2) Better throughput:
   - Transaction throughput refers to the number of transactions executed per second (TPS). TPS is calculated from block size, which is determined by the number of transactions per block, the execution time for the consensus protocol, etc. Transaction verification is required to add valid blocks to a blockchain. It becomes obvious that the speed of a blockchain system will degrade along with an increase in the number of nodes (scalability) and an increase in the number of transactions in a block. However, to maintain the decentralization of a blockchain network, optimal block size and new node addition frequency must be carefully regulated [52]. Efficient consensus mechanisms, high bandwidth, and low latency are needed to boost the throughput of a blockchain [50]. Using 5G communication channels, ultra-high speed and low latency could be obtained [51]. Personalized agents could be assigned to perform a designated set of activities, including the creation of blocks on behalf of IoT devices to reduce the bandwidth requirements of the blockchain network [7].

3) Off-chain storage:
   - Off-chain data refers to any structured or unstructured data that must be stored outside of a blockchain. Many off-chain techniques for storing large amounts of data in IoT have been proposed, which help to minimize latency and increase performance [12]. Instead of keeping all blockchain data on-chain, critical industrial data should be kept elsewhere to be accessed through a more secure environment [7].

4) Standardization of blockchain-enabled IIoT:
   - According to IIoT experts, blockchain standardization will play a critical role in determining the technology’s future. Blockchain standards should be able to provide guidelines for blockchain developers and clients. Due to the elimination of the controlling authority and the distributed nature of blockchain, traditional legislation is unable to provide governance. The smart contract technology that converts the legislation into code in the blockchain, on the other hand, may implement laws. Furthermore, smart contracts must be legally enforceable to avoid conflicts between transacting parties [50].

5) Privacy protection:
   - Although removing specific personal information from an existing block could alter the hash pointers between the blocks, the IIoT platform may need to update the pointers by re-hashing the blocks [40] to accommodate an editable blockchain. Homomorphic encryption [50], federated learning [50], and differential privacy have been shown to overcome the privacy concerns associated with blockchain systems.

VI. CONCLUSION AND FUTURE SCOPE

Many businesses worldwide are grappling with how to integrate blockchain, IoT, and 5G networks into their business operations. The industries have been slow to adopt these innovations because they believe that government regulations will force them to make major changes to processes and architectures in the years ahead. A variety of opportunities can be explored through the combination of 5G and 6G technologies, IoT networks, and blockchain to provide the successful deployment of IIoT solutions rooted in these technologies. With the help of a comprehensive literature...
We first described the idea of Industry 4.0 and its major aspects, Industry 5.0, and the potential presented through the merging of IIoT and blockchain technologies. A literature review and important future direction were also provided to help researchers identify significant gaps in the research that have already been carried out. The lack of a detailed review of the pairing of blockchain and IIoT with 5G networks is the driving force for this work. We addressed blockchain and its operation, structure, and components, and provided a reasonable discussion that demonstrated the capabilities of blockchain. We offered a clear understanding of IIoT, its architecture, and the key issues and challenges collected and analyzed from recent literature. After providing the necessary background and fundamental concepts of IIoT and blockchain, we highlighted several integration opportunities so that future research can tackle the limitations and issues of these two revolutionary domains. The complementary nature of these two domains has been demonstrated through the provision of solutions for the highlighted problems. Finally, we concluded that blockchain innovation can become a great solution for resolving IoT restrictions in the industry. The following are the main outcomes of this research:

1) Through inherent characteristics such as decentralization, privacy, and transparency, blockchain offers the ability to overcome the shortcomings of resource-constrained IoT devices.

2) Even though the integration of blockchain and IIoT is still in its early stages, the use of blockchain in IIoT faces several problems, including inefficient consensus techniques, poor throughput rates, and massive data storage management. The potential solutions to these problems as proposed in this study could undoubtedly assist the widespread adoption of blockchain in the industry.

3) Furthermore, the use of 5G networks in conjunction with blockchain can enhance the data rates and throughput offered in the existing industry domain.
In the future, the authors will choose to work to improve existing consensus techniques to address certain issues, such as low efficiencies, lack of trust, and high processing demands in IoT devices. Finally, this research aimed to assist in determining the impact of blockchain technology in improving the performance and applicability of IoT in the industry by reducing human intervention and assisting in the automation of industry operations.

VII. CONFLICTS OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

REFERENCES

[1] S. K. Dwivedi, P. Roy, C. Karda, S. Agrawal, and R. Amin, “Blockchain-based Internet of Things and industrial IoT: A comprehensive survey,” Secur. Commun. Netw., vol. 2021, pp. 1–21, Aug. 2021.
[2] W. Zhang, Z. Wu, G. Han, Y. Feng, and L. Shu, “LDC: A lightweight dada consensus algorithm based on the blockchain for the industrial Internet of Things for smart city applications,” Future Gen. Comput. Syst., vol. 108, pp. 574–582, Jul. 2020.
[3] J. Jovovic, S. Husnjak, I. Forenbacher, and S. Macek, “5G blockchain and IPFS: A general survey with possible innovative applications in industry 4.0,” in Proc. 3rd EAI Int. Conf. Manage. Manuf. Syst., vol. 2. Ghent, Belgium: European Alliance for Innovation, 2018, p. 157.
[4] E. Sisinni, A. Safiullah, S. Han, U. Jennehag, and M. Gidlund, “Industrial Internet of Things: Challenges, opportunities, and directions,” IEEE Trans. Ind. Informat., vol. 14, no. 11, pp. 4724–4734, Nov. 2018.
[5] J. Z. Reis and R. F. Gonçalves, “The role of internet of services (IOS) on industry 4.0 through the service oriented architecture (SOA),” in Proc. IFIP Int. Conf. Adv. Prod. Manage. Syst. Seoul, South Korea: Springer, 2018, pp. 20–26.
[6] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, and G. Dhiman, “Application of blockchain and Internet of Things in healthcare and medical sector: Applications, challenges and future perspectives,” J. Food Qual., vol. 2021, pp. 1–20, May 2021.
[7] G. Wang, “Sok: Applying blockchain technology in industrial internet of things,” Cryptol. ePrint Arch., vol. 2021, p. 776. [Online]. Available: https://eprint.iacr.org/2021/776
[8] Z. Li, R. Y. Zhong, Z. G. Tian, H. N. Dai, A. V. Barenji, and G. Q. Huang, “Industrial blockchain: A state-of-the-art survey,” Robot. Comput. Integr. Manuf., vol. 70, Aug. 2021, Art. no. 102124.
[9] E. K. Wang, Z. Liang, C.-M. Chen, S. Kumari, and M. K. Khan, “PoRX: A reputation incentive scheme for blockchain consensus of IoT,” Future Gen. Comput. Syst., vol. 102, pp. 140–151, Jan. 2020.
[10] M. Ali, H. Karimipour, and M. Tariq, “Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges,” Comput. Secur., vol. 108, Sep. 2021, Art. no. 102355.
[11] J. Sengupta, S. Ruj, and S. D. Bit, “A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT,” J. Netw. Comput. Appl., vol. 149, Jan. 2020, Art. no. 102481.
[12] B. Farahani, F. Firooz, and M. Luecking, “The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions,” J. Netw. Comput. Appl., vol. 177, Mar. 2021, Art. no. 102936.
[13] Y. Wu, Z. Wang, Y. Ma, and V. C. M. Leung, “Deep reinforcement learning for blockchain in industrial IoT: A survey,” Comput. Netw., vol. 191, May 2021, Art. no. 108004.
[14] J. Wang, B. Wei, J. Zhang, X. Yu, and P. K. Sharma, “An optimized transaction verification method for trustworthy blockchain-enabled IIoT,” Ad Hoc Netw., vol. 119, Aug. 2021, Art. no. 102526.
[15] L. Yu, X.-F. Zhao, Y. Jin, H.-Y. Cai, B. Wei, and B. Hu, “Low powered blockchain consensus protocols based on consistent hash,” Frontiers Inf. Technol. Electron. Eng., vol. 20, no. 10, pp. 1361–1377, Oct. 2019.
[16] Z. Guan, X. Lu, N. Wang, J. Wu, X. Du, and M. Guizani, “Towards secure and efficient energy trading in IIoT-enabled energy internet: A blockchain approach,” Future Gen. Comput. Syst., vol. 110, pp. 686–695, Sep. 2020.
[17] E. K. Wang, R. Sun, C.-M. Chen, Z. Liang, S. Kumari, and M. K. Khan, “Proof of X-repute blockchain consensus protocol for IoT systems,” Comput. Secur., vol. 95, Aug. 2020, Art. no. 101871.
[40] S. Zhao, S. Li, and Y. Yao, “Blockchain enabled industrial Internet of Things technology,” IEEE Trans. Comput. Social Syst., vol. 6, no. 6, pp. 1442–1453, Dec. 2019.

[41] S. Kaur, S. Chaturvedi, A. Sharma, and J. Kar, “A research survey on applications of consensus protocols in blockchain,” Secur. Commun. Netw., vol. 2021, pp. 1–22, Jan. 2021.

[42] K. Omote and M. Yano, “Bitcoin and blockchain technology,” in Blockchain and Crypto Currency, M. Yano, C. Dai, K. Masuda, and Y. Kishimoto, Eds. Singapore: Springer, 2020, pp. 129–136.

[43] M. S. Ferdous, M. J. M. Chowdhury, and M. A. Hoque, “A survey of consensus algorithms in public blockchain systems for crypto-currencies,” J. Netw. Comput. Appl., vol. 182, May 2021, Art. no. 103035.

[44] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Decentralized Bus. Rev., p. 21260, Oct. 2008. [Online]. Available: https://www.debr.io/article/21260-bitcoin-a-peer-to-peer-electronic-cash-system

[45] S. Gomathi, M. Soni, G. Dhiman, R. Govindaraj, and P. Kumar, “A survey on applications and security issues of blockchain technology in business sectors,” Mater. Today, Proc., Mar. 2021, doi: 10.1016/j.matpr.2021.02.088.

[46] G. Rathee, F. Ahmad, R. Sandhu, C. A. Kerrache, and M. A. Azad, “On the design and implementation of a secure blockchain-based hybrid framework for industrial Internet-of-Things,” Inf. Process. Manage., vol. 58, no. 3, May 2021, Art. no. 102526.

[47] S. Khan, “Modern Internet of Things as a challenge for higher education,” Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, p. 34, 2018.

[48] I. Ungurean and N. C. Gaitan, “A software architecture for the industrial Internet of Things—A conceptual model,” Sensors, vol. 20, no. 19, p. 5603, Sep. 2020.

[49] M. Z. Khan, O. H. Alhazmi, M. A. Javed, H. Ghandorh, and K. S. Aloufi, “Reliable Internet of Things: Challenges and future trends,” Electronics, vol. 10, no. 19, p. 2377, Sep. 2021.

[50] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, “A survey on the adoption of blockchain in IoT: Challenges and solutions,” Blockchain: Res. Appl., vol. 2, no. 2, Jun. 2021, Art. no. 100006.

[51] S. Singh, P. K. Sharma, B. Yoon, M. Shojaifar, G. H. Cho, and I.-H. Ra, “Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city,” Sustain. Cities Soc., vol. 63, Dec. 2020, Art. no. 102364.

[52] F. Jameel, U. Javaid, W. U. Khan, M. N. Aman, H. Pervaiz, and R. Jantti, “Reinforcement learning in blockchain-enabled IoT networks: A survey of recent advances and open challenges,” Sustainability, vol. 12, no. 12, p. 5161, Jun. 2020.

**MANPREET KAUR** received the B.Tech. degree in computer science and engineering from Punjab Technical University, Punjab, India, in 2007, and the M.Tech. degree from the College of Agricultural Engineering and Technology, Punjab Agriculture University, Ludhiana, in 2010. She is currently pursuing the Ph.D. degree in blockchain technologies with Chandigarh University. She is an Assistant Professor with Guru Nanak Dev Engineering College, Ludhiana. She has been engaged in teaching and research in the field of software engineering. She has published four international journal articles and two international conference papers along with one chapter in a book. Her research interests include the opinion mining, blockchain technology and its consensus mechanism, and artificial intelligence.

**M. KAUR et al.: Adoption of Blockchain With 5G Networks for Industrial IoT**

**MOHAMMAD ZUBAIR KHAN** received the M.Tech. degree in computer science and engineering from U.P. Technical University, Lucknow, India, and the Ph.D. degree in computer science and information technology from the Faculty of Engineering, M. J. P. Rohilkhand University, Bareilly, India. He was the Head and an Associate Professor with the Department of Computer Science and Engineering, Invertis University, Bareilly. He is currently an Associate Professor with the Department of Computer Science, College of Computer Science and Engineering, Taibah University. He has more than 15 years of teaching and research experience. He has published more than 60 journal articles and conference papers. His current research interests include the IoT, machine learning, parallel and distributed computing, and computer networks. He has been a member of the Computer Society of India, since 2004.

**SHIKHA GUPTA** is currently an Academician and a Researcher with vast academic experience in institutes of repute. Presently, she is associated with Chandigarh University as a Professor with the University Institute of Engineering (computer science). Her research interests include data analytics, artificial intelligence, data mining, blockchain technology, machine learning, deep learning, and algorithm development and analysis.

**ABDULLAH ALSAEEEDI** received the B.Sc. degree in computer science from the College of Computer Science and Engineering, Taibah University, Madinah, Saudi Arabia, in 2008, the M.Sc. degree in advanced software engineering from the Department of Computer Science, The University of Sheffield, Sheffield, U.K., in 2011, and the Ph.D. degree in computer science from The University of Sheffield, in 2016. He is currently an Assistant Professor at the Computer Science Department, Taibah University. His research interests include software engineering, software model inference, grammar inference, and machine learning.

**VOLUME 10, 2022**

---

**IEEE Access**

---

[36x183][52] F. Jameel, U. Javaid, W. U. Khan, M. N. Aman, H. Pervaiz, and R. Jäntti, S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I.-H. Ra, M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, “A M. Z. Khan, O. H. Alhazmi, M. A. Javed, H. Ghandorh, and K. S. Aloufi, I. Ungurean and N. C. Gaitan, “A software architecture for the industrial Internet of Things—A conceptual model,” Sensors, vol. 20, no. 19, p. 5603, Sep. 2020. G. Rathee, F. Ahmad, R. Sandhu, C. A. Kerrache, and M. A. Azad, “On the design and implementation of a secure blockchain-based hybrid framework for industrial Internet-of-Things,” Inf. Process. Manage., vol. 58, no. 3, May 2021, Art. no. 102526. S. Khan, “Modern Internet of Things as a challenge for higher education,” Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, p. 34, 2018. I. Ungurean and N. C. Gaitan, “A software architecture for the industrial Internet of Things—A conceptual model,” Sensors, vol. 20, no. 19, p. 5603, Sep. 2020. M. Z. Khan, O. H. Alhazmi, M. A. Javed, H. Ghandorh, and K. S. Aloufi, “Reliable Internet of Things: Challenges and future trends,” Electronics, vol. 10, no. 19, p. 2377, Sep. 2021. M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, “A survey on the adoption of blockchain in IoT: Challenges and solutions,” Blockchain: Res. Appl., vol. 2, no. 2, Jun. 2021, Art. no. 100006. S. Singh, P. K. Sharma, B. Yoon, M. Shojaifar, G. H. Cho, and I.-H. Ra, “Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city,” Sustain. Cities Soc., vol. 63, Dec. 2020, Art. no. 102364. F. Jameel, U. Javaid, W. U. Khan, M. N. Aman, H. Pervaiz, and R. Jantti, “Reinforcement learning in blockchain-enabled IoT networks: A survey of recent advances and open challenges,” Sustainability, vol. 12, no. 12, p. 5161, Jun. 2020.