Mechanical Systems and Signal Processing 135 (2020) 106382

Contents lists available at ScienceDirect

Mechanical Systems and Signal Processing

journal homepage: www.elsevier.com/locate/ymssp

Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges

Ishan Mistry [a], Sudeep Tanwar [a,*], Sudhanshu Tyagi [b], Neeraj Kumar [c]

[a] Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India
[b] Department of Electronics and Communication Engineering, Thapar Institute of Engineering and Technology, Deemed to be University, Patiala, Punjab, India
[c] Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Deemed to be University, Patiala, Punjab, India

ARTICLE INFO

Article history:
Received 9 April 2019
Received in revised form 26 July 2019
Accepted 19 September 2019

Keywords:
Security
Blockchain
IoT
5G
Healthcare 4.0
Industrial automation

ABSTRACT

Internet-of-Things (IoT) has made ubiquitous computing a reality by extending Internet connectivity in various applications deployed across the globe. IoT connect billions of objects together for high speed data transfer especially in 5G-enabled industrial environment during information collection and processing. Most of the issues such as access control mechanism, time to fetch the data from different devices and protocols used may not be applicable infor future applications as these protocols are based upon a centralized architecture. This centralized architecture may have a single point of failure alongwith the computational overhead. So, there is a need for an efficient decentralized access control mechanism for device-to-device (D2D) communication in various industrial sectors IoT-enabled industrial automation. In such an environment, security and privacy preservation are major concerns as most of the solutions are based upon the centralized architecture. To mitigate the aforementioned issues, in this paper, we present an in-depth survey of state-of-the-art proposals having 5G-enabled IoT as a backbone for blockchain-based industrial automation for the applications such as-Smart city, Smart Home, Healthcare 4.0, Smart Agriculture, Autonomous vehicles and Supply chain management. From the existing proposals, it has been observed that blockchain can revolutionize most of the current and future industrial applications in different sectors by providing a fine-grained decentralized access control. Various transactions and database logs can be traced efficiently using blockchain for consistency and preivacy preservation in the aforementiioned industrial sectors. The open issues and challenges of 5G-enabled IoT for blockchain-based Industrial automation are also analyzed in the text. Finally, a comparison of existing proposals with respect to various parameters is presented which allows the end users to select one of the proposals in comparison to its merits over the others.

1. Introduction

IoT and its usage in various industrial sectors is growing at an exponential rate from the past few years. According to Gartner, the number of IoT-enabled devices may reach to 24 billions by 2020 [1]. Enormous data is being generated from these devices and there is a need of efficient storage & processing techniques to handle it. This process also includes an increase in

* Corresponding author.
E-mail addresses: 15bce042@nirmauni.ac.in (I. Mistry), sudeep.tanwar@nirmauni.ac.in (S. Tanwar), s.tyagi@thapar.edu (S. Tyagi), neeraj.kumar@thapar.edu (N. Kumar).

https://doi.org/10.1016/j.ymssp.2019.106382
0888-3270/

the data exchanges from machine-to-machine (M2M) and D2D [2–4] interactions. In order to cope up with this huge data proliferation, a robust IoT protocols stack is required which can handle all issues related to data transmission and processing at various stages. With the help of standardized protocols and layers, an architecture can be developed to execute the relevant services by IoT devices [5]. These devices have been actively used in the automotive industry to meet the demands of the end users and to achieve their conservative business goals. In recent years, there is a need for competitive, good quality product with reduced product cost. The IoT has changed these scenarios using 5G infrastructure, in which real-time interaction between machines, data, and human is possible to plug-in the aforementioned issues.

Nowadays, majority of IoT-based systems are built using the centralized client-server, cloud servers, strong database [6,7] and the Internet. Two major limitations of the IoT centralized infrastructure have been observed by the authors; (i) the single point failure, which can potentially topple the entire system and (ii) the lack of trust between the entities involved in the system [8]. To overcome the aforementioned limitations, decentralized architectures can be used for peer-to-peer (P2P) communications among the nodes. However, these systems have several privacy and security concerns, which can open the doors for the intruders to launch various attacks.

A large number of applications are there using IoT devices for the betterment of the service, likesuch as -smart home [9], smart factory [10] smart city [11], secure vehicular AdHoc network [12]. Future is that However, 5G drive-based IoT deployment to maintain the security IoT devices can utilize Blockchain. For securing IoT network [13,14], a lot of Blockchain solutions are available few operate on fast trusted networks and other work faster on unreliable networks. For the situation, where new blockchain operates efficiently and rapidly over unreliable networks then 5G enabled IoT devices can utilize the same in the real-time. Security may not be the only task for the utilization of blockchain also can take part for data distribution, as it works in faster mode. However, as per the knowledge of authors, an independent mathematical proof for the fast solutions is still unavailable. After the availability of the mathematical proof, a perfect environment is possible where fast and trusted nodes have been connected in the network and can take the benefit from 5G by using specific cloud or fog layers.

So, blockchain-based decentralized system is one of the solutions. One of the advantages of using blockchain technologies is the ability to store information in an immutable manner, which requires no centralized database. In addition to this, it also provides a way to track and execute transactions among various participants in a trusted environment. With the usage of strong encryption with public-private key pairs, blockchain also provides high levels of security to its participants.

Some decentralized applications (DApps) are available in the market which have been developed using IoT and blockchain. Using IoT infrastructure, the 'information sharing' of devices can be done with the usage of embedded sensors and sufficient network connectivity. The omnipresent network connectivity, which is very difficult to achieve in modern era, can be achieved from the 5G. These technologies decrease the latency by 100 times as compared to 4G. Moreover, integrating blockchain with IoT enable to maintain an immutable ledger of transactions of information exchange. By achieving this in a decentralized P2P manner, the 'middle-man-attack' can be eliminated, which allow the users to share without relying on a trusted third party [15].

Motivated from the aforementioned discussion, in this paper, we provides an overview of the integration of blockchain with 5G-enabled IoT for industrial automation. Then, we discuss some open issues and challenges which may hinder the growth of blockchain technology.

1.1. Scope of this survey

Preexisting surveys explored various aspects of blockchain with IoT [16–23]. Some of these are discussed as follows. Khan et al. [18] focused on the security requirements of IoT using blockchain. Florea et al. [19] described the use of blockchain technology as a data provider in IoT applications. Miraz et al. [20] assessed the implementation of blockchain for IoT security. Dorri et al. [16] proposed a secure and lightweight architecture for IoT, based on blockchain technology. Atlam et al. [21] provided an overview of the integration of IoT and blockchain, while highlighting its benefits and challenges. Singh et al. [22] also focused on the security aspects of blockchain based IoT systems. Christidis et al. [17] examined the potential of blockchain in the IoT sector. Hwang et al. [23] proposed a dynamic access control method for directing communication between devices. But, to the best of our knowledge, these had been focused on how to use blockchain with IoT for either security purposes or decentralized storage purpose only. None has considered the potential of blockchain with 5G for industrial automation. Therefore, this comprehensive survey has covered the span of last four years (2015-till date) mainly. Table 1 shows the comparison of the existing surveys with the proposed survey.

1.2. Contribution of this survey

Although several research proposals exist in the literature covering blockchain and IoT, but few had considered the potential of high-speed connectivity in the IoT devices using blockchain. In this paper, we investigated the role of blockchain for industrial automation with 5G-enabled IoT devices. Following are the major research contributions of this paper:

- We present a comprehensive and systematic review of blockchain-based 5G-enabled IoT and discussed its potential industrial applications.
- We also discuss various applications for integration of blockchain with 5G-enabled IoT.

Table 1
Comparison of the existing surveys with the proposed survey.

Authors	Year	Description	Merits	Demerits
Dorri et al. [16]	2016	Proposed a secure and lightweight architecture for IoT, based on blockchain.	Use of overlay networks to reduce the computation time for blocks.	Security against certain vulnerabilities, such DoS attacks, not clarified.
Christidis et al. [17]	2016	Examined the potential of blockchain in IoT sector.	Exhaustive discussion on the role of blockchain and smart contracts for IoT.	Challenges related to the implementation not explored.
Khanet al. [18]	2018	Focused on the security requirements of IoT using blockchain.	Discussion of state of the art IoT security issues and solutions.	Detailed discussion of implementing blockchain together with IoT not included.
Florea et al.[19]	2018	Described the use of blockchain technology as a data provider in IoT applications.	Discussed IOTA network, which is labeled as the 'backbone of IoT'.	Field devices are currently not configured to do PoW.
Miraz et al. [20]	2018	Assessed the implementation of blockchain for IoT security.	Detailed research to ascertain the applicability of blockchain for augmented IoT security.	Blockchain usage in Industrial automation was not explored.
Atlam et al. [21]	2018	Provided an overview of the integration of IoT and blockchain, while highlighting its benefits and challenges.	Detailed comparison of current and blockchain-based IoT systems.	Device-to-device communication not considered.
Singh et al. [22]	2018	Focused on the security aspects of blockchain-based IoT systems.	Discussed the techniques to strengthen IoT security with blockchain.	Challenges related to the implementation not covered in detail.
Hwang et al. [23]	2018	Proposed a dynamic access control method for directing data communication between devices.	Dynamic access control flow using blockchain.	Lack of verification of newly modified control messages.
Proposed survey	–	To provide an overview of the potential applications of blockchain in industrial automation.	Detailed study about applications and explored emergent challenges for the adoption of blockchain.	–

- Finally, this paper bridges the gap between the scalability, interoperability, and other research challenges for blockchain applications with 5G-enabled IoT in industrial automation.

1.3. Organization and reading map

Rest of paper is structured as follows. In Section 2, the basic information about blockchain; its structure, brief working, characteristics, and its informal classification are elaborated. Also, we discussed briefly about how the 5G wireless technologies helps to overcome some of the issues of the traditional systems. In Section 3, we discussed in detail about nine major areas, where 5G-enabled IoT is integrated with blockchain in different industries. Finally, we illustrated various open issues and challenges for amalgamation of blockchain and industrial automation in Section 4. Lastly, paper is concluded in Section 5.

2. Background of blockchain and 5G-enabled IoT devices

This section covered the background of blockchain, 5G-enabled IoT, and is divided into three subsections. First, we discuss the basic information about blockchain, and how it is 'disrupting' the modern era. Then, we discuss the concept of IoT, its characteristics, limitations, and how 5G revolutionize the IoT paradigm. Lastly, we discuss the potential advantages of combining these two paradigms which forms the foundation of the paper.

2.1. Blockchain

The advent of crypto-currencies like Bitcoin [24] blockchain technology has emerged as the next disruptive technology. It works at the heart of the transition from a centralized client-server Internet system to a decentralized, cryptographically secured network. Moreover, the blockchain is a distributed and immutable ledger which is able to record financial transactions. It consists of a chain of time-stamped blocks that are linked together using cryptographic hashes [5]. They enable the users to have a distributed P2P network, where non-trusting members can exchange information with each other without the need of any trusted intermediary [17].

Trust is an important feature of blockchain, which is achieved by utilizing the resultant hash of the previous block to create the next block. In order to achieve consensus, 'miner' nodes are responsible to validate the resulting hash, followed to find the hash for the next block. A bunch of transactions are bundled together into blocks using a Merkle tree and only the Merkle root hash is added to the block. This method is known as the Proof-of-Work (POW) and the miner nodes are

rewarded for the work performed on the network [19]. Such incentive models motivate the miner nodes to participate in the network to exchange computational power provided by them for mining blocks. Moreover, blockchain is different from other distributed systems based on consensus and following properties [25]:

- *Trust-less*: The entities involved in the network are unknown to each other. However, they can communicate, cooperate, and collaborate with each other without knowing each other which means there is no requirement of certified digital identity to perform any transaction between the entities.
- *Permission-less*: There is no restriction of who can or cannot operate within the network, i.e., there are no kind of permissions.
- *Censorship resistant*: Being a network without controllers, anyone can interact or transact on the blockchain. Moreover, any confirmed transaction cannot be modified or censored.

In addition to the aforementioned proprieties, Blockchain technology has four main components [22], which are discussed as follows:

- *Consensus*: The PoW protocol is responsible to verify every action in the network which is essential to prevent a single miner node from dominating the entire blockchain network and also to manipulate the transactions history [26].
- *Ledger*: It is a shared and distributed database which contains information about all transactions performed within the network. It is immutable by nature, where information once stored cannot be deleted by any means. It guarantees that every transaction is verified and then accepted as a valid one, by majority of the clients involved at a particular instant of time [18].
- *Cryptography*: It ensures that all data of the network is secured with strong cryptographic encryption. It allows only authorized users to decrypt the information.
- *Smart Contract*: It is used to validate and verify the participants of the network.

There are different types of blockchain, which can be classified on the basis of parameters, on the managed data, its availability, and access control. The notion that public or permissionless and private or permissioned are synonymous is misleading. The difference lies in the concepts of *authentication*, which indicates who can access the blockchain (public vs private) and *authorization* which indicates what the participants can do (permissioned vs permissionless).

In case of public blockchains, anyone can participate in the network, regardless of any kind of approval. They can choose to either act as a simple participating node or as a miner node, which assists in the validation process. Miners are rewarded with certain incentives in public blockchains like Bitcoin and Ethereum. On the other hand, in private blockchains, participation is restricted, where the approval of the owner is required to access the network. A number of private blockchains are also permissioned, which controls the type of action that can be perfomred by the users. For example, user can deploy smart contracts, or can act as a miner node in the network. Moreover, permissionless private blockchains exist, such as Hyperledger-Fabric [27] or Ripple [28].

2.2. 5G-enabled IoT

IoT denotes the network of various distinct electronic or electrical devices those are capable to interact with each other using the any open channel such as-Internet. This connection is made using wireless technology such as-sensor networks, radio frequency identification (RFID), near field communication (NFC), M2M, and ZigBee [20,29]. Then, IoT has revolutionized the realm of ubiquitous computing with numerous industrial applications built with various types of sensors. However, there are certain limitations with the usage of IoT, which need to be resolved in order to evolve it into a more efficient system [30,31]:

- *Security*: As the number of connected devices of the network increases, the chances to exploit vulnerabilities by external attacks also increases. This is happened due to the utilization of low standard devices.
- *Privacy*: The data collected from IoT devices is transmitted to a central cloud storage for analysis and processing, which includes a third party. This type of distribution of data without the consent of the user can further cause data leaks. Thus, compromising the privacy of the end users.
- *Standards*: Lack of standards and regulations can cause undesirable consequences while dealing with the configured devices.
- *Latency*: The current communication standards used for interaction between multiple IoT devices experiences latency issues.

Increase in the number of IoT-enabled devices causes a need for a technology that can support this huge amount of data transmissions efficiently at an extremely high bandwidth. Moreover, the devices themselves must be able to handle these changes in configuration such as-large bandwidth capacity, improved data-rate, and low latencies [32]. The advent of faster wireless technologies, especially, the 5th generation wireless systems (5G) is a driver for the 5G-enabled IoT applications. It also helps to handle large number of IoT-enabled devices [33]. The term 5G includes Massive-Input Massive-Output (MIMO), which help to achieve network capabilities than the current 4G LTE, and also “small cells”, which allows a more condensed network infrastructure [34]. Compared to the existing 4G technology, which uses frequencies below 6 GHz, 5G networks

support an extremely higher frequencies which ranges from 30 GHz to 300 GHz. Moreover, it enables to create a new industrial applications which operate outside of the current mobile broadband range. This omnipresent connectivity is the stepping stone to achieve higher availability, which has been targeted since the inception of cellular system [35]. It makes the 5G technology a key enabler for IoT technology. Thus, it complements IoT to provide higher data rates, reduced latencies, lower energy requirements, and higher scalability [36].

With the rapid growth of IoT technology, its expectations to bring tangible benefits to end users, especially, consumers and business corporations increases [31]. *Consumers* are offered certain services based on their activities. For example, they can travel more efficiently by avoiding traffic jams and riding on an alternate route, when notified by the smart IoT enabled device installed in their car. Moreover, they can remain healthy by using wearable devices which provide feedback related to their health, after analyzed their activities and body signs throughout the day. *Businesses* can use the data of users to provide better services and products. Also, they can use location trackers and remote locking on certain equipment to secure their assets. *Government and public authorities* can incur reduced healthcare costs with the provision of better health support by remote health monitoring, especially for elder people. Moreover, road safety and smart street lighting can make the citizens' life easier with reduced overall cost to maintain the structures.

2.3. Usage of blockchain in 5G-enabled IoT

With the development of smart applications to improve the quality of life of the citizens, IoT plays a vital role in the digitization of services. With the rapid growth in IoT, more access points to access and share information on the network (the Internet) arises. Centralized data storage systems such as-cloud computing has contributed significantly to the development of IoT. However, it seems to act as a black box, where the participants are unaware of the usage of the information they share on the network. Then, such a centralized structure may fails to provide data transparency [37]. To enhance security and privacy, use of blockchain technology is a viable solution. Fig. 1 shows benefits of using blockchain with 5G-enabled IoT for industrial automation.

Blockchain has the ability to revolutionize IoT with an open, trusted, and auditable sharing platform, where any information exchanged is reliable and traceable. Some of the benefits of this integration are as follows [37,16,21]:

- *Decentralization and Scalability*: The paradigm shift from centralized to decentralized can eliminate any single points of failure which improves the fault tolerance. It also prevents oligarchy of resources, where a few powerful corporations could control the collection and processing of data of a large number of people.
- *Identity*: The use of a common (or universal) blockchain allows a better identification of each device. Being immutable, it can also be able to trace the origin of any required information. Moreover, it can also provide a trusted means for authentication and authorization of IoT devices.
- *Autonomy*: Using blockchain, devices can interact with each other without the involvement of any intermediary. It can pave way to develop device-agnostic IoT-based industrial applications.
- *Security*: With the help of smart contracts, information exchanges are treated as a transactions, which provides secure inter-device communication.
- *Reliability*: This integration enables the users to verify the authenticity of any transaction with certainty and also provides accountability.
- *Secure code deployment*: Being an immutable ledger, a manufacturer can trace the update history easily. Moreover, it allows them to securely update IoT devices [38].

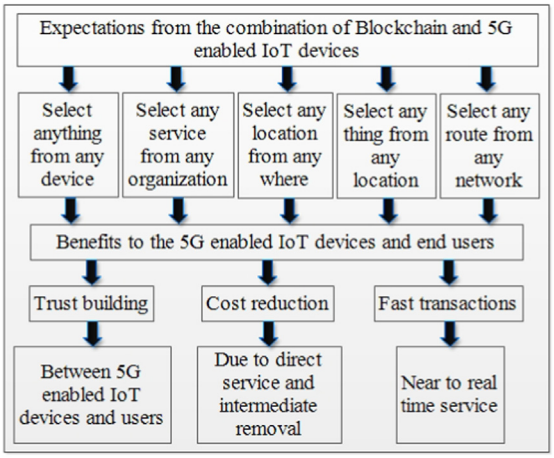

Fig. 1. Key benefits of using blockchain with 5G-enabled IoT for industrial automation.

3. Blockchain deployment in 5G-enabled smart industrial automation

A master taxonomy of blockchain-based industrial applications in 5G-enabled IoT is shown in Fig. 2, which includes existing areas of interest for application such as-Smart city, Smart Home, Healthcare 4.0, Industry 4.0, Agriculture, Autonomous vehicles and Supply chain management. In all these applications, blockchain and 5G are used to improve the security, to increase the bandwidth, and to reduce the overall operational as well as capital expenditure, respectively. The detailed description of these applications is discussed in the following subsections.

3.1. Smart home

A smart home is an embodiment of a technologically enriched living environment, which aims to improve the quality of life of inhabitants [39]. It provides security, convenience, and comfort to the owners, by allowing them to control the settings according to their preference with the help of a smart-phone application. With the IoT, smart home systems coordinate with the devices to automate certain actions based on the usage statistics to provide real-time uninterrupted services according to the users' preferences. Several research proposals have been discussed in the literature to design an energy-efficient smart homes.

A general infrastructure of a smart home consists of the following resources: network connectivity (usually Wi-Fi), IoT-enabled sensor devices, and a mobile application for remote access [40]. Some essential services provided by smart homes include smart lighting, smart door lock, smart thermostat, video surveillance, and smart parking [41]. In order provide the best possible experience to the people living inside it, these different services must continuously exchange relevant information to co-exist efficiently.

A *smart door lock system* is an essential part for any smart home. Its primary objective is to prevent unauthorized users to enter the house. The details about the inhabitants is stored in a central server, which allows white-listed individuals to access the house. However, the data handled by such system could be forged by any intruder who tries to circumvent the lock system to gain unauthorized access to the system. To address this issue, Han et al. [42] proposed a blockchain-based smart door lock system, which provides security features like authentication, data integrity, and non-repudiation. They used a set of Passive Infrared (PIR) sensor, ultrasonic sensor, and a motion sensor to detect indoor/outdoor intruders. The blockchain network-blocks stored the information about transactions which involve *open/lock* command. The immutable nature of the blockchain network makes it impossible for any intruder to gain unauthorized access to the system and make any modification to already executed transactions. However, the latency of IoT devices (sensors) can possibly be a hurdle to detect any kind of intrusion. This issue can be addressed with the usage of 5G wireless technology, which provides relatively low latency, fast intrusion detection, and block mining of the transactions on the blockchain.

The model discussed in [42] had a minor drawback that it had high latency for transaction confirmation, which was addressed by Dorri et al. [43]. Authors used a distributed trust to eliminate PoW. Moreover, they claimed that their model of 'overlay network' decreased the processing time by ≈50%. This model could potentially be an improvement over the model proposed in [42], provided the network security was not compromised. Moreover, this model could be used in smart homes, which was described in detail by [44]. Dorri et al. [44] proposed a blockchain-based smart home model, which consists of three basic tiers: the smart home, overlay, and the cloud storage. In this model, IoT devices were managed centrally by a miner, being located in the smart home tier. The overlay network introduced the distributed nature to this architecture and is quite similar to the P2P network as used in Bitcoin [24].

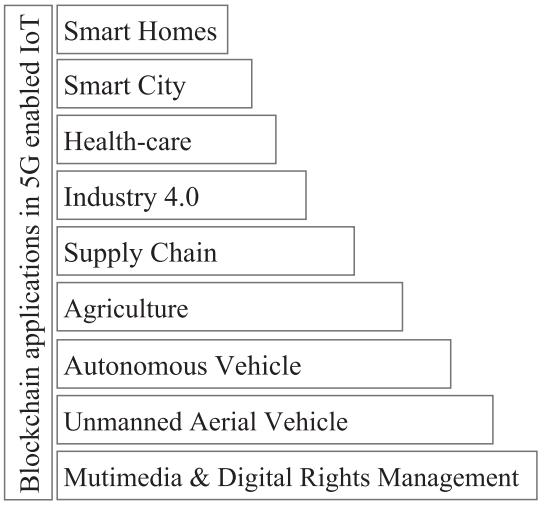

Fig. 2. Applications of Blockchain for 5G-enabled IoT.

Table 2
Relative comparison of existing approaches for Smart Home.

Author	Year	Description	Merits	Demerits	1	2	3	4	5
Skouby et al. [39]	2014	Proposed a 4-layer model combining smart homes, smart cities, and IoT.	Uses advanced ICT technologies, such as 5G and AI.	Working of the model not discussed in detail.	✓	Model	5G	✗	✓
Roshan et al. [40]	2016	Discussed challenges and risks associated to implement IoT in smart homes in India.	Extensive study of challenges for IoT adoption in India.	Ignored any potential solutions to the risks discussed.	✗	Survey	HTTP	✗	✓
Lazaroiu et al. [41]	2017	Proposed a smart district model, which is necessary for building a smart city.	Home automation interface discussed in detail.	Challenges and issues of the model not discussed.	✓	Model	Konnex (KNX) protocol	✓	✗
Han et al. [42]	2017	Proposed a blockchain-based smart door lock system.	Handles intrusion detection for smart homes. Addresses several privacy and security issues, with blockchain.	Lacks robustness; model is designed for a small network only.	✓	Model	Bluetooth or ZigBee	✗	✗
Dorri et al. [43]	2017	Uses distributed trust to reduce block validation processing time.	Virtually eliminates overheads of blockchain, especially proof-of-work.	Proper communication protocol not defined.	✓	Model	Not Defined	✗	✗
Dorri et al. [44]	2017	Proposed a blockchain-based smart home framework. Outlines three main tiers of smart homes.	Significant security and privacy benefits.	Added energy and time overheads.	✓	Model	6LoWPAN (IPv6 over Low Power Wireless Personal Area Network)	✗	✗
Aung et al. [46]	2017	Presents an approach of a private blockchain implementation for a smart home system, to cope with privacy and security issues.	Discussed smart contract policies for the smart home system.	Transaction time of 20 s; not suitable for time-sensitive conditions.	✓	Model and Survey	Not Defined	✗	✓

1: Usage of Blockchain, 2: Model/Survey, 3: Communication Standard, 4: Home Automation Interface, 5: Challenges and Open Issues, Notation: ✓: considered, ✗: not considered.

Communication among IoT devices is crucial to ensure synchronization. With the advent of IoT technology, the number of such devices increases for seamless data transfer to take place between them. This happened because of the potential limitation of the current 'server-client' model to handle such a large load. To overcome this issue, authors of [45] proposed a blockchain-based IoT system using Ethereum as the platform. In similar line, Aung et al. [46] proposed a decentralized approach of data management to cope with the smart home system security and privacy issues. Table 2 provides the detailed comparison of existing approaches in smart homes with reference to parameters such as-blockchain, communication standard, home automation interface, challenges and issues, and pros, cons of the existing approaches.

3.2. Smart city

The increasing trend of people to migrate to urban areas coupled with the associated process of urbanization, It creates many complex challenges regarding the cities' overall infrastructure and their ability to provide citizens with the basic necessities like water, energy, transportation, and healthcare. This unprecedented urban growth is due to factors such as-climate change, increase in population, and scarcity of resources. A proactive response to these problems is the notion of "smart city", which ensures an optimal and efficient utilization of available resources, by leveraging technologies such as-IoT and cloud computing. The aim of any smart city is to provide better quality of services to the citizens, while reducing the overall operational costs of public administration [47]. A survey of IoT-based smart cities highlights various applications, benefits, and disadvantages was proposed by Talari et al. [48], which also included some practical instances of smart cities, especially the case of the 'Padova Smart City' [49]. Fig. 3 shows the conceptual framework of the smart city proposed in [49], whereas Fig. 4 shows a high level illustration of a smart city framework.

An essential component of smart city is intelligent parking system, which aids in the development of traffic management systems to reduce the cost incurred by hiring relevant staff. For example, Pham et al. [50] proposed an algorithm which increased the efficiency of the cloud-based smart-parking systems based on IoT technology. Their objective was to reduce

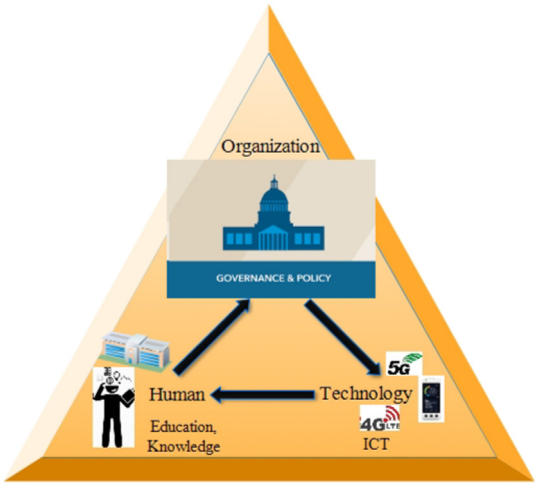

Fig. 3. Conceptual framework of a smart city [48].

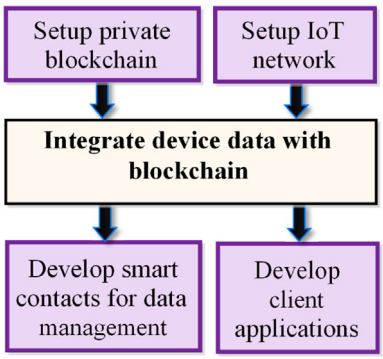

Fig. 4. Typical framework of a smart city [48].

the number of instances, where users fail to find a parking spot, while simultaneously decreased the average waiting time of users for parking. However, it lacks certain security features such as-large waiting time, real-time deployment. Security of such smart systems can potentially be achieved with help of distributed ledger technology. For example, Lazaroiu et al. [41], of a proposed a smart parking system model which considers two entities, *A* and *B*, together in a blockchain-based smart parking system. Entity *A* represents the visitor, who paid the parking fees to entity *B* (system authority). The information regarding this transaction was included in the blockchain, which was represented online as a block containing information about the block number, hash of the previous block, and POW. Once the majority of the nodes verify the authenticity of the transaction, the block was appended to the blockchain. Finally, the execution of a pre-decided smart contract triggers the fund transfer from the wallet of entity *A* to entity *B*, and the transaction was deemed to be complete.

The important aspect to focus on while conceptualizing smart cities is the information received from IoT sensor devices. This data forms the core to build a smart city and is highly essential to design the general architecture of the smart city. However, with an increase in the number and type of IoT devices, the amount of data generated is becoming astronomical. The current centralized communication model, which is the client/server model, enables storage of data at a central server, but it becomes difficult to carry out faster automated communication among the IoT devices. Fan et al. [51] proposed a simulated environment based on Ethereum, where blockchain was an efficient solution for IoT-based large scale data management systems.

Before applying the blockchain technology in smart cities, it is imperative to identify the essential elements of the system. For example, Sun et al. [52] proposed a triangular framework to identify the features of smart cities from the perspective of sharing economy. Sharing economy is the economic/social model which was concerned with the process to share urban resources. Hence, understanding smart city through the perspective of a sharing economy help the users to allocate resources effectively. A report by Kasperky Labs indicates that smart-terminals such as-information kiosks and self-service machines have many security flaws [53]. They are prone to external malicious attacks, which can compromise several personal and financial details of the users. Biswas et al. [54] proposed a blockchain-based security framework which allowed the entities to communicate in a smart city, while preserving privacy and security. They aimed to tackle various security threats which are discussed as follows:

- *Availability threats*: It is concerned with unauthorized upholding of resources.
- *Integrity threats*: It is concerned with unauthorized modification to the data. For example, data corruption or manipulation.
- *Confidentiality threats*: It is concerned with disclosing of private information by any unauthorized entity.
- *Authenticity threats*: It is concerned to gain access to sensitive data without proper authorization.
- *Accountability threats:* It is concerned with repudiation of transmission or reception of messages by an entity.

Table 3
Relative comparison of existing approaches for Smart City.

Author	Year	Description	Merits	Demerits	1	2	3	4
Lazaroiu et al. [41]	2017	Proposed a smart district model, which was necessary to build a smart city.	Home automation interface was discussed in detail.	Challenges and issues of the model were not exploited to its full potential.	✓	Framework	✓	✓
Zanella et al. [47]	2014	Surveyed the enabling technologies, protocols, and architecture for an urban IoT.	Case study of Padova smart city.	Issues related to conceptualization of Padova were not discussed.	✗	Review	✗	✓
Talari et al. [48]	2017	Conducted an inclusive review of the concept of a smart city.	Detailed discussion on applications of IoT.	Practical use cases were not discussed in detail.	✗	Review	✓	✓
Pham et al. [50]	2015	Developed an algorithm to improve current cloud-based smart-parking system.	Proposed model implemented in real world successfully.	Overlooked the Security aspects.	✗	Framework	✗	✗
Fan et al. [51]	2018	Simulate the application of IoT devices in smart city initiatives.	IoT data management using Ethereum blockchain.	Framework was not summarized in detail.	✓	Framework	✗	✗
Sun et al. [52]	2016	Proposed a triangle framework to identify features of smart cities from the sharing economy perspective.	Discussing the foundation of 'smart' in smart cities from the sharing economy perspective.	Challenges associated with blockchain-based sharing services not fully explored.	✓	Framework	✓	✗
Biswas et al. [54]	2016	Proposed a security framework to provide secure communication platform in a smart city.	Security threats to smart cities discussed.	Downsides of using blockchain for security was ignored.	✓	Framework	✓	✗

1: Usage of Blockchain, 2: Framework/Survey, 3: Security, 4: Applications, Notation: ✓: considered, ✗: not considered.

To address the aforementioned security issues, the model should be able to provide several features such as-improved reliability during communication, better fault tolerance, and faster, efficient operation, and scalability. Moreover, the model contains four layers, where each individual layer is supposed to carry some specific areas of operation:

- *Physical Layer*: It consists of IoT sensor and actuator devices, which collect and forward the data to the upper layers.
- *Communication Layer*: Networks use various communication mechanism such as-Bluetooth, 3G/4G, Ethernet to exchange real-time information among different systems. The upcoming 5G technology enhances the communication standards in this layer. To provide security features during data exchange, blockchain technology such as-Ethereum are integrated with this layer. However, this integration step is quite challenging, since the requirements are different for different industrial applications. This can be overcome by implementing multiple blockchains to provide specific functionalities, which might not be achieved with the usage of a single blockchain.
- *Database Layer*: It uses private ledgers to ensure security, performance, and scalability, especially for real-time systems such as-traffic control system in a smart city.
- *Interface Layer*: It consists of various smart industrial applications such as-smart home, smart parking, and smart health, those work together to make an effective decision.

Table 3 provides the detailed comparison of existing approaches in smart city with reference to parameters such as-blockchain, security, applications, and pros, cons of the existing approaches.

3.3. Healthcare 4.0

Healthcare is one of the most essential aspect for the overall development of any nation. It can be considered as an indication of a society's general well-being. With an increase in population and medical conditions, the burden on modern healthcare systems also increases in recent times. 5G-enabled IoT considered as a potential solution to alleviate the pressures on healthcare system [55–57]. One of the solutions is remote health monitoring, which involves the usage of IoT sensor devices to measure and analyze various health parameters of a user remotely. For example, Baker et al. [58] identified the key components of an end-to-end IoT-based healthcare system for remote monitoring of health of critically ill patient.

Electronic health records (EHR) [59] is the collection of digital version of patients health information. Whereas, personal health record (PHR) is related to the digital record of an individual patient. EHR enables secure, real-time sharing of medical and treatment histories of patients to certain authorized medical personnel [60]. Ekblaw et al. [61] proposed a decentralized record management system termed as *MedRec* to handle EHRs using blockchain technology. It handle private information and manage crucial considerations such as-authentication, confidentiality, accountability, and data sharing. It encourages medical stakeholders such as-public health authorities, researchers, and doctors to participate in the blockchain network as a 'miners' to provide certain incentives.

Saravanan et al. [62] proposed a healthcare paradigm termed as Secured Mobile Enabled Assisting Device (SMEAD) for diabetes monitoring. It is an end-to-end blockchain-based healthcare system, which performs real-time monitoring of

Table 4
Relative comparison of existing approaches for Healthcare 4.0.

Author	Year	Description	Merits	Demerits	1	2	3	4	5	6
Islam et al. [57]	2015	Surveyed the advances in IoT-based healthcare technologies.	Applications of IoT in healthcare industry discussed in detail.	Some applications of IoT were not discussed in detail.	✗	Survey	✓	✗	✓	✓
Baker et al. [58]	2017	Proposed a standard model for application in future IoT healthcare systems.	Extensive discussion about wearable healthcare systems.	Perceivable impact of motion on sensors, which may hinder the purpose of these wearables.	✗	Survey	✓	✓	✓	✓
Cenedese et al. [61]	2014	Proposed a prototype for managing EHR and medical research data.	One-of-its-kind record management system, which handles sensitive medical data.	Limitations regarding privacy, while auditing.	✓	Model	✗	✗	✓	✓
Saravanan et al. [62]	2017	Proposed a healthcare paradigm for diabetes monitoring.	Working of the model in emergency situations discussed.	Challenges of the model, apart form emergency situations, not discussed.	✓	Model	✓	✗	✓	✗
Solanas et al. [63]	2014	Introduced the concept of 'smart health'.	Comparison between m-health and s-health.	Concept of m-health not discussed in detail.	✗	Model	✗	✓	✓	✓
Capossele et al. [64]	2018	Proposed a model for fostering the development of s-health applications.	Detailed lists of main challenges in the s-health ecosystem.	Security aspects of s-health applications not outlined.	✓	Model	✗	✓	✗	✓

1: Usage of Blockchain, 2: Model/Survey, 3: Wearables, 4: Smart-Health, 5: Security, 6: Open Issues and Challenges, Notation: ✓: considered, ✗: not considered.

diabetic patients. Moreover, it was based on the promise that wearable devices were not suitable for emergency situations and were merely used for monitoring purposes. It assist patients who seek special care and constant supervision from specialized doctors.

Solanas et al. [63] proposed *smart health* (or s-health) as "the natural complement of mobile health (m-health) in the context of smart cities". They recognized it as a subset of e-health. The primary goal of smart health apps is to prioritize health within the smart city (or society in general) in an efficient and sustainable manner. Later, Capossele et al. [64] proposed a model that fostered the development of such s-health applications. It was intended as an upgraded version of the existent e-health or m-health solutions [63,65]. It requires data collected from the various EHR and PHR, as well as access to the smart cities' data and infrastructure using technologies like IoT and 5G to deliver relevant real-time feedback to the citizens. But, this approach has some security issues those need to be addressed. The trust-less environment of the platform implied that there was a need for a secure middleware to get rid of any third party access. To tackle the aforementioned issue, the authors of [64] proposed a blockchain-based s-health platform to ensure security, privacy, consistency, interoperability, and trust using 5G and IoT. Moreover, it allows the connection of multiple IoT devices with low latency and high reliability.

Table 4 provides the detailed comparison of existing approaches in healthcare, with reference to parameters such as usage of blockchain, wearables, smart health, security, open issues and challenges, and pros, cons of the existing approaches.

3.4. Industry 4.0

In present era, the complete automation of industrial and business processes become a reality. Massive developments in technology and their introduction into industry has resulted in the emergence of a new approach to production, known as *Industry 4.0*. It aims to combine the prowess of various technological domains, such as-IoT, Blockchain, Cyber-Physical Systems (CPS) [66]. In Industry 4.0, IoT is expected to offer promising transformational solutions to existing industrial systems. Thus, being considered to be a key enabler for the next generation of advanced industrial automation [67].

Due to the highly competitive market, companies aim to gain business advantages at any cost. This forces business process management (BPM) systems in Industry 4.0 to digitize and automate business processes to increase their profits. However, by adding autonomous agents to these business processes, the transaction costs and risks associated with them also increases. A possible solution to handle these risks is that each agent to communicate directly with each other. It solved the problem of transaction costs for autonomous agents. But, there arises a question of trust between these participating agents. In order to tackle all aforementioned issues, Kapitonov et al. [68,69] suggested the use of decentralized systems (blockchain technology) for efficient and secure communication between the autonomous agents in a multi-agent system. Moreover, they developed the Autonomous Intelligent Robot Agen (*project AIRA*) [70], which implemented a standard of economic interaction between human-agent and agent-agent. On the similar line, Viryasitavat et al. [66] explored the possibility to implement the automation in BPM systems using blockchain technology. Leveraging blockchain in business process ensures inter-operation of services with trust and security among the involved parties. The benefits of using blockchain technology in BPM are as follows:

- *Build Trust*: To build trust between parties and devices and to reduce the risk of collision and tampering.
- *Reduce Cost*: To reduce costs and to remove overhead associated with middlemen and intermediaries.
- *Accelerate transactions*: To reduce settlement time from days to near instantaneous.

Real-time QoS monitoring is also an essential part of the modern business processes. With an increase in number of services due to IoT and cloud technologies, a challenge to select the most preferable among these services arises for an efficient business process work-flow composition. Viryasitavat et al. [66] explored the blockchain technology using a "value-driven BPM" framework. The key aspects are as follows:

Table 5
Relative comparison of existing approaches for Industry 4.0.

Author	Year	Description	Merits	Demerits	1	2	3	4	5	6	7
Viryasitavat et al. [66]	2018	Proposed a solution to integrate blockchain with automated BPM systems.	Service selection and composition in Industry 4.0	Proposed QoS blockchain is incapable of detecting transaction frauds.	Framework	✓	✓	✓	✓	✗	✓
Xu et al. [67]	2018	Survey of the state of the art in Industry 4.0 as it relates to industries.	Cyber-Physical Systems (CPS) discussed in detail.	Security aspects related to Industry 4.0 were not explored.	Survey	✗	✓	✗	✗	✗	✓
Kapitonov et al. [68]	2018	Proposed a framework to organize economic interactions between agents using a P2P network based on blockchain.	Architecture of economic interaction protocol.	Issues and challenges of the protocol were not discussed.	Framework	✓	✗	✗	✓	✓	✗

1: Framework/Survey, 2: Usage of Blockchain, 3: BPM, 4: QoS, 5: Smart Contracts, 6: AIRA protocol, 7: Challenges, Notation: ✓: considered, ✗: not considered.

- *Efficiency and quality*: Increase in efficiency by reducing time and cost; automatic upgrades without the need of a central agent.
- *Agility and compliance*: Automated compliance checking increases the agility of modern businesses.
- *Integration and networking*: Automation to integrate cross-organizational business process by eliminating manual operations carried out by intermediaries.

Unlike other distributed ledgers like Ethereum and Bitcoin, which experience high delays, being based on the PoW, the QoS blockchain requires real-time updation of information. In this scenario, the timely execution of a smart contract makes the chaining of a new block to the main blockchain possible in real-time. For example, *UNCHAINET* [71] is a heterogeneous cloud infrastructure powered by blockchain which connects underutilized data resources with clients those need them. Moreover, clients those have extra computing power can get UNET tokens as rewards, if they allocate those unused resources into the *Unchainet* network. The role of 'QoS chain' is to verify the quality, throughput, and reliability of the network providers. It enhances service quality, making *Unchainet* fit for large-scale adoption.

Table 5 provides the detailed comparison of existing approaches in industry 4.0, with reference to parameters such as usage of blockchain, BPM, QoS, smart contracts, use of AIRA protocol, challenges and issues, and pros, cons of the existing approaches.

3.5. Supply chain management

Supply chain is the network of individuals, organizations, resources, and activities that are involved in the life cycle of a product. It starts from product creation to its sale, from the delivery of raw materials from supplier to manufacturer, right up to its delivery to the end user. The usual flow in a supply chain begins with the supplier, followed by the manufacturer, wholesaler, retailer, and finally to the consumer. Supply Chain Management (SCM) is the procedure to manage materials, information, and finances as they move through a process in the supply chain [72]. Given the significance of supply chains, it also faces challenges, some of which are as follows [73]:

- Logistic mismanagement
- Lack of visibility and assets
- Improper handling of data
- Inefficient handling of stack
- Ineffective risk management

Dewey et al. [34] discussed the impact of two technologies on supply chain; blockchain and 5G-enabled IoT. 5G-enabled IoT increases the bandwidth capacity for secure transmission of goods-related data. Blockchain provides an immutable, distributed ledger which enables secure storage of data. Moreover, it can be used as a tool to prevent the occurrence of malicious IoT devices into the network. Besides economical impact of blockchain technology on companies in terms of operational cost, it can potentially help to mitigate legal fees arising from disputes. The main component blochchain technology is *smart contract* which can enable automatic payment of goods upon their receipt, thereby eliminate the need for a third-party confirmation. Another important aspect is to eliminate disputes regarding whether a distributor is entitled to a volume incentive rebate. This can be handled by using smart contracts coupled with 5G to track a shipment.

Casado-Vara et al. [74] suggested a model of supply chain, where the use of blockchain is to provide security to the information of companies involved in the agricultural supply chain along with multi-agent systems for effective coordination of internal activities. Fig. 5 shows the conceptual architecture of a supply chain management with blockchain. This model enables a new market model called *circular economy*. It uses the "Make-Use-Recycle" model, rather than the current "Take-Make-Dispose" model. It allows the economy to be self-sufficient.

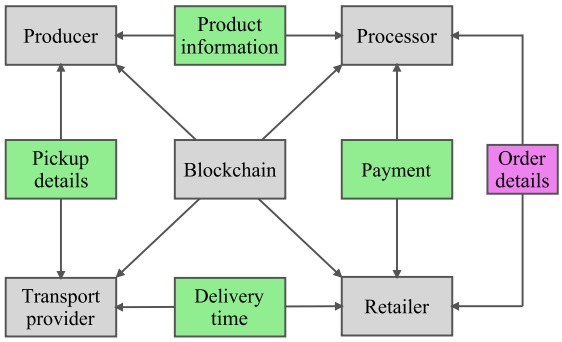

Fig. 5. Supply chain management with blockchain [74].

Table 6
Relative comparison of existing approaches for Supply Chain Management.

Author	Year	Description	Merits	Demerits	1	2	3	4
Dewey et al. [34]	2018	Explores the uses of blockchain, IoT, and 5G technology in supply chains and trade finance.	Detailed discussion on using blockchain with 5G/IoT.	Practical experiences not discussed in detail.	✓	Review	General	✓
Kothari et al. [73]	2018	Explores how IoT addresses the challenges of current supply chain.	Conceptual model of IoT in SCM.	Challenges related to IoT were not discussed.	✗	Survey	General	✗
Casado-Vara et al. [74]	2018	Presents the concept of circular economy.	Thorough comparison of current and blockchain-based supply chain.	Use case of circular economy was ignored.	✓	Model	Alimentary	✓
Mylrea et al. [75]	2018	Software patch and configuration management using blockchain.	Detailed diagrammatic explanation of the research area.	Applied use case of the concept was not discussed.	✓	Model	Software Development	✓
Bocek et al. [76]	2017	Presented 'modum.io', which uses blockchain and IoT in pharma supply chain.	Sequence diagram of the product.	Certain security weaknesses, especially with the data inside the sensor.	✓	Model	Pharmaceutical	✓
Tse et al. [77]	2017	Application of blockchain in food supply information security, especially in China.	PEST analysis of applying blockchain in food supply chain.	Challenges of blockchain in Chinese market not discussed at length.	✓	Model	Agricultural	✓
Holland et al. [78]	2018	Describes the use of DRM in Additive Manufacturing methods.	Discussion of business development by SAMPL ecosystem.	Implementation part was not explained in detail.	✓	Model	3D Print	✓

1: Usage of Blockchain, 2: Model/Review, 3: Type of Industry, 4: Challenges and Issues, Notation: ✓: considered, ✗: not considered.

Unlike physical assets, utilities do not have an inventory of their critical cyber assets. Moreover, they lack the ability to track the different activities associated with software and hardware such as-their development, shipment, and installation, which some time make the systems vulnerable to external cyber attacks. The use of blockchain in this case assist to audit and track the details of the software and hardware supply chain [75]. Bocek et al. [76] discussed in detail about a non-financial start-up worked with blockchains and IoT devices in the pharmaceutical supply chain. The start-up, named as *modum.io*, which enables efficient quality control and regulatory compliance for the transportation of medical products to monitor the temperature of every item during shipment. A smart contract evaluates the data to check for anomalies, while it is stored on the blockchain. Use blockchain technology for pharmaceutical supply chains reduce the number of intermediaries in the logistic process, thereby reducing the operational costs as well as risks related to product tampering.

Table 6 provides the detailed comparison of existing approaches in supply chain, with reference to parameters such as usage of blockchain, type of industry, challenges and issues, and pros, cons of the existing approaches.

3.6. Agriculture

Smart agriculture use modern technologies, such as IoT, GPS, and Big Data to improve the quality and quantity of the resultant agricultural products. Information like temperature, light, soil moisture, and humidity can be stored in a central control system and analyzed using certain AI algorithms [79]. The amalgamation of various technologies in smart agriculture aims to make the agricultural supply chain cost-effective without any compromise in the product quality. Distributed Ledger Technologies (DLTs) are deemed to have the greatest potential to increase the efficiency and transparency in these agricultural supply chains [80]. The most essential aspect that DLTs provide is enhanced traceability. They are able to track any

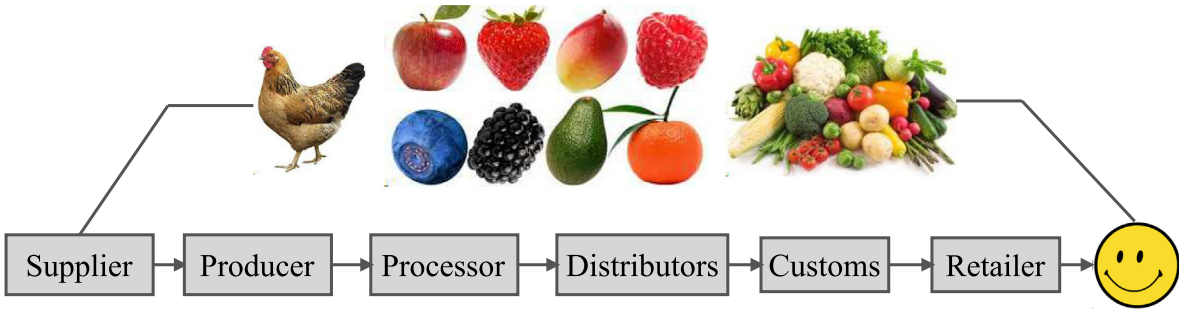

Fig. 6. Agricultural Supply Chain on Distributed Ledger Technologies [80].

transactions those occurs throughout the supply chain in real-time. Then, regulatory control becomes easier, since the product can be traced with every movement in the supply chain, as shown in Fig. 6, which outlines the agriculture supply chain in a distributed ledger technologies.

The use of blockchain in agriculture is focused on food supply chain because agriculture and food supply chain are complementary aspects, where the end-products of agriculture are almost certainly used as inputs in various multi-agent distributed supply chain. In such food supply chains, the consumer is usually the final client [81]. For example, *AgriDigital* was credited with executing the world's first settlement for the sale of 23.46 tons of grain on blockchain in 2016 [82]. The success of *AgriDigital* proved to be as an inspiration for other organizations to consider the potential use of blockchain in the agricultural supply chain. But, with an increase in the food supply the food security can be compromised, which requires a proper food traceability system that able to supervise the food quality and safety during the entire agricultural supply chain. Motivated from the aforementioned discussion, Lin et al. [79] proposed a trusted food traceability system based on blockchain and IoT in a trust-less environment. It is based on the traditional Enterprise Resource Planning (ERP) legacy system, along with a new IoT system. A user at any node (of the supply chain) can use their smart-phone to access the data stored on the blockchain. Moreover, Zhang et al. [77] proposed a blockchain-based traceability system for agricultural food supply chain, specifically for the Chinese market which addressed the issues related to food safety.

Hua et al. [83] proposed a blockchain-based agricultural provenance system, which aims to tackle the trust issues in supply chain industry. It records all information related to the production supply chain, so that it can be monitored by the involved third parties. In order to avoid unnecessary complexities to store information on the blockchain, they designed two related structures:

- *Basic Planting Information:* Information related to a specific process of the supply chain such as-production, storage, and other processes is stored.
- *Provenance Record:* Information related to a certain agricultural operation is stored.

A similar model was proposed by Tse et al. [84], where they used the concept of blockchain technology to improve security of the food supply chain in China.

Caro et al. [85] proposed a blockchain-based decentralized traceability system for agri-food supply chain management, known as *AgriBlockIoT*. It promises transparency and auditable asset traceability to store data from the IoT devices along the complete supply chain in the underlying blockchain. It uses modern edge devices as nodes of the layered blockchain, thus

Table 7
Relative comparison of existing approaches for Smart Agriculture.

Author	Year	Description	Merits	Demerits	1	2	3	4	5
Lin et al. [79]	2018	Proposed a food traceability system based on blockchain and IoT.	Discussed the data processing flow and structure.	Difficult for law-executors to find and process issues in the system.	✓	Model	✓	✓	✗
Tripoli et al. [80]	2018	Explored the opportunities of application of blockchain in agri-food industry.	Exhaustive discussion about DLT in agricultural sector.	Real life examples were not included.	✓	Survey	✗	✓	✗
Kamilaris et al. [81]	2018	Surveyed the impact of blockchain in agricultural and food supply chain.	Extensive survey of blockchain initiatives, in relation to agricultural sector.	Detailed explanation of agricultural supply chain was missing.	✓	Survey	✗	✓	✗
Hua et al. [83]	2018	Proposed an agricultural provenance system based on blockchain.	Detailed use of data nodes explained.	Data uploaded by participating companies will be visible to all participants, which means there is lack of access control.	✓	Model	✗	✓	✗
Caro et al. [85]	2018	Presented a blockchain-based traceability solution for agri-food supply chain.	'Farm-to-folk' use case.	Using a single language for implementing smart-contracts, may interfere while developing more sophisticated business logic.	✓	Model	✗	✓	✗
Sushanth et al. [86]	2018	Proposed a smart agriculture system based on IoT and WSN.	End-to-end algorithm for smart farming system.	Requirement of continuous internet connectivity, which may not be always available.	✗	Model	✓	✗	✓
Pallavi et al. [87]	2017	Proposed a method for remote sensing of agricultural parameters for greenhouse.	Complete architecture explained it detail.	Security aspects of the system were ignored.	✗	Model	✓	✗	✓

1: Usage of Blockchain, 2: Model/Survey, 3: Smart Agriculture, 4: Food Traceability, 5: Algorithm, Notation: ✓: considered, ✗: not considered.

enhanced the robustness of the network. The primary modules of *AgriBlockIoT* were *API*, *Controller*, and *Blockchain*. Another important aspect of smart agriculture, besides agricultural supply chain, is the smart irrigation, which aims at wiser utilization of water. The available freshwater resources worldwide forces the users to devise certain strategies to utilize water resources sensibly, given the advancements in science and technologies such as-IoT, cloud computing, and big data. Automation of irrigation systems coupled with thermal imaging has been a possible solution for smart irrigation, which measures the water levels in the soil and controls the actuators to irrigate. It is an improvement to the current scheduled irrigation, thus causing a more controlled utilization of water. Sushanth et al. [86] proposed a smart agriculture system, based on the concepts of IoT and cloud computing. It enables a farmer to devise an efficient, feasible irrigation schedule for their farm based on their preferences. Based on the farmer's inputs, an automated smart irrigation system was developed, which provides the suitable schedule for them. Then, with the help of relevant sensors and actuators, a specific procedure was executed to control the water quantity while irrigation was carried out. A similar model was proposed by Pallavi et al. [87], where they suggested a control system for greenhouse agriculture using IoT devices for remote sensing of relevant parameters. Their objective was to encourage organic farming, while increasing the yield. The parameters taken into consideration included carbon dioxide emission, temperature, soil moisture, and light. Zhai et al. [88] proposed a similar greenhouse monitor system based on IoT technology. Table 7 provides the detailed comparison of existing approaches in agriculture, with reference to parameters such as-usage of blockchain, smart agriculture, food traceability, algorithm, and pros, cons of the existing approaches.

3.7. Autonomous vehicles

With rapid technological developments in sensing, communication, analysis, and computation, the growth of Intelligent Transportation Systems (ITS) has been formidable. ITS has enabled smarter, safer, and more convenient transport facilities and services. However, a critical security risk regarding ITS is its tendency towards centralization, which may cause the centralized authorities to be temporarily down due to certain external malicious attacks. Moreover, lack of adequate trust among the ITS agents need to be tackled. To overcome the aforementioned challenges, Yuan et al. [89] proposed a blockchain-based secured, trusted, and decentralized autonomous ecosystem for ITS, known as B^2ITS. It is steeping stone for PtMS (Parallel Transportation Management Systems) framework, which aims to optimize the real-world transportation systems using parallel interactions with their counterparts.

One of the applications of the B^2 ITS framework is a real-time ride-sharing, named as *La'zooz* [90]. It was a "blockchained-version of Uber"whose aims was to built an open-source, decentralized ride-sharing network to challenge the currently established private transportation systems. The advantages such decentralized applications are; to eliminate the unwanted decisions and risks taken by the central system such as-surge pricing, and privacy leaks. Complementing such novel ventures, Huckle et al. [15] proposed an automatic payment system, known as *AutoPay*, which was a service that provides security and trust by 'embodying' the user through the use of smart contracts on its blockchain interface. It allows the vehicle to synchronize automatically with the user's *AutoPay* service, which can be use for external payment related services such as-fuel payment.

Singh et al. [91] proposed a reward-based intelligent vehicle (IV) communication framework based on blockchain technology. It was used to ensure a trusted environment to share the information between these vehicles, with Proof-of-Driving (PoD). Moreover, it focused on a secure and fast communication system among the intelligent vehicles (also called 'self-driving cars') [92]. It has three basic components which are as follows:

Table 8
Relative comparison of existing approaches for Autonomous Vehicles.

Author	Year	Description	Merits	Demerits	1	2	3	4	5
Huckle et al. [15]	2016	Discussed possible use of IoT and blockchain together in creating secure shared economy applications.	Blockchain integrated IoT scenarios.	Security and scaling challenges of IoT were not addressed.	✓	Survey	✗	✗	✗
Yuan et al. [89]	2016	Conducts a preliminary study of blockchain-based ITS.	Case study of La'zooz.	Issues and challenges of the model were not discussed.	✓	Model	✗	✓	✗
Singh et al. [91]	2017	Proposed an intelligent vehicles data sharing framework.	Seven-layer conceptual model for the framework.	Compatible with real-time traffic data.	✓	Model	✓	✓	✗
Leiding et al. [93]	2016	Proposed self-managed, blockchain-based VANET.	Ethereum integrated with VANET.	Optional applications were not explored, along with mandatory applications.	✓	Model	✓	✗	✗
Ortega et al. [94]	2018	Presented enabling technologies for secure vehicular communications.	Network slicing using 5G in VANET.	Lack of standardized consensus protocol for VANET.	✓	Model	✓	✗	✓

1: Usage of Blockchain, 2: Model/Survey, 3: VANET, 4: ITS, 5: 5G, Notation: ✓: considered, ✗: not considered.

- *Network-enabled connected device*: A device with Internet connectivity, which helps to communicate in the Vehicular Ad-Hoc Network (VANET). In this scenario, the device is an IV.
- *Vehicular Cloud Computing (VCC)*: Enhanced traffic management and road safety with the help of real-time monitoring of other IVs.
- *Blockchain*: Ensured secured and reliable information sharing among IVs.

Leiding et al. [93] proposed the concept of a self-managed blockchain-based VANET, where the use of smart contracts enables the deployment of any type of applications on the blockchain platform. Authors fostered the development of certain mandatory applications which enforced network rules and regulations. These include traffic regulation, vehicle tax, and insurance applications. A similar model was proposed by Ortega et al. [94], where they explored the pros and cons to implement a completely autonomous and decentralized permissioned blockchain, instead of the traditional client-server architecture. Their objective was to alleviate the risks associated with data tampering or data corruption; and also to provide a robust and cheaper solution.

Table 8 provides the detailed comparison of existing approaches in autonomous vehicles, with reference to parameters such as blockchain, VANET, ITS, 5G, and pros, cons of the existing approaches.

3.8. Unmanned Aerial Vehicles

Unmanned Aerial Vehicle (UAV), also known as drone, is an airborne system or an aircraft operated remotely by a human operator or autonomously by an on-board computer [95]. The images obtained from UAVs can provide support in various industrial applications such as-urban modelling, surveillance, large scale mapping, delivery, communications and media, search-and-rescue operations, and agriculture [96]. UAVs are operated by several military forces and also by certain civilian organizations. Majority of the commercial UAVs depend on Wi-Fi connectivity to be remotely accessible. However, Wi-Fi connectivity is not sufficient for beyond the visual line-of-sight (LOS) communication. Instead, ubiquitous mobile networks such as-5G can be used to operate them beyond the LOS communication. Moreover, they offer wide-area, high speed, and secure wireless connectivity, which can improve the control and safety of the device [97]. With the rise of autonomous UAVs, risks of intrusion or interception increases. A large number of attacks target such UAV networks; for example, to jam the communication network, inject false data, and disrupting the network operations. Sedjelmaci et al. [98] implemented a cyber-security system based on Intrusion Detection Systems (IDS) to safeguard UAVs from external cyber attacks [99]. In this model, every UAV can monitor the behaviour of its peers. In case an IDS agent is suspected to be malicious, it is barred to operate as a monitoring node.

Strong encryption, which is currently employed for data link protection is difficult to manage. To improve this situation, the encryption capabilities must be simplified to distribute data to predefined operating locations. It allows the UAV to perform its job more efficiently without the need to focus on other tasks such as-to validate users, to transmit important information, or operational changes to the route [100].

Kuzmin et al. [100] proposed a distributed, scalable, and secure model called UAV communication network *(UAVNet)*, as a potential means of safe, real-time information exchange between UAVs. UAVNet was a blockchain network with each UAV acts as a blockchain node. Each node has inbuilt functionalities to create and read transactions from the block along with some tools to enable transaction exchange with other UAVs. In this model, blockchain ensures the UAV be autonomous, even when signals from other UAVs were not perceivable. The nodes must have the capability to operate even without coordinate

Table 9
Relative comparison of existing approaches for Unmanned Aerial Vehicles.

Author	Year	Description	Merits	Demerits	1	2	3	4
Kapitonov et al. [69]	2017	Describes a method to organize a communication system between agents in P2P network.	Secure communication system within a multi-agent system.	Issues of AIRA protocol were not discussed.	✓	Model	Autonomous agents communication scheme.	AIRA protocol
Lin et al. [97]	2018	Discussed LTE connectivity for low-altitude small UAVs.	Providing beyond line-of-sight communication with UAV using LTE.	Drone-to-drone NLOS communication was not discussed in detail.	✗	Survey	Aerial Channel Characteristics.	LTE
Motlagh et al. [101]	2017	Proposed the usage of IoT-enabled UAVs for crowd surveillance.	Performance enhancements in semi-autonomous UAVs.	Role of mobile networks in drone communication was not discussed.	✗	Model	UAV-based IoT platform	5G
Kuzmin et al. [100]	2018	Proposed a secure network for inter-UAV communication.	Minimizing UAVNet cyber-security threats using blockchain.	The 51% attack not taken into account.	✓	Model	UAVNet	LTE/4G/5G

1: Usage of Blockchain, 2: Proposed any model, 3: Focused on, 4: Communication Standard, Notation: ✓: considered, ✗: not considered.

with the satellite navigation system by executing relevant smart contracts at the required time. Moreover, an external storage can also be included in this model: a blockchain repository, similar to a black-box of an airplane.

Another use case of UAV is crowd surveillance. Motlagh et al. [101] proposed a UAV-based crowd surveillance model using facial recognition with Open Source Computer Vision *(OpenCV)*. In this model, when UAVs are equipped with remotely controlled IoT devices then it can offer various value added services (VAS). When coupled with more advanced communication standards such as-5G networks, UAVs can have the support for extreme real-time video surveillance and streaming. Moreover, UAVs can be used as a backbone to provide support for the coverage of 5G. An example is Google's *SkyBender* project, which used UAVs to deliver high-speed Internet [102].

Table 9 provides the detailed comparison of existing approaches in agriculture, with reference to parameters such as-usage of blockchain, focus, communication standard, and pros, cons of the existing approaches.

3.9. Multimedia and digital right management

Media distribution is a form of digital distribution of multimedia contents such as-audio, image, and video [106]. Compared to the past platforms to deliver media such as-compact discs, delivery medium such as-P2P or cloud services have become the current standard for multimedia delivery. The advantages of the current online content delivery medium include high availability, cost effectiveness, and higher performance. Due to these reasons, cloud-based Content Delivery Networks (CDNs) are generally preferred over the traditional CDNs, owing to their lower housing cost, since owning of infrastructure is not required. However, these systems have certain inherent issues which are difficult to resolve, given the centralized architecture of current Digital Rights Management systems (DRM). For example, modifications to the original media cannot be traced, difficulty to protect copyrights, and lack of an efficient profit model [105].

Kishigami et al. [104] proposed a blockchain-based content distribution system to assist the media creators demand an efficient way for digital rights management. In this technique, right holders themselves have the power to operate the system. This framework complements the current DRM systems, where the latter requires an authentication mechanism, which is provided by the former, using blockchain. However, being an initial prototype, it had a drawback that it had no incentive model; so the miners can not get any rewards for the successful mining of a block.

A similar model was proposed by Xu et al. [105], which was a DRM system for network media. It was able to confirm copyrights in real-time using smart contracts along with digital signatures and secure hash to validate the transactions. Also,

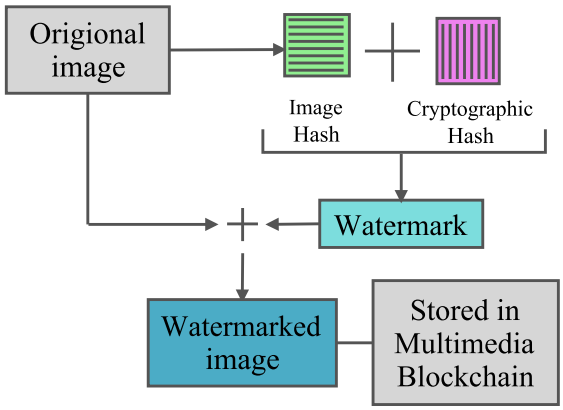

Fig. 7. Watermarking-based multimedia blockchain framework [106].

Table 10
Relative comparison of existing approaches for Multimedia and DRM.

Author	Year	Description	Merits	Demerits
Fujimara et al. [103]	2015	Proposed a decentralized rights management system.	Usage of license key explained in detail.	Latency of five seconds may be high for some applications.
Kishigami et al. [104]	2015	Proposed a blockchain-based digital content distribution system.	Detailed explanation of high reolution video content distribution system.	Lack of incentive mechanism.
Xu et al. [105]	2017	Proposed a blockchain-based digital rights management scheme.	Real-time copyright confirmation using consensus mechanism.	Challenges faced by the model were not discussed.
Bhomwik et al. [106]	2017	Proposed a distributed and tamper-proof media transaction framework.	Self-embedding watermarking algorithm.	Storage of images and their watermarks not discussed in detail.

Fujimura et al. [103] proposed a trial implementation called Blockchain-based RIGHTs management system *(BRIGHT)*, which focused mainly on the rights management of video files on blockchain. The problem with current multimedia distribution is that they do not preserve any information about the ownership or modification history of the media. The original media can often be tampered with for some specific purposes, either for creative work, or to spread false propaganda over social media. Moreover, there is no proven technique with which one can identify with confidence and any modifications to such media. Bhowmik et al. [106] proposed a watermarking-based multimedia blockchain framework to address these issues. The unique watermark contains information about the following two aspects:

- *Image Hash*: It is used to preserve the original media content so it can be easily retrieved when required.
- *Cryptographic Hash*: It contains the transaction history, which indicate any kind of modification to the original media.

Fig. 7 illustrate an overview of the usage of blockchain in multimedia and digital right management. In this framework, the use of blockchain technology helps the creators of media maintain their digital rights efficiently.

In addition to multimedia, the concept of digital rights management is also used to protect the Intellectual Property Rights (IPR) of 3D print supply chain, which comes under the umbrella of Industry 4.0. Its task is to differentiate between 'original', 'copy', and 'counterfeit' spare parts. The general technique to address this issue is to use licensing models, which are common in the areas of software and digital media. Regarding the physical parts, the overall decrease in the cost of 3D printing materials have cause the level of plagiarism of 3D printed items to increase to a significant amount. Hence, it is imperative for firms to focus on counterfeiting protection, since it can potentially cause them annual losses in billions. To address the aforementioned issues, Holland et al. [78] proposed the concept of "Secure Additive Manufacturing Platform" *(SAMPL)*, which develops a secure chain of trust for additive manufacturing procedures. Similar concepts are also applicable for copy machines to tackle the counterfeiting of money using 'secure elements'. When these secure elements are installed on trusted printers, the controlled communication with the blockchain allow the making of a complete chain of trust from copyright holder to the service provider.

Table 10 provides the detailed comparison of existing approaches with their pros, cons.

4. Open issues and challenges

While the amalgamation of IoT and blockchain is received considerable research interest both from academia and industry. The Bitcoin-style blockchain which are based on the PoW concept have some characteristics which make them poorly suited for many IoT scenarios. Based on the extensive literature review, challenges discussed with blockchain based 5G-enabled IoT applications and issues delineated is shown in Fig. 8, we have identified major research challenges related to blockchain based 5G-enabled IoT. Hence, before considering to apply this concept in existing systems, these issues need to investigated further:

- With the rapid increase in IoT devices being battery-powered (and thus resource restricted), but their energy requirements are limited. However, with the introduction of blockchain, where block mining is a computation-intensive task. In these scenario, the energy requirements and processing time of devices need to be explored further.

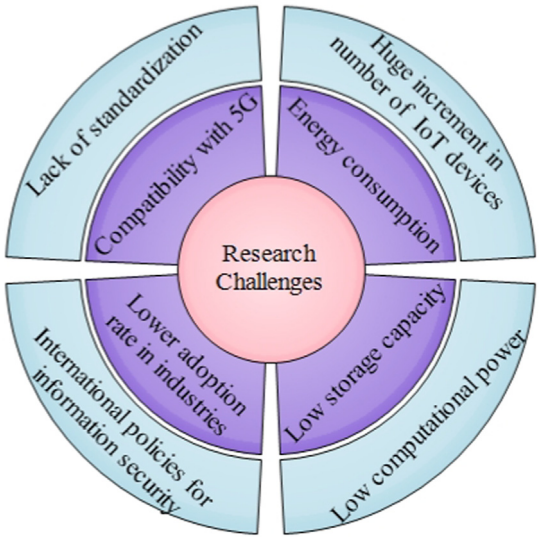

Fig. 8. Research challenges in blockchain based 5G-enabled IoT.

- Blockchain was introduced to supplant the current client/ server systems. But, this information is be stored in the nodes, which are usually the IoT devices. These devices have low computational power and very low storage capacity, so this would prove a big hurdle in the adoption of this technology.
- Blockchain scales poorly as the number of nodes in the network increases which should be addressed as soon as possible.
- There still remains some unanswered questions about blockchain such as-the elimination of certain vulnerabilities like DoS attacks and the infamous 51% attack with regards to establishing distributed trust.
- Lack of proper standardization and no interoperability means different ledgers cannot directly communicate with each other. But, they require the involved stakeholders to highly compromise (ranging from complete data to the policies) to achieve full interoperability. It requires international policies for collective trust and information security.
- Lack of solid business cases due to large number of uncertainties. Being a relatively new technology, people are in a dilemma of its adoption in their industries.
- It also has the ability to connect different stakeholders from different regions (possibly countries) without the need for any kind of legal compliance to follow. It is a challenge for both service providers and manufacturers and could be a significant barrier for adopting blockchain in many business cases.
- With the advent of 5G technologies, IoT devices should be upgraded so as to be compatible with the high-speed network connectivity.

5. Conclusion

In future, end user will be enjoying the services of 5G then the integration of blockchain with IoT devices becomes a game changer. In this paper, we provide insights to the readers about the industrial applications of blockchain in 5G-enabled IoT devices. Here, discussion is divided into three parts, firstly discussed the background of blockchain, IoT, and 5G briefly followed by respective industrial applications. Lastly, open issues and challenge have been covered mainly for industrial applications. Owing to the high-end hardware requirements and the lack of compatibility for high network connectivity, use of the technologies covered in this work on a common platform is still far from a reality. Most of the industrial applications have been covered in this work, where blockchain will be used to maintain the security faster data flow. But, beyond the small-scale developments and deployments of specific applications, a great amount of technological research is require to address the specific demands pertaining to the collaboration of these technologies. Therefore, lastly comparative analysis of the existing blockchain-based industrial applications is performed on the basis of specific parameters.

In future, we would minimize our discussion on healthcare only and plan to propose a blockchain based secured healthcare system.

References

[1] Mark Hung, Leading the IoT, 2017.
[2] I. Budhiraja et al, CR-NOMA Based Interference Mitigation Scheme for 5G Femtocells Users, in: 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 1–6.
[3] I. Budhiraja et al, Cross layer NOMA interference mitigation for Femtocell users in 5G environment, IEEE Trans. Veh. Technol. 68 (5) (May 2019) 4721–4733.
[4] I. Budhiraja et al, DIYA: tactile internet driven delay assessment NOMA-based scheme for D2D communication, IEEE Trans. Ind. Inf. (2019) 1, https://doi.org/10.1109/TII.2019. 2910532.
[5] T.M. Fernandez-Carames, P. Fraga-Lamas, A review on the use of blockchain for the internet of things, IEEE Access 6 (2018) 32979–33001.
[6] Muhammad Habib ur Rehman et al, The role of big data analytics in industrial Internet of Things, Future Gener. Comput. Syst. 99 (2019) 247–259.
[7] Hong-Ning Dai et al, Big data analytics for manufacturing internet of things: opportunities, challenges and enabling technologies, Enterprise Inf. Syst. (2019) 1–25.
[8] Rahul Agrawal et al, Continuous security in IoT using blockchain, in: 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2018, pp. 6423–6427.
[9] S. Tanwar et al, An advanced internet of thing based security alert system for smart home, in: 2017 International Conference on Computer, Information and Telecommunication Systems (CITS), 2017, pp. 25–29.
[10] J. Wan et al, A blockchain-based solution for enhancing security and privacy in smart factory, IEEE Trans. Ind. Inf. 15 (6) (June 2019) 3652–3660.
[11] Sudeep Tanwar, Sudhanshu Tyagi, Sachin Kumar, The Role of Internet of Things and Smart Grid for the Development of a Smart City, in: Yu-Chen Hu et al. (Eds.), Intelligent Communication and Computational Technologies, Springer Singapore, Singapore, 2018, pp. 23–33.
[12] Sudeep Tanwar et al, A systematic review on security issues in vehicular ad hoc network, Secur. Privacy 1 (5) (2018) e39.
[13] Sana Moin et al, Securing IoTs in distributed blockchain: analysis, requirements and open issues, Future Gener. Comput. Syst. 100 (2019) 325–343.
[14] Hasan Ali Khattak et al, Perception layer security in Internet of Things, Future Gener. Comput. Syst. 100 (2019) 144–164.
[15] Steve Huckle et al, Internet of things, blockchain and shared economy applications, Proc. Comput. Sci. 98 (2016) 461–466.
[16] Ali Dorri, Salil S Kanhere, Raja Jurdak, Blockchain in internet of things: challenges and solutions, 2016. arXiv:1608.05187.
[17] Konstantinos Christidis, Michael Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.
[18] Sumaiyya Z. Khan, Snehal R. Kamble, Ambarish R. Bhuyar, A review on BIoT: blockchain IoT, IJREAM 04 (03) (2018) 808–812.
[19] Bogdan Cristian Florea, Blockchain and Internet of Things data provider for smart applications, in: 2018 7th Mediterranean Conference on Embedded Computing (MECO), IEEE, 2018, pp. 1–4.
[20] Mahdi H. Miraz, Maaruf Ali, Blockchain enabled enhanced IoT ecosystem security, in: International Conference for Emerging Technologies in Computing, Springer, 2018, pp. 38–46.
[21] Hany F Atlam et al, Blockchain with internet of things: benefits, challenges, and future directions, Int. J. Intell. Syst. Appl. 10 (6) (2018) 40–48.
[22] Madhusudan Singh, Abhiraj Singh, Shiho Kim, Blockchain: a game changer for securing IoT data, in: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), pp. 51–55.
[23] DongYeop Hwang, JungYong Choi, Ki-Hyung Kim, Dynamic Access Control Scheme for IoT Devices using Blockchain, in: 2018 International Conference on Information and Communication Technology Convergence (ICTC), IEEE, pp. 713–715.
[24] Satoshi Nakamoto, Bitcoin: a peer-to-peer electronic cash system, 2008.

[25] Alfonso Panarello et al, Blockchain and iot integration: a systematic survey, Sensors 18 (8) (2018) 2575.
[26] Hossein Shafagh, et al., Towards blockchain-based auditable storage and sharing of iot data, in: Proceedings of the 2017 on Cloud Computing Security Workshop, ACM, pp. 45–50.
[27] Hyperledger Fabric. URL:https://www.hyperledger.org/projects/fabric (visited on 02/21/2019).
[28] Ripple – One Friction-less Experience To Send Money Globally. URL:https://ripple.com/ (visited on 02/21/2019).
[29] Sajjad Hussain Shah, Ilyas Yaqoob, A survey: Internet of Things (IOT) technologies, applications and challenges, in: 2016 IEEE Smart Energy Grid Engineering (SEGE), pp. 381–385.
[30] Er Pooja Yadav, Er Ankur Mittal, Hemant Yadav, IoT: challenges and issues in indian perspective, in: 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), IEEE, pp. 1–5.
[31] Yogita Pundir, Nancy Sharma, Yaduvir Singh, Internet of things (IoT): challenges and future directions, Int. J. Adv. Res. Comput. Commun. Eng. 5 (3) (2016) 960–964.
[32] Jyoti Mante Khurpade, Devakanta Rao, Parth D. Sanghavi, A survey on IOT and 5G network, in: 2018 International Conference on Smart City and Emerging Technology (ICSCET), pp. 1–3.
[33] Waleed Ejaz et al, Internet of Things (IoT) in 5G wireless communications, IEEE Access 4 (2016) 10310–10314.
[34] Josias N. Dewey, Robert Hill, Rebecca Plasencia, Blockchain and 5G-enabled Internet of Things (IOT) will redefine Supply Chains and Trade Finance, Secured Lender (2018) 42–45.
[35] Aaron Yi Ding, Marijn Janssen, Opportunities for applications using 5G networks: requirements, challenges, and outlook, in: Proceedings of the Seventh International Conference on Telecommunications and Remote Sensing, ACM, 2018, pp. 27–34.
[36] Mashael M. Alsulami, Nadine Akkari, The role of 5G wireless networks in the internet-of-things (IoT), in: 2018 1st International Conference on Computer Applications Information Security (ICCAIS), IEEE, pp. 1–8.
[37] Ana Reyna et al, On blockchain and its integration with IoT. Challenges and opportunities, Future Gener. Comput. Syst. 88 (2018) 173–190.
[38] Aymen Boudguiga, et al., Towards better availability and accountability for iot updates by means of a blockchain, 2017 IEEE European Symposium on Security and Privacy Workshops (EuroSPW), pp. 50–58.
[39] Knud Erik Skouby, Per Lynggaard, Smart home and smart city solutions enabled by 5G, IoT, AAI and CoT services, in: Contemporary Computing and Informatics (IC3I), 2014 International Conference on, pp. 874–878.
[40] Rakesh Roshan, Abhay Kr Ray, Challenges and risk to implement IOT in smart homes: an Indian perspective, Int. J. Comput. Appl. 153 (2016) 16–19.
[41] Cristian Lazaroiu, Mariacristina Roscia, Smart district through IoT and blockchain, in: 2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA), pp. 454–461.
[42] Donhee Han, Hongjin Kim, Juwook Jang, Blockchain based smart door lock system, in: Information and Communication Technology Convergence (ICTC), 2017 International Conference on, pp. 1165–1167.
[43] Ali Dorri, Salil S Kanhere, Raja Jurdak, Towards an optimized blockchain for IoT, in: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, ACM, 2017, pp. 173–178.
[44] Ali Dorri, et al., Blockchain for IoT security and privacy: the case study of a smart home, in: Pervasive Computing and Communications Workshops (PerComWorkshops), 2017 IEEE International Conference on, pp. 618–623.
[45] Seyoung Huh, Sangrae Cho, Soohyung Kim, Managing IoT devices using blockchain platform, in: Advanced Communication Technology (ICACT), 2017 19th International Conference on, pp. 464–467.
[46] Yu Nandar Aung, Thitinan Tantidham, Review of ethereum: smart home case study, in: Information Technology (INCIT), 2017 2nd International Conference on, pp. 1–4.
[47] Andrea Zanella et al, Internet of things for smart cities, IEEE Internet Things J. 1 (1) (2014) 22–32.
[48] Saber Talari et al, A review of smart cities based on the internet of things concept, Energies 10 (4) (2017) 421.
[49] Angelo Cenedese et al, Padova smart city: an urban internet of things experimentation, in: Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2014, pp. 1–6.
[50] Thanh Nam Pham et al, A cloud-based smart-parking system based on Internet-of-Things technologies, IEEE Access 3 (2015).
[51] Lingjun Fan et al, Investigating blockchain as a data management tool for IoT devices in smart city initiatives, in: 19th Annual International Conference on Digital Government Research: Governance in the Data Age, ACM, 2018, p. 100.
[52] Jianjun Sun, Jiaqi Yan, Kem ZK Zhang, Blockchain-based sharing services: what blockchain technology can contribute to smart cities, Financial Innovation 2 (1) (2016) 26.
[53] Denis Makrushin, V. Dashchenko, Fooling the 'Smart City' (Technical Report), 2016, pp. 1–22.
[54] Kamanashis Biswas, Vallipuram Muthukkumarasamy, Securing smart cities using blockchain technology, in: 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS), pp. 1392–1393.
[55] Aparna Kumari et al, Fog computing for Healthcare 4.0 environment: opportunities and challenges, Comput. Electr. Eng. 72 (2018) 1–13.
[56] Akshay Gapchup et al, Health care systems using internet of things, IJIRCCE 4 (2016) 12.
[57] S.M. Riazul Islam et al, The internet of things for health care: a comprehensive survey, IEEE Access 3 (2015) 678–708.
[58] Stephanie B. Baker, Wei Xiang, Ian Atkinson, Internet of things for smart healthcare: technologies, challenges, and opportunities, IEEE Access 5 (2017) 26521–26544.
[59] Jigna J Hathaliya et al, Securing electronics healthcare records in Healthcare 4.0: a biometric-based approach, Comput. Electr. Eng. 76 (2019) 398–410.
[60] What is an electronic health record (EHR)? URL:https://www.healthit.gov/faq/what-electronic-health-record-ehr.
[61] Ariel Ekblaw et al, A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data, Proceedings of IEEE Open Big Data Conference, vol. 13, 2016, p. 13.
[62] M. Saravanan, et al., SMEAD: A secured mobile enabled assisting device for diabetics monitoring, in: 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1–6.
[63] Agusti Solanas et al, Smart health: a context-aware health paradigm within smart cities, IEEE Commun. Mag. 52 (8) (2014) 74–81.
[64] Angelo Capossele et al, Leveraging blockchain to enable smart-health applications, in: IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI), 2018, pp. 1–6.
[65] J. Vora et al, BHEEM: a blockchain-based framework for securing electronic health records, in: 2018 IEEE Globecom Workshops (GC Wkshps), 2018, pp. 1–6.
[66] Wattana Viryasitavat et al, Blockchain-based business process management (BPM) framework for service composition in industry 4.0, J. Intell. Manuf. (2018) 1–12.
[67] Li Da Xu, Eric L. Xu, Ling Li, Industry 4.0: state of the art and future trends, Int. J. Prod. Res. 56 (8) (2018) 2941–2962.
[68] Aleksandr Kapitonov, et al., Blockchain based protocol for economical communication in Industry 4.0, in: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), pp. 41–44.
[69] Aleksandr Kapitonov, et al., Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs, in: Research, Education and Development of Unmanned Aerial Systems (REDUAS), 2017 Workshop on, pp. 84–89.
[70] AIRA – open source software for smart cities and Industry 4.0 projects. URL:https://aira.life (visited on 02/12/2019).
[71] UNCHAINET – decentralized cloud platform. URL:https://www.unchainet.com/ (visited on 02/17/2019).
[72] What is supply chain (SC)? URL:https://whatis.techtarget.com/definition/supply-chain (visited on 02/17/2019).
[73] Sneha S. Kothari, Simran V. Jain, Abhishek Venkteshwar, The Impact of IOT in Supply Chain Management, 2018.
[74] Roberto Casado-Vara et al, How blockchain improves the supply chain: case study alimentary supply chain, Proc. Comput. Sci. 134 (2018) 393–398.

[75] Michael Mylrea, Sri Nikhil Gupta Gourisetti, Blockchain for Supply Chain Cybersecurity, Optimization and Compliance, in: 2018 Resilience Week (RWS), pp. 70–76.
[76] Thomas Bocek, et al., Blockchains everywhere-a use-case of blockchains in the pharma supply-chain, in: Integrated Network and Service Management (IM), 2017 IFIP/IEEE Symposium on, pp. 772–777.
[77] Daniel Tse, et al., Blockchain application in food supply information security, in: 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), pp. 1357–1361.
[78] Martin Holland, Josip Stjepandi, Christopher Nigischer, Intellectual property protection of 3D print supply chain with blockchain technology, in: 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), pp. 1–8.
[79] Jun Lin, et al., Blockchain and IoT based food traceability for smart agriculture, in: Proceedings of the 3rd International Conference on Crowd Science and Engineering, ACM, 2018, p. 3.
[80] M. Tripoli, J. Schmidhuber, Emerging opportunities for the application of blockchain in the agri-food industry, in: FAO and ICTSD: Rome and Geneva. Licence: CC BY-NC-SA 3, 2018.
[81] Andreas Kamilaris, Agusti Fonts, Francesc X. Prenafeta-Boldý, The rise of the blockchain technology in agriculture and food supply chain, 2018.
[82] Perspectives for ICT and Agribusiness in ACP countries: start-up financing, 3D printing and blockchain. URL:http://www.fao.org/e-agriculture/events/cta-workshop-perspectives-ict-and-agribusiness-acp-countries-start-financing-3d-printing-and (visited on 02/16/2019).
[83] Jing Hua, et al., Blockchain based provenance for agricultural products: a distributed platform with duplicated and shared bookkeeping, in: 2018 IEEE Intelligent Vehicles Symposium (IV), pp. 97–101.
[84] Daniel Tse, et al., Blockchain application in food supply information security, in: 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), pp. 1357–1361.
[85] Miguel Pincheira Caro et al, Blockchain-based traceability in Agri-Food supply chain management: a practical implementation, in: IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany), 2018, pp. 1–4.
[86] G. Sushanth, S. Sujatha, IOT based smart agriculture system, in: 2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE, 2018, pp. 1–4.
[87] S. Pallavi, Jayashree D. Mallapur, Kirankumar Y. Bendigeri, Remote sensing and controlling of greenhouse agriculture parameters based on IoT, in: 2017 International Conference on Big Data, IoT and Data Science (BID), pp. 44–48.
[88] Ji-chun Zhao, et al., The study and application of the IOT technology in agriculture, in: Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, vol. 2, pp. 462–465.
[89] Yong Yuan, Fei-Yue Wang, Towards blockchain-based intelligent transportation systems, in: 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), pp. 2663–2668.
[90] LaZooz. URL:https://lazooz.org (visited on 02/13/2019).
[91] Madhusudan Singh, Shiho Kim, Blockchain Based Intelligent Vehicle Data sharing Framework. arXiv:1708.09721 (2017).
[92] Madhusudan Singh, Dhananjay Singh, Antonio Jara, Secure cloud networks for connected & automated vehicles, in: International Conference on Connected Vehicles and Expo (ICCVE), 2015, pp. 330–335.
[93] Benjamin Leiding, Parisa Memarmoshrefi, Dieter Hogrefe, Selfmanaged and blockchain-based vehicular ad-hoc networks, in: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, pp. 137–140.
[94] Victor Ortega, Faiza Bouchmal, Jose F. Monserrat, Trusted 5G vehicular networks: blockchains and content-centric networking, IEEE Veh. Technol. Mag. 13 (2) (2018) 121–127.
[95] Applications of Unmanned Aerial Vehicle (UAV) based Remote Sensing in NE Region – ISRO. URL:https://www.isro.gov.in/applications-of-unmanned-aerial-vehicle-uav-based-remote-sensing-ne-region.
[96] Sathyanarayanan Chandrasekharan et al, Designing and implementing future aerial communication networks, IEEE Commun. Mag. 54 (5) (2016) 26–34.
[97] Xingqin Lin et al, The sky is not the limit: LTE for unmanned aerial vehicles, IEEE Commun. Mag. 56 (4) (2018) 204–210.
[98] Hichem Sedjelmaci, Sidi Mohammed Senouci, Mohamed-Ayoub Messous, How to detect cyber-attacks in unmanned aerial vehicles network?, in: Global Communications Conference (GLOBECOM), IEEE, 2016, pp 1–6.
[99] Mandrita Banerjee, Junghee Lee, Kim-Kwang Raymond Choo, A blockchain future for internet of things security: a position paper, Digital Commun. Netw. 4 (3) (2018) 149–160.
[100] Alexander Kuzmin, Evgeny Znak, Blockchain-base structures for a secure and operate network of semi-autonomous Unmanned Aerial Vehicles, in: 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), pp. 32–37.
[101] Naser Hossein Motlagh, Miloud Bagaa, Tarik Taleb, UAV-based IoT platform: a crowd surveillance use case, IEEE Commun. Mag. 55 (2) (2017) 128–134.
[102] Mark Harris, Project Skybender: Google's secretive 5G internet drone tests revealed, Guardian 29 (2016).
[103] Shigeru Fujimura, et al., BRIGHT: a concept for a decentralized rights management system based on blockchain, in: 2015 IEEE 5th International Conference on Consumer Electronics-Berlin (ICCE-Berlin), pp. 345–346.
[104] Junichi Kishigami, et al., The blockchain-based digital content distribution system, in: 2015 IEEE Fifth International Conference on Big Data and Cloud Computing (BDCloud), pp. 187–190.
[105] Ruzhi Xu, et al., Design of network media's digital rights management scheme based on blockchain technology, in: 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS), pp. 128–133.
[106] Deepayan Bhowmik, Tian Feng, The multimedia blockchain: a distributed and tamper-proof media transaction framework, in: Digital Signal Processing (DSP), 2017 22nd International Conference on, pp. 1–5.