Alexandria Engineering Journal (2022) 61, 6001–6022

HOSTED BY

Alexandria University

Alexandria Engineering Journal

www.elsevier.com/locate/aej
www.sciencedirect.com

A Survey on blockchain for industrial Internet of Things

R.Lakshmana Kumar [a], Firoz Khan [b], Seifedine Kadry [c], Seungmin Rho [d,*]

[a] *Head- Centre of Excellence for Artificial Intelligence and Machine Learning, Hindusthan College of Engineering and Technology, India*
[b] *Dubai Men's College, Higher Colleges of Technology, Dubai, UAE*
[c] *Department of Applied Data Science, Noroff University College, Kristiansand, Norway*
[d] *Department of Industrial Security, Chung-Ang University, Seoul 06974, Republic of Korea*

Received 10 July 2021; revised 16 September 2021; accepted 5 November 2021
Available online 19 November 2021

KEYWORDS

Internet of Things;
Blockchain;
Industry 4.0;
SmartEnvironments;
Survey

Abstract Blockchain and the Internet of Things (IoT) are separately regarded as highly capable popular technologies. Blockchain is a database used for decentralized transaction purposes. It provides novel directions to store and manage data, whereas IoT relates to the propagation of linked machines by providing information through the Internet. A mixture of Blockchain and the IoT appears hopeful, even though blockchain requires real-time data application, and IoT describes processes to store and manage information overloads safely and proficiently. The technology is significant to the manufacturing business, experiencing a digital revolution by incorporating equipment, developments, and data, leading to the Industrial IoT (IIoT). Such a combination of IIoT and blockchain is termed Blockchain for Industrial Internet of Things (BIIoT). The paper gives a detailed survey on BIIoT and discusses all relevant aspects of this novel concept. Firstly, IoT as a concept has been explored briefly, and relevant threats to IoT has been investigated. Furthermore, the domain of IIoT and the relevant challenges to IIoT is discussed. Additionally, an overview of blockchain technology is presented. Subsequently, a combination of IIoT and blockchain is explored, and the BIIoT structural design proposal is submitted. Finally, issues related to the use of IIoT with blockchain for industrial applications of BIIoT is explored. Thus, all relevant open research directions in Blockchain and IIoT are summarized in this paper. This survey shows that the proposed BIIoT is used to develop a redundant, traceable, and secure complex interconnected IIoT environment. Furthermore, the BIIoT system enables us to communicate with each other without the need for a trusted intermediary in a decentralized, unreliable, peer-to-peer network.

© 2021 THE AUTHORS. Published by Elsevier BV on behalf of Faculty of Engineering, Alexandria University. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

* Corresponding author.
E-mail addresses: research.laksha@gmail.com (R. Kumar), fk7@hotmail.com (F. Khan), smrho@cau.ac.kr (S. Rho).
Peer review under responsibility of Faculty of Engineering, Alexandria University.

https://doi.org/10.1016/j.aej.2021.11.023
1110-0168 © 2021 THE AUTHORS. Published by Elsevier BV on behalf of Faculty of Engineering, Alexandria University.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

The Internet of Things (IoT) is an efficient Internet and management environment that jointly forms an intelligently linked globe is the Internet of Things (IoT)[1]. While deployed smartly, IoT permits users to broadcast their data to the server. IoT is employed in various fields, including industries, businesses, environmental engineering, mobile devices, and governance. Additionally, IoT is utilised to support various industries, like transport, healthcare, farming, energy, and environment management. Furthermore, IoT can promote various industrial applications related to logistics, manufacturing, food production and services.

The Industrial Internet of Things (IIoT) comprises extensive awareness from industries and academics, which could be a significant factor in the upcoming conversion of industrial schemes [2]. The industrial IoT is heavily discussed within Industry 4.0, and IIoT is also intensively discussed in government and academic circles. The significant difference between IoT and IIoT is various automation equipment and industrial devices in an IoT environment; IIoT is usually utilised in applications like smart factories and smart manufacturing [115]. IIoT presents intelligence and interconnection to industrial schemes using actuators and sensing tools, including omnipresent network and processing capabilities. The goal of implementing IIoT is to enhance business competence and manufacture throughput, decrease the device's downtime and improve the excellence of the produced product. Precisely, IIoT consists of the following characteristics: 1) IIoT systems decentralization, 2) a varied selection of IIoT applications and schemes, 3) IIoT information heterogeneity with 4) strain on the network.

Development in the field of blockchain techniques enhances the possibilities of overcoming the identified IIoT challenges. Blockchain is the underlying technology for bitcoin [3]. Blockchain permits software applications to transmit and store communications or transactions during a reliable and disseminated (peer-to-peer) method [52]. Blockchain is being quickly adopted and mainly utilised for applications with smart contracts [31], digital assets and disseminated storage [4]. The Blockchain in IIoT [5] capable applications contain recording actions (such as humidity, heat or location variances) while creating obstruct challenge ledgers that are understandable solitary to particular contributors, e.g., specific contributors throughout a supply chain.

Blockchain technology has transformed from an abstract technique to a reliable technique resolution [58]. At present, current unrestricted blockchain proposal, like Ethereum, Hyperledger Fabric, Enterprise operating system (EOS), allows persons to make decentralized applications (Dapps) using blockchain technique [47]. By organizing smart contracts, these proposals enable consumers to avail the benefits of blockchain. In the blockchain group, all nodes are responsible for allotting the ledger replica to the entire or every other contributing node in the sequence that the data contained by the blockchain is obstructed evidence [50].

Blockchain is an excellent complement to IIoT due to its properties of enhanced interoperability, confidentiality, safety, dependability and measurability [35]. During this work, a novel concept of incorporating IIoT with blockchain is examined. A mixture of IIoT and blockchain is termed Blockchain for Industrial Internet of Things (BIIoT).

Broadly, Blockchain 1.0 is usually related to cryptocurrency and expense (e.g. Bitcoin) [53,57,85,101], and Blockchain 2.0 is related to automatic digital economics by using smart contracts. Newer Blockchain 3.0 development concentrates on tackling the digital world's requirements, like Industry 4.0 concerning smart cities. Industry 4.0 is permanently energized by the IoT[60]. In 2011, the German government-defined Industry 4.0 was broadly adopted by both academia and industry. Industrial IoT (IIoT) is a related concept. However, it includes a further concentration on IoT use in industries (with one being able to consider IIoT as an enhancement of IoT).

Furthermore, Industry 4.0 is usually related to responsible manufacturing works organisations. Therefore, the digitalization and interconnectivity of the association and the predominance of IoT equipment ease the conversion from conventional business to smart business or Industrial IoT. Specifically, BIIoT has the following merits:

- Traceability can locate and confirm a data block's secular and spatial data kept inside the blockchain [51]. Furthermore, every information block kept during a blockchain is appended by an appropriate timestamp, subsequently ensuring data discovery [59].
- Interoperability can interact with the physical equipment and transmit data within the IIoTequipment [56]. Within the blockchain-composite layer, interoperability can be attained by constructing an overlay peer-to-peer (P2P) network on top with consistent access diagonally various IIoT schemes.
- Autonomic interactions discuss the potential of IIoT cooperating exclusive of the interference from a trusted third party (TTP). Smart contracts enabled by blockchains achieve this autonomy. Especially, contract sections surrounded in smart contracts will be implemented routinely after a particular condition is fulfilled.
- Reliability is the quality of IIoT information being reliable. Reliability is guaranteed by implementing cryptographic methods consisting of asymmetric cryptography and hash signature generation, all intrinsic in blockchains [54].

1.1. Objective

The latest on-demand production model that improves IoT technologies is called Cloud-Based Manufacturing (CBM). CBM allows omnipresent, suitable, as needed network access to a distributed pool of configurable production resources, which could be quickly given with a minimum amount of management attempt or communication of service provider. This survey proposes a decentralized, peer-to-peer system known as BIIoT for blockchain-based industrial Internet of Things. The BIIoT system acts as a key operator for CBM, improving the practicality of previous CBM systems, particularly to integrate legacy store floor apparatus in cloud surroundings. Furthermore, CBM enables on-demand access to production resources, requiring reliable intermediaries for transactions between users who desire to obtain production services. By

using blockchain technology, the BIIoT system allows peers to communicate with each other on a decentralized, peer-to-peer network without the need for a reliable mediator.

Even though BIIoT can complement IIoT, several challenges need to be addressed before successfully implementing and taking full advantage of the capability of BIIoT. Therefore, this paper aims to provide a detailed survey of the architecture that addresses challenges and discusses research problems related to BIIoT.

1.2. Contributions of this Survey article and Comparison with related Survey Articles

Several published papers talk about the combination of blockchain with IIoT. For instance, Wen et al. [6] present an information distributing system that uses blockchain within Supply Chain networks using IIoT. The system combines IIoT nodes to the blockchain, and the system monitors IIoT nodes and stores concurrent information inside the network using smart contracts. Additionally, a supply chain design based on blockchain is proposed. The proposed design suggests cooperation resolutions connecting several items inside the supply chain. Within this design for the supply chain, a well-grained distributing information system is proposed.

Li and Kang [7] have exploited the consortium blockchain technique to suggest an energy blockchain safe power business scheme [194]. This type of blockchain is widely used in universal P2P power buy and sell businesses, removing a mediator. Moreover, to reduce the contract restriction effects from contract verification slowdowns on the energy blockchain, the researchers have proposed a credit-based fee scheme to encourage short and recurrent power buy and sell by businesses.

Teslya et al. [8] have given a summary of blockchain platforms being used in Industrial IoT. The researchers provide an analysis of the most widely used consensus mechanisms and specific features of the public (permissionless) and private (permissioned) blockchains. Furthermore, an outline of blockchain platforms that satisfy the necessities for the IIoT platform development is provided.

The authors [9] have proposed a storage space arrangement, namely ChainSplitter [9], based on a hierarchical blockchain where the bulk of the blockchain is warehoused inside the clouds. The foremost new blocks are stored inside the overlying network, the separate IIoT networks [118]. The ChainSplitter flawlessly attaches native IIoT networks, the overlay network of blockchain, and therefore the cloud communications are enabled using two connectors, the blockchain and the cloud connector [46,173].

Liu et al. [10] have proposed a blockchain-enabled IIoT based deep reinforcement learning (DRL) framework. The objectives of the proposal are three-fold: 1) presenting a policy for assessing the scheme using the features of decentralization, scalability, security and latency [73]; 2) enhancing the measurability of the fundamental blockchain without disturbing the scheme's latency, decentralization, and safety; 3) outlining a blockchain which is modulable, where the producers, size and interval of the block, consensus algorithm, are chosen by the technique of Deep Reinforcement Learning (DRL).

Currently, there are surveys available on the integration of IIoT with blockchain. Explicitly, Alladi et al. [11] have given a scientific literature review on Blockchain Applications Industrial IoT and Industry 4.0 [112]. The work of [12] has reviewed blockchain technology alongside its usage in industrial IoT. Furthermore, Silva et al. [13] have surveyed the convergence of Blockchain and Industry 4.0. Fraga-Lamas et al. [14] have reviewed the use of blockchain technologies with IoT for a complicated and cyber-resilient automotive industry. Lu et al. [15] have proposed a review of applications, changes, challenges, and dangers for Blockchain technique within the gas and oil industry. Xie et al. [16] have proposed a blockchain technique survey that applies to smart cities [94,109,111,197, 200]. Juma et al. [17] have proposed the survey of trade supply chain resolutions. Furthermore, Soni [18] have planned a review on Blockchain Urgency within the IoT in the Healthcare environment.

Table 1 summarizes a selection of existing surveys on blockchain in combination with IoT. One can also observe that previous surveys concentrate on utilising blockchain in IIoT applications [114]. Therefore, the inspiration for this study comes from these earlier surveys. Principally, a study of the current works will be done, and the various benefits and challenges related to the implementation of blockchain in IIoT will be discussed.

While analyzing previous work, one aims to (i) present a conceptual preamble on IoT, IIoT and blockchain, (ii) provide a detailed examination on the ability to integrate IIoT into blockchains and (iii) offer perceptive consultations of addressing technological challenges while implementing BIIoT. In summary, the contributions are highlighted below:

1) Introduction to IoT provided an overview of the crucial feature of IoT. Additionally, challenges related to IoT are summarized.
2) Furthermore, a quick introduction to IIoT is provided along with a summary of the key characteristics of IIoT. Furthermore, research challenges related to IIoT are also outlined.

Table 1 Recent literature surveys on Blockchain for Industrial Internet of Things (IIoT).

Blockchain-based IIoT Survey Contributions	Recent Survey Articles	Addressed in this Survey
Survey of blockchain in the Food industry	[131,132,133]	✓
Survey of blockchain in Smart manufacturing industry	[63,47]	✓
Survey of blockchain in the Healthcare industry	[18,23,134]	✓
Survey of blockchain in Automotive industry	[14,137,138]	✓
Survey of blockchain in Oil and Gas industry	[15]	✓
Survey of blockchain in Trade Supply Chain industry	[17]	✓
Survey of blockchain in the Financial industry	[19,20,22]	✓
Survey of blockchain in the Energy industry	[21]	✓
Survey of blockchain in Smart Cities	[16]	✓

3) An overview of key blockchain technologies is then discussed with a summary of the key characteristics of blockchain systems.
4) The main portion of this paper is concentrated on the combination of IIoT and blockchain. Furthermore, the chances of combining IIoT with blockchain are initially examined. BIIoT Architecture is then discussed and exemplified.
5) Finally, this paper explains the BIIoT applications and descriptions of the research problems in BIIoT.

1.3. Organization of the Survey

The remaining structure of the paper is organized as follows. A summary of IoT is initially presented in Section II. Furthermore, a review of the purpose of IIoT is highlighted in Section III. Section IV provides an introduction to blockchain techniques. Finally, section V describes the integration of blockchain with IIoT.

Additionally, section VI presents the applications related to BIIoT. Section VII explains Open research problems. Finally, Section VIII concludes the paper.

2. Introduction to the Internet of Things

A group of "things" embedded by software, electronics, actuators, sensors, which are linked through the web to gather and swap information with one another [24], is termed as Internet of Things (IoT). The IoT nodes consist of sensor devices and processing energy to be present and prevalent in various industries. Fig. 1 provides numerous general IoT applications [29,102] concerning the smart city [199], smart home, healthcare and medical tools [27], smart grids, linked vehicles, among others. IoT home automation is the capability to handle domestic equipment through electronically controlled, Internet-connected systems. In addition, IoT provides novel chances for cities to utilize information to handle transportation, reduce pollution, create superior infrastructure utilisation, and maintain citizens security and cleanliness. Following that, the Smart Grid is a portion of an IoT system that could remotely monitor and handle anything like lights, traffic signs, traffic jams, parking, and prediction of things similar to power influxes as the consequences of extreme weather and earthquakes. IoT devices equipped with sensors are utilized to monitor the real-time position of medical apparatus such as wheelchairs, oxygen pumps, defibrillators, and other surveillance apparatus. One of the best promises of automotive IoT is forecast maintenance. The system collects performance data of chips and sensors placed throughout the connected car, which can be processed in the cloud and forecast before maintenance is required. Industrial IoT could link machines, apparatus, and sensors into the outlet, giving process engineers and managers much-required visibility into manufacture. For instance, companies could spontaneously monitor areas as they move by the assembly utilizing sensors including brake beams and RFID.

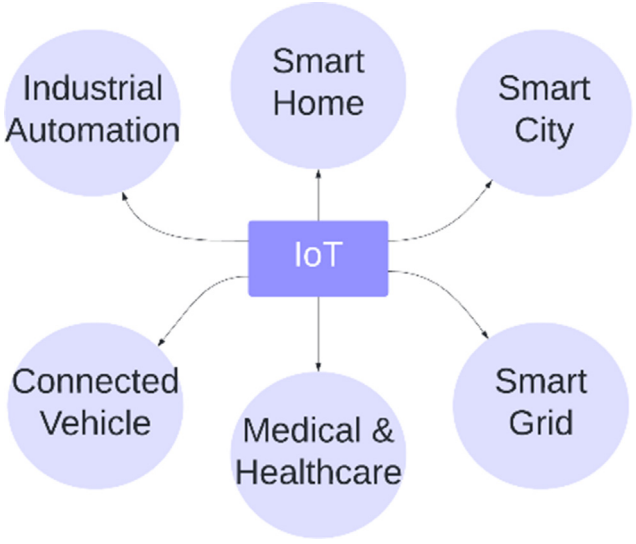

Fig. 1 Internet-of-Things Applications.

The International Data Corporation (IDC) has assured in the report published in 2013 that the rapid progression of the variety of IoT equipment used is forecasted to achieve 41 billion by 2020 with an $8.9 trillion market [1]. The difference between IoT and conventional Internet is the absence of human responsibility [30]. IoT nodes can create data related to a person's activities, examine it, and assign appropriate actions [32]. Services presented using IoT applications have enabled the improvement of human life and existence. However, confidentiality and data privacy are of paramount concern while extracting human interface data through IoT devices and sensors [48,152]. *IoT Challenges:*

The two most essential requirements in IoT devices are the battery life span along with lightweight computational requirements.

- Battery life span

Several IoT nodes are placed in the natural world where battery charge is not available. The nodes just include a bounded power to perform the planned purpose and essential safety commands that usually exhaust the node's battery power [61]. The battery life problem can be alleviated using three feasible methods. The most important method is to utilize the smallest safety needs on the node, which is not suggested, particularly when managing sensitive information [84]. The second method is to expand the battery capability. Most IoT nodes are planned and designed to be of small volume and weight, resulting in lesser space for a larger battery. The final method derives adequate power from natural sources (examples being heat, light, wind, vibration). However, these enhancements to nodes would need advanced parts and would consequently increase the financial price of nodes.

- Lightweight computation

Traditional security schemes cannot be implemented on IoT environments because the nodes contain limited memory space that cannot manage the processing and storage space necessities of improved safety procedures. The investigators have recommended using predefined tasks to assist and implement safety mechanisms for the limited battery nodes. An example would be to utilize physical layer verification by using signal progression at the receiver side to confirm that commu-

nication has arrived from the predicted spreader into the indicated spot [113]. This way of verification has little to negligible power usage as it takes advantage of radio signals.

IoT has introduced novel challenges that cannot be overcome by utilizing existing solutions available for the "conventional" Internet. Therefore, overcoming these disadvantages of IoT is of paramount importance to justify the ultimate usage of IoT and in what capacity.

- The safety and confidentiality challenge

Though it is believed that the safety resolutions presently used in the web are profitable and feasible, employing them on IoT will not produce the required outcomes for the following purposes [25]:

a. To execute complicated security procedures, nodes usually do not contain the necessary processing powers.
b. Nodes may not be physically secured and are exposed to evil users while implemented in many IoT applications.
c. To join through a node may not always be possible. For instance, a node may also be mobile and inaccessible just now, or the node is moving to be in "sleep mode" for saving power.

In several cases, these challenges are still very significant as nodes can gather sensitive and confidential data [33] and manage the essential features of our daily lives [55]. From these features, the requirement for a novel, flexible and healthy, safety resolutions that will not rely ahead on the contents and capacities of the nodes is required.

- The challenge of sustainability

While clients learn to differ or improve their "conventional" processing nodes, this is frequently not the case with IoT equipment similar to their oven, refrigerator, or car. Nevertheless, update cycles of IoT create issues regarding how such nodes will endure through a linked world. For instance, will the nodes improve their OS during their life span, or will one end up with a segregated network comprising older, insecure devices.

Furthermore, while implementing IoT instances, a node is an element of advanced communication or a remote installation node that substitutes complicated, expensive, or unfeasible implementations. For instance, earthquake or temperature sensors with flames alarms are frequently installed through the construction of a building or a river bridge, as are contamination discovery sensors installed in seabeds.

- The challenge of the trust method

Perhaps, the most significant innovation with the advent of IoT is the enhanced communication possibilities between virtual and physical worlds [26]. IoT has been imagined to incorporate everyday usage machines as nodes, which will significantly change our lives. A trusted method is desired to permit these nodes' successful and productive communication through minimal individual interference, or perhaps no interference at all [28]. The technique must incorporate performances occurring within the sensors and actuators that are valid and, at times, during critical crashes, must permit communications and allow new reward and responsibility methods [88].

3. Industrial Internet of Things introduction

New standards, innovative trade methods, competitive pressure, and the need to transport goods in time are challenges of new business establishments in the current world. As a result, many enterprises rely upon the Industrial Internet of Things (IIoT) [36], which refers to all or any performances executed by businesses to model, supervise and enhance their business processes during insights gathered from thousands of linked machines, things and computers to assist them in achieving economic profit. An IIoT, as its name implies, is a concept that connects and manages industrial things, computers, devices and machines using the Internet [83].

The combination of the industrial value chain merged with IoT is indicated as "Industry 4.0". The IIoT is the most suitable driver for innovation that can be used to save on operating expenses (OPEX) and capital expenditures (CAPEX), observe and enhance business procedures regardless of their difficulty, and permit imaginative business models [37]. IIoT has benefited from increased interest from academia and industry, giving rise to exponential innovations in newer techniques employed in the field. For instance, many sensor information is gathered and transmitted to the cloud for a smart choice using big data techniques. The 3D printing technique in manufacturing also creates modified products of multiple forms at lower prices within minimal intervals [38].

Numerous industrial and technological advancements have led to the rapid growth of the industrial IoT within recent years. The most crucial industrial development was guided by the introduction of steam engines in the 18th century. The mechanization allowed by the steam engines improved industrial manufacture from the era of clean manual labour to the automation era, which resulted in a considerable increase in production. During the 1870s, steam power machines were replaced with machines powered by electrical energy and simultaneously, the division of labour into specialized industries resulted in another industrial innovation by production explosion. The 3rd industrial revolution occurred around the 1960s, which is called "digitalization". During this revolution, programmable logic controllers and superior electronics implemented to enhance production effectiveness led to innovative automation systems.

From the 20th century to the beginning of the 21st century, information and communication methodologies evolved rapidly, producing newer technological spectrums [82]. These techniques notably enhanced industrial productivity by improving the smartness within the sensing, networking, decision making [164], and manufacturing sectors [124]. With the idea of integration, superior data gathering techniques within conventional industries, the Industrial Internet of Things is recently standard in educational and industrial sectors. In 2011, Industry 4.0 was primarily used at the Hanover Fair to introduce the 4th industrial revolution and create much awareness in Europe. Table 2 summarizes the milestones of the IIoT.

Within IIoT, machines interact to realize jobs without human intervention and are smart for different application situations related to healthcare, manufacturing, supply chain,

Table 2 Milestones of the IIoT

Revolution	Year	Technology
Manual Labor	The 1760s	Mechanization
Industrial Revolution	The 1850s	Mass Production
	The	Identification of Radio Frequency
Electrical	1940s	
Revolution	The	Digitalization and Artificial
	1950s	Intelligence
	190s	Machine Learning
	The	First Generation of Sensor
	1970s	Network
	The	3D Printing
Digital Revolution	1980s	
	1991	IoT
	2005	Cyber-Physical Systems
	2006	Cloud Computing
	2008	Big Data
	2011	Industry 4.0
IIoT Revolution	Current	IIoT

Table 3 Research Challenges of IIoT

Challenges	Description
Complexity	In IIoT, there are varieties of transmission protocols available. Standard transmission protocols consist of Bluetooth, NFC, WirelessHART, 6LoWPAN, LoRa and Sigfox; all provide various network services. For instance, the 6LoWPAN transmission coverage area is within 100 m, but the LPWAN transmission coverage area is within 1–10 km [40 41].
Heterogeneity	IIoT works using heterogeneous IIoT data types, heterogeneous communication protocols and heterogeneous IIoT devices. The heterogeneity is based on many challenges, similar to confidentiality, interoperability, and safety [74].
Resource constraints	IIoT nodes are affected by limited resources with limited battery energy, limited storage space and limited processing resource [42]. Furthermore, resource constraint leads to the IIoT nodes being susceptible to malevolent attacks [190].
Poor interoperability	Due to the heterogeneity and decentralization of IIoT systems, swapping data between various IIoTsystems, strategic centres, and industrial sectors is a challenging task. Therefore, IIoT interoperability is difficult to be achieved.
Security vulnerability	Due to the heterogeneity and decentralization of IIoT systems, security is essential for the industry. The typical methodologies of authorization [188], encryption, decryption, and authentication [75], are not suitable for IIoT due to resource constraint problems [45].
Privacy vulnerability	Due to the heterogeneity, complexity and decentralization of IIoT systems, privacy is of utmost importance. Privacy ensures that private industry data is not exposed without owner consent [165 43 119].

and home automation. Machine to Machine (M2M) [108] contact permits the IoT nodes to swap data with one another in an independent manner. The successful utilization of the machine created 'Big data' technology benefits the gathered information to improve the scheme execution by making valuable knowledge of the domain. The features of IIoT omnipresent sense, information communication, information gathering with information investigation, is considered a hopeful resolution to modernize the successful applications by linking the things and permitting combined mechanization between things and industrial processes intelligent improvement [39].

4. IIoT challenges

The IIoT guarantees the link of different things with the help of various software systems, actuators, and sensors used to sense and gather data from the physical surroundings and, consequently, generate actions using devices. The distinctive characteristics present in IIoT give rise to different research challenges, as shown in Table 3.

Some intrinsic limitations of IIoT have been overcome due to the recent advancements in information and communication technology (ICT). For example, ambient backscatter aided interactions [42] can assist IIoT devices, achieves more power. Additionally, edge computing of mobile devices [177] can expand the capability of the IIoT device by offloading the process-intensive jobs to edge servers [44 192]. Furthermore, current progress in blockchain techniques presents challenges similar to weak interoperability, safety and confidentiality vulnerabilities.

5. Blockchain technologies overview

5.1. Blockchain

A blockchain is a disseminated ledger propagating over the entire distributed system [64]. Blockchains can permit a contract to happen and validate jointly disseminated items without a trusted third party [69], with decentralized consent. Therefore, blockchains are capable of conducting decentralized confirmation [92] of contract and thereby significantly reducing the cost and reducing the operational traffic at the central organisation [70 71 186]. Furthermore, all transaction stored in blockchains is unchallengeable since all node inside the network maintains a ledger of the executed transactions inside the blockchain [67]. In the meantime, cryptographic methods assure honesty to the information blocks inside the blockchain [63 65]. Hence, the blockchains can guarantee non-negation of communications [125]. Additionally, with the assigned significant timestamp, all contracts are trackable to all users [155].

Blockchain consists of well-organized components termed blocks that have headers with transactions [72]. All header of block and other metadata are reflected by its predecessor using a predecessor's hash. The first position is hard encoded within the primary block designated the genesis block, which has no predecessor. Ethereum and Bitcoin transactions are hashed within Merkle Trees [62]. Fig. 2 shows a blockchain instance that contains blocks and repeated chains. All block during a blockchain points to its immediately preceding block (called parent block) through a converse suggestion that is, in essence, the parent block hash value. For example, block i includes the block i – 1 hash, as demonstrated in Fig. 2.

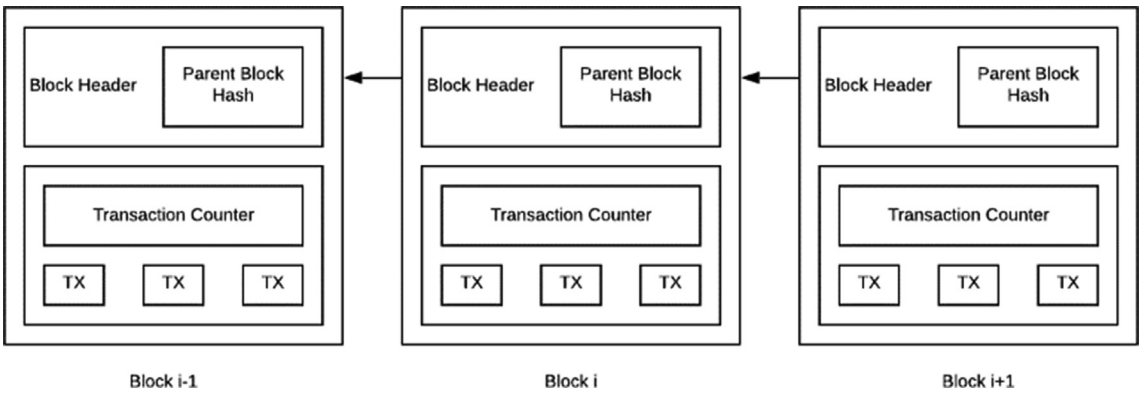

Fig. 2 Blockchain example with continuous blocks sequence.

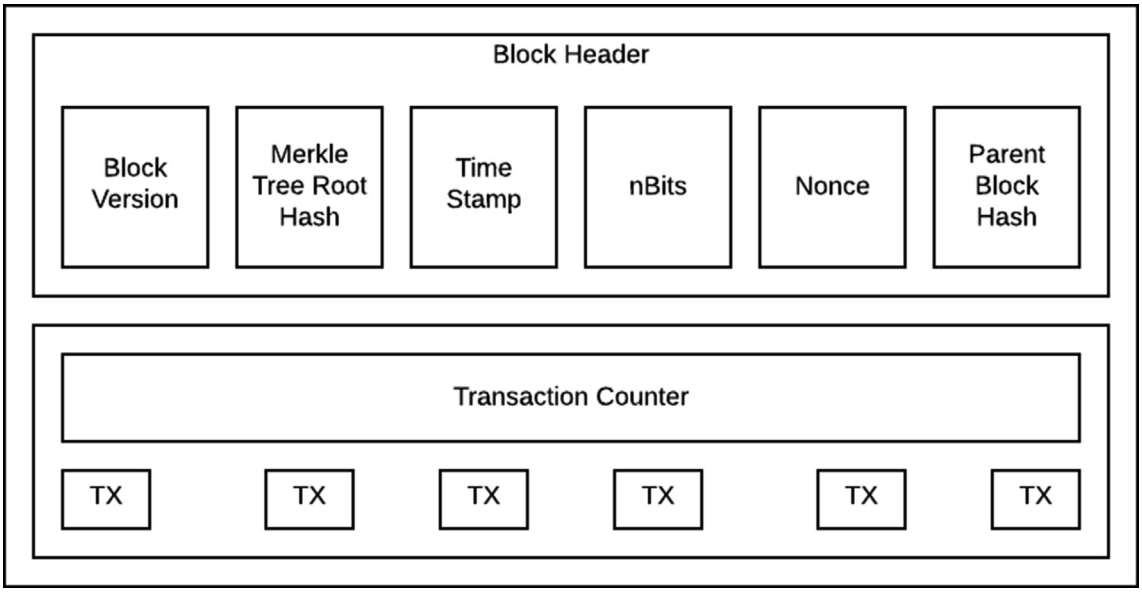

Fig. 3 Block structure.

Fig. 3 demonstrates a block that has the block header and the body. Specifically, the header of the block comprises:

1) **Block version:** denotes which block validation regulations are set to follow.
2) **Hash of Parent block:** denotes the initial block hash value, which is a 256-bit hash value.
3) **Merkle tree root hash:** which contains all transactions hash value inside the block.
4) **Nonce:** frequently begins with 0 and increases for all calculation of hash, which is a 4-byte value.
5) **Timestamp:** which has time at seconds in universal time from 1970, January 1.
6) **nBits:** a genuine block hash Point threshold.

The body of the block contains a counter for the transactions. Blockchain utilises an asymmetric cryptography method to verify the authentication of the transaction. Digital signature supported asymmetric cryptography is employed in dishonest environments [93,201].

5.2. Consensus algorithms

Within decentralized, trustless environments that exclusively require the authority of a trusted third party, one of the advantages of blockchain techniques is to confirm the trustfulness of the block. On the other hand, in distributed environments, a consensus is demanded. It needs to be reached on a recently created block since the consensus could also be biased in favour of evil devices [78 81]. This confirmation of trustfulness through decentralized environments is frequently reached with consensus algorithms [91,153]. Standard consensus algorithms comprise Practical Byzantine Fault Tolerance (PBFT), Proof of Stake (PoS) and Proof of Work (PoW). The goal of the consensus algorithms is to safely bring up to date duplicated distributed conditions and are the necessary puzzle part in efficient blockchain functioning rules. Inside the blockchain, a system called "position machine duplication", consensus protocols guarantee all copies of the distributed state are coordinated and in the contract at some specific position in time.

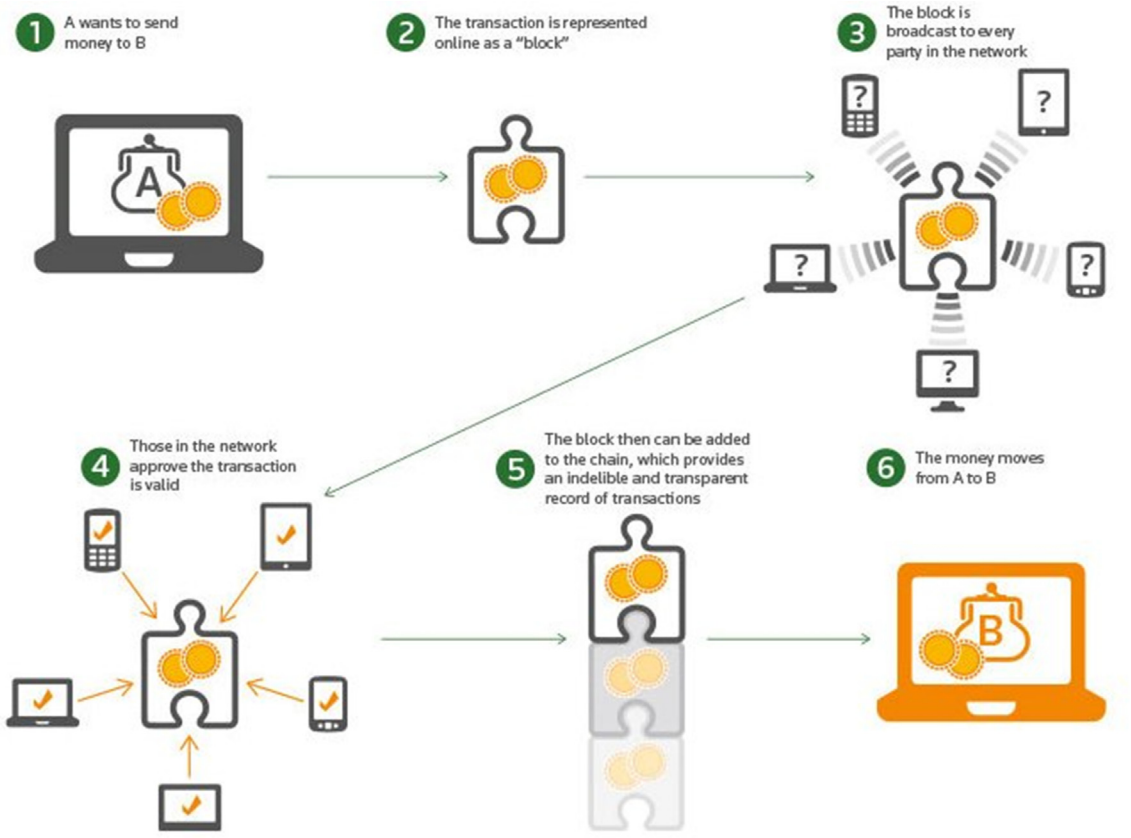

Fig. 4 Working Flow of Blockchains.

5.3. *Working flow of blockchains*

Fig. 5 illustrates the working example of the blockchain. Take a money transfer as an example, as shown in Fig. 4. In summary, blockchain technologies have a subsequent workflow.

Step 1: Person A wants to transfer an amount of cash to Person B.
Step 2: They primarily start the contract at a system using their wallet of Bitcoin [66]. The transaction includes the sender's wallet, the receiver's address, and the cash amount. The transaction is represented online as a "block".
Step 3: The block is broadcast to each node/party within the network.
Step 4: Those within the network who approve the transaction is valid.
Step 5: Next, a validated transaction is then appended to the top of the chain of contacts, subsequently developing a new block inside the blockchain.
Step 6: Finally, the cash shifts from A to B.

6. Blockchain key Characteristics:

Table 4 summarises the key characteristics of blockchain.

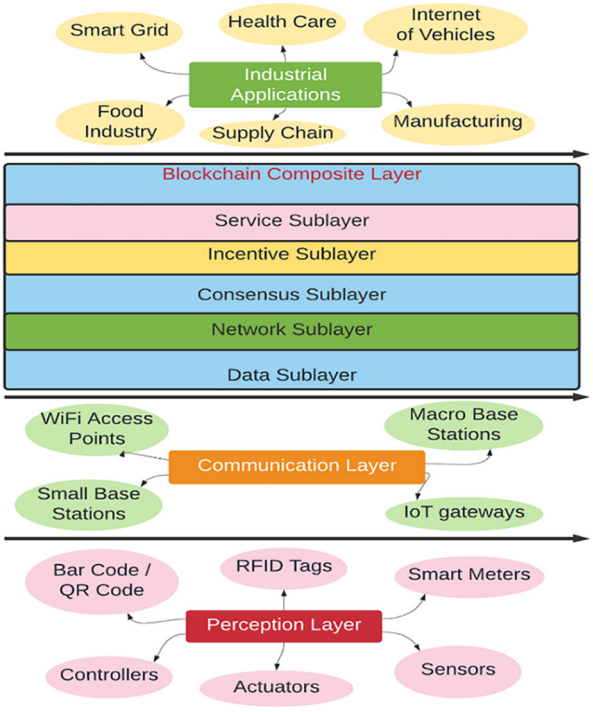

Fig. 5 Architecture of BIIoT.

Table 4 Blockchain Key Characteristics

Key Characteristics	Explanation
Immutability	A blockchain contains blocks repeatedly connected to a chain, through which all link is a converse hash of the previous block. Any alteration on the last block invalidates all the consequently created blocks. In the meantime, the Merkle tree root hash stores the hash of all the participated transactions. Any modification on any transactions makes a novel Merkle root. So, any fabrication will be easily identified. The mixing of the different hash spots and the Merkle tree can assure the truthfulness of the information.
Decentralization	In traditional decentralized transaction schemes, all transactions should be authenticated, unavoidably resulting in the expense and the implementation of traffic at the central servers. Unlike the decentralized method, the third party is not needed for several long hours. In the blockchain, consensus algorithms are needed to keep information consistent in the dispersed network.
Transparency	The blockchain information is transparent to all users who can use and confirm the participated transactions within the blockchain [104].
Non-repudiation	The process of validating the genuineness of the private keys is utilised to place the signature to the transaction, which might then be usable and confirmed by others using the equivalent public key. Therefore, the transaction which was signed cryptographically cannot be refused by the transaction originator.
Traceability	All transaction stored inside the blockchain is affixed using a timestamp. Therefore, users can confirm and track the beginning of historical information items after examining the blockchain information with equivalent timestamps.
Pseudonymity	Blockchain can protect confidentiality at a specific stage since blockchain attacks are necessary trackable through inference [157]. Blockchain information can assist in identifying scams and illegal transactions. Therefore, blockchain can just protect pseudonymity very well to provide confidentiality.
Persistency	Transactions are frequently authenticated rapidly, and truthful miners would not permit invalid transactions. It is almost impossible to delete transactions one time they are incorporated inside the blockchain. Blocks having unacceptable transactions will be revealed instantly.
Auditability	Once the current transaction is stored inside the blockchain, Bitcoin changes unspent transactions from unspent to spend. This way, transactions can be confirmed and traced [89].
Anonymity	All users can cooperate with the blockchain using a created address, which does not disclose the user's individuality. However, a point to note is that blockchain cannot assure proper confidentiality protection because of the important limitation.

Table 5 Comparison of blockchain types

Key Characteristics	PublicBlockchain	Private Blockchain	Consortium Blockchain
Scalability	Weak	Excellent	Good
Decentralization	Decentralized	Centralized	Half Decentralized
Flexibility	Weak	Excellent	Good
Consensus	PoW, PoS	Ripple	PBFT, PoA, PoET
Transparency	Apparent	Opaque	Half Transparent
Traceability	Traceable	Traceable	Partially Traceable
Immutability	Immutable	Alterable	Partially Immutable

7. Smart Contract

Smart contracts are programmable applications saved inside the blockchain that control transactions beneath particular conditions using terms. Smart contracts built on top of blockchain technology have piqued the interest of varied industries and stakeholders, leading to the technology being adopted because of its benefits by allowing the automation of verifiable and enforceable digital processes between the parties involved [76]. Therefore, smart contracts are the digital equivalent of conventional financial contracts among various appointed members [80].

Centralized approving entities force conventional contracts; a blockchain system does not need approving mediators to ensure that the restriction during a smart contract is encountered. In blockchain networks, smart contracts do the purpose of completing transactions during a pre-arranged style, prescribed by groups contributing within the contract. Smart contract code is saved within the blockchain when deployed, with the purposes marked within the smart contract are frequently evoked through some contributor at all moments.

The smart contract is usually named an "independent agent" because of the actual truth that smart contracts contain their blockchain accounts, with their addresses of blockchain. So, the contract can grasp possession of tokenized properties while appointing the contributor's employment to fulfil the approved winning circumstances. Therefore, in different fields similar to IoT and monetary services, the Smart contract is transformatively capable.

To execute and broaden purposes inside a blockchain network; Smart contracts are frequently used, such as:

1) Allowing automated transactions activated using specific actions. In numerous approaches, this functionality can occur; for instance, transactions automatically transmit at prearranged periods, or transactions transmit in reply to transactions of others.

2) They permit transactions of 'multi-signature, whereby a transaction is merely distributed when a popular or a necessary participants percentage verify to sign it.
3) Permitting storage space for particular application data, similar to membership records, boolean or lists states.
4) They give usefulness to the smart contracts of others. For instance, inheritances are often recorded into smart contracts in Ethereum, where a single contract can appeal to purposes recorded in the contract.

8. Taxonomy of Blockchain Systems

Blockchains are categorised into three categories: 1) public, 2) private, and 3) consortium blockchain [86]. Public blockchains are permissionless, where every member can contribute to distributing new blocks and using blockchain content. Public blockchains are named decentralized as it permits everyone to maintain a blockchain copy by cooperating in verifying new blocks.

Permissioned blockchains are Private blockchains, and all nodes are participating in the network [105]. Private blockchains are appropriated to one enterprise and are used as a coordinated, disseminated database destined to host data swaps between various individuals or departments. Consortium blockchains are almost similar to private blockchains. It is a permissioned network [68 95 159 199]. Consortium networks span numerous organisations and assist in keeping clarity among the participated parties [90]. A consortium blockchain is used as an auditable and dependably coordinated dispersed database that maintains data swaps fascinating path place between the contributing consortium entities [87]. Table 5 presents a contrast of blockchains three types.

8.1. Chances of combining IIoT with blockchain

IIoT systems face many challenges like weak interoperability, heterogeneity, and constraints of resource, confidentiality and safety vulnerabilities [129]. Blockchain techniques can balance IIoT systems using enhanced interoperability in addition to enhanced confidentiality and safety [100 116]. Furthermore, blockchain can improve the dependability and measurability of the IIoT system [117,163]. Thus, a combination of blockchain with IIoT is termed BIIoT. Table 6 shows the potential benefits of BIIoT in contrast to traditional IIoT systems.

9. Architecture of BIIoT

This subsection proposes the BIIoT architecture, as shown in Fig. 5. The blockchain-composite layer is utilised as a middleware through this architecture between IoT and industrial applications [103,154]. Two crucial advantages are available in this design: 1) providing a concept from the bottom IIoT layers and 2) presenting users with services based on blockchain. In particular, the blockchain-composite layer segregates the bottom layers heterogeneity [106]. Conversely, the blockchain-composite layer provides different blockchain-based services, the necessary application programming interface (API) to maintain various industrial applications [110]. Consequently, the difficulty of implementing industrial applications can be removed with the help of the concept attained through the blockchain-composite layer [127]. Specifically, the blockchain-composite layer contains five sub-layers, as shown in Fig. 6 (from bottom to top):

Furthermore, Table 7 shows the explanations of 5 sub-layers of the blockchain-composite layer.

A typical IoT infrastructure and framework that contains the subsequent layer [34] sub-scheme (from bottom to top) is highlighted in Fig. 6.

- **Perception Layer:** Several IoT devices (like actuators, sensors, RFID tags, controllers, and smart meters) can sense and gather information from the physical surroundings.
- **Communication Layer:** Numerous IoT devices can join using WiFi Access Points (APs), IoT gateways [49], macro BS, and little base stations (BS) to create an industrial network. Connectivity among IoT sensors is possible using a variety of communication protocols similar to Near Field Communications (NFC), Bluetooth, Wireless Highway Addressable Remote Transducer (WirelessHART), Low-power Wireless Personal Area Networks (6LoWPAN), Low Power Wide Area Networks (LPWAN) techniques with LoRa, Sigfox, industrial Ethernet and Narrowband IoT (NB-IoT).

Table 6 Potential Benefits of BIIoT

Potential Benefits	Explanation
Improved security	IIoT information is protected through blockchains as they are saved as blockchain transactions digitally signed and encrypted using cryptographic keys [96 147]. Furthermore, the IIoT systems combined with blockchain methodologies can improve the protection of the IIoT system by automatically updating IIoT nodes firmware to protect against susceptibility violations, thereby enhancing the system's safety [130].
Enhanced interoperability	Blockchain can enhance the interoperability of the IIoT systems while transmitting and saving IIoT information inside blockchains. Through this process, heterogeneous types of IIoT information are transformed, managed, obtained, ultimately saved and compressed in blockchains. Furthermore, the interoperability aids in directly delivering via conflicting divided network varieties while blockchains are set up on a P2P overlay network.
Autonomic interactions	Blockchain technologies can allow IIoT nodes to communicate with one another automatically. For instance, Being executed through smart contracts, Distributed autonomous Corporations (DACs) [97] can automatically execute exclusive human interference, subsequently storing the cost.
Traceability and Reliability	All the chronological transactions saved inside the blockchains are traceable [98]. Furthermore, the immutability of the blockchain guarantees IIoT information reliability since it is almost unfeasible to modify or forge each transaction saved in blockchains.

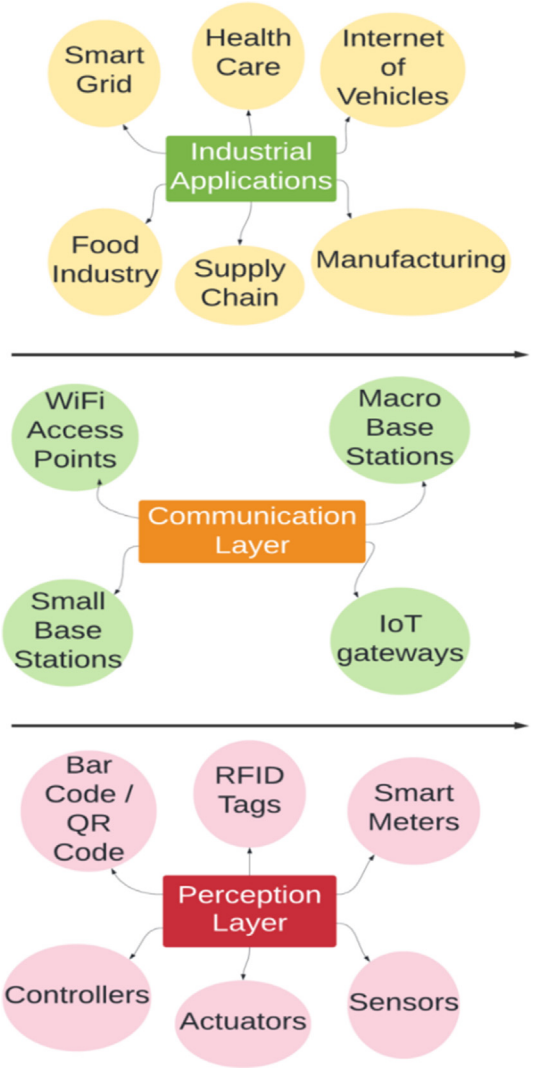

Fig. 6 Internet of Things (IoT) and Industrial Applications.

- **Industrial Applications:** IoT can be broadly used to maintain different industrial applications [107]. The typical industrial applications consist of supply chain [145], manufacturing [122], smart grid, food industry [79], Internet of vehicles [77,126] and health care.

9.1. Deployment of BIIoT

The BIIoT genuine deployment is of enormous significance, even though, due to the imitations of IIoT nodes, it is challenging to save the entire blockchain at IIoT nodes. There are two forms of storage [99]: i) partial storage, during which only information blocks subset is saved locally. Moreover, partial storage nodes are also called lightweight nodes [128]. ii) full storage, during which the whole blockchain is saved. Moreover, the full storage nodes are also called full nodes (For example, edge server, cloud server). A full node has sufficient processing resources since it needs an enormous storage space to store many entire blockchains and present processing ability to resolve puzzles of consensus. Conversely, resource-limited IoT devices [121] are lightweight devices that confirm the transaction faithfulness exclusive of extracting or storing the entire blockchain. It is a value indicating that the lightweight devices extremely trust the complete devices [120].

The BIIoT deployment is feasible in numerous communication methods between blockchain and IIoT [48]: (a) direct communication between blockchain and IIoT, during which IIoT nodes can directly use blockchain information stored at edge servers collocated by Macro Base Stations (MBS) and gateways of IIoT [186],; (b) direct communication between IIoT devices, during which IIoT devices can directly swap partial blockchain information via D2D connections; (c) hybrid communication of edge servers and cloud through IIoT nodes, through which IIoT nodes can interrelate with blockchain information via cloud or edge servers [180].

Table 7 5 sub-layers of blockchain-composite layer

Sub-layers	Description
Data sub-layer	The Data sub-layer gathers the IoT information from the perception layers and enfolds the encrypted information using hash methods and asymmetric cryptographic techniques. These repeatedly linked information blocks create the blockchain after dispersed confirmation. Different blockchain proposals may select different hash methods and cryptographic techniques. For instance, the Bitcoin blockchain selects SHA-256 for the hash method.
Network sub-layer	In an overlay peer to peer network, a Network sub-layer is essential, which runs on top of the communication layer. This network contains either physical or virtual connections linking devices inside the robust networks of communication. One node transmits the transactions block to its connected peers. Once getting the transactions block, another peer will locally confirm it. If it is legitimate, the block will be propagating to another device via the overlay network.
Consensus sub-layer	For the block reliance, the Consensus sub-layer mainly participates in the disseminated consensus. The consensuses are attained using consensus algorithms similar to PoS, PoW, DPOS and PBFT [21].
Incentive sub-layer	The subsequent jobs Incentive sub-layer is chargeable: 1) issuing digital money, 2) sharing digital money, 3) reward method designing, 4) transaction price managing, among others. In particular, it is essential to design a proper digital money financial policy, disseminate rewards to contributors who participate in disseminated consensus.
Service sub-layer	In numerous industrial areas consisting of logistics, manufacturing, food industry and supply chains [123], service sub-layer offers users services based on blockchain. For instance, a contract of payment is implemented automatically when a customer obtains a product.

9.2. BIIoT applications

Currently, a novel rapid growing trend is the combination of Blockchain with IIoT. Since a Blockchain technique can assist in addressing the challenges of IIoT, this section presents a BIIoT applications summary. The value of the summary is to declare that there is a superior variety of applications of blockchains [158]. Through this paper, the essential concentration is on industrial applications.

9.3. Food sector

BIIoT can improve the life cycle of commodities visibility, mainly in the food industry. Especially, traceability of food products is essential to make sure of food protection [146]. However, it is difficult for the current IoT to ensure food traceability inside the entire food supply chain [131]. For instance, a food-producing organisation could be stipulated by numerous providers [139]. Therefore, there is a need to digitize materials from sources to the entire food manufacturing sector [141]. Through this process, blockchain techniques can ensure the tracking ability and origin of the food [142].

[131] highlighted the need to utilize the blockchain technique and RFID to establish a supply chain platform from farming to food manufacturers in China. To guarantee the food supply-chain data trackability, this methodology has been established [143]. In the meantime, the work of [132] demonstrates that blockchain techniques can assist in increasing food protection by the accessibility of trackable food productions [144]. Furthermore, it shows in [132] that the combination of blockchain in the food supply chain can allow consumers to track the total procedure of food manufacture [148]. Researchers moreover provide a use-case of using blockchain for the Colombian natural coffee industry.

Additionally, [133] poses a food protection trackability scheme encouraged by the Electronic Product Code (EPC) IoT tags and blockchain. In particular, this method can prevent information interference and confidentiality revelation through smart contracts [73]. An archetype of the posed architecture has been executed to show efficiency [176].

9.4. Smart manufacturing sector

The manufacturing industry is experiencing improvement from "mechanical to smart manufacturing" [63]. In the manufacturing industry, big data analytics plays a vital role in this improvement procedure. Enormous information is created through every phase of the life cycle of commodities containing material supply, manufactured goods designing, sharing, manufacturing, after-sales repair and retail. However, the manufacturing information is extremely pieced, resulting in information aggregation and analytics [149]. BIIoT can tackle the interoperability problem by connecting IIoT systems via Peer to Peer networks and permitting information distribution across industrial divisions.

For instance, numerous dispersed blockchains are frequently built to support multiple sectors, and every blockchain supports an individual sector. BIIoT can enhance smart manufacturing security [124]. During one of the most crucial traffic restrictions, the improvement of factories is that the IIoT schemes are kept centralized. For instance, IIoT firmware should be improved frequently to address safety violations. Although, most of the firmware improved are imported from a central server and then is physically installed at IIoT nodes. It is costly and cumbersome to deploy the firmware upgrades in a disseminated IIoT. The work of [63] presents a routine firmware improvement resolution that engages blockchains and smart contracts. Specifically, smart contracts addressing the firmware improvement approaches are organized across the entire industrial network.

Nodes can install and import the hashes of firmware using smart contracts and are implemented by design. Furthermore, an automatic manufacturing proposal based on decentralized blockchain was posed in [63] to provide a more robust safety and confidentiality defence than usually centralized architecture. Moreover, in smart manufacturing, a mobile crowdsensing system based on blockchain was posed to solve the problem by information excellence pledge [47].

9.5. Healthcare sector

Healthcare is in transition as the fast convergence of digital technologies holds the promise to liberate clinical data and provide a more cost-effective way of improving clinical processes and outcomes. Healthcare poses novel challenges in current healthcare services because of the limited resources of hospitals [150]. The recent progress in wearable healthcare equipment and BDA in healthcare information increases the chances of encouraging remote healthcare facilities. Therefore, the resources of hospital burdens are frequently and capably discharged. For instance, senior citizens residing at their houses are wearing the healthcare equipment on their bodies. This equipment [174] always determine and gather healthcare information containing sugar level, rate of heartbeat, and blood pressure analysis. Healthcare teams and doctors can use healthcare information anywhere and anytime through the networks of healthcare. However, using healthcare information comes with issues related to confidentiality, privacy and security.

Vulnerabilities present in healthcare equipment and networks heterogeneity propose challenges in protecting confidentiality and guaranteeing healthcare information safety. Integrating healthcare networks into blockchains can capably overcome challenges in confidentiality protection and safety pledge of healthcare information. For instance, [134] demonstrates that one can defend healthcare information saved in cloud servers based on blockchain techniques. Notably, the healthcare information created with medical sensors is frequently and routinely gathered and broadcast to the scheme based on smart contracts to sustain real-time patient observation. Through the whole process, using blockchains, confidentiality is frequently conserved.

Moreover, in decentralized healthcare blockchain systems [152], Rahman et al. [135] place signature schemes based on the attribute. This scheme can confirm the healthcare information genuineness and detection of the healthcare information possessor. Conversely, this scheme moreover can protect the confidentiality of the healthcare information possessor. The current work [135] provides a framework for in-home therapy managing by combining blockchain-based MEC and IoT to provide confidentiality and secrecy. Furthermore, blockchain gives traceability options over the patients who are infected

through several infectious viruses similar to Middle East Respiratory Syndrome (MERS), Severe Acute Respiratory Syndrome (SARS), and Novel COVID-19 [136]. Notably, the suspected or infected patients wearing IIoT equipment can be tracked sequentially, similar to quarantine while protecting the patient's confidentiality. Despite the potentially transformative effects, research on blockchain in the healthcare field is still in its infancy. As a result, our knowledge of the impacts of blockchain is still far from conclusive.

9.6. Automotive Industry

The automotive industry is among the leading technically superior sectors by novelties scaling from electric, hybrid, and self-driving smart cars to the industrial Internet of Things (IIoT) combination inside IoT linked cars. However, underneath the Industry 4.0 concept, which characterizes the stage following the digitalization sector, the automotive industry is countenancing operational incompetence and safety problems that direct needless casualties, cyber-attacks, defeats, occurrences, prices inflated costs for services and fractions [192]. Such issues are recently approved on to the different and heterogeneous stakeholders who participated in the vehicle's lifecycle [181]. Industry 4.0 exploits the progress from numerous fields, which allow for the deployment of the enormous sensors, the application of immense information technologies, the advances in processing energy, and connectivity the appearance of newest machine learning methods, the latest processing methods growth, IIoT improvements [138], new human to machine interfaces [137] or 3D or 4-D printing and the robotics use.

The growing abilities presented through complicated heterogeneous linked and independent networked organisms permit various services and features. However, they exist by the malicious attacks risk or other threats that need cybersecurity to be more robust. Moreover, in situations where the restricted organisms are vehicle-associated systems, open protection is pledged, so robust cyber safety becomes a significant necessity [196]. To distress this difficulty, BIIoT technology can be utilised in the automotive industry.

9.7. Oil and gas sector

For the next 20–30 years, oil and gas will still control the global energy market. As oil and gas resources play a significant role inside the energy field, the oil and gas industry technologies have been implemented rapidly in current years, including clever drilling techniques, marine digital platforms and smart oil and gas fields. It is frequently seen that the oil and gas industry is progressively implementing digitalization, intellectualization, and automation. Though its organisation manner is comparatively aged, it is the individuality of short effectiveness, high price, high threat and long period.

These industries are separated into three sections consistent with the market division: downstream, midstream and upstream. The downstream refers to the sales and storage, the midstream refers to the oil and gas transportation [151], and the upstream refers to the growth and exploration of oil and gas. In several markets, there are numerous limitations in managing, which are shown in Table 8.

Based on the above issues, the time has come for the oil and gas industry to varying its management mode. A blockchain technique possesses a huge capacity of being utilised in the industry of oil and gas. In 2008, the Bitcoin appearance activated a boom inside the blockchain technique improvement [15,175]. Within the opening, the oil and gas industry has been grasping a wait-and-see approach and rarely comprised. Until 2017, British Petroleum (BP) started testing the blockchain scheme, and due to this, the oil and gas industry took the most critical step towards using the blockchain technique. BIIoT can resolve the above problems and improve the safety of the oil and gas industry.

9.8. Trade supply chain industry

The trade supply chain ultimately leads to distributing the products to the customer [17]. The trading method contains a lawful combined contract between buyer and seller, which denotes all parties' circumstances for successful trade achievement. As an example, these situations could identify the appropriate transport technique for merchandise. A third party frequently checks the trading procedure. The significant task of this entity is to outline particular that all party satisfies the conditions of the contract.

In case of an argument between buyer and seller, the regulatory entity will solve the issue. For example, consumers who utilize the Amazon trading platform can notify the platform's administration if they obtained commodities that do not match the posted depiction by the vendors. The used data-distribution method must confirm the swapped data truth to simplify the trading technique between buyer and seller [193]. The difficulty of the trading procedure rises notably within worldwide trading.

Global trade contains many parties, mostly with the trading group of people (exporters and importers), shipping agents,

Table 8 Problems and Outcomes in Several Markets in the Oil and Gas Industry

Market	Issue	Cause	Consequence
Upstream	Equipment Tracking Difficulties	The number of devices is significant, and also the management of asset integrity is not perfect.	Human error, huge supervision fine.
	Data Leakage	The location where the information is generated is different, or the information is not well stored and processed.	Incorrect data result in wrong decisions.
Midstream	Data handling and Replication	Duplicate third party transactions or duplicate contracts between different parties.	Increases operating costs, erroneous transactions and delayed transactions.
Downstream	Integrity and Security	Close networks are susceptible to external attacks.	Fraud, Loss of Trust, increased validation cost.

customs agencies, freight forwarders, port operators, and customs brokers. The difficulty of guaranteeing the honesty of the swapped data is frequently tackled by presenting a trackable protected scheme that allows the trade contributors to understand access to the data during a suitable style. Once a document is submitted through this system, contributors gain access to the current report assisted by their position inside the trade model. Moreover, the scheme must be ready to allow users to trace the shipment status through the whole trade supply chain model [140]. Towards this end, BIIoT can be used to optimize the (international) trade supply chain. BIIoT has modernized the method during which faith is often recognized between entities [156]. Thus, the trade supply chain contributors can distribute their data with no confidentiality concern.

Table IX summarizes major BIIoT applications. Notably, in Table 9, it can be seen that integrating IoT with blockchain can bring a variety of advantages within the applications mentioned above. In outline, BIIoT has benefits similar to ensuring safety, decreasing the cost for trusted third parties, confirming the authenticity of the information, enhancing information traceability and preserving confidentiality.

9.9. BIIoT open research issues

The combination of IIoT with blockchain provides numerous opportunities for improving the industry. However, there are many challenges [161 184] that needs to be tackled before the capability of BIIoT is frequently and wholly utilised. In this section, many fundamental challenges involved in integrating IIoT into the blockchain has been explored. Table 10 shows the overview of the open research problems for BIIoT.

9.10. Privacy leakage

Blockchain techniques contain several mechanisms to protect from extracting information confidentiality of transaction reports stored in blockchains [166]. For instance, transactions are created in Bitcoin using IP addresses rather than consumers genuine individuality, thereby guaranteeing individual anonymity [172 179]. Furthermore, one-time accounts can be made in Bitcoin to aid the user's anonymity even though; these defence systems are unreliable and insufficient. For example, it

Table 9 Comparison of BIIoT Applications

Applications	Benefits
Food industry	• Enhancing food safety • Improving data traceability
Smart manufacturing industry	• Business trading of P2P computerization • Improving interoperability • Trusted third party price decreasing
Healthcare industry	• Preserving privacy • Assuring security • Verifying authenticity
Automotive industry	• Securing energy-trading in electric vehicles • Assuring trustworthiness of messages • Guaranteeing mutual-confidence among Unmanned Aerial Vehicles
Financial industry	• Decreasing the time and financial prices of the transaction • Decreasing the threats of mistake, scam, and ineffectiveness in transactions • Reducing cost for trusted third party • Reducing risks from cyber-attacks
Trade Supply Chain industry	• Decreasing the prices in services • Assuring data provenance • Diminishing the supply chain threat

Table 10 Open research problems for BIIoT

Research Direction	Description
Privacy leakage	• Full storage of transaction data on the blockchain can also lead to potential privacy leakage [162].
Security vulnerability	• Blockchain systems have their safety vulnerabilities similar to program deficiencies of smart contracts [168]. • Malevolent users can use Border Gateway Protocol (BGP) routing system to hijack blockchain messages [167].
Resource constraints	• IIoT nodes may have processing difficulty for directly providing transactions to the blockchain. • Blockchain linked gateways of IIoT require significant processing and storage space abilities to be a peer.
Scalability	• Many blockchain systems are experiencing weak throughput. • Blockchain systems may not be appropriate for applications with a vast quantity of transactions, particularly for IIoT.
Big data Difficulty	• IIoT nodes, due to the limitations of the resources, cannot use the usual BDA approaches. • It is challenging to perform information analytics on anonymous blockchain information.

is observed [66] that consumer pseudonyms are frequently cracked through deducing and learning the numerous transactions associated with one general user. Moreover, the whole storage space of transaction information on the blockchain can still affect the capable confidentiality leakage, as pointed in [66].

9.11. Security vulnerability

Even though integrating blockchain techniques into IIoT can enhance the IIoT security using cryptography and signature generation by blockchains, the protection remains severe anxiety to BIIoT because of the vulnerabilities of blockchain and IIoT systems [169]. On the one hand, there is a rising tendency in establishing wireless networks within industrial environments because of the measurability and possibility of wireless communication organisations. However, on the other hand, the open wireless channel creates issues in IIoT by the safety violations similar to jamming, submissive overhearing, and repeating attacks [24 185]. Furthermore, due to the constraints of resources of IIoT nodes, usual extreme weighted encryption techniques may not be feasible in IIoT [1 188]. Moreover, it is tough to supervise the keys in dispersed environments [170].

Meanwhile, blockchain schemes still have their security vulnerabilities similar to program deficiencies of smart contracts. Mainly, it can be seen in [53] that malevolent users can use the Border Gateway Protocol (BGP) routing method to control blockchain messages, thereby most relevant to the block broadcasting upper delay. The work of [53] explains that a Decentralized Autonomous Organization (DAO) attack stole the $50 million value of Ethereum by influencing the smart contracts vulnerability.

9.12. Constraints of resources

Many IIoT nodes are resource-constrained. For instance, RFID tags, sensors and smart meters have lesser processing ability, bounded storage space, low battery energy and weak network linkability. Additionally, the blockchains decentralized consensus algorithms frequently need more processing power and have higher power expenditure [189]. For instance, PoW in Bitcoin is shown to present high power expenditure [46]. Therefore, the consensus method [195] with enormous power expenditure might not be possible for low-energy IIoT nodes.

Conversely, the large size of blockchain information moreover directs to the impossibility of entirely deploying blockchains across IIoT. For instance, by the end of September 2018, the size of the Bitcoin blockchain almost attained 185 GB. It is unfeasible to save the whole blockchain on an IIoT node entirely. Furthermore, blockchains are mostly planned for a situation supported by the steady network link, which cannot be possible for IIoT that forever affects the weak network link of IIoT nodes and the unsteady network due to the failure of the node.

9.13. Scalability

The current blockchains scalability restricts the use of the broad blockchain in extensive IIoT [171]. The transactions throughput per second frequently measures the scalability of the blockchain and the IIoT nodes size, and the number of simultaneous workloads [59]. Many blockchain schemes have suffered due to weak throughput [179]. For instance, it can be seen in [59] that Bitcoin developed seven transactions per second. On the contrary, PayPal has a throughput of 170 transactions per second, and VISA can create almost 2,000 transactions per second [182]. Ref. [59] shows that the blockchain of Bitcoin might not be appropriate for IIoT because of the weak measurability. Therefore, the current blockchain systems might not suit applications with many transactions, particularly for IIoT.

9.14. Big data difficulty

There are large numbers of IIoT information and data being created in most real-time approaches. The IIoT information is seen to be of enormous volume, heterogeneity and large industry worth. Big data examination on IIoT information can extract hidden information and create smart choices. However, it is difficult to apply traditional big data investigation methods in BIIoT because of the following reason:

- ***Traditional Big Data Analysis (BDA) systems cannot be used on IIoT nodes because of resource limitations***. While IIoT nodes have lesser processing ability, the intricate BDA systems cannot directly be organized at IIoT nodes. Furthermore, the large blockchain information size makes it challenging to use the native storage space of blockchain information at IIoT nodes. Though cloud computing can tackle these problems, exporting the data to remote cloud servers can guide the confidentiality violation and increase latency [160].
- ***It is challenging to conduct information analytics on unknown blockchain information***. Blockchain techniques can defend information confidentiality using cryptography and signature generation schemes on information reports. Nevertheless, it frequently needs information cryptography previous to performing information analytics. However, the cryptography procedure is often time-consuming and contributes to data investigation's ineffectiveness [160]. Therefore, it is challenging to design information analytics methods on blockchain information exclusive of cryptography.

This section shows blockchain as a promising methodology with plenty of opportunity for more expansion, particularly in the IIoT field.

10. Conclusion

Recent Industrial Internet of Things technologies incorporates numerous challenges that include weak interoperability, heterogeneity, confidentiality and safety vulnerabilities and limitations of resources. Challenges found in IIoT can be overcome by using a current form of blockchain techniques that provides solutions by enhanced confidentiality, interoperability, trackability, safety, and dependability. Throughout this paper, a study has been conducted by combining IIoT with blockchain. Such a combination of blockchain with IIoT is termed BIIoT, and a full survey of existing research in this field has been undertaken in this paper. Mainly, the Internet of Things, Industrial Internet of Things and blockchain technol-

ogy has been researched and presented. The article has also evaluated the possibilities of using BIIoT and portrays BIIoT architecture. BIIoT capable applications have been further depicted along with a summary of BIIoT open research problems. The existing security systems of IIoT are highly centralized, meaning they have a single point of failure. But Blockchain-based IIoT is very resilient to hacking and other external attacks. There is no risk of data loss as the same data is stored on all nodes in the blockchain. Future work will implement and demonstrate the BIIoT system for realistic solutions such as device self-service and on-demand manufacturing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This paper was supported by Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (P0008703, The Competency Development Program for Industry Specialist) and also supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2021-2018-0-01799) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation).

References

[1] Y. Yang, L. Wu, G. Yin, L. Li, H. Zhao, A survey on security and privacy issues in internet-of-things, IEEE Internet Things J. 4 (5) (2017) 1250–1258.
[2] Guizi Chen, Wee Siong Ng, "An Efficient Authorization Framework for Securing Industrial Internet of Things"., Proc. of the 2017 IEEE Region 10 Conference (TENCON), Malaysia, November 5-8, 2017.
[3] M. Tiago, Fernández-Caramés, Paula Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things", IEEE Access VOLUME X (2018), https://doi.org/10.1109/ACCESS.2018.2842685.
[4] Hoang Giang Do, Wee Keong Ng, "Blockchain-based System for Secure Data Storage with Private Keyword Search", 2017 IEEE 13th World Congress on Services, DOI 10.1109/SERVICES.2017.23, 2017.
[5] J. Huang, L. Kong, G. Chen, M.Y. Wu, X. Liu, P. Zeng, Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism, IEEE Trans. Ind. Inf. 15 (6) (Jun. 2019) 3680–3689.
[6] Q. Wen, Y. Gao, Z. Chen, D. Wu, A Blockchain-based Data Sharing Scheme in The Supply Chain by IIoT, 2019 IEEE International Conference on Industrial Cyber-Physical Systems (ICPS), 2019.
[7] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, Y. Zhang, Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things, 2017 IEEE Transactions on Industrial Informatics, 2017.
[8] N. Teslya, I. Ryabchikov, Blockchain Platforms Overview for Industrial IoT Purposes, 2019 IEEE proceeding of the 22nd conference of fruct association, 2019.
[9] G. Wang, Z. J. Shi, M. Nixon and S. Han, "ChainSplitter: Towards Blockchain-based Industrial IoT Architecture for Supporting Hierarchical Storage", 2019 IEEE International Conference on Blockchain (Blockchain) DOI 10.1109/Blockchain.2019.00030.
[10] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, M. Song, "Performance Optimization for Blockchain-Enabled Industrial Internet of Things (IIoT) Systems: A Deep Reinforcement Learning Approach"., 2018 IEEE Transactions on Industrial Informatics, DOI 10.1109/TII.2019.2897805.
[11] T. Alladi, V. Chamola, R.M. Parizi, K.K.R. Choo, Blockchain Applications for Industry 4.0 and Industrial IoT: A Review, IEEE Distributed Computing Infrastructure for Cyber-Physical Systems (November 2019), https://doi.org/10.1109/ACCESS.2019.2956748.
[12] Rathee G., Gupta S.D., Jaglan N. (2020) A Review on Blockchain and Its Necessitate in Industrial IoT. In: Saini H., Sayal R., Buyya R., Aliseri G. (eds) Innovations in Computer Science and Engineering. Lecture Notes in Networks and Systems, vol 103 Springer, Singapore.
[13] Silva T.B, Morais E.S, Almeida L.F.F, Rosa Righi R, Alberti A.M. (2020) Blockchain and Industry 4.0: Overview, Convergence, and Analysis. In: Rosa Righi R., Alberti A., Singh M. (eds) Blockchain Technology for Industry 4.0. Blockchain Technologies Springer, Singapore.
[14] P. Fraga-Lamas and T. M. Fernández-Caramés, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," IEEE Access, vol. 7, pp. 17 578–17 598, 2019.
[15] H. Lu, K. Huang, M. Azimi, and L. Guo, "Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks," IEEE Access, vol. 7, pp. 41 426–41 444, 2019.
[16] J. Xie, H. Tang, T. Huang, F.R. Yu, R. Xie, J. Liu, Y. Liu, A survey of blockchain technology applied to smart cities: Research issues and challenges, IEEE Commun. Surv. Tutorials (2019).
[17] H. Juma, K. Shaalan, I. Kamel, A Survey on Using Blockchain in Trade Supply Chain Solutions, IEEE Access 7 (December 2019), https://doi.org/10.1109/ACCESS.2019.2960542.
[18] R. Soni, G. Kumar, A Review on Blockchain Urgency in the Internet of Things in Healthcare, IEEE Int. Conf. Intell. Sustain. Syst. (ICISS) (November 2019), https://doi.org/10.1109/ISS1.2019.8908021.
[19] R. Beck, M. Avital, M. Rossi, et al, Blockchain Technology in Business and Information Systems Research, Bus Inf Syst Eng 59 (2017) 381–384, https://doi.org/10.1007/s12599-017-0505-1.
[20] N. Atzei, M. Bartoletti, T. Cimoli, "A survey of attacks on ethereum smart contracts (SoK),'.' in Principles of Security and Trust, Springer, Berlin, Germany, 2017, pp. 164–186.
[21] Megha S., Lamptey J., Salem H.M., Mazzara M. (2020) "A Survey of Blockchain-Based Solutions for Energy Industry", Artificial Intelligence and Network Applications, WAINA 2020, Advances in Intelligent Systems and Computing, vol 1150, Springer, Cham.
[22] A. Lazarenko, S. Avdoshin, "Financial Risks of the Blockchain Industry: A Survey of Cyberattacks" Proceedings of the Future Technologies Conference, Advances in Intelligent Systems and Computing vol 881 (2019).
[23] Tariq F., Anwar M., Janjua A.R., Khan M.H., Khan A.U., Javaid N. (2020) "Blockchain in WSNs, VANets, IoTs and Healthcare: A Survey", Artificial Intelligence and Network Applications, WAINA 2020. Advances in Intelligent Systems and Computing, vol 1150, Springer, Cham
[24] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications, IEEE

Internet Things J. 4 (5) (2017) 1125–1142, https://doi.org/10.1109/JIOT.2017.2683200.
[25] Imran Makhdoom, Mehran Abolhasan, Justin Lipman, Ren Ping Liu, Wei Ni, "Anatomy of threats to the Internet of Things", IEEE Commun. Surv. Tutorials, DOI 10.1109/COMST.2018.2874978, 2018.
[26] Arsalan Mohsen Nia, Niraj K. Jha, "A comprehensive study of the security of Internet-of-Things"., IEEE Trans. Emerg. Top. Comput. (2017), https://doi.org/10.1109/TETC.2016.2606384.
[27] Yang Yang, Ximeng Liu, Robert H. Deng, Lightweight break-glass access control system for healthcare Internet-of-Things, IEEE Trans. Ind. Inf. (2017), https://doi.org/10.1109/TII.2017.2751640.
[28] Wen-Long Chin, Wan Li, and Hsiao-Hwa Chen, "Energy Big Data Security Threats in IoT-Based Smart Grid Communications", IEEE Communications Magazine, October 2017.
[29] Shahid Mumtaz, Ahmed Alsohaily, Zhibo Pang, Ammar Rayes, Kim FUNG Tsang, And Jonathan Rodriguez, "Massive Internet Of Things For Industrial Applications. Addressing Wireless IIoT Connectivity Challenges and Ecosystem Fragmentation", IEEE Industrial Electronics Magazine, March 2017.
[30] KimchaiYeow, Abdullah Gani, Raja Wasim Ahmad, Joel J. P. C. Rodrigues, "Decentralized Consensus ForEdgecentric Internet Of Things: A Review, Taxonomy, And Research Issues", IEEE Access Preliminary Draft Copy Only, IEEE Access Journal, Vol 18, No 8, October 2017.
[31] Yuanyu Zhang, Shoji Kasahara, Yulong Shen, Xiaohong Jiang, Jianxiong Wan, Smart contract-based access control for the internet of things, IEEE Internet Things J. (2018), https://doi.org/10.1109/JIOT.2018.2847705.
[32] Vangelis Gazis, A survey of standards for machine-to-machine and the Internet of Things, IEEE Commun. Surv. Tutorials (2017), https://doi.org/10.1109/COMST.2016.2592948.
[33] Marco Conoscenti, Antonio Vetro, Juan Carlos De Martin, "Peer to Peer for Privacy and Decentralization in the Internet of Things"., IEEE/ACM 39th IEEE International Conference on Software Engineering Companion 2017.
[34] Jingzhong Wang, Mengru Li, Yunhua He, Hong Li, Ke Xiao, and Chao Wang, "A Blockchain-Based New Secure Multi-Layer Network Model for Internet of Things", IEEE Access, Volume 6, 2018.
[35] Hong-Ning Dai, Zibin Zheng, Yan Zhang, Blockchain for the Internet of Things: A Survey, IEEE Internet Things J. (2019), https://doi.org/10.1109/JIOT.2019.2920987.
[36] P. Lade, R. Ghosh, S. Srinivasan, Manufacturing Analytics and Industrial Internet of Things, IEEE Intell. Syst. Volume: 32 (2017) Issue: 3.
[37] S. Katsikeas, K. Fysarakis, A. Miaoudakis, A. V. Bemten, I. Askoxylakis, I. Papaefstathiou and A. Plemenos, "Lightweight & secure industrial IoT communications via the MQ telemetry transport protocol", IEEE Symposium on Computers and Communications (ISCC), 2017.
[38] J. q. Li, F. R. Yuy, G. Deng, C. Luo, Z. Ming, and Q. Yan, "Industrial Internet: a survey on the enabling technologies, applications, and challenges", IEEE Communications Surveys & Tutorials, DOI 10.1109/COMST.2017.2691349, 2017.
[39] Zhaozong Meng, Wu. Zhipeng, Cahyo Muvianto, John Gray, A data-oriented M2M messaging mechanism for industrial iot applications, IEEE Internet Things J. (2017), https://doi.org/10.1109/JIOT.2017.2646375.
[40] M. Chen, Y. Miao, Y. Hao, and K. Hwang, "Narrow Band Internet of Things," IEEE Access, vol. 5, pp. 20 557–20 577, 2017.
[41] O. Khutsoane, B. Isong, A.M. Abu-Mahfouz, IoT devices and applications based on LoRa/LoRaWAN, in: in IECON 2017–43rd Annual Conference of the IEEE Industrial Electronics Society, 2017, pp. 6107–6112.
[42] X. Lu, D. Niyato, H. Jiang, D.I. Kim, Y. Xiao, Z. Han, Ambient Backscatter Assisted Wireless Powered Communications, IEEE Wirel. Commun. 25 (2) (April 2018) 170–177.
[43] J. Zhou, Z. Cao, X. Dong, A.V. Vasilakos, Security and Privacy for Cloud-Based IoT: Challenges, IEEE Commun. Mag. 55 (1) (January 2017) 26–33.
[44] J. He, J. Wei, K. Chen, Z. Tang, Y. Zhou, Y. Zhang, Multitier fog computing with large-scale iot data analytics for smart cities, IEEE Internet Things J. 5 (2) (April 2018) 677–686.
[45] A. AlAbdullatif, K. AlAjaji, N. S. A. Serhani, R. Zagrouba, M. AlDossary, "Improving an Identity Authentication Management Protocol in IIoT"., 2nd International Conference on Computer Applications & Information Security (ICCAIS), July 2019.
[46] C. Xu, K. Wang, M. Guo, "Intelligent resource management in blockchain-based cloud data centres", IEEE Cloud Computing, 2017.
[47] J. Huang, L. Kong, H.N. Dai, W. Ding, L. Cheng, G. Chen, X. Jin, P. Zeng, Blockchain-based mobile crowdsensing in industrial systems, IEEE Trans. Ind. Inf. (2020).
[48] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey", IEEE Communications Surveys & Tutorials, Vol. 21, No. 2, Second Quarter 2019.
[49] C. H. Chen, M.Y. Lin, and C.C. Liu, "Edge computing gateway of the industrial internet of things using multiple collaborative microcontrollers", IEEE Network, January/February 2018.
[50] Xu. Xiwei, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, Paul Rimba, A taxonomy of blockchain-based systems for architecture design, IEEE Int. Conf. Softw. Archit. (2017), https://doi.org/10.1109/ICSA.2017.33.
[51] Q. Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability", IEEE Software, November/December 2017.
[52] P. K. Sharma, S. Singh, Y.S. Jeong, and J. H. Park, "Distblocknet: A distributed blockchain-based secure SDN architecture for IoT networks", IEEE Communications Magazine, September 2017, Digital Object Identifier: 10.1109/MCOM.2017.1700041
[53] M. Apostolaki, A. Zohar, L. Vanbever, Hijacking Bitcoin: Routing attacks on cryptocurrencies, IEEE Sympos. Secur. Priv. (2017) 375–392, https://doi.org/10.1109/SP.2017.29.
[54] Y. Rahulamathavan, R.C.W. Phan, M. Rajarajan, S. Misra, A. Kondoz, Privacy-preserving Blockchain-based IoT Ecosystem using attribute-based encryption, IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2017.
[55] Ali Dorri, Salil S. Kanhere, Raja Jurdaky, Praveen Gauravaramz, Blockchain for IoT security and privacy: The case study of a smart home, 2nd IEEE Percom Workshop on Security Privacy and Trust in the Internet of Things, 2017.
[56] H. Derhamy, J. Eliasson, J. Delsing, IoT interoperability – on-demand and low latency transparent multiprotocol translator, IEEE Internet Things J. 4 (5) (October 2017).
[57] G. Ateniese, B. Magri, D. Venturi, E.R. Andrade, Redactable blockchain - or-rewriting history in bitcoin and friends, IEEE Eur. Sympos. Secur. Priv. (2017), https://doi.org/10.1109/EuroSP.2017.37.
[58] C. George, Polyzos and Nikos Fotiou, "Blockchain-assisted information distribution for the internet of things", IEEE Int.

Conf. Inf. Reuse Integr. (2017), https://doi.org/10.1109/IRI.2017.83.
[59] T.T.A. Dinh, R. Liu, M. Zhang, G. Chen, B.C. Ooi, J. Wang, Untangling Blockchain: A Data Processing View of Blockchain Systems, IEEE Trans. Knowl. Data Eng. (2017), https://doi.org/10.1109/TKDE.2017.2781227.
[60] A. Dorri, S. S. Kanhere, R. Jurdak, "Towards an Optimized BlockChain for IoT"., IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), June 2017, Pittsburgh, PA, USA.
[61] S. Sanju, S. Sankaran, K. Achuthan, Energy Comparison of Blockchain Platforms for Internet of Things, IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS) (2018).
[62] F.M. Bencic, I.P. Zarko, Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph, in: IEEE 38th International Conference on Distributed Computing Systems, 2018, https://doi.org/10.1109/ICDCS.2018.00171.
[63] J. Wan, J. Li, M. Imran, D. Li, and Fazal-E-Amin, "A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory," IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3652–3660, 2019.
[64] F.R. Yu, J. Liu, Y. He, P. Si, Y. Zhang, Virtualization for Distributed Ledger Technology (vDLT), IEEE Access 6 (2018) 25019–25028.
[65] Dorri, Ali, et al. "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home." 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), IEEE, 2017, pp. 618–23, DOI.org (Crossref), doi:10.1109/PERCOMW.2017.7917634.
[66] M. Conti, S. K. E, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin", IEEE Communications Surveys & Tutorials (Volume: 20, Issue: 4, Fourth quarter pp. 1–1, 2018), DOI: 10.1109/COMST.2018.2842460.
[67] H. Li, K. Wang, T. Miyazaki, C. Xu, S. Guo, Y. Sun, "Trust enhanced content delivery in blockchain-based information-centric networking", IEEE Network, Volume: 33, Issue: 5, 2019.
[68] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, E. Hossain, Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains, IEEE Trans. Ind. Inform. 13 (6) (Dec. 2017) 3154–3164.
[69] NuttakitVatcharatiansakul, PanwitTuwanut, "A performance evaluation for Internet of Things based on Blockchain technology"., 2019 5th International Conference on Engineering, IEEE July 2019.
[70] Y. Liu, K. Zheng, P. Craig, Y. Li, Y. Luo, X. Huang, "Evaluating the Reliability of Blockchain-Based Internet of Things Applications", Proceedings of 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN 2018).
[71] M.A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, H. Janicke, Blockchain technologies for the Internet of Things: Research issues and challenges, IEEE Internet Things J. 6 (2) (Apr. 2019) 2188–2204.
[72] C.K. Pyoung, S.J. Baek, Blockchain of Finite-Lifetime Blocks With Applications to Edge-Based IoT, Internet of Things Journal IEEE 7 (3) (2020) 2102–2116.
[73] M.A. Ferrag, L. Shu, X. Yang, A. Derhab, L. Maglaras, Security and Privacy for Green IoT-Based Agriculture: Review Blockchain Solutions and Challenges, Access IEEE 8 (2020) 32031–32053.
[74] Yinqiu Liu, Kun Wang, Kai Qian, Du. Miao, Song Guo, Tornado: Enabling Blockchain in Heterogeneous Internet of Things Through a Space-Structured Approach, Internet of Things Journal IEEE 7 (2) (2020) 1273–1286.
[75] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, K.K.R. Choo, HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes, Internet of Things Journal IEEE 7 (2) (2020) 818–829.
[76] Y. Jiang, Y. Zhong, X. Ge, Smart Contract-Based Data Commodity Transactions for Industrial Internet of Things, Access IEEE 7 (2019) 180856–180866.
[77] Kang Liu, Wuhui Chen, Zibin Zheng, Zhenni Li, Wei Liang, A Novel Debt-Credit Mechanism for Blockchain-Based Data-Trading on Internet of Vehicles, Internet Things J. IEEE 6 (5) (2019) 9098–9111.
[78] Beverley MacKenzie, Robert Ian Ferguson, Xavier Bellekens, "An Assessment of Blockchain Consensus Protocols for the Internet of Things", 2018 International Conference on IoT, Embedded Systems and Communications (IINTEC), DOI: 10.1109/IINTEC.2018.8695298, Dec 2018.
[79] S. Madumidha, P. Siva Ranjani, S. SreeVarsinee, P.S. Sundari, Transparency and Traceability. In Food Supply Chain System using Blockchain Technology with the Internet of Things, Proceedings of the Third International Conference on Trends in Electronics and Informatics, 2019.
[80] Joshua Ellul, Gordon J. Pace, "AlkylVM: A Virtual Machine for Smart Contract Blockchain Connected Internet of Things", 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, April 2018, Paris, France, DOI: 10.1109/NTMS.2018.8328732.
[81] Wei She, Qi Liu, Zhao Tian, Jian-Sen Chen, Bo Wang, Wei Liu, Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks, Access IEEE 7 (2019) 38947–38956.
[82] Rajesh Gupta, Sudeep Tanwar, Fadi Al-Turjman, PritItaliya, Ali Nauman, Sung Won Kim, "Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools Techniques and Challenges", Access IEEE, vol. 8, pp. 24746–24772, 2020.
[83] Bogdan Cristian Florea, "Blockchain and Internet of Things data provider for smart applications", 7th Mediterranean Conference on Embedded Computing (MECO), IEEE, July 2018, Budva, Montenegro, DOI: 10.1109/MECO.2018.8406041.
[84] Han Zhang, Weimin Lang, "Research on the Blockchain Technology in the Security of Internet of things", IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), February 2020, Chengdu, China, DOI: 10.1109/IAEAC47372.2019.8997876.
[85] Feng Gao, Liehuang Zhu, Meng Shen, Kashif Sharif, Zhiguo Wan, and Kui Ren, "A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks", IEEE Network, 2018, Digital Object Identifier: 10.1109/MNET.2018.1700269
[86] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, P. Rimba, A taxonomy of blockchain-based systems for architecture design, in: in IEEE International Conference on Software Architecture (ICSA), 2017, pp. 243–252.
[87] Ke Huang, Xiaosong Zhang, Yi Mu, Xiaofen Wang, Guomin Yang, "Building Redactable Consortium Blockchain for Industrial Internet-of-Things", IEEE Transactions on Industrial Informatics, vol 15, issue 6, DOI 10.1109/TII.2019.2901011.
[88] Ke Huang, Xiaosong Zhang, Mu. Yi, Fatemeh Rezaeibagha, Du. Xiaojiang, Nadra Guizani, Achieving Intelligent Trust-Layer for Internet-of-Things via Self-Redactable Blockchain, Ind. Inform. IEEE Trans. 16 (4) (2020) 2677–2686.
[89] Ke Huang, Xiaosong Zhang, Mu. Yi, Fatemeh Rezaeibagha, Xiaofen Wang, Jingwei Li, Qi Xia, Jing Qin, EVA: Efficient Versatile Auditing Scheme for IoT-Based Data market in Jointcloud, Internet Things J. IEEE 7 (2) (2020) 882–892.
[90] Jiawen Kang, Yu. Rong, Xumin Huang, SabitaMaharjan, "Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium

Blockchains", IEEE Trans. Ind. Inf. (2017), https://doi.org/10.1109/TII.2017.2709784.
[91] Gaolei Li, Wu. Jun, Jianhua Li, Zhitao Guan, Longhua Guo, Fog Computing-Enabled Secure Demand Response for Internet of Energy Against Collusion Attacks Using Consensus and ACE, Access IEEE 6 (2018) 11278–11288.
[92] Tianyu Yang, Qinglai Guo, Xue Tai, Hongbin Sun, Boming Zhang, Wenlu Zhao, Chenhui Lin, "Applying blockchain technology to decentralized operation in future energy internet", Energy Internet and Energy System Integration (EI2) 2017 IEEE Conference on, pp. 1-5, 2017.
[93] Hong Liu, Yan Zhang, Tao Yang, Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing, Network IEEE 32 (3) (2018) 78–83.
[94] Bo Zhang, Chi Harold Liu, Jian Tang, Zhiyuan Xu, Jian Ma, Wendong Wang, "Learning-Based Energy-Efficient Data Collection by Unmanned Vehicles in Smart Cities", Ind. Inform. IEEE Trans. 14 (4) (2018) 1666–1676.
[95] Zhetao Li, Jiawen Kang, Yu. Rong, Dongdong Ye, Qingyong Deng, Yan Zhang, Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things, Ind. Inform. IEEE Trans. 14 (8) (2018) 3690–3700.
[96] S. M. Farooq, S. M. S. Hussain, T. S. Ustun, "Elliptic Curve Digital Signature Algorithm (ECDSA) Certificate-Based Authentication Scheme for Advanced Metering Infrastructure", Innovations in Power and Advanced Computing Technologies (i-PACT), IEEE, January 2020, Vellore, India, DOI: 10.1109/i-PACT44901.2019.8959967.
[97] M. Moser, R. Bohme, Anonymous Alone Measuring Bitcoin's Second-Generation Anonymization Techniques, IEEE Eur. Sympos. Secur. Priv. Workshops (EuroS&PW) (2017), https://doi.org/10.1109/EuroSPW.2017.48.
[98] Q. Lu, X. Xu, Adaptable blockchain-based systems: A case study for product traceability, IEEE Softw. 34 (6) (2017) 21–27.
[99] A. Reyna, C. Martn, J. Chen, E. Soler, M. Daz, On blockchain and its integration with IoT Challenges and opportunities, Future Generation Comput. Syst. 88 (2018) 173–190.
[100] G. Sagirlar, B. Carminati, E. Ferrari, J.D. Sheehan, E. Ragnoli, "Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things - PoW Sub-Blockchains", IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics (2018), https://doi.org/10.1109/Cybermatics_2018.2018.00189.
[101] M.S. Ali, M. Vecchio, F. Antonelli, Enabling a Blockchain-Based IoT Edge, Internet Things Magazine IEEE 1 (2) (2018) 24–29.
[102] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, C. Rong, A Comprehensive Survey of Blockchain: From Theory to IoT Applications and Beyond, Internet Things J. IEEE 6 (5) (2019) 8114–8154.
[103] Toqeer Ali Syed, Ali Alzahrani, Salman Jan, Muhammad Shoaib Siddiqui, Adnan Nadeem, Turki Alghamdi, "A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations", Access IEEE 7 (2019) 176838–176869.
[104] Kai Lei, Du. Maoyu, Jiyue Huang, Tong Jin, Groupchain: Towards a Scalable Public Blockchain in Fog Computing of IoT Services Computing, Serv. Comput. IEEE Trans. 13 (2) (2020) 252–262.
[105] JiewuLeng, Douxi Yan, Qiang Liu, Kailin Xu, J. Leon Zhao, Rui Shi, Lijun Wei, Ding Zhang, Xin Chen, "ManuChain: Combining Permissioned Blockchain With a Holistic Optimization Model as Bi-Level Intelligence for Smart Manufacturing", Systems Man and Cybernetics: Systems IEEE Transactions on, vol. 50, no. 1, pp. 182-192, 2020.
[106] S. Fu, Q. Fan, Y. Tang, H. Zhang, X. Jian, X. Zeng, "Cooperative Computing in Integrated Blockchain-Based Internet of Things", IEEE Internet of Things Journal (Volume: 7, Issue: 3, March 2020), October 2019, DOI: 10.1109/JIOT.2019.2948144.
[107] C. Lee, N. Sung, L. Nkenyereye, J. Song, "Blockchain-Enabled Internet-of-Things Service Platform for Industrial Domain", IEEE International Conference on Industrial Internet (ICII), November 2018, Seattle, WA, USA, and DOI: 10.1109/ICII.2018.00033.
[108] X. Wu, B. Duan, Y. Yan, Y. Zhong, M2m blockchain: The case of demand-side management of smart grid, in: Parallel and Distributed Systems (ICPADS) 2017 IEEE 23rd International Conference, 2017, pp. 810–813.
[109] Charles Shen, Feniosky Pena-Mora, Blockchain for Cities—A Systematic Literature Review, Access IEEE 6 (2018) 76787–76819.
[110] L. Cui, S. Yang, Z. Chen, Y. Pan, M. Xu, K. Xu, An Efficient and Compacted DAG-Based Blockchain Protocol for Industrial Internet of Things, Ind. Inf. IEEE Trans. 16 (6) (2020) 4134–4145.
[111] X. Sun, N. Ansari, Dynamic resource caching in the IoT application layer for smart cities, IEEE Internet Things J., Apr. 5 (2) (2018) 606–613.
[112] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, Y. Zhang, A blockchain-based nonrepudiation network computing service scheme for industrial IoT, IEEE Trans. Ind. Inform. 15 (6) (Jun. 2019) 3632–3641.
[113] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, K. Li, A secure fabric blockchain-based data transmission technique for industrial internet-of-things, IEEE Trans. Ind. Inform. 15 (6) (Jun. 2019) 3582–3592.
[114] Chenlong Yang, Yu.Yu. Xiangxue Li, Ziping Wang, Basing Diversified Services of Complex IIoT Applications on Scalable Block Graph Platform, Access IEEE 7 (2019) 22966–22975.
[115] Tiago M. Fernández-Caramés, Paula Fraga-Lamas, A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories, Access IEEE 7 (2019) 45201–45218.
[116] Haipeng Yao, Tianle Mai, Jingjing Wang, Zhe Ji, Chunxiao Jiang, Yi Qian, Resource Trading in Blockchain-Based Industrial Internet of Things, Ind. Inf. IEEE Trans. 15 (6) (2019) 3602–3609.
[117] Mengting Liu, F. Richard Yu, Yinglei Teng, Victor C. M. Leung, Mei Song, "Performance Optimization for Blockchain-Enabled Industrial Internet of Things (IIoT) Systems: A Deep Reinforcement Learning Approach", Industrial Informatics IEEE Transactions on, vol. 15, no. 6, pp. 3559-3570, 2019.
[118] Wei Tong, Xuewen Dong, Yulong Shen, Xiaohong Jiang, "A Hierarchical Sharding Protocol for Multi-Domain IoT Blockchains", Communications (ICC) ICC 2019 - 2019 IEEE International Conference on, pp. 1-6, 2019.
[119] Christian Rondanini, Barbara Carminati, Elena Ferrari, "Confidential Discovery of IoT Devices through Blockchain"., Internet of Things (ICIOT), in: 2019 IEEE International Congress on, 2019, pp. 1–8.
[120] Ananda Maiti, Ali Raza, Byeong Ho Kang, Lachlan Hardy, "Estimating Service Quality in Industrial Internet-of-Things Monitoring Applications with Blockchain", Access IEEE 7 (2019) 155489–155503.
[121] Kentaroh Toyoda, MojtabaShakeri, Xu Chi, Allan N. Zhang, "Performance Evaluation of Ethereum-based On-chain Sensor Data Management Platform for Industrial IoT"., Big Data (Big Data), in: 2019 IEEE International Conference on, 2019, pp. 3939–3946.
[122] Yongping Zhang, Xu. Xiwei, Ang Liu, Lu. Qinghua, Xu. Lida, Fei Tao, Blockchain-Based Trust Mechanism for IoT-Based

Smart Manufacturing System, Comput. Soc. Syst. IEEE Trans. 6 (6) (2019) 1386–1394.
[123] Paul Kengfai Wan, Lizhen Huang, Halvor Holtskog, "Blockchain-Enabled Information Sharing Within a Supply Chain: A Systematic Literature Review", Access IEEE 8 (2020) 49645–49656.
[124] Joseph E. Kasten, Engineering and Manufacturing on the Blockchain: A Systematic Review, Eng. Manage. Rev. IEEE 48 (1) (2020) 31–47.
[125] F. JunfengXie, Richard Yu, Tao Huang, RenchaoXie, Jiang Liu, Yunjie Liu, "A Survey on the Scalability of Blockchain Systems", Network IEEE 33 (5) (2019) 166–173.
[126] Y. Song, Y. Fu, F.R. Yu, L. Zhou, Blockchain-Enabled Internet of Vehicles With Cooperative Positioning: A Deep Neural Network Approach, Internet of Things J. IEEE 7 (4) (2020) 3485–3498.
[127] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, M.A. Imran, Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment, IEEE Internet Things J. 6 (3) (Jun. 2019) 5791–5802.
[128] K. Liu, Y. Wang, W. Lin, Xu, "LightChain: A lightweight blockchain system for Industrial Internet of Things", IEEE Trans. Ind. Inf. 15 (6) (Jun. 2019) 3571–3581.
[129] W. Chen et al, Cooperative and distributed computation offloading for blockchain-empowered Industrial Internet of Things, IEEE Internet Things J. 6 (5) (Oct. 2019) 8433–8446.
[130] S. Biswas, K. Sharif, F. Li, B. Nour, Y. Wang, A scalable blockchain framework for secure transactions in IoT, IEEE Internet Things J. 6 (3) (Jun. 2019) 4650–4659.
[131] D. Tse, B. Zhang, Y. Yang, C. Cheng, H. Mu, Blockchain application in food supply information security, in: in 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Dec 2017, pp. 1357–1361.
[132] R. Bettín-Díaz, A. E. Rojas, and C. Mejía-Moncayo, "Methodological approach to defining a blockchain system for the food industry supply chain traceability," in Computational Science and Its Applications – ICCSA 2018. Cham: Springer International Publishing, 2018, pp. 19–33.
[133] Q. Lin, H. Wang, X. Pei, and J. Wang, "Food safety traceability system based on blockchain and epics"., IEEE Access, vol. 7, pp. 20 698– 20 707, 2019.
[134] C. Esposito, A.D. Santis, G. Tortora, H. Chang, K.R. Choo, Blockchain: A panacea for healthcare cloud-based data security and privacy?, IEEE Cloud Comput 5 (1) (Jan 2018) 31–37.
[135] M. A. Rahman, M. S. Hossain, G. Loukas, E. Hassanain, S. S. Rahman, M. F. Alhamid, and M. Guizani, "Blockchain-based mobile edge computing framework for secure therapy applications," IEEE Access, vol. 6, pp. 72 469–72 478, 2018.
[136] L. Zhong, L. Mu, J. Li, J. Wang, Z. Yin, D. Liu, "Early Prediction of the 2019 Novel Coronavirus Outbreak in the Mainland China Based on Simple Mathematical Model", IEEE Access (Volume: 8), DOI: 10.1109/ACCESS.2020.2979599, March 2020.
[137] Ó. Blanco-Novoa, T.M. Fernández-Caramés, P. Fraga-Lamas, M.A. Vilar-Montesinos, A Practical Evaluation of Commercial IndustrialAugmented Reality Systems in an Industry 4.0 Shipyard, IEEE Access 6 (2018) 8201–8218.
[138] P. Fraga-Lamas, T.M. Fernández-Caramés, Ó. Blanco-Novoa, M.A. Vilar-Montesinos, "A Review on Industrial Augmented Reality Systemsfor the Industry 4.0 Shipyard", IEEE Access 6 (2018) 13358–13375.
[139] C. Brewster, I. Roussaki, N. Kalatzis, K. Doolin, K. Ellis, IoT in Agriculture: Designing a Europe-Wide Large-Scale Pilot, IEEE Commun Mag. 55 (9) (2017) 26–33.
[140] G. Perboli, S. Musso, M. Rosano, Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases, Access IEEE 6 (2018) 62018–62028.
[141] M. Kim, B. Hilton, Z. Burks, J. Reyes, Integrating Blockchain Smart Contract-Tokens and IoT to Design a Food Traceability Solution, in: Information Technology Electronics and Mobile Communication Conference (IEMCON) 2018 IEEE 9th Annual, 2018, pp. 335–340.
[142] Q. Lin, H. Wang, X. Pei, J. Wang, Food Safety Traceability System Based on Blockchain and EPCIS, Access IEEE 7 (2019) 20698–20707.
[143] K. Salah, N. Nizamuddin, R. Jayaraman, M. Omar, Blockchain-Based Soybean Traceability in Agricultural Supply Chain, Access IEEE 7 (2019) 73295–73305.
[144] G. Baralla, A. Pinna, G. Corrias, Ensure Traceability in European Food Supply Chain by Using a Blockchain System, in: Emerging Trends in Software Engineering for Blockchain (WETSEB) 2019 IEEE/ACM 2nd International Workshop on, 2019, pp. 40–47.
[145] P. Gonczol, P. Katsikouli, L. Herskind, N. Dragoni, Blockchain Implementations and Use Cases for Supply Chains-A Survey, Access IEEE 8 (2020) 11856–11871.
[146] Xin Zhang, Pengcheng Sun, Xu. Jiping, Xiaoyi Wang, Yu. Jiabin, Zhiyao Zhao, Yunfeng Dong, Blockchain-Based Safety Management System for the Grain Supply Chain, Access IEEE 8 (2020) 36398–36410.
[147] Ikwhan Chang JenilThakker, Younghee Park, "Secure Data Management in Internet-of-Things Based on Blockchain"., Consumer Electronics (ICCE), in: 2020 IEEE International Conference on, 2020, pp. 1–5.
[148] A. Shahid, A. Almogren, N. Javaid, F.A.A. Zahrani, M. Zuair, M. Alam, Blockchain-Based Agri-Food Supply Chain: A Complete Solution, Access IEEE 8 (2020) 69230–69243.
[149] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, R. Ranjan, IoTChain: Establishing trust in the Internet of Things ecosystem using blockchain, IEEE Cloud Comput. 5 (4) (2018) 12–23.
[150] S. Wang et al, Blockchain-powered parallel healthcare systems based on the ACP approach, IEEE Trans. Comput. Social Syst. 5 (4) (Dec. 2018) 942–950.
[151] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C.P.A. Ogah, Z. Sun, Blockchain-based dynamic key management for heterogeneous intelligent transportation systems, IEEE Internet Things J. 4 (6) (Dec. 2017) 1832–1843.
[152] Y. Rahulamathavan, R.C.W. Phan, M. Rajarajan, S. Misra, A. Kondoz, Privacy-preserving blockchain-based iot ecosystem using attribute-based encryption, in: 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2017, pp. 1–6.
[153] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, L. Xie, A decentralized solution for iot data trusted exchange based on blockchain, in: 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 2017, pp. 1180–1184.
[154] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture consensus and future trends, Proc. IEEE Int. Congr. Big Data (BigData Congress) (Jun. 2017) 557–564.
[155] R. Abe, H. Watanabe, S. Ohashi, S. Fujimura, A. Nakadaira, "Storage Protocol for Securing Blockchain Transparency", Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC), pp. 577–581, Jul. 2018.
[156] A. Anjum, M. Sporny, A. Sill, Blockchain standards for compliance and trust, IEEE Cloud Comput. 4 (4) (2017) 84–90.
[157] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla, "ProvChain: A blockchain-based data provenance architecture in a cloud environment with enhanced privacy and availability", Proc. 17th IEEE/ACM Int. Symp. Cluster Cloud Grid Comput., pp. 468-477, May 2017.
[158] Lu. Yunlong, Xiaohong Huang, Ke Zhang, SabitaMaharjan, Yan Zhang, "Blockchain Empowered Asynchronous Federated Learning for Secure Data Sharing on Internet of

Vehicles", Vehicular Technology IEEE Transactions on 69 (4) (2020) 4298–4311.
[159] Chao Qiu, Haipeng Yao, F. Richard Yu, Chunxiao Jiang, Song Guo, "A Service-Oriented Permissioned Blockchain for the Internet of Things", Services Computing IEEE Transactions on, vol. 13, no. 2, pp. 203–215, 2020.
[160] N. Wang, X. Xiao, Y. Yang, T.D. Hoang, H. Shin, J. Shin, G. Yu, Privtrie: Effective frequent term discovery under local differential privacy, in IEEE International Conference on Data Engineering (ICDE), 2018.
[161] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, Industrial Internet of Things: Challenges opportunities and directions, IEEE Trans. Ind. Inf. 14 (11) (Nov. 2018) 4724–4734.
[162] C. Yin, J. Xi, R. Sun, J. Wang, Location privacy protection based on differential privacy strategy for big data in the industrial Internet of Things, IEEE Trans. Ind. Inf. 14 (8) (Aug. 2018) 3628–3636.
[163] C.H. Liu, Q. Lin, S. Wen, Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning, IEEE Trans. Ind. Inf. 15 (6) (Jun. 2019) 3516–3526.
[164] A.H. Sodhro, S. Pirbhulal, V.H.C. de Albuquerque, Artificial intelligence-driven mechanism for edge computing-based industrial applications, IEEE Trans. Ind. Inf. 15 (7) (Jul. 2019) 4235–4243.
[165] A.K. Sangaiah, D.V. Medhane, T. Han, M.S. Hossain, G. Muhammad, Enforcing position-based confidentiality with machine learning paradigm through mobile edge computing in real-time industrial informatics, IEEE Trans. Ind. Information. 15 (7) (Jul. 2019) 4189–4196.
[166] Lu. Xiaofeng, Yuying Liao, Pietro Lio, Pan Hui, Privacy-Preserving Asynchronous Federated Learning Mechanism for Edge Network Computing, Access IEEE 8 (2020) 48970–48981.
[167] R. Agrawal, P. Verma, R. Sonanis, U. Goel, A. De, S. A. Kondaveeti, "Continuous Security in IoT Using Blockchain", IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), September 2018, DOI: 10.1109/ICASSP.2018.8462513.
[168] H. Arslan, H. Aslan, H. D. Karkı, A. G. Yüksel, "Blockchain and Security in the IoT Environments: Literature Review", 3rd International Conference on Computer Science and Engineering (UBMK), December 2018, Sarajevo, Bosnia-Herzegovina, DOI: 10.1109/UBMK.2018.8566378.
[169] Gohar Sargsyan, Nicolas Castellon, Raymond Binnendijk, Peter Cozijnsen, "Blockchain Security by Design Framework for Trust and Adoption in IoT Environment", IEEE World Congress on Services (SERVICES), August 2019, Milan, Italy, DOI: 10.1109/SERVICES.2019.00018.
[170] S. Brotsis et al, Blockchain solutions for forensic evidence preservation in IoT environments, IEEE NetSoft (2019).
[171] S. Biswas, K. Sharif, F. Li, B. Nour, Y. Wang, A Scalable Blockchain Framework for Secure Transactions in IoT, IEEE Internet of Things Journal (Volume: 6, Issue: 3, June 2019), DOI: 10.1109/JIOT.2018.2874095.
[172] E. Luo, PrivacyProtector: Privacy-protected patient data collection in IoT-based healthcare systems, IEEE Commun. Mag. 56 (2) (Feb. 2018) 163–168.
[173] J. Pan, J. McElhannon, Future edge cloud and edge computing for Internet of Things applications, IEEE Internet Things J. 5 (1) (Feb. 2018) 439–449.
[174] H. Sun, Z. Zhang, R.Q. Hu, Y. Qian, Wearable communications in 5G: Challenges and enabling technologies, IEEE Veh. Technol. Mag. 13 (3) (Sep. 2018) 100–109.
[175] C. Xu, C. Gao, Z. Zhou, Z. Chang, Y. Jia, Social network-based content delivery in device-to-device underlay cellular networks using matching theory, IEEE Access 5 (2017) 924–937.
[176] O. Novo, Blockchain meets IoT: An architecture for scalable access management in IoT, IEEE Internet Things J. 5 (2) (Apr. 2018) 1184–1195.
[177] Luobin Liu XiaoyuQiu, Wuhui Chen, Zicong Hong, Zibin Zheng, "Online Deep Reinforcement Learning for Computation Offloading in Blockchain-Empowered Mobile Edge Computing", Vehicular Technology IEEE Transactions on 68 (8) (2019) 8050–8062.
[178] Keke Gai, Wu. Yulu, Liehuang Zhu, Zijian Zhang, MeikangQiu, "Differential Privacy-Based Blockchain for Industrial Internet-of-Things", Industrial Informatics IEEE Transactions on 16 (6) (2020) 4156–4165.
[179] Sujit Biswas, Kashif Sharif, Fan Li, SabitaMaharjan, Saraju P. Mohanty, Yu Wang, "PoBT: A Lightweight Consensus Algorithm for Scalable IoT Business Blockchain", Internet of Things Journal IEEE, vol. 7, no. 3, pp. 2343-2355, 2020.
[180] Zhihua Cui, Fei XUE, Shiqiang Zhang, Xingjuan Cai, Yang Cao, Wensheng Zhang, Jinjun Chen, "A Hybrid Blockchain-based Identity Authentication Scheme for Multi-WSN", Serv. Comput. IEEE Trans. 13 (2) (2020) 241–251.
[181] Yuancheng Li, Hu. Baiji, An Iterative Two-Layer Optimization Charging and Discharging Trading Scheme for Electric Vehicle Using Consortium Blockchain, Smart Grid IEEE Trans. 11 (3) (2020) 2627–2637.
[182] Abubakar Sadiq Sani, Dong Yuan, Wei Bao, PheeLep Yeoh, Zhao Yang Dong, Branka Vucetic, "Xyreum: A High-Performance and Scalable Blockchain for IIoT Security and Privacy", IEEE 39th International Conference on Distributed Computing Systems (ICDCS), October 2019, Dallas, TX, USA, DOI: 10.1109/ICDCS.2019.00190.
[183] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, Industrial Internet of Things: Challenges Opportunities and Directions, IEEE Trans. Ind. Inf. 14 (11) (2018) 4724–4734.
[184] N.Z. Aitzhan, D. Svetinovic, Security and Privacy in Decentralized Energy Trading Through Multi-Signatures Blockchain and Anonymous Messaging Streams, IEEE Trans. Dependable Secure Comput. 15 (5) (2018) 840–852.
[185] M. Singh, A. Singh, S. Kim, "Blockchain: A Game Changer for Securing IoT Data", IEEE World Forum on Internet of Things, 2018.
[186] S.-C. Cha, J.-F. Chen, C. Su, K.-H. Yeh, "A Blockchain Connected Gateway for BLE-based Devices in the Internet of Things"., IEEE Access 4 (2018) 24639–24649.
[187] N. Rifi, E. Rachkidi, N. Agoulmine, N. C. Taher, "Towards Using Blockchain Technology for IoT data access protection", IEEE International Conference on Ubiquitous Wireless Broadband, 2017.
[188] O. J. A. Pinno, A. R. A. Gregio, L. C. E. D. Bona, "Controlchain: Blockchain as a central enabler for access control authorizations in the iot", IEEE GLOBECOM 2017, 2017.
[189] Tam Le, Matt W. Mutka, "A Lightweight Block Validation Method for Resource-Constrained IoT Devices in Blockchain-Based Applications"., IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), August 2019, Washington, DC, USA, DOI: 10.1109/WoWMoM.2019.8792979.
[190] Panagiotis Sarigiannidis, Eirini Karapistoli, Anastasios A. Economides, Modeling the Internet of Things Under Attack: A G-network Approach, Internet of Things Journal IEEE 4 (6) (2017) 1964–1977.
[191] Dongjin Xu, Liang Xiao, Limin Sun, Min Lei, "Game-theoretic study on blockchain-based secure edge networks"., Communications in China (ICCC) 2017 IEEE/CIC International Conference on, pp. 1-5, 2017.
[192] Md Golam Moula Mehedi Hasan, Amarjit Datta, Mohammad Ashiqur Rahman, Hossain Shahriar, "Chained of Things: A Secure and Dependable Design of Autonomous Vehicle

Services", Computer Software and Applications Conference (COMPSAC) 2018 IEEE 42nd Annual, vol. 02, pp. 498–503, 2018.

[193] Caciano Machado, Antônio Augusto Medeiros Fröhlich, "IoT Data Integrity Verification for Cyber-Physical Systems Using Blockchain", Real-Time Distributed Computing (ISORC), in: 2018 IEEE 21st International Symposium on, 2018, pp. 83–90.

[194] Sriram Sankaran, Sonam Sanju, KrishnashreeAchuthan, "Towards Realistic Energy Profiling of Blockchains for Securing the Internet of Things", Distributed Computing Systems (ICDCS) 2018 IEEE 38th International Conference on, pp. 1454–1459, 2018.

[195] Qingqiang He, Nan Guan, Wang Yi MingsongLv, On the Consensus Mechanisms of Blockchain/DLT for Internet of Things, in: Industrial Embedded Systems (SIES) 2018 IEEE 13th International Symposium on, 2018, pp. 1–10.

[196] Lijing Zhou, Licheng Wang, Yiru Sun, Pin Lv, BeeKeeper: A Blockchain-Based IoT System with Secure Storage and Homomorphic Computation, Access IEEE 6 (2018) 43472–43488.

[197] Lei Cui, Gang Xie, Qu. Youyang, Longxiang Gao, Yunyun Yang, Security and Privacy in Smart Cities: Challenges and Opportunities, Access IEEE 6 (2018) 46134–46145.

[198] Michael Cash, Mostafa Bassiouni, "Two-Tier Permissioned and Permission-Less Blockchain for Secure Data Sharing"., Smart Cloud (SmartCloud), in: 2018 IEEE International Conference on, 2018, pp. 138–144.

[199] P. Kumar, R. Kumar, G. Srivastava, G.P. Gupta, R. Tripathi, T.R. Gadekallu, N.P.P.S.F. Xiong, A Privacy-Preserving and Secure Framework using Blockchain-based Machine-Learning for IoT-driven Smart Cities, IEEE Trans. Network Sci. Eng. (2021), Jun 16.

[200] R. Ch, G. Srivastava, T.R. Gadekallu, P.K. Maddikunta, S. Bhattacharya, Security and privacy of UAV data using blockchain technology, J. Inf. Secur. Appl. 1 (55) (2020 Dec) 102670.

[201] W. Wang, H. Xu, M. Alazab, T.R. Gadekallu, Z. Han, C. Su, Blockchain-Based Reliable and Efficient Certificateless Signature for IIoT Devices, IEEE Trans. Ind. Inf. (2021 May 28).